MISP taxonomies and classification as machine tags

Table of Contents

Introduction

The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators, financial fraud or counter-terrorism information. The MISP project includes multiple sub-projects to support the operational requirements of analysts and improve the overall quality of information shared.

Taxonomies that can be used in MISP (2.4) and other information sharing tool and expressed in Machine Tags (Triple Tags). A machine tag is composed of a namespace (MUST), a predicate (MUST) and an (OPTIONAL) value. Machine tags are often called triple tag due to their format. The following document is generated from the machine-readable JSON describing the MISP taxonomies.

Funding and Support

The MISP project is financially and resource supported by CIRCL Computer Incident Response Center Luxembourg .

A CEF (Connecting Europe Facility) funding under CEF-TC-2016-3 - Cyber Security has been granted from 1st September 2017 until 31th August 2019 as **Improving MISP as building blocks for next-generation information sharing**.

Co-financed by the European Union

Connecting Europe Facility

If you are interested to co-fund projects around MISP, feel free to get in touch with us.

MISP taxonomies

CERT-XLM

CERT-XLM namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

CERT-XLM Security Incident Classification.

abusive-content

Abusive Content.

CERT-XLM:abusive-content="spam"

spam

Spam or 'unsolicited bulk e-mail', meaning that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having identical content.

CERT-XLM:abusive-content="harmful-speech"

Harmful Speech

Discretization or discrimination of somebody (e.g. cyber stalking, racism and threats against one or more individuals) May be found on a forum, email, tweet etc...

CERT-XLM:abusive-content="violence"

Child/Sexual/Violence/...

Any Child pornography, glorification of violence, may be found on a website, forum, email, tweet etc...

malicious-code

Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.

CERT-XLM:malicious-code="virus"

Virus

Malicious code that replicate itself and infects the computer and files;

CERT-XLM:malicious-code="worm"

Worm

Malware that self-replicates and spread itself to other computers in the network without any user interaction;

CERT-XLM:malicious-code="ransomware"

Ransomware

Ransomware is a type of malicious software from cryptovirology that blocks access to the victim's data or threatens to publish it until a ransom is paid.

CERT-XLM:malicious-code="trojan-malware"

Trojan/Malware

This category regroups many common malware types (Banking, POS, Mining malware).

CERT-XLM:malicious-code="spyware-rat"

Spyware/Rat

This category regroups malware types and tools that may have a bigger impact on the breached infrastructure and usually need further investigations (Common Spyware/Rat, State sponsored malwares, StealersHacking tool).

CERT-XLM:malicious-code="dialer"

Dialer

Computer program used to identify the phone numbers that can successfully make a connection with a computer modem. Use this category to classify overpriced SMS sent by malicious mobile application.

CERT-XLM:malicious-code="rootkit"

Rootkit

Malware, which alter the standard functionality of an operating system in order to do its malicious actions in a stealthy way. In practice, Rootkits hijacks systems functions in order to alter the returning values to hide themselves from simple analysis tools.

information-gathering

This group is for the reconnaissance; generally, it is the step before attacking.

CERT-XLM:information-gathering="scanner"

Scanning

Attacks that send requests to a system to discover weak points. This also includes some kinds of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT,).

CERT-XLM:information-gathering="sniffing"

Sniffing

Observing and recording network traffic (wiretapping).

CERT-XLM:information-gathering="social-engineering"

Social Engineering

Gathering information from a human being in a non-technical way (eg, lies, tricks, bribes, or threats).

intrusion-attempts

This group is for attack detected/tried but without success.

CERT-XLM:intrusion-attempts="exploit-known-vuln"

Exploiting known vulnerabilities

An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (eg, buffer overflow, backdoors, cross side scripting, etc).

CERT-XLM:intrusion-attempts="login-attempts"

Login attempts

Multiple login attempts (guessing / cracking of passwords, brute force).

CERT-XLM:intrusion-attempts="new-attack-signature"

New attack signature

An attempt using an unknown exploit.

intrusion

This group is for successful unauthorized access to a system.

CERT-XLM:intrusion="privileged-account-compromise"

Privileged Account Compromise

A successful full compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access.

CERT-XLM:intrusion="unprivileged-account-compromise"

Unprivileged Account Compromise

A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access. The intruded did not achieve to escale his privileges locally.

CERT-XLM:intrusion="botnet-member"

Botnet member

The compromised asset is also being part of a botnet. This is reserved mainly for public web servers. See malicious code in priority for workstations or internal server's compromise. For example, phpmailer, etc…

CERT-XLM:intrusion="domain-compromise"

Domain Compromise

The whole domain is compromised; this is commonly used for active directory and detected by a "pass the ticket" attack or a discovery of "ad dumps" files.

CERT-XLM:intrusion="application-compromise"

Application Compromise

An application is compromised; the attacker possess an uncontrolled access to data, server, and assets used by this application (CMDB, DB, Backend services, etc.).

availability

By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes.

CERT-XLM:availability="dos"

DoS

An attacker attempts to prevent legitimate users from accessing information or services.

CERT-XLM:availability="ddos"

DDoS

Form of electronic attack involving multiple computers, which send repeated requests (HTTP requests, pings, TCP or UDP Flood) to a server to load it down and render the service inaccessible for a period of time.

CERT-XLM:availability="sabotage"

Sabotage

Deliberate and malicious acts that result in the disruption of the normal processes and functions or the destruction or damage of equipment or information.

CERT-XLM:availability="outage"

Outage (no malice)

Unavailability of the system but done with no malice.

information-content-security

This group is dealing with non-legitimate access or modification to data.

CERT-XLM:information-content-security="Unauthorised-information-access"

Unauthorised access to information

Any access to unauthorized data. It may be access of data on improperly restricted server share or database exfiltered by using a SQLi.

CERT-XLM:information-content-security="Unauthorised-information-modification"

Unauthorised modification of information

Unauthorized tampering of data on files, documents or database.

fraud

This group is for unauthorized use of resources using resources for unauthorized purposes including profit-making ventures (eg, the use of e-mail to participate in illegal profit chain letters or pyramid schemes).

CERT-XLM:fraud="copyright"

Copyright

Selling or installing copies of unlicensed commercial software or other copyright protected materials (Warez).

CERT-XLM:fraud="masquerade"

Masquerade

Types of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it. This attack may be used for president fraud requesting transactions.

CERT-XLM:fraud="phishing"

Phishing

Masquerading as another entity in order to persuade the user to reveal a private credential.

vulnerable

Vulnerable

CERT-XLM:vulnerable="vulnerable-service"

Open for abuse

Open resolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus, signatures not up to date, etc. This includes for example default SNMP community or default password on any application.

conformity

This group is for catching breach about controls given by the company or externals entities.

CERT-XLM:conformity="regulator"

Regulator

All lack about regulator rules (CSSF, GDPR, etc.).

CERT-XLM:conformity="standard"

Standard

All lack about standards certification of the company (ISO27000, NIS, ISAE3402, etc.).

CERT-XLM:conformity="security-policy"

Security policy

All lack about the internal security policy of the company.

CERT-XLM:conformity="other-conformity"

Other

All lack that do not fit in one of previous categories should be put on this class.

other

Other

CERT-XLM:other="other"

other

All incidents that do not fit in one of the given categories should be put into this class. If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.

test

Meant for testing.

DFRLab-dichotomies-of-disinformation

DFRLab-dichotomies-of-disinformation namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

DFRLab Dichotomies of Disinformation.

primary-target

This should be filled out even when the target is not a nation. When a campaign targets a non-state political actor, the nation of origin of that non-state political actor is filled in this field, if that information is available. Distinguishable territories are nations.

DFRLab-dichotomies-of-disinformation:primary-target="AD"

Andorra

DFRLab-dichotomies-of-disinformation:primary-target="AE"

United Arab Emirates

DFRLab-dichotomies-of-disinformation:primary-target="AF"

Afghanistan

DFRLab-dichotomies-of-disinformation:primary-target="AG"

Antigua and Barbuda

DFRLab-dichotomies-of-disinformation:primary-target="AI"

Anguilla

DFRLab-dichotomies-of-disinformation:primary-target="AL"

Albania

DFRLab-dichotomies-of-disinformation:primary-target="AM"

Armenia

DFRLab-dichotomies-of-disinformation:primary-target="AO"

Angola

DFRLab-dichotomies-of-disinformation:primary-target="AQ"

Antarctica

DFRLab-dichotomies-of-disinformation:primary-target="AR"

Argentina

DFRLab-dichotomies-of-disinformation:primary-target="AS"

American Samoa

DFRLab-dichotomies-of-disinformation:primary-target="AT"

Austria

DFRLab-dichotomies-of-disinformation:primary-target="AU"

Australia

DFRLab-dichotomies-of-disinformation:primary-target="AW"

Aruba

DFRLab-dichotomies-of-disinformation:primary-target="AX"

Aland Islands

DFRLab-dichotomies-of-disinformation:primary-target="AZ"

Azerbaijan

DFRLab-dichotomies-of-disinformation:primary-target="BA"

Bosnia and Herzegovina

DFRLab-dichotomies-of-disinformation:primary-target="BB"

Barbados

DFRLab-dichotomies-of-disinformation:primary-target="BD"

Bangladesh

DFRLab-dichotomies-of-disinformation:primary-target="BE"

Belgium

DFRLab-dichotomies-of-disinformation:primary-target="BF"

Burkina Faso

DFRLab-dichotomies-of-disinformation:primary-target="BG"

Bulgaria

DFRLab-dichotomies-of-disinformation:primary-target="BH"

Bahrain

DFRLab-dichotomies-of-disinformation:primary-target="BI"

Burundi

DFRLab-dichotomies-of-disinformation:primary-target="BJ"

Benin

DFRLab-dichotomies-of-disinformation:primary-target="BL"

Saint-Barthelemy

DFRLab-dichotomies-of-disinformation:primary-target="BM"

Bermuda

DFRLab-dichotomies-of-disinformation:primary-target="BN"

Brunei Darussalam

DFRLab-dichotomies-of-disinformation:primary-target="BO"

Bolivia

DFRLab-dichotomies-of-disinformation:primary-target="BQ"

Bonaire, Saint Eustatius and Saba

DFRLab-dichotomies-of-disinformation:primary-target="BR"

Brazil

DFRLab-dichotomies-of-disinformation:primary-target="BS"

Bahamas

DFRLab-dichotomies-of-disinformation:primary-target="BT"

Bhutan

DFRLab-dichotomies-of-disinformation:primary-target="BV"

Bouvet Island

DFRLab-dichotomies-of-disinformation:primary-target="BW"

Botswana

DFRLab-dichotomies-of-disinformation:primary-target="BY"

Belarus

DFRLab-dichotomies-of-disinformation:primary-target="BZ"

Belize

DFRLab-dichotomies-of-disinformation:primary-target="CA"

Canada

DFRLab-dichotomies-of-disinformation:primary-target="CC"

Cocos (Keeling) Islands

DFRLab-dichotomies-of-disinformation:primary-target="CD"

Congo, Democratic Republic of the

DFRLab-dichotomies-of-disinformation:primary-target="CF"

Central African Republic

DFRLab-dichotomies-of-disinformation:primary-target="CG"

Congo

DFRLab-dichotomies-of-disinformation:primary-target="CH"

Switzerland

DFRLab-dichotomies-of-disinformation:primary-target="CI"

Cote d’Ivoire

DFRLab-dichotomies-of-disinformation:primary-target="CK"

Cook Islands

DFRLab-dichotomies-of-disinformation:primary-target="CL"

Chile

DFRLab-dichotomies-of-disinformation:primary-target="CM"

Cameroon

DFRLab-dichotomies-of-disinformation:primary-target="CN"

China

DFRLab-dichotomies-of-disinformation:primary-target="CO"

Colombia

DFRLab-dichotomies-of-disinformation:primary-target="CR"

Costa Rica

DFRLab-dichotomies-of-disinformation:primary-target="CU"

Cuba

DFRLab-dichotomies-of-disinformation:primary-target="CV"

Cape Verde

DFRLab-dichotomies-of-disinformation:primary-target="CW"

Curacao

DFRLab-dichotomies-of-disinformation:primary-target="CX"

Christmas Island

DFRLab-dichotomies-of-disinformation:primary-target="CY"

Cyprus

DFRLab-dichotomies-of-disinformation:primary-target="CZ"

Czech Republic

DFRLab-dichotomies-of-disinformation:primary-target="DE"

Germany

DFRLab-dichotomies-of-disinformation:primary-target="DJ"

Djibouti

DFRLab-dichotomies-of-disinformation:primary-target="DK"

Denmark

DFRLab-dichotomies-of-disinformation:primary-target="DM"

Dominica

DFRLab-dichotomies-of-disinformation:primary-target="DO"

Dominican Republic

DFRLab-dichotomies-of-disinformation:primary-target="DZ"

Algeria

DFRLab-dichotomies-of-disinformation:primary-target="EC"

Ecuador

DFRLab-dichotomies-of-disinformation:primary-target="EE"

Estonia

DFRLab-dichotomies-of-disinformation:primary-target="EG"

Egypt

DFRLab-dichotomies-of-disinformation:primary-target="EH"

Western Sahara

DFRLab-dichotomies-of-disinformation:primary-target="ER"

Eritrea

DFRLab-dichotomies-of-disinformation:primary-target="ES"

Spain

DFRLab-dichotomies-of-disinformation:primary-target="ET"

Ethiopia

DFRLab-dichotomies-of-disinformation:primary-target="FI"

Finland

DFRLab-dichotomies-of-disinformation:primary-target="FJ"

Fiji

DFRLab-dichotomies-of-disinformation:primary-target="FK"

Faeroe Islands

DFRLab-dichotomies-of-disinformation:primary-target="FM"

Micronesia (Federated States of)

DFRLab-dichotomies-of-disinformation:primary-target="FO"

Falkland Islands (Malvinas)

DFRLab-dichotomies-of-disinformation:primary-target="FR"

France

DFRLab-dichotomies-of-disinformation:primary-target="GA"

Gabon

DFRLab-dichotomies-of-disinformation:primary-target="GB"

United Kingdom

DFRLab-dichotomies-of-disinformation:primary-target="GD"

Grenada

DFRLab-dichotomies-of-disinformation:primary-target="GE"

Georgia

DFRLab-dichotomies-of-disinformation:primary-target="GF"

French Guiana

DFRLab-dichotomies-of-disinformation:primary-target="GG"

Guernsey

DFRLab-dichotomies-of-disinformation:primary-target="GH"

Ghana

DFRLab-dichotomies-of-disinformation:primary-target="GI"

Gibraltar

DFRLab-dichotomies-of-disinformation:primary-target="GL"

Greenland

DFRLab-dichotomies-of-disinformation:primary-target="GM"

Gambia

DFRLab-dichotomies-of-disinformation:primary-target="GN"

Guinea

DFRLab-dichotomies-of-disinformation:primary-target="GP"

Guadeloupe

DFRLab-dichotomies-of-disinformation:primary-target="GQ"

Equatorial Guinea

DFRLab-dichotomies-of-disinformation:primary-target="GR"

Greece

DFRLab-dichotomies-of-disinformation:primary-target="GS"

South Georgia and the South Sandwich Islands

DFRLab-dichotomies-of-disinformation:primary-target="GT"

Guatemala

DFRLab-dichotomies-of-disinformation:primary-target="GU"

Guam

DFRLab-dichotomies-of-disinformation:primary-target="GW"

Guinea-Bissau

DFRLab-dichotomies-of-disinformation:primary-target="GY"

Guyana

DFRLab-dichotomies-of-disinformation:primary-target="HK"

Hong Kong

DFRLab-dichotomies-of-disinformation:primary-target="HM"

Heard Island and McDonal Islands

DFRLab-dichotomies-of-disinformation:primary-target="HN"

Honduras

DFRLab-dichotomies-of-disinformation:primary-target="HR"

Croatia

DFRLab-dichotomies-of-disinformation:primary-target="HT"

Haiti

DFRLab-dichotomies-of-disinformation:primary-target="HU"

Hungary

DFRLab-dichotomies-of-disinformation:primary-target="ID"

Indonesia

DFRLab-dichotomies-of-disinformation:primary-target="IE"

Ireland

DFRLab-dichotomies-of-disinformation:primary-target="IL"

Israel

DFRLab-dichotomies-of-disinformation:primary-target="IM"

Isle of Man

DFRLab-dichotomies-of-disinformation:primary-target="IN"

India

DFRLab-dichotomies-of-disinformation:primary-target="IO"

British Virgin Islands

DFRLab-dichotomies-of-disinformation:primary-target="IQ"

Iraq

DFRLab-dichotomies-of-disinformation:primary-target="IR"

Iran (Islamic Republic of)

DFRLab-dichotomies-of-disinformation:primary-target="IS"

Iceland

DFRLab-dichotomies-of-disinformation:primary-target="IT"

Italy

DFRLab-dichotomies-of-disinformation:primary-target="JE"

Jersey

DFRLab-dichotomies-of-disinformation:primary-target="JM"

Jamaica

DFRLab-dichotomies-of-disinformation:primary-target="JO"

Jordan

DFRLab-dichotomies-of-disinformation:primary-target="JP"

Japan

DFRLab-dichotomies-of-disinformation:primary-target="KE"

Kenya

DFRLab-dichotomies-of-disinformation:primary-target="KG"

Kyrgyzstan

DFRLab-dichotomies-of-disinformation:primary-target="KH"

Cambodia

DFRLab-dichotomies-of-disinformation:primary-target="KI"

Kiribati

DFRLab-dichotomies-of-disinformation:primary-target="KM"

Comoros

DFRLab-dichotomies-of-disinformation:primary-target="KN"

Saint Kitts and Nevis

DFRLab-dichotomies-of-disinformation:primary-target="KP"

Korea, Democratic People’s Republic of

DFRLab-dichotomies-of-disinformation:primary-target="KR"

Korea, Republic of

DFRLab-dichotomies-of-disinformation:primary-target="KW"

Kuwait

DFRLab-dichotomies-of-disinformation:primary-target="KY"

Cayman Islands

DFRLab-dichotomies-of-disinformation:primary-target="KZ"

Kazakhstan

DFRLab-dichotomies-of-disinformation:primary-target="LA"

Lao People’s Democratic Republic

DFRLab-dichotomies-of-disinformation:primary-target="LB"

Lebanon

DFRLab-dichotomies-of-disinformation:primary-target="LC"

Saint Lucia

DFRLab-dichotomies-of-disinformation:primary-target="LI"

Liechtenstein

DFRLab-dichotomies-of-disinformation:primary-target="LK"

Sri Lanka

DFRLab-dichotomies-of-disinformation:primary-target="LR"

Liberia

DFRLab-dichotomies-of-disinformation:primary-target="LS"

Lesotho

DFRLab-dichotomies-of-disinformation:primary-target="LT"

Lithuania

DFRLab-dichotomies-of-disinformation:primary-target="LU"

Luxembourg

DFRLab-dichotomies-of-disinformation:primary-target="LV"

Latvia

DFRLab-dichotomies-of-disinformation:primary-target="LY"

Libya

DFRLab-dichotomies-of-disinformation:primary-target="MA"

Morocco

DFRLab-dichotomies-of-disinformation:primary-target="MC"

Monaco

DFRLab-dichotomies-of-disinformation:primary-target="MD"

Moldova, Republic of

DFRLab-dichotomies-of-disinformation:primary-target="ME"

Montenegro

DFRLab-dichotomies-of-disinformation:primary-target="MF"

Saint Martin (French part)

DFRLab-dichotomies-of-disinformation:primary-target="MG"

Madagascar

DFRLab-dichotomies-of-disinformation:primary-target="MH"

Marshall Islands

DFRLab-dichotomies-of-disinformation:primary-target="MK"

Macedonia, The former Yugoslav Republic of

DFRLab-dichotomies-of-disinformation:primary-target="ML"

Mali

DFRLab-dichotomies-of-disinformation:primary-target="MM"

Myanmar

DFRLab-dichotomies-of-disinformation:primary-target="MN"

Mongolia

DFRLab-dichotomies-of-disinformation:primary-target="MO"

Macao

DFRLab-dichotomies-of-disinformation:primary-target="MP"

Northern Mariana Islands

DFRLab-dichotomies-of-disinformation:primary-target="MQ"

Martinique

DFRLab-dichotomies-of-disinformation:primary-target="MR"

Mauritania

DFRLab-dichotomies-of-disinformation:primary-target="MS"

Montserrat

DFRLab-dichotomies-of-disinformation:primary-target="MT"

Malta

DFRLab-dichotomies-of-disinformation:primary-target="MU"

Mauritius

DFRLab-dichotomies-of-disinformation:primary-target="MV"

Maldives

DFRLab-dichotomies-of-disinformation:primary-target="MW"

Malawi

DFRLab-dichotomies-of-disinformation:primary-target="MX"

Mexico

DFRLab-dichotomies-of-disinformation:primary-target="MY"

Malaysia

DFRLab-dichotomies-of-disinformation:primary-target="MZ"

Mozambique

DFRLab-dichotomies-of-disinformation:primary-target="NA"

Namibia

DFRLab-dichotomies-of-disinformation:primary-target="NC"

New Caledonia

DFRLab-dichotomies-of-disinformation:primary-target="NE"

Niger

DFRLab-dichotomies-of-disinformation:primary-target="NF"

Norfolk Island

DFRLab-dichotomies-of-disinformation:primary-target="NG"

Nigeria

DFRLab-dichotomies-of-disinformation:primary-target="NI"

Nicaragua

DFRLab-dichotomies-of-disinformation:primary-target="NL"

Netherlands

DFRLab-dichotomies-of-disinformation:primary-target="NO"

Norway

DFRLab-dichotomies-of-disinformation:primary-target="NP"

Nepal

DFRLab-dichotomies-of-disinformation:primary-target="NR"

Nauru

DFRLab-dichotomies-of-disinformation:primary-target="NU"

Niue

DFRLab-dichotomies-of-disinformation:primary-target="NZ"

New Zealand

DFRLab-dichotomies-of-disinformation:primary-target="OM"

Oman

DFRLab-dichotomies-of-disinformation:primary-target="Other"

Other

DFRLab-dichotomies-of-disinformation:primary-target="PA"

Panama

DFRLab-dichotomies-of-disinformation:primary-target="PE"

Peru

DFRLab-dichotomies-of-disinformation:primary-target="PF"

French Polynesia

DFRLab-dichotomies-of-disinformation:primary-target="PG"

Papua New Guinea

DFRLab-dichotomies-of-disinformation:primary-target="PH"

Philippines

DFRLab-dichotomies-of-disinformation:primary-target="PK"

Pakistan

DFRLab-dichotomies-of-disinformation:primary-target="PL"

Poland

DFRLab-dichotomies-of-disinformation:primary-target="PM"

Saint Pierre and Miquelon

DFRLab-dichotomies-of-disinformation:primary-target="PN"

Pitcairn

DFRLab-dichotomies-of-disinformation:primary-target="PR"

Puerto Rico

DFRLab-dichotomies-of-disinformation:primary-target="PS"

Palestinian Territory, Occupied

DFRLab-dichotomies-of-disinformation:primary-target="PT"

Portugal

DFRLab-dichotomies-of-disinformation:primary-target="PW"

Palau

DFRLab-dichotomies-of-disinformation:primary-target="PY"

Paraguay

DFRLab-dichotomies-of-disinformation:primary-target="QA"

Qatar

DFRLab-dichotomies-of-disinformation:primary-target="RE"

Reunion

DFRLab-dichotomies-of-disinformation:primary-target="RO"

Romania

DFRLab-dichotomies-of-disinformation:primary-target="RS"

Serbia

DFRLab-dichotomies-of-disinformation:primary-target="RU"

Russian Federation

DFRLab-dichotomies-of-disinformation:primary-target="RW"

Rwanda

DFRLab-dichotomies-of-disinformation:primary-target="SA"

Saudi Arabia

DFRLab-dichotomies-of-disinformation:primary-target="SB"

Solomon Islands

DFRLab-dichotomies-of-disinformation:primary-target="SC"

Seychelles

DFRLab-dichotomies-of-disinformation:primary-target="SD"

Sudan

DFRLab-dichotomies-of-disinformation:primary-target="SE"

Sweden

DFRLab-dichotomies-of-disinformation:primary-target="SG"

Singapore

DFRLab-dichotomies-of-disinformation:primary-target="SH"

Saint Helena

DFRLab-dichotomies-of-disinformation:primary-target="SI"

Slovenia

DFRLab-dichotomies-of-disinformation:primary-target="SJ"

Svalbard and Jan Mayen Islands

DFRLab-dichotomies-of-disinformation:primary-target="SK"

Slovakia

DFRLab-dichotomies-of-disinformation:primary-target="SL"

Sierra Leone

DFRLab-dichotomies-of-disinformation:primary-target="SM"

San Marino

DFRLab-dichotomies-of-disinformation:primary-target="SN"

Senegal

DFRLab-dichotomies-of-disinformation:primary-target="SO"

Somalia

DFRLab-dichotomies-of-disinformation:primary-target="SR"

Suriname

DFRLab-dichotomies-of-disinformation:primary-target="SS"

South Sudan

DFRLab-dichotomies-of-disinformation:primary-target="ST"

Sao Tome and Principe

DFRLab-dichotomies-of-disinformation:primary-target="SV"

El Salvador

DFRLab-dichotomies-of-disinformation:primary-target="SX"

Sint Maarten (Dutch part)

DFRLab-dichotomies-of-disinformation:primary-target="SY"

Syrian Arab Republic

DFRLab-dichotomies-of-disinformation:primary-target="SZ"

Swaziland

DFRLab-dichotomies-of-disinformation:primary-target="TC"

Turks and Caicos Islands

DFRLab-dichotomies-of-disinformation:primary-target="TD"

Chad

DFRLab-dichotomies-of-disinformation:primary-target="TF"

French Southern Territories

DFRLab-dichotomies-of-disinformation:primary-target="TG"

Togo

DFRLab-dichotomies-of-disinformation:primary-target="TH"

Thailand

DFRLab-dichotomies-of-disinformation:primary-target="TJ"

Tajikistan

DFRLab-dichotomies-of-disinformation:primary-target="TK"

Tokelau

DFRLab-dichotomies-of-disinformation:primary-target="TL"

Timor-Leste

DFRLab-dichotomies-of-disinformation:primary-target="TM"

Turkmenistan

DFRLab-dichotomies-of-disinformation:primary-target="TN"

Tunisia

DFRLab-dichotomies-of-disinformation:primary-target="TO"

Tonga

DFRLab-dichotomies-of-disinformation:primary-target="TR"

Turkey

DFRLab-dichotomies-of-disinformation:primary-target="TT"

Trinidad and Tobago

DFRLab-dichotomies-of-disinformation:primary-target="TV"

Tuvalu

DFRLab-dichotomies-of-disinformation:primary-target="TW"

Taiwan, Province of China

DFRLab-dichotomies-of-disinformation:primary-target="TZ"

Tanzania, United Republic of

DFRLab-dichotomies-of-disinformation:primary-target="UA"

Ukraine

DFRLab-dichotomies-of-disinformation:primary-target="UG"

Uganda

DFRLab-dichotomies-of-disinformation:primary-target="UM"

United States Minor Outlying Islands

DFRLab-dichotomies-of-disinformation:primary-target="US"

United States of America

DFRLab-dichotomies-of-disinformation:primary-target="UY"

Uruguay

DFRLab-dichotomies-of-disinformation:primary-target="UZ"

Uzbekistan

DFRLab-dichotomies-of-disinformation:primary-target="Unknown"

Unknown

DFRLab-dichotomies-of-disinformation:primary-target="VA"

Holy See

DFRLab-dichotomies-of-disinformation:primary-target="VC"

Saint Vincent and the Grenadines

DFRLab-dichotomies-of-disinformation:primary-target="VE"

Venezuela (Bolivarian Republic of)

DFRLab-dichotomies-of-disinformation:primary-target="VG"

British Virgin Islands

DFRLab-dichotomies-of-disinformation:primary-target="VI"

United States Virgin Islands

DFRLab-dichotomies-of-disinformation:primary-target="VN"

Viet Nam

DFRLab-dichotomies-of-disinformation:primary-target="VU"

Vanuatu

DFRLab-dichotomies-of-disinformation:primary-target="WF"

Wallis and Futuna Islands

DFRLab-dichotomies-of-disinformation:primary-target="WS"

Samoa

DFRLab-dichotomies-of-disinformation:primary-target="YE"

Yemen

DFRLab-dichotomies-of-disinformation:primary-target="YT"

Mayotte

DFRLab-dichotomies-of-disinformation:primary-target="ZA"

South Africa

DFRLab-dichotomies-of-disinformation:primary-target="ZM"

Zambia

DFRLab-dichotomies-of-disinformation:primary-target="ZW"

Zimbabwe

platforms-advertisement

Advertisement through which a campaign targets an actor.

platforms-email

Email through which a campaign targets an actor.

primary-disinformant

This should be filled out even when the attacker is not a national government. When a campaign is run by a non-state political actor, the nation of origin of that non-state political actor is filled in this field, if that information is available. Likewise, this should be filled out if the preponderance of attacker activity originates from within a single nation. Distinguishable territories are nations.

DFRLab-dichotomies-of-disinformation:primary-disinformant="AD"

Andorra

DFRLab-dichotomies-of-disinformation:primary-disinformant="AE"

United Arab Emirates

DFRLab-dichotomies-of-disinformation:primary-disinformant="AF"

Afghanistan

DFRLab-dichotomies-of-disinformation:primary-disinformant="AG"

Antigua and Barbuda

DFRLab-dichotomies-of-disinformation:primary-disinformant="AI"

Anguilla

DFRLab-dichotomies-of-disinformation:primary-disinformant="AL"

Albania

DFRLab-dichotomies-of-disinformation:primary-disinformant="AM"

Armenia

DFRLab-dichotomies-of-disinformation:primary-disinformant="AO"

Angola

DFRLab-dichotomies-of-disinformation:primary-disinformant="AQ"

Antarctica

DFRLab-dichotomies-of-disinformation:primary-disinformant="AR"

Argentina

DFRLab-dichotomies-of-disinformation:primary-disinformant="AS"

American Samoa

DFRLab-dichotomies-of-disinformation:primary-disinformant="AT"

Austria

DFRLab-dichotomies-of-disinformation:primary-disinformant="AU"

Australia

DFRLab-dichotomies-of-disinformation:primary-disinformant="AW"

Aruba

DFRLab-dichotomies-of-disinformation:primary-disinformant="AX"

Aland Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="AZ"

Azerbaijan

DFRLab-dichotomies-of-disinformation:primary-disinformant="BA"

Bosnia and Herzegovina

DFRLab-dichotomies-of-disinformation:primary-disinformant="BB"

Barbados

DFRLab-dichotomies-of-disinformation:primary-disinformant="BD"

Bangladesh

DFRLab-dichotomies-of-disinformation:primary-disinformant="BE"

Belgium

DFRLab-dichotomies-of-disinformation:primary-disinformant="BF"

Burkina Faso

DFRLab-dichotomies-of-disinformation:primary-disinformant="BG"

Bulgaria

DFRLab-dichotomies-of-disinformation:primary-disinformant="BH"

Bahrain

DFRLab-dichotomies-of-disinformation:primary-disinformant="BI"

Burundi

DFRLab-dichotomies-of-disinformation:primary-disinformant="BJ"

Benin

DFRLab-dichotomies-of-disinformation:primary-disinformant="BL"

Saint-Barthelemy

DFRLab-dichotomies-of-disinformation:primary-disinformant="BM"

Bermuda

DFRLab-dichotomies-of-disinformation:primary-disinformant="BN"

Brunei Darussalam

DFRLab-dichotomies-of-disinformation:primary-disinformant="BO"

Bolivia

DFRLab-dichotomies-of-disinformation:primary-disinformant="BQ"

Bonaire, Saint Eustatius and Saba

DFRLab-dichotomies-of-disinformation:primary-disinformant="BR"

Brazil

DFRLab-dichotomies-of-disinformation:primary-disinformant="BS"

Bahamas

DFRLab-dichotomies-of-disinformation:primary-disinformant="BT"

Bhutan

DFRLab-dichotomies-of-disinformation:primary-disinformant="BV"

Bouvet Island

DFRLab-dichotomies-of-disinformation:primary-disinformant="BW"

Botswana

DFRLab-dichotomies-of-disinformation:primary-disinformant="BY"

Belarus

DFRLab-dichotomies-of-disinformation:primary-disinformant="BZ"

Belize

DFRLab-dichotomies-of-disinformation:primary-disinformant="CA"

Canada

DFRLab-dichotomies-of-disinformation:primary-disinformant="CC"

Cocos (Keeling) Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="CD"

Congo, Democratic Republic of the

DFRLab-dichotomies-of-disinformation:primary-disinformant="CF"

Central African Republic

DFRLab-dichotomies-of-disinformation:primary-disinformant="CG"

Congo

DFRLab-dichotomies-of-disinformation:primary-disinformant="CH"

Switzerland

DFRLab-dichotomies-of-disinformation:primary-disinformant="CI"

Cote d’Ivoire

DFRLab-dichotomies-of-disinformation:primary-disinformant="CK"

Cook Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="CL"

Chile

DFRLab-dichotomies-of-disinformation:primary-disinformant="CM"

Cameroon

DFRLab-dichotomies-of-disinformation:primary-disinformant="CN"

China

DFRLab-dichotomies-of-disinformation:primary-disinformant="CO"

Colombia

DFRLab-dichotomies-of-disinformation:primary-disinformant="CR"

Costa Rica

DFRLab-dichotomies-of-disinformation:primary-disinformant="CU"

Cuba

DFRLab-dichotomies-of-disinformation:primary-disinformant="CV"

Cape Verde

DFRLab-dichotomies-of-disinformation:primary-disinformant="CW"

Curacao

DFRLab-dichotomies-of-disinformation:primary-disinformant="CX"

Christmas Island

DFRLab-dichotomies-of-disinformation:primary-disinformant="CY"

Cyprus

DFRLab-dichotomies-of-disinformation:primary-disinformant="CZ"

Czech Republic

DFRLab-dichotomies-of-disinformation:primary-disinformant="DE"

Germany

DFRLab-dichotomies-of-disinformation:primary-disinformant="DJ"

Djibouti

DFRLab-dichotomies-of-disinformation:primary-disinformant="DK"

Denmark

DFRLab-dichotomies-of-disinformation:primary-disinformant="DM"

Dominica

DFRLab-dichotomies-of-disinformation:primary-disinformant="DO"

Dominican Republic

DFRLab-dichotomies-of-disinformation:primary-disinformant="DZ"

Algeria

DFRLab-dichotomies-of-disinformation:primary-disinformant="EC"

Ecuador

DFRLab-dichotomies-of-disinformation:primary-disinformant="EE"

Estonia

DFRLab-dichotomies-of-disinformation:primary-disinformant="EG"

Egypt

DFRLab-dichotomies-of-disinformation:primary-disinformant="EH"

Western Sahara

DFRLab-dichotomies-of-disinformation:primary-disinformant="ER"

Eritrea

DFRLab-dichotomies-of-disinformation:primary-disinformant="ES"

Spain

DFRLab-dichotomies-of-disinformation:primary-disinformant="ET"

Ethiopia

DFRLab-dichotomies-of-disinformation:primary-disinformant="FI"

Finland

DFRLab-dichotomies-of-disinformation:primary-disinformant="FJ"

Fiji

DFRLab-dichotomies-of-disinformation:primary-disinformant="FK"

Faeroe Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="FM"

Micronesia (Federated States of)

DFRLab-dichotomies-of-disinformation:primary-disinformant="FO"

Falkland Islands (Malvinas)

DFRLab-dichotomies-of-disinformation:primary-disinformant="FR"

France

DFRLab-dichotomies-of-disinformation:primary-disinformant="GA"

Gabon

DFRLab-dichotomies-of-disinformation:primary-disinformant="GB"

United Kingdom

DFRLab-dichotomies-of-disinformation:primary-disinformant="GD"

Grenada

DFRLab-dichotomies-of-disinformation:primary-disinformant="GE"

Georgia

DFRLab-dichotomies-of-disinformation:primary-disinformant="GF"

French Guiana

DFRLab-dichotomies-of-disinformation:primary-disinformant="GG"

Guernsey

DFRLab-dichotomies-of-disinformation:primary-disinformant="GH"

Ghana

DFRLab-dichotomies-of-disinformation:primary-disinformant="GI"

Gibraltar

DFRLab-dichotomies-of-disinformation:primary-disinformant="GL"

Greenland

DFRLab-dichotomies-of-disinformation:primary-disinformant="GM"

Gambia

DFRLab-dichotomies-of-disinformation:primary-disinformant="GN"

Guinea

DFRLab-dichotomies-of-disinformation:primary-disinformant="GP"

Guadeloupe

DFRLab-dichotomies-of-disinformation:primary-disinformant="GQ"

Equatorial Guinea

DFRLab-dichotomies-of-disinformation:primary-disinformant="GR"

Greece

DFRLab-dichotomies-of-disinformation:primary-disinformant="GS"

South Georgia and the South Sandwich Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="GT"

Guatemala

DFRLab-dichotomies-of-disinformation:primary-disinformant="GU"

Guam

DFRLab-dichotomies-of-disinformation:primary-disinformant="GW"

Guinea-Bissau

DFRLab-dichotomies-of-disinformation:primary-disinformant="GY"

Guyana

DFRLab-dichotomies-of-disinformation:primary-disinformant="HK"

Hong Kong

DFRLab-dichotomies-of-disinformation:primary-disinformant="HM"

Heard Island and McDonal Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="HN"

Honduras

DFRLab-dichotomies-of-disinformation:primary-disinformant="HR"

Croatia

DFRLab-dichotomies-of-disinformation:primary-disinformant="HT"

Haiti

DFRLab-dichotomies-of-disinformation:primary-disinformant="HU"

Hungary

DFRLab-dichotomies-of-disinformation:primary-disinformant="ID"

Indonesia

DFRLab-dichotomies-of-disinformation:primary-disinformant="IE"

Ireland

DFRLab-dichotomies-of-disinformation:primary-disinformant="IL"

Israel

DFRLab-dichotomies-of-disinformation:primary-disinformant="IM"

Isle of Man

DFRLab-dichotomies-of-disinformation:primary-disinformant="IN"

India

DFRLab-dichotomies-of-disinformation:primary-disinformant="IO"

British Virgin Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="IQ"

Iraq

DFRLab-dichotomies-of-disinformation:primary-disinformant="IR"

Iran (Islamic Republic of)

DFRLab-dichotomies-of-disinformation:primary-disinformant="IS"

Iceland

DFRLab-dichotomies-of-disinformation:primary-disinformant="IT"

Italy

DFRLab-dichotomies-of-disinformation:primary-disinformant="JE"

Jersey

DFRLab-dichotomies-of-disinformation:primary-disinformant="JM"

Jamaica

DFRLab-dichotomies-of-disinformation:primary-disinformant="JO"

Jordan

DFRLab-dichotomies-of-disinformation:primary-disinformant="JP"

Japan

DFRLab-dichotomies-of-disinformation:primary-disinformant="KE"

Kenya

DFRLab-dichotomies-of-disinformation:primary-disinformant="KG"

Kyrgyzstan

DFRLab-dichotomies-of-disinformation:primary-disinformant="KH"

Cambodia

DFRLab-dichotomies-of-disinformation:primary-disinformant="KI"

Kiribati

DFRLab-dichotomies-of-disinformation:primary-disinformant="KM"

Comoros

DFRLab-dichotomies-of-disinformation:primary-disinformant="KN"

Saint Kitts and Nevis

DFRLab-dichotomies-of-disinformation:primary-disinformant="KP"

Korea, Democratic People’s Republic of

DFRLab-dichotomies-of-disinformation:primary-disinformant="KR"

Korea, Republic of

DFRLab-dichotomies-of-disinformation:primary-disinformant="KW"

Kuwait

DFRLab-dichotomies-of-disinformation:primary-disinformant="KY"

Cayman Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="KZ"

Kazakhstan

DFRLab-dichotomies-of-disinformation:primary-disinformant="LA"

Lao People’s Democratic Republic

DFRLab-dichotomies-of-disinformation:primary-disinformant="LB"

Lebanon

DFRLab-dichotomies-of-disinformation:primary-disinformant="LC"

Saint Lucia

DFRLab-dichotomies-of-disinformation:primary-disinformant="LI"

Liechtenstein

DFRLab-dichotomies-of-disinformation:primary-disinformant="LK"

Sri Lanka

DFRLab-dichotomies-of-disinformation:primary-disinformant="LR"

Liberia

DFRLab-dichotomies-of-disinformation:primary-disinformant="LS"

Lesotho

DFRLab-dichotomies-of-disinformation:primary-disinformant="LT"

Lithuania

DFRLab-dichotomies-of-disinformation:primary-disinformant="LU"

Luxembourg

DFRLab-dichotomies-of-disinformation:primary-disinformant="LV"

Latvia

DFRLab-dichotomies-of-disinformation:primary-disinformant="LY"

Libya

DFRLab-dichotomies-of-disinformation:primary-disinformant="MA"

Morocco

DFRLab-dichotomies-of-disinformation:primary-disinformant="MC"

Monaco

DFRLab-dichotomies-of-disinformation:primary-disinformant="MD"

Moldova, Republic of

DFRLab-dichotomies-of-disinformation:primary-disinformant="ME"

Montenegro

DFRLab-dichotomies-of-disinformation:primary-disinformant="MF"

Saint Martin (French part)

DFRLab-dichotomies-of-disinformation:primary-disinformant="MG"

Madagascar

DFRLab-dichotomies-of-disinformation:primary-disinformant="MH"

Marshall Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="MK"

Macedonia, The former Yugoslav Republic of

DFRLab-dichotomies-of-disinformation:primary-disinformant="ML"

Mali

DFRLab-dichotomies-of-disinformation:primary-disinformant="MM"

Myanmar

DFRLab-dichotomies-of-disinformation:primary-disinformant="MN"

Mongolia

DFRLab-dichotomies-of-disinformation:primary-disinformant="MO"

Macao

DFRLab-dichotomies-of-disinformation:primary-disinformant="MP"

Northern Mariana Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="MQ"

Martinique

DFRLab-dichotomies-of-disinformation:primary-disinformant="MR"

Mauritania

DFRLab-dichotomies-of-disinformation:primary-disinformant="MS"

Montserrat

DFRLab-dichotomies-of-disinformation:primary-disinformant="MT"

Malta

DFRLab-dichotomies-of-disinformation:primary-disinformant="MU"

Mauritius

DFRLab-dichotomies-of-disinformation:primary-disinformant="MV"

Maldives

DFRLab-dichotomies-of-disinformation:primary-disinformant="MW"

Malawi

DFRLab-dichotomies-of-disinformation:primary-disinformant="MX"

Mexico

DFRLab-dichotomies-of-disinformation:primary-disinformant="MY"

Malaysia

DFRLab-dichotomies-of-disinformation:primary-disinformant="MZ"

Mozambique

DFRLab-dichotomies-of-disinformation:primary-disinformant="NA"

Namibia

DFRLab-dichotomies-of-disinformation:primary-disinformant="NC"

New Caledonia

DFRLab-dichotomies-of-disinformation:primary-disinformant="NE"

Niger

DFRLab-dichotomies-of-disinformation:primary-disinformant="NF"

Norfolk Island

DFRLab-dichotomies-of-disinformation:primary-disinformant="NG"

Nigeria

DFRLab-dichotomies-of-disinformation:primary-disinformant="NI"

Nicaragua

DFRLab-dichotomies-of-disinformation:primary-disinformant="NL"

Netherlands

DFRLab-dichotomies-of-disinformation:primary-disinformant="NO"

Norway

DFRLab-dichotomies-of-disinformation:primary-disinformant="NP"

Nepal

DFRLab-dichotomies-of-disinformation:primary-disinformant="NR"

Nauru

DFRLab-dichotomies-of-disinformation:primary-disinformant="NU"

Niue

DFRLab-dichotomies-of-disinformation:primary-disinformant="NZ"

New Zealand

DFRLab-dichotomies-of-disinformation:primary-disinformant="OM"

Oman

DFRLab-dichotomies-of-disinformation:primary-disinformant="Other"

Other

DFRLab-dichotomies-of-disinformation:primary-disinformant="PA"

Panama

DFRLab-dichotomies-of-disinformation:primary-disinformant="PE"

Peru

DFRLab-dichotomies-of-disinformation:primary-disinformant="PF"

French Polynesia

DFRLab-dichotomies-of-disinformation:primary-disinformant="PG"

Papua New Guinea

DFRLab-dichotomies-of-disinformation:primary-disinformant="PH"

Philippines

DFRLab-dichotomies-of-disinformation:primary-disinformant="PK"

Pakistan

DFRLab-dichotomies-of-disinformation:primary-disinformant="PL"

Poland

DFRLab-dichotomies-of-disinformation:primary-disinformant="PM"

Saint Pierre and Miquelon

DFRLab-dichotomies-of-disinformation:primary-disinformant="PN"

Pitcairn

DFRLab-dichotomies-of-disinformation:primary-disinformant="PR"

Puerto Rico

DFRLab-dichotomies-of-disinformation:primary-disinformant="PS"

Palestinian Territory, Occupied

DFRLab-dichotomies-of-disinformation:primary-disinformant="PT"

Portugal

DFRLab-dichotomies-of-disinformation:primary-disinformant="PW"

Palau

DFRLab-dichotomies-of-disinformation:primary-disinformant="PY"

Paraguay

DFRLab-dichotomies-of-disinformation:primary-disinformant="QA"

Qatar

DFRLab-dichotomies-of-disinformation:primary-disinformant="RE"

Reunion

DFRLab-dichotomies-of-disinformation:primary-disinformant="RO"

Romania

DFRLab-dichotomies-of-disinformation:primary-disinformant="RS"

Serbia

DFRLab-dichotomies-of-disinformation:primary-disinformant="RU"

Russian Federation

DFRLab-dichotomies-of-disinformation:primary-disinformant="RW"

Rwanda

DFRLab-dichotomies-of-disinformation:primary-disinformant="SA"

Saudi Arabia

DFRLab-dichotomies-of-disinformation:primary-disinformant="SB"

Solomon Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="SC"

Seychelles

DFRLab-dichotomies-of-disinformation:primary-disinformant="SD"

Sudan

DFRLab-dichotomies-of-disinformation:primary-disinformant="SE"

Sweden

DFRLab-dichotomies-of-disinformation:primary-disinformant="SG"

Singapore

DFRLab-dichotomies-of-disinformation:primary-disinformant="SH"

Saint Helena

DFRLab-dichotomies-of-disinformation:primary-disinformant="SI"

Slovenia

DFRLab-dichotomies-of-disinformation:primary-disinformant="SJ"

Svalbard and Jan Mayen Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="SK"

Slovakia

DFRLab-dichotomies-of-disinformation:primary-disinformant="SL"

Sierra Leone

DFRLab-dichotomies-of-disinformation:primary-disinformant="SM"

San Marino

DFRLab-dichotomies-of-disinformation:primary-disinformant="SN"

Senegal

DFRLab-dichotomies-of-disinformation:primary-disinformant="SO"

Somalia

DFRLab-dichotomies-of-disinformation:primary-disinformant="SR"

Suriname

DFRLab-dichotomies-of-disinformation:primary-disinformant="SS"

South Sudan

DFRLab-dichotomies-of-disinformation:primary-disinformant="ST"

Sao Tome and Principe

DFRLab-dichotomies-of-disinformation:primary-disinformant="SV"

El Salvador

DFRLab-dichotomies-of-disinformation:primary-disinformant="SX"

Sint Maarten (Dutch part)

DFRLab-dichotomies-of-disinformation:primary-disinformant="SY"

Syrian Arab Republic

DFRLab-dichotomies-of-disinformation:primary-disinformant="SZ"

Swaziland

DFRLab-dichotomies-of-disinformation:primary-disinformant="TC"

Turks and Caicos Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="TD"

Chad

DFRLab-dichotomies-of-disinformation:primary-disinformant="TF"

French Southern Territories

DFRLab-dichotomies-of-disinformation:primary-disinformant="TG"

Togo

DFRLab-dichotomies-of-disinformation:primary-disinformant="TH"

Thailand

DFRLab-dichotomies-of-disinformation:primary-disinformant="TJ"

Tajikistan

DFRLab-dichotomies-of-disinformation:primary-disinformant="TK"

Tokelau

DFRLab-dichotomies-of-disinformation:primary-disinformant="TL"

Timor-Leste

DFRLab-dichotomies-of-disinformation:primary-disinformant="TM"

Turkmenistan

DFRLab-dichotomies-of-disinformation:primary-disinformant="TN"

Tunisia

DFRLab-dichotomies-of-disinformation:primary-disinformant="TO"

Tonga

DFRLab-dichotomies-of-disinformation:primary-disinformant="TR"

Turkey

DFRLab-dichotomies-of-disinformation:primary-disinformant="TT"

Trinidad and Tobago

DFRLab-dichotomies-of-disinformation:primary-disinformant="TV"

Tuvalu

DFRLab-dichotomies-of-disinformation:primary-disinformant="TW"

Taiwan, Province of China

DFRLab-dichotomies-of-disinformation:primary-disinformant="TZ"

Tanzania, United Republic of

DFRLab-dichotomies-of-disinformation:primary-disinformant="UA"

Ukraine

DFRLab-dichotomies-of-disinformation:primary-disinformant="UG"

Uganda

DFRLab-dichotomies-of-disinformation:primary-disinformant="UM"

United States Minor Outlying Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="US"

United States of America

DFRLab-dichotomies-of-disinformation:primary-disinformant="UY"

Uruguay

DFRLab-dichotomies-of-disinformation:primary-disinformant="UZ"

Uzbekistan

DFRLab-dichotomies-of-disinformation:primary-disinformant="Unknown"

Unknown

DFRLab-dichotomies-of-disinformation:primary-disinformant="VA"

Holy See

DFRLab-dichotomies-of-disinformation:primary-disinformant="VC"

Saint Vincent and the Grenadines

DFRLab-dichotomies-of-disinformation:primary-disinformant="VE"

Venezuela (Bolivarian Republic of)

DFRLab-dichotomies-of-disinformation:primary-disinformant="VG"

British Virgin Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="VI"

United States Virgin Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="VN"

Viet Nam

DFRLab-dichotomies-of-disinformation:primary-disinformant="VU"

Vanuatu

DFRLab-dichotomies-of-disinformation:primary-disinformant="WF"

Wallis and Futuna Islands

DFRLab-dichotomies-of-disinformation:primary-disinformant="WS"

Samoa

DFRLab-dichotomies-of-disinformation:primary-disinformant="YE"

Yemen

DFRLab-dichotomies-of-disinformation:primary-disinformant="YT"

Mayotte

DFRLab-dichotomies-of-disinformation:primary-disinformant="ZA"

South Africa

DFRLab-dichotomies-of-disinformation:primary-disinformant="ZM"

Zambia

DFRLab-dichotomies-of-disinformation:primary-disinformant="ZW"

Zimbabwe

target-category

When a campaign targets an actor, the category of that actor is filled in this field, if that information is available. Categories are not mutually exclusive. All relevant categories can be added.

DFRLab-dichotomies-of-disinformation:target-category="government-civilian"

Government: Civilian

The governing body and functions of a state, including national leaders, institutions, and non-military departments and agencies. Includes incumbent politicians running for re-election.

DFRLab-dichotomies-of-disinformation:target-category="government-military"

Government: Military

Military departments and agencies which enjoy the sanctioned use of force

DFRLab-dichotomies-of-disinformation:target-category="political-party"

Political Party

Organized competitors for political power who can obtain or wield power directly. Includes politicians currently in office, as well as non-incumbent politicians running for office who are associated with a political party. Can also be an individual working for a party.

DFRLab-dichotomies-of-disinformation:target-category="non-state-political-actor"

Non-State Political Actor

Organized competitors for political power who can obtain or wield power, even if indirectly; not necessarily enfranchised. Non-state political actors are formally organized, coordinated, and cohesive. e.g. Greenpeace, the NRA, or the KKK.

DFRLab-dichotomies-of-disinformation:target-category="business"

Business

Includes groups that contract out to the government, individuals looking for financial gain, and mercenaries.

DFRLab-dichotomies-of-disinformation:target-category="influential-individuals"

Influential Individuals

Individuals who are influential but who do not belong to a ruling government coalition. Includes groups of individuals who are not formally organized but work together. e.g. journalists, former politicians, or organized 4channers. For individuals who operate their own charitable foundations (and thus could be placed in Non-State Political Actor), coding depends on whether or not the disinformation is foremost targeting the individual, their foundation, or both.

DFRLab-dichotomies-of-disinformation:target-category="electorate"

Electorate

The enfranchised population in a specific country or within a demarcated boundary.

DFRLab-dichotomies-of-disinformation:target-category="racial"

Racial

A specific minority/majority group.

DFRLab-dichotomies-of-disinformation:target-category="ethnic"

Ethnic

A specific minority/majority group.

DFRLab-dichotomies-of-disinformation:target-category="sexual-identity-group"

Sexual Identity Group

A specific minority/majority group.

DFRLab-dichotomies-of-disinformation:target-category="religious"

Religious

A specific minority/majority group.

target-concurrent-events

When a campaign targets an actor, events which take place during the campaign are said to be concurrent events.

DFRLab-dichotomies-of-disinformation:target-concurrent-events="inter-state-war"

Inter-State War

Threshold is 1,000 conflict deaths. Use COW data for 2007 and before. 2008 and after, supplement with research.

DFRLab-dichotomies-of-disinformation:target-concurrent-events="extra-state-war"

Extra-State War

Threshold is 1,000 conflict deaths. Use COW data for 2007 and before.

DFRLab-dichotomies-of-disinformation:target-concurrent-events="intra-state-war"

Intra-State War

Threshold is 1,000 conflict deaths. Use COW data for 2007 and before. 2008 and after, supplement with research.

DFRLab-dichotomies-of-disinformation:target-concurrent-events="non-state-war"

Non-State War

War in non-state territory or across state borders. Threshold is 1,000 conflict deaths. Use COW data for 2007 and before. 2008 and after, supplement with research.

DFRLab-dichotomies-of-disinformation:target-concurrent-events="federal-election"

Federal Election

Includes elections at province, municipality, administrative region, department, prefecture, and local levels.

DFRLab-dichotomies-of-disinformation:target-concurrent-events="state-election"

State Election

Includes elections at province, municipality, administrative region, department, prefecture, and local levels.

platforms-open-web

Open web media platform through which a campaign targets an actor.

DFRLab-dichotomies-of-disinformation:platforms-open-web="state-media"

State Media

Includes “state-adjacent” media, operated by government proxies or otherwise beholden to the state.

DFRLab-dichotomies-of-disinformation:platforms-open-web="independent-media"

Independent Media

Media institutions that are not beholden to the government and can be reasonably assessed to score

> 60 by the NewsGuard rating process.

DFRLab-dichotomies-of-disinformation:platforms-open-web="junk-news-websites"

Junk News Websites

A website that trafficks in deceptive headlines, fails to correct errors, avoids disclosure of funding sources, and avoids labeling advertisements. One that can be reasonably assessed to score < 60 by the NewsGuard rating process.

platforms-social-media

Social media platform through which a campaign targets an actor.

DFRLab-dichotomies-of-disinformation:platforms-social-media="facebook"

Facebook

Social media accounts created by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-social-media="instagram"

Instagram

Social media accounts created by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-social-media="twitter"

Twitter

Social media accounts created by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-social-media="youtube"

YouTube

Social media accounts created by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-social-media="linkedin"

LinkedIn

Social media accounts created by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-social-media="reddit"

Reddit

Social media accounts created by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-social-media="vk"

VK

Social media accounts created by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-social-media="forum"

Forum

Social media accounts created by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-social-media="other"

Other

Social media accounts created by the disinformants for deceptive purposes.

platforms-messaging

Messaging platform through which a campaign targets an actor.

DFRLab-dichotomies-of-disinformation:platforms-messaging="whatsapp"

WhatsApp

Messaging platforms used by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-messaging="telegram"

Telegram

Messaging platforms used by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-messaging="signal"

Signal

Messaging platforms used by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-messaging="line"

Line

Messaging platforms used by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-messaging="wechat"

WeChat

Messaging platforms used by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-messaging="sms"

SMS

Messaging platforms used by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms-messaging="other"

Other

Messaging platforms used by the disinformants for deceptive purposes.

platforms

Platforms through which a campaign targets an actor.

DFRLab-dichotomies-of-disinformation:platforms="advertisement"

Advertisement

Advertisements purchased by disinformants to disseminate a message of disinformation. Includes ads on social media and the open web.

DFRLab-dichotomies-of-disinformation:platforms="email"

Email

Email used by the disinformants for deceptive purposes.

DFRLab-dichotomies-of-disinformation:platforms="other"

Other

Other platforms used by the disinformants for deceptive purposes.

content-language

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="english"

English

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="russian"

Russian

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="french"

French

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="chinese"

Chinese

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="german"

German

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="spanish"

Spanish

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="hindi"

Hindi

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="portuguese"

Portuguese

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="bengali"

Bengali

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="japanese"

Japanese

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="turkish"

Turkish

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="polish"

Polish

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="ukrainian"

Ukrainian

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="arabic"

Arabic

The language of the disinformation.

DFRLab-dichotomies-of-disinformation:content-language="iranian-persian"

iranian-persian

The language of the disinformation.

content-topic

The subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="government"

Government

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="military"

Mility

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="political-party"

Political Party

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="elections"

Elections

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="non-state-political-actor"

Non-State Political Actor

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="business"

Business

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="influential-individuals"

Influential Individuals

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="racial"

Racial

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="ethnic"

Ethnic

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="religious"

Religious

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="sexual-identity-group"

Sexual Identity Group

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="terrorism"

Terrorism

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="immigration"

Immigration

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="economic-issue"

Economic Issue

Subject evident in the campaign.

DFRLab-dichotomies-of-disinformation:content-topic="other"

Other

Subject evident in the campaign.

methods-tactics

The tactics evident in the campaign.

DFRLab-dichotomies-of-disinformation:methods-tactics="brigading"

Brigading

Patriotic trolls or organic coordination in which disinformants seemingly operate under their real identities. A concentrated effort by one online group to manipulate another, e.g. through mass-commenting a certain message.

DFRLab-dichotomies-of-disinformation:methods-tactics="sockpuppets"

Sockpuppets

Inauthentic social media accounts used for the purpose of deception which evidence a high likelihood of human operation. This includes catfishing and other highly tailored operations conducted under inauthentic personas.

DFRLab-dichotomies-of-disinformation:methods-tactics="botnets"

Botnets

Inauthentic social media accounts used for the purpose of deception which evidence a high likelihood of automation. These accounts evidence no sustained human intervention beyond the effort necessary to program them initially. They often form large networks for the purpose of inauthentic amplification. This includes both fresh and repurposed accounts.

DFRLab-dichotomies-of-disinformation:methods-tactics="search-engine-manipulation"

Search Engine Manipulation

Undermining search engine optimization techniques with the intention of creating an inorganic correlation of search queries and results. Often realized by way of cooperative efforts by online communities. e.g. “Google Bombing.” May also include typosquatting with the intention to mislead or redirect to another URL.

DFRLab-dichotomies-of-disinformation:methods-tactics="ddos"

Hacking: DDos

Distributed denial-of-service. Malicious attempt to disrupt server traffic. In the context of political disinformation campaigns, this is intended to make it more difficult for the target to launch an effective counter-messaging effort.

DFRLab-dichotomies-of-disinformation:methods-tactics="data-exfiltration"

Hacking: Data Exfiltration

The unauthorized movement of data. In the context of political disinformation campaigns, this is the acquisition of sensitive information through spearphishing or similar techniques that can be subsequently released by the disinformant to boost their messaging effort.

DFRLab-dichotomies-of-disinformation:methods-tactics="deep-learning-processes"

Deceptive Content Manipulation: Deep Learning Processes

Any content that has been deceptively edited by use of Photoshop or similar software. This includes the deceptive co-option and re-use of extant media branding and style guides. This does not include the use of deep learning processes.

DFRLab-dichotomies-of-disinformation:methods-tactics="other"

Other

Inauthentic social media accounts used for the purpose of deception which evidence a high likelihood of human operation. This includes catfishing and other highly tailored operations

conducted under inauthentic personas.

methods-narrative-techniques

The narrative techniques evident in the campaign.

DFRLab-dichotomies-of-disinformation:methods-narrative-techniques="constructive-activate"

Constructive: Activate

Bandwagon, pander, ignite. e.g., “If you love Mr. Trump, RT this.”

DFRLab-dichotomies-of-disinformation:methods-narrative-techniques="constructive-astroturf"

Constructive: Astroturf

Artificial consensus-building, inflation, or amplification. Also called a “Potemkin Village.” e.g., “The #1 trending hashtag can’t be wrong.”

DFRLab-dichotomies-of-disinformation:methods-narrative-techniques="destructive-suppress"

Destructive: Suppress

Harass, intimidate, exhaust. Often targets influential individuals.

DFRLab-dichotomies-of-disinformation:methods-narrative-techniques="destructive-discredit"

Destructive: Discredit

Libel, leak, tarnish. Often targets government, political parties, elections, or other institutions.

DFRLab-dichotomies-of-disinformation:methods-narrative-techniques="oblique-troll"

Oblique: Troll

Confusion by way of discourse infiltration and targeted distraction. Conscious efforts by disinformants to derail political movements through tailored engagement.

DFRLab-dichotomies-of-disinformation:methods-narrative-techniques="oblique-flood"

Oblique: Flood

Confusion by way of hashtag invasion and mass noise generation. The hijacking of an online

political movement through appropriation of an existing hashtag and addition of large quantity of unrelated material.

disinformant-category

When a disinformant targets an actor, the category of that disinformant is filled in this field, if that information is available. Categories are not mutually exclusive. All relevant categories can be added.

DFRLab-dichotomies-of-disinformation:disinformant-category="government-direct-attribution"

Government: Direct Attribution

Public, definitive attribution to a national government by a social media platform or trusted government entity. These entities have access to signals intelligence and other publicly unavailable information.

DFRLab-dichotomies-of-disinformation:disinformant-category="government-inferred-attribution"

Government: Proxy/Inferred Attribution

Informed attribution to a government or government-adjacent proxy in which definitive proof is absent. Such attribution is based on open-source data and inference. This includes attribution to political parties, non-state political actors, businesses, and influential individuals who are suspected to be working at the government's direction.

DFRLab-dichotomies-of-disinformation:disinformant-category="political-party"

Political Party

Organized competitors for political power who can obtain or wield power directly. Includes politicians currently in office, as well as non-incumbent politicians running for office who are associated with a political party. Can also be an individual working for a party.

DFRLab-dichotomies-of-disinformation:disinformant-category="non-state-political-actor"

Non-State Political Actor

Organized competitors for political power who can obtain or wield power, even if indirectly; not necessarily enfranchised. Non-state political actors are formally organized, coordinated, and cohesive. e.g. Greenpeace, the NRA, or the KKK.

DFRLab-dichotomies-of-disinformation:disinformant-category="business"

Business

Includes groups that contract out to the government, individuals looking for financial gain, and mercenaries.

DFRLab-dichotomies-of-disinformation:disinformant-category="influential-individuals"

Influential Individuals

Individuals who are influential but who do not belong to a ruling government coalition. Includes groups of individuals who are not formally organized but work together. e.g. journalists, former politicians, or organized 4channers. For individuals who operate their own charitable foundations (and thus could be placed in Non-State Political Actor), coding depends on whether or not the disinformation is foremost targeting the individual, their foundation, or both.

DFRLab-dichotomies-of-disinformation:disinformant-category="electorate"

Electorate

The enfranchised population in a specific country or within a demarcated boundary.

DFRLab-dichotomies-of-disinformation:disinformant-category="racial"

Racial

A specific minority/majority group.

DFRLab-dichotomies-of-disinformation:disinformant-category="ethnic"

Ethnic

A specific minority/majority group.

DFRLab-dichotomies-of-disinformation:disinformant-category="sexual-identity-group"

Sexual Identity Group

A specific minority/majority group.

DFRLab-dichotomies-of-disinformation:disinformant-category="religious"

Religious

A specific minority/majority group.

disinformant-concurrent-events

When a disinformant targets an actor, the category of that disinformant is filled in this field, if that information is available. Categories are not mutually exclusive. All relevant categories can be added.

DFRLab-dichotomies-of-disinformation:disinformant-concurrent-events="inter-state-war"

Inter-State War

Threshold is 1,000 conflict deaths. Use COW data for 2007 and before. 2008 and after, supplement with research.

DFRLab-dichotomies-of-disinformation:disinformant-concurrent-events="extra-state-war"

Extra-State War

Threshold is 1,000 conflict deaths. Use COW data for 2007 and before.

DFRLab-dichotomies-of-disinformation:disinformant-concurrent-events="intra-state-war"

Intra-State War

Threshold is 1,000 conflict deaths. Use COW data for 2007 and before. 2008 and after, supplement with research.

DFRLab-dichotomies-of-disinformation:disinformant-concurrent-events="non-state-war"

Non-State War

War in non-state territory or across state borders. Threshold is 1,000 conflict deaths. Use COW data for 2007 and before. 2008 and after, supplement with research.

DFRLab-dichotomies-of-disinformation:disinformant-concurrent-events="federal-election"

Federal Election

Includes elections at province, municipality, administrative region, department, prefecture, and local levels.

DFRLab-dichotomies-of-disinformation:disinformant-concurrent-events="state-election"

State Election

Includes elections at province, municipality, administrative region, department, prefecture, and local levels.

disinformant-intent

This is the intent of the primary disinformant and any other disinformants coded.

DFRLab-dichotomies-of-disinformation:disinformant-intent="civil"

Civil

To include electoral interference, policy change.

DFRLab-dichotomies-of-disinformation:disinformant-intent="social"

Social

To include marginalization of majority/minority groups and general social fissure.

DFRLab-dichotomies-of-disinformation:disinformant-intent="economic"

Economic

To include suppression of economic activity, destruction of capital.

DFRLab-dichotomies-of-disinformation:disinformant-intent="military"

Military

To include complement to offensive military campaign, or information paralysis of an adversary's military institutions.

DML

DML namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Detection Maturity Level (DML) model is a capability maturity model for referencing ones maturity in detecting cyber attacks. It's designed for organizations who perform intel-driven detection and response and who put an emphasis on having a mature detection program.

8

If the actor is part of a larger organized operation they may be receiving their goals from a higher level source or handler. Depending on how organized and sophisticated the adversary's campaigns are, these goals may not even be shared with the operator(s) themselves. In cases of non-targeted threat actors, this may be much less organized or distributed. Goals are nearly impossible to detect (directly) but they're almost always the toughest question C-level leaders ask about post-breach. "Who was it and why?" These kinds of questions can never truthfully be answered unless you're operating at Detection Maturity Level 8 against your adversary and can prove reliably that you know what their goals are. Short of that, it's guessing at what the adversary's true intentions were based on behavioral observations made at lower DMLs (e.g. data stolen, directories listed, employees or programs targeted, etc). I anticipate less than a handful of organizations truly operate at this level, consistently, against the threat actors they face because it's nearly impossible to detect based on goals alone.

DML:8

Goals

If the actor is part of a larger organized operation they may be receiving their goals from a higher level source or handler. Depending on how organized and sophisticated the adversary's campaigns are, these goals may not even be shared with the operator(s) themselves. In cases of non-targeted threat actors, this may be much less organized or distributed. Goals are nearly impossible to detect (directly) but they're almost always the toughest question C-level leaders ask about post-breach. "Who was it and why?" These kinds of questions can never truthfully be answered unless you're operating at Detection Maturity Level 8 against your adversary and can prove reliably that you know what their goals are. Short of that, it's guessing at what the adversary's true intentions were based on behavioral observations made at lower DMLs (e.g. data stolen, directories listed, employees or programs targeted, etc). I anticipate less than a handful of organizations truly operate at this level, consistently, against the threat actors they face because it's nearly impossible to detect based on goals alone.

7

```
 If the adversary's high level goal is to "replicate Acme Company's Super Awesome
Product Foo in 2 years or less" their supporting strategies might include:
1.  Implant physical persons into the companies that produce this technology, in
positions with physical access to the information necessary to fulfill this goal.
2.  Compromise these organizations via cyber attack, and exfiltrate data from the
systems containing the information necessary to fulfill this goal.
For less targeted attacks, the strategy may be completely different, with shorter
durations or different objectives. The important distinguishing factor about Goals
(DML-8) and Strategy (DML-7) is that they are largely subjective in nature.  They are
very non-technical, and are often reflective of the adversary's (or their handler's)
true intentions (and strategies for fulfilling those intentions).  They represent what
the adversary wants.  For these reasons, they are not easily detectable via
conventional cyber means for most private organizations.   It's very common for DML-8
or DML-7 to not even be on the day-to-day radar of most Detection or Response
specialists, and if they are it's typically in the context of having received a
strategic intelligence report from an intelligence source about the adversary.
```

DML:7

Strategy


```
 If the adversary's high level goal is to "replicate Acme Company's Super Awesome
Product Foo in 2 years or less" their supporting strategies might include:
1.  Implant physical persons into the companies that produce this technology, in
positions with physical access to the information necessary to fulfill this goal.
2.  Compromise these organizations via cyber attack, and exfiltrate data from the
systems containing the information necessary to fulfill this goal.
For less targeted attacks, the strategy may be completely different, with shorter
durations or different objectives. The important distinguishing factor about Goals
(DML-8) and Strategy (DML-7) is that they are largely subjective in nature.  They are
very non-technical, and are often reflective of the adversary's (or their handler's)
true intentions (and strategies for fulfilling those intentions).  They represent what
the adversary wants.  For these reasons, they are not easily detectable via
conventional cyber means for most private organizations.   It's very common for DML-8
or DML-7 to not even be on the day-to-day radar of most Detection or Response
specialists, and if they are it's typically in the context of having received a
strategic intelligence report from an intelligence source about the adversary.
```


6

To successfully operate at DML-6, one must be able to reliably detect a tactic being employed regardless of the Technique or Procedure used by the adversary, the Tools they chose to use, or the Artifacts and Atomic Indicators left behind as a result of employing the tactic. While this may sound impossible on the surface, it absolutely is possible. In nearly all cases, tactics are not detected directly by a single indicator or artifact serving as the smoking gun, or a single detection signature or analytic technique. Tactics become known only after observation of multiple activities in aggregate, with respect to time and circumstance. As a result, detection of tactics are usually done

by skilled analysts, rather than technical correlation or analytics systems.

DML:6

Tactics

To successfully operate at DML-6, one must be able to reliably detect a tactic being employed regardless of the Technique or Procedure used by the adversary, the Tools they chose to use, or the Artifacts and Atomic Indicators left behind as a result of employing the tactic. While this may sound impossible on the surface, it absolutely is possible. In nearly all cases, tactics are not detected directly by a single indicator or artifact serving as the smoking gun, or a single detection signature or analytic technique. Tactics become known only after observation of multiple activities in aggregate, with respect to time and circumstance. As a result, detection of tactics are usually done by skilled analysts, rather than technical correlation or analytics systems.

5

From a maturity perspective, being able to detect an adversary's techniques is superior to being able to detect their procedures. The primary difference being techniques are specific to an individual. So when respecting this distinction, the ability to detect a specific actor operating within your environment by technique exclusively is an advantage. The best analogy to this is a rifled barrel, which leaves uniquely identifiable characteristics in the side of a bullet. Because of this, ballistics specialists can forensically match a spent round to the exact weapon from which it was fired with a high degree of certainty. Not just any weapon by calibur or model, but the exact weapon used to fire that specific round. Human beings are creatures of habit, and most adversaries aren't aware of the fact that every time they attack they're leaving evidence of their personal techniques behind for us to find. The same applies for the tool builders writing the tools these adversaries use. It's our obligation to find these distinctions and ensure we're looking for them. It's personal behavior and habits that are the hardest for humans to change, so put the hurt on your adversaries by finding creative ways to detect their behaviors and habits in your environment.

DML:5

Techniques

From a maturity perspective, being able to detect an adversary's techniques is superior to being able to detect their procedures. The primary difference being techniques are specific to an individual. So when respecting this distinction, the ability to detect a specific actor operating within your environment by technique exclusively is an advantage. The best analogy to this is a rifled barrel, which leaves uniquely identifiable characteristics in the side of a bullet. Because of this, ballistics specialists can forensically match a spent round to the exact weapon from which it was fired with a high degree of certainty. Not just any weapon by calibur or model, but the exact weapon used to fire that specific round. Human beings are creatures of habit, and most adversaries aren't aware of the fact that every time they attack they're leaving evidence of their personal techniques behind for us to find. The same applies for the tool builders writing the tools these adversaries use. It's our obligation to find these distinctions and ensure we're looking for them. It's personal behavior and habits that are the hardest for humans to change, so put the hurt on your adversaries by finding creative ways to detect their behaviors and habits in your environment.

4

Given today’s detection technology, and readily available correlation and analytics techniques, it’s amazing that more organizations haven’t reached Detection Maturity Level 4 for most of their adversaries. Procedures are one of the most effective ways of detecting adversary activity and can really inflict the most pain against lesser experienced "B-teams". In it’s most simple form, detecting a procedure is as simple as detecting a sequence of two or more of the individual steps employed by the actor. The goal here is to isolate activities that the adversary appears to perform methodically, two or more times during an incident.

DML:4

Procedures

Given today’s detection technology, and readily available correlation and analytics techniques, it’s amazing that more organizations haven’t reached Detection Maturity Level 4 for most of their adversaries. Procedures are one of the most effective ways of detecting adversary activity and can really inflict the most pain against lesser experienced "B-teams". In it’s most simple form, detecting a procedure is as simple as detecting a sequence of two or more of the individual steps employed by the actor. The goal here is to isolate activities that the adversary appears to perform methodically, two or more times during an incident.

3

Being able to detect at DML-3 means you can reliably detect the adversary’s tools, regardless of minor functionality changes to the tool, or the Artifacts or Atomic Indicators it may leave behind. Detecting tools falls into two main areas. The first is detecting the transfer and presence of the tool. This includes being able to observe the tool being transferred over the network, being able to locate it sitting at rest on a file system, or being able to identify it loaded in memory. The second, and more important area of tool detection, is detecting the tool reliably by functionality. For example, let’s take a given webshell that has 25 functions. If we want to claim DML-3 level detection for this webshell we have to exercise each of those 25 functions and understand what each of them do. What do they look like at the host, network, and event log level when they are exercised? We then aim to build detections for as many of those 25 functions across those data domains as we possibly can, reliably, balancing false positives and other constraints. The reason behind this is simple, we want to be able to detect this version of the tool and as many future variants of the tool as we can by function that it performs. If the adversary decides to change up 5 of the 25 functions for which we have detections, we’re still detecting the entire tool. In order for the adversary to use this tool completely undetected in our environment, they’ll be forced to change every one of those functions; or at least the ones that we were able to reliably build detections against.

DML:3

Tools

Being able to detect at DML-3 means you can reliably detect the adversary’s tools, regardless of minor functionality changes to the tool, or the Artifacts or Atomic Indicators it may leave behind. Detecting tools falls into two main areas. The first is detecting the transfer and presence of the tool.

This includes being able to observe the tool being transferred over the network, being able to locate it sitting at rest on a file system, or being able to identify it loaded in memory. The second, and more important area of tool detection, is detecting the tool reliably by functionality. For example, let's take a given webshell that has 25 functions. If we want to claim DML-3 level detection for this webshell we have to exercise each of those 25 functions and understand what each of them do. What do they look like at the host, network, and event log level when they are exercised? We then aim to build detections for as many of those 25 functions across those data domains as we possibly can, reliably, balancing false positives and other constraints. The reason behind this is simple, we want to be able to detect this version of the tool and as many future variants of the tool as we can by function that it performs. If the adversary decides to change up 5 of the 25 functions for which we have detections, we're still detecting the entire tool. In order for the adversary to use this tool completely undetected in our environment, they'll be forced to change every one of those functions; or at least the ones that we were able to reliably build detections against.

2

DML-2 is where most organizations spend too much of their resources; attempting to collect what they call "threat intelligence" in the form of Host & Network Artifacts. The reality is, these are merely just indicators that are observed either during or after the attack. They're like symptoms of the flu but not the flu itself. I often use the analogy "chasing the vapor trail" when I think of DML-2 because chasing after Host & Network Artifacts is much like chasing the vapor trail behind an aircraft. We know the enemy aircraft is up there in front of us somewhere, if we just keep chasing this vapor trial we'll eventually catch up to the aircraft and find our enemy right? Wrong. Having a mature detection and response program means your operating above DML-2 and you're actually locked onto the aircraft itself. You know how it operates, you know what it's capabilities are, you know the Tactics, Techniques, and Procedures of it's pilot and you can almost predict what it's next moves might be. This is precisely why good Cyber Intelligence Analysts will almost never attribute activity to a specific threat actor, group, or country based on just Host & Network Artifacts alone; they understand this DML concept and realize when they're likely just staring at the vapor trail. They understand that in reality the vapor trail (indicators) could be from any number of aircraft (tools), with any number of pilots (actors) behind the stick.

DML:2

Host & Network Artifacts

DML-2 is where most organizations spend too much of their resources; attempting to collect what they call "threat intelligence" in the form of Host & Network Artifacts. The reality is, these are merely just indicators that are observed either during or after the attack. They're like symptoms of the flu but not the flu itself. I often use the analogy "chasing the vapor trail" when I think of DML-2 because chasing after Host & Network Artifacts is much like chasing the vapor trail behind an aircraft. We know the enemy aircraft is up there in front of us somewhere, if we just keep chasing this vapor trial we'll eventually catch up to the aircraft and find our enemy right? Wrong. Having a mature detection and response program means your operating above DML-2 and you're actually locked onto the aircraft itself. You know how it operates, you know what it's capabilities are, you know the Tactics, Techniques, and Procedures of it's pilot and you can almost predict what it's next moves might be. This is precisely why good Cyber Intelligence Analysts will almost never attribute activity to a specific threat actor, group, or country based on just Host & Network Artifacts alone;

they understand this DML concept and realize when they're likely just staring at the vapor trail. They understand that in reality the vapor trail (indicators) could be from any number of aircraft (tools), with any number of pilots (actors) behind the stick.

1

These are the atomic particles that make up Host & Network artifacts. If you're detecting at Detection Maturity Level 1, it means you are probably taking "feeds of intel" from various sharing organizations and vendors in the form of lists, like domains and IP addresses, and feeding them into your detection technologies. Let me be clear on my position here. There are a few, and I mean a very precious few, circumstances where this makes sense and can be done reliably. These are edge cases where specific atomic indicators have a high enough "shelf life" where it makes sense to go ahead and create detection capabilities from them. Examples of this include unique strings found inside a binary, or perhaps an adversary is foolish enough to sit on the same recon, delivery, C2, or exfiltration infrastructure allowing you to detect reliably on their domain names or IP addresses. These might be viable cases where detecting on atomic indicator alone makes sense. Unfortunately, for the remaining 99% of the time, attempting to detect on this kind of data is suboptimal, for a number of reasons.

DML:1

Atomic IOCs

These are the atomic particles that make up Host & Network artifacts. If you're detecting at Detection Maturity Level 1, it means you are probably taking "feeds of intel" from various sharing organizations and vendors in the form of lists, like domains and IP addresses, and feeding them into your detection technologies. Let me be clear on my position here. There are a few, and I mean a very precious few, circumstances where this makes sense and can be done reliably. These are edge cases where specific atomic indicators have a high enough "shelf life" where it makes sense to go ahead and create detection capabilities from them. Examples of this include unique strings found inside a binary, or perhaps an adversary is foolish enough to sit on the same recon, delivery, C2, or exfiltration infrastructure allowing you to detect reliably on their domain names or IP addresses. These might be viable cases where detecting on atomic indicator alone makes sense. Unfortunately, for the remaining 99% of the time, attempting to detect on this kind of data is suboptimal, for a number of reasons.

0

For organizations who either don't operate at DML-1 or higher, or they don't even know where they operate on this scale, we have Detection Maturity Level - 0. Instead of pointing out all the negative things associated with this level, I'll take the high road and lend a bit of positive encouragement. Congratulations, you are at ground zero. It can only get better from here.

DML:0

None or Unknown

For organizations who either don't operate at DML-1 or higher, or they don't even know where they

operate on this scale, we have Detection Maturity Level - 0. Instead of pointing out all the negative things associated with this level, I'll take the high road and lend a bit of positive encouragement. Congratulations, you are at ground zero. It can only get better from here.

PAP

PAP namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Permissible Actions Protocol - or short: PAP - was designed to indicate how the received information can be used.

Exclusive flag set which means the values or predicate below must be set exclusively.

RED

PAP:RED

(PAP:RED) Non-detectable actions only. Recipients may not use PAP:RED information on the network. Only passive actions on logs, that are not detectable from the outside.

AMBER

PAP:AMBER

(PAP:AMBER) Passive cross check. Recipients may use PAP:AMBER information for conducting online checks, like using services provided by third parties (e.g. VirusTotal), or set up a monitoring honeypot.

GREEN

PAP:GREEN

(PAP:GREEN) Active actions allowed. Recipients may use PAP:GREEN information to ping the target, block incoming/outgoing traffic from/to the target or specifically configure honeypots to interact with the target.

WHITE

PAP:WHITE

(PAP:WHITE) No restrictions in using this information.

access-method

access-method namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The access method used to remotely access a system.

brute-force

Access was gained through systematic trial of credentials in bulk.

access-method:brute-force

Brute force

Access was gained through systematic trial of credentials in bulk.

password-guessing

Access was gained through guessing passwords through trial and error.

access-method:password-guessing

Password guessing

Access was gained through guessing passwords through trial and error.

remote-desktop-application

Access was gained through an application designed for remote access.

access-method:remote-desktop-application

Remote desktop application

Access was gained through an application designed for remote access.

stolen-credentials

Access was gained with stolen credentials.

access-method:stolen-credentials

Stolen credentials

Access was gained with stolen credentials.

pass-the-hash

Access was gained through use of an existing known hash.

access-method:pass-the-hash

Pass the hash

Access was gained through use of an existing known hash.

default-credentials

Access was gained through use of the system's default credentials.

access-method:default-credentials

Default credentials

Access was gained through use of the system's default credentials.

shell

Access was gained through the use of a shell.

access-method:shell

Shell

Access was gained through the use of a shell.

other

Access was gained through another method.

access-method:other

Other

Access was gained through another method.

accessnow

accessnow namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Access Now classification to classify an issue (such as security, human rights, youth rights).

anti-corruption-transparency

The organization campaigns, or takes other actions against corruption and transparency.

accessnow:anti-corruption-transparency

Anti-Corruption and transparency

The organization campaigns, or takes other actions against corruption and transparency.

anti-war-violence

The organization campaigns, or takes other actions against war

accessnow:anti-war-violence

Anti-War / Anti-Violence

The organization campaigns, or takes other actions against war

culture

The organization campaigns or acts to promote cultural events

accessnow:culture

Culture

The organization campaigns or acts to promote cultural events

economic-change

Issues of economic policy, wealth distribution, etc.

accessnow:economic-change

Economic Change

Issues of economic policy, wealth distribution, etc.

education

The organization is concerned with some form of education

accessnow:education

Education

The organization is concerned with some form of education

election-monitoring

The organization is an election monitor, or involved in election monitoring

accessnow:election-monitoring

Election Monitoring

The organization is an election monitor, or involved in election monitoring

environment

The organization campaigns or acts to protect the environment

accessnow:environment

Environment

The organization campaigns or acts to protect the environment

freedom-expression

The organization is concerned with freedom of speech issues

accessnow:freedom-expression

Freedom of Expression

The organization is concerned with freedom of speech issues

freedom-tool-development

The organization develops tools for use in defending or extending digital rights

accessnow:freedom-tool-development

Freedom Tool Development

The organization develops tools for use in defending or extending digital rights

funding

```
The organization is a funder of organizations or projects working with at risk users
```

accessnow:funding

Funding

```
The organization is a funder of organizations or projects working with at risk users
```

health

The organization prevents epidemic illness or acts on curing them

accessnow:health

Health Issues

The organization prevents epidemic illness or acts on curing them

human-rights

relating to the detection, recording, exposure, or challenging of abuses of human rights

accessnow:human-rights

Human Rights Issues

relating to the detection, recording, exposure, or challenging of abuses of human rights

internet-telecom

Issues of digital rights in electronic communications

accessnow:internet-telecom

Internet and Telecoms

Issues of digital rights in electronic communications

lgbt-gender-sexuality

Issues relating to the Lesbian, Gay, Bi, Transgender community

accessnow:lgbt-gender-sexuality

LGBT / Gender / Sexuality

Issues relating to the Lesbian, Gay, Bi, Transgender community

policy

The organization is a policy think-tank, or policy advocate

accessnow:policy

Policy

The organization is a policy think-tank, or policy advocate

politics

The organization takes a strong political view or is a political entity

accessnow:politics

Politics

The organization takes a strong political view or is a political entity

privacy

Issues relating to the individual’s reasonable right to privacy

accessnow:privacy

Privacy

Issues relating to the individual’s reasonable right to privacy

rapid-response

The organization provides rapid response type capability for civil society

accessnow:rapid-response

Rapid Response

The organization provides rapid response type capability for civil society

refugees

Issues relating to displaced people

accessnow:refugees

Refugees

Issues relating to displaced people

security

Issues relating to physical or information security

accessnow:security

Security

Issues relating to physical or information security

womens-right

Issues pertaining to inequality between men and women, or issues of particular relevance to women

accessnow:womens-right

Women's Rights

Issues pertaining to inequality between men and women, or issues of particular relevance to women

youth-rights

Issues of particular relevance to youth

accessnow:youth-rights

Youth Rights

Issues of particular relevance to youth

action-taken

action-taken namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Action taken in the case of a security incident (CSIRT perspective).

informed ISP/Hosting Service Provider

action-taken:informed ISP/Hosting Service Provider

Informed ISP/Hosting Service Provider

informed Registrar

action-taken:informed Registrar

Informed Registrar

informed Registrant

action-taken:informed Registrant

Informed Registrant

informed abuse-contact (domain)

action-taken:informed abuse-contact (domain)

Informed abuse-contact (domain)

informed abuse-contact (IP)

action-taken:informed abuse-contact (IP)

Informed abuse-contact (IP)

informed legal department

action-taken:informed legal department

Informed legal department

admiralty-scale

admiralty-scale namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Admiralty Scale or Ranking (also called the NATO System) is used to rank the reliability of a source and the credibility of an information. Reference based on FM 2-22.3 (FM 34-52) HUMAN INTELLIGENCE COLLECTOR OPERATIONS and NATO documents.

source-reliability

Exclusive flag set which means the values or predicate below must be set exclusively.

admiralty-scale:source-reliability="a"

Completely reliable

No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability

Associated numerical value="100"

admiralty-scale:source-reliability="b"

Usually reliable

Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time

Associated numerical value="75"

admiralty-scale:source-reliability="c"

Fairly reliable

Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past

Associated numerical value="50"

admiralty-scale:source-reliability="d"

Not usually reliable

Significant doubt about authenticity, trustworthiness, or co mpetency but has provided valid information in the past

Associated numerical value="25"

admiralty-scale:source-reliability="e"

Unreliable

Lacking in authenticity, trustworthiness, and competency; history of invalid information

admiralty-scale:source-reliability="f"

Reliability cannot be judged

No basis exists for evaluating the reliability of the source

Associated numerical value="50"

admiralty-scale:source-reliability="g"

Deliberatly deceptive

information-credibility

Exclusive flag set which means the values or predicate below must be set exclusively.

admiralty-scale:information-credibility="1"

Confirmed by other sources

Confirmed by other independent sources; logical in itself; Consistent with other information on the subject

Associated numerical value="100"

admiralty-scale:information-credibility="2"

Probably true

Not confirmed; logical in itself; consistent with other information on the subject

Associated numerical value="75"

admiralty-scale:information-credibility="3"

Possibly true

Not confirmed; reasonably logical in itself; agrees with some other information on the subject

Associated numerical value="50"

admiralty-scale:information-credibility="4"

Doubtful

Not confirmed; possible but not logical ; no other information on the subject

Associated numerical value="25"

admiralty-scale:information-credibility="5"

Improbable

Not confirmed; not logical in itself; contradicted by other information on the subject

admiralty-scale:information-credibility="6"

Truth cannot be judged

No basis exists for evaluating the validity of the information

Associated numerical value="50"

adversary

adversary namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

An overview and description of the adversary infrastructure

infrastructure-status

adversary:infrastructure-status="unknown"

Infrastructure ownership and status is unknown

adversary:infrastructure-status="compromised"

Infrastructure compromised by or in the benefit of the adversary

adversary:infrastructure-status="own-and-operated"

Infrastructure own and operated by the adversary

infrastructure-action

adversary:infrastructure-action="passive-only"

Only passive requests shall be performed to avoid detection by the adversary

adversary:infrastructure-action="take-down"

Take down requests can be performed in order to deactivate the adversary infrastructure

adversary:infrastructure-action="monitoring-active"

Monitoring requests are ongoing on the adversary infrastructure

adversary:infrastructure-action="pending-law-enforcement-request"

Law enforcement requests are ongoing on the adversary infrastructure

adversary:infrastructure-action="sinkholed"

Infrastructure of the adversary is sinkholed and information is collected

infrastructure-state

adversary:infrastructure-state="unknown"

Infrastructure state is unknown or cannot be evaluated

adversary:infrastructure-state="active"

Infrastructure state is active and actively used by the adversary

adversary:infrastructure-state="down"

Infrastructure state is known to be down

infrastructure-type

adversary:infrastructure-type="unknown"

Infrastructure usage by the adversary is unknown

adversary:infrastructure-type="proxy"

Infrastructure used as proxy between the target and the adversary

adversary:infrastructure-type="drop-zone"

Infrastructure used by the adversary to store information related to his campaigns

adversary:infrastructure-type="exploit-distribution-point"

Infrastructure used to distribute exploit towards target(s)

adversary:infrastructure-type="vpn"

Infrastructure used by the adversary as Virtual Private Network to hide activities and reduce the traffic analysis surface

adversary:infrastructure-type="panel"

Panel used by the adversary to control or maintain his infrastructure

adversary:infrastructure-type="tds"

Traffic Distribution Systems including exploit delivery or/and web monetization channels

adversary:infrastructure-type="c2"

C2 infrastructure without known specific type.

ais-marking

ais-marking namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The AIS Marking Schema implementation is maintained by the National Cybersecurity and Communication Integration Center (NCCIC) of the U.S. Department of Homeland Security (DHS)

TLPMarking

Exclusive flag set which means the values or predicate below must be set exclusively.

ais-marking:TLPMarking="WHITE"

WHITE

ais-marking:TLPMarking="GREEN"

GREEN

ais-marking:TLPMarking="AMBER"

AMBER

AISConsent

Exclusive flag set which means the values or predicate below must be set exclusively.

ais-marking:AISConsent="EVERYONE"

EVERYONE

ais-marking:AISConsent="USG"

USG

ais-marking:AISConsent="NONE"

NONE

CISA_Proprietary

Exclusive flag set which means the values or predicate below must be set exclusively.

ais-marking:CISA_Proprietary="true"

true

ais-marking:CISA_Proprietary="false"

false

AISMarking

Exclusive flag set which means the values or predicate below must be set exclusively.

ais-marking:AISMarking="Is_Proprietary"

Is_Proprietary

ais-marking:AISMarking="Not_Proprietary"

Not_Proprietary

analyst-assessment

analyst-assessment namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A series of assessment predicates describing the analyst capabilities to perform analysis. These assessment can be assigned by the analyst him/herself or by another party evaluating the analyst.

experience

The analyst experience expressed in years range in the field tagged. The year range is based on a standard 40-hour work week.

analyst-assessment:experience="less-than-1-year"

Less than 1 year

Associated numerical value="20"

analyst-assessment:experience="between-1-and-5-years"

Between 1 and 5 years

Associated numerical value="40"

analyst-assessment:experience="between-5-and-10-years"

Between 5 and 10 years

Associated numerical value="60"

analyst-assessment:experience="between-10-and-20-years"

Between 10 and 20 years

Associated numerical value="80"

analyst-assessment:experience="more-than-20-years"

More than 20 years

Associated numerical value="100"

binary-reversing-arch

Architecture that the analyst has experience with.

analyst-assessment:binary-reversing-arch="x86"

x86-32 & x86-64

analyst-assessment:binary-reversing-arch="arm"

ARM & ARM-64

analyst-assessment:binary-reversing-arch="mips"

mips & mips-64

analyst-assessment:binary-reversing-arch="powerpc"

PowerPC

binary-reversing-experience

The analyst experience in reversing expressed in years range in the field tagged. The year range is based on a standard 40-hour work week.

analyst-assessment:binary-reversing-experience="less-than-1-year"

Less than 1 year

Associated numerical value="20"

analyst-assessment:binary-reversing-experience="between-1-and-5-years"

Between 1 and 5 years

Associated numerical value="40"

analyst-assessment:binary-reversing-experience="between-5-and-10-years"

Between 5 and 10 years

Associated numerical value="60"

analyst-assessment:binary-reversing-experience="between-10-and-20-years"

Between 10 and 20 years

Associated numerical value="80"

analyst-assessment:binary-reversing-experience="more-than-20-years"

More than 20 years

Associated numerical value="100"

os

Operating System that the analyst has experience with.

analyst-assessment:os="windows"

Current Microsoft Windows system

analyst-assessment:os="linux"

GNU/linux derivative OS

analyst-assessment:os="ios"

Current IOS

analyst-assessment:os="macos"

Current Apple OS

analyst-assessment:os="android"

Current Android OS

analyst-assessment:os="bsd"

BSD

web

Web application vulnerabilities and technique that the analyst has experience with.

analyst-assessment:web="ipex"

Inter-protocol exploitations

analyst-assessment:web="common"

Common vulnerabilities as SQL injections, CSRF, XSS, CSP bypasses, etc.

analyst-assessment:web="js-desobfuscation"

De-obfuscation of Javascript payloads

web-experience

The analyst experience expressed to web application security in years range in the field tagged.

analyst-assessment:web-experience="less-than-1-year"

Less than 1 year

Associated numerical value="20"

analyst-assessment:web-experience="between-1-and-5-years"

Between 1 and 5 years

Associated numerical value="40"

analyst-assessment:web-experience="between-5-and-10-years"

Between 5 and 10 years

Associated numerical value="60"

analyst-assessment:web-experience="between-10-and-20-years"

Between 10 and 20 years

Associated numerical value="80"

analyst-assessment:web-experience="more-than-20-years"

More than 20 years

Associated numerical value="100"

crypto-experience

The analyst experience related to cryptography expressed in years range in the field tagged.

analyst-assessment:crypto-experience="less-than-1-year"

Less than 1 year

Associated numerical value="20"

analyst-assessment:crypto-experience="between-1-and-5-years"

Between 1 and 5 years

Associated numerical value="40"

analyst-assessment:crypto-experience="between-5-and-10-years"

Between 5 and 10 years

Associated numerical value="60"

analyst-assessment:crypto-experience="between-10-and-20-years"

Between 10 and 20 years

Associated numerical value="80"

analyst-assessment:crypto-experience="more-than-20-years"

More than 20 years

Associated numerical value="100"

approved-category-of-action

approved-category-of-action namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A pre-approved category of action for indicators being shared with partners (MIMIC).

cat1

Minimal Exposure - Passive Collection: CAT 1 actions provide the least exposure of an indicator, either through adversary observation or disclosure. Usage of the indicator is restricted to passive monitoring on Government or Cleared Partner networks, or through a classified passive capability or Operation. CAT 1 actions do not interact with or affect malicious network traffic.

approved-category-of-action:cat1

Cat1

Minimal Exposure - Passive Collection: CAT 1 actions provide the least exposure of an indicator, either through adversary observation or disclosure. Usage of the indicator is restricted to passive monitoring on Government or Cleared Partner networks, or through a classified passive capability or Operation. CAT 1 actions do not interact with or affect malicious network traffic.

cat2

Moderate Exposure - Government or Cleared Partner Internal Active Collection: CAT 2 actions expose the usage of an indicator through non-disruptive collection techniques which require interactions with an adversary, within Government or Cleared Partner networks. While it is not the intent to disrupt the adversary it is possible that an adversary may discover they are subject to such techniques.

approved-category-of-action:cat2

Cat2

Moderate Exposure - Government or Cleared Partner Internal Active Collection: CAT 2 actions expose the usage of an indicator through non-disruptive collection techniques which require interactions with an adversary, within Government or Cleared Partner networks. While it is not the intent to disrupt the adversary it is possible that an adversary may discover they are subject to such techniques.

cat3

Moderate Exposure - Government or Cleared Partner Internal Countermeasures: CAT 3 actions expose the usage of an indicator through inward-facing countermeasures. Malicious network traffic is affected in some manner, however the results are not directly observable to the adversary or external parties and is, therefore, more difficult to attribute as a deliberate action. Usage of the indicator is restricted to Government and Cleared Partner networks, or a classified capability or Operation. This implies a lower likelihood for non-approved disclosures.

approved-category-of-action:cat3

Cat3

Moderate Exposure - Government or Cleared Partner Internal Countermeasures: CAT 3 actions expose the usage of an indicator through inward-facing countermeasures. Malicious network traffic is affected in some manner, however the results are not directly observable to the adversary or external parties and is, therefore, more difficult to attribute as a deliberate action. Usage of the indicator is restricted to Government and Cleared Partner networks, or a classified capability or Operation. This implies a lower likelihood for non-approved disclosures.

cat4

Moderate Exposure - Government Actions on External Networks: CAT 4 actions expose the usage of an indicator through actions which occur on internet accessible networks, without the authorization of the network or information owner. Such actions are conducted as classified Operations under the auspices of national legislative and compliance provisions. Action consequences are observable to the adversary and other, public parties and it is possible they may be attributed as Government sanctioned actions.

approved-category-of-action:cat4

Cat4

Moderate Exposure - Government Actions on External Networks: CAT 4 actions expose the usage of an indicator through actions which occur on internet accessible networks, without the authorization of the network or information owner. Such actions are conducted as classified Operations under the auspices of national legislative and compliance provisions. Action consequences are observable to the adversary and other, public parties and it is possible they may be attributed as Government sanctioned actions.

cat5

High Exposure - Public Actions Which Enable Internal Countermeasures: CAT 5 actions expose the usage of an indicator through the public release of information which enables internal actions on networks not owned and controlled by the Government (i.e. industry, commercial or foreign governments). These actions are official public releases and are attributable as Government sanctioned actions.

approved-category-of-action:cat5

Cat5

High Exposure - Public Actions Which Enable Internal Countermeasures: CAT 5 actions expose the usage of an indicator through the public release of information which enables internal actions on networks not owned and controlled by the Government (i.e. industry, commercial or foreign governments). These actions are official public releases and are attributable as Government sanctioned actions.

cat6

High Exposure - Actions on Adversary Infrastructure: CAT 6 actions expose the usage of an indicator through actions which occur on adversary owned networks, without the authorization of the network or information owner. Such actions are conducted as classified Operations under the auspices of national legislative and compliance provisions. Action consequences are observable to the adversary, and possibly other public parties, and it is possible they may deduce this as FVEY action.

approved-category-of-action:cat6

Cat6

High Exposure - Actions on Adversary Infrastructure: CAT 6 actions expose the usage of an indicator through actions which occur on adversary owned networks, without the authorization of the network or information owner. Such actions are conducted as classified Operations under the auspices of national legislative and compliance provisions. Action consequences are observable to the adversary, and possibly other public parties, and it is possible they may deduce this as FVEY action.

binary-class

binary-class namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Custom taxonomy for types of binary file.

Exclusive flag set which means the values or predicate below must be set exclusively.

type

binary-class:type="good"

Known Good/Safe

binary-class:type="malicious"

Known Bad/Malicious

binary-class:type="unknown"

Not yet known

cccs

cccs namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Internal taxonomy for CCCS.

event

Type of event associated to the internal reference

cccs:event="beacon"

Beacon

A host infected with malware is connecting to threat actor owned infrastructure.

cccs:event="browser-based-exploitation"

Browser based exploitation

A browser component is being exploited in order to infect a host.

cccs:event="dos"

Dos

An attack in which the goal is to disrupt access to a host or resource.

cccs:event="email"

Email

Malicious emails sent to a department (baiting, content delivery, phishing).

cccs:event="exfiltration"

Exfiltration

Unauthorized transfer of data from a target's network to a location a threat actor controls.

cccs:event="generic-event"

Generic event

Represents a collection of virtually identical events within a range of time.

cccs:event="improper-usage"

Improper usage

Technology used in a way that compromises security or violates policy.

cccs:event="malware-artifacts"

Malware artifacts

Signs of the presence of malware observed on a host.

cccs:event="malware-download"

Malware download

Malware was transferred (downloaded/uploaded) to a host.

cccs:event="phishing"

Phishing

Information or credentials disclosed to a threat actor.

cccs:event="remote-access"

Remote access

A threat actor is attempting to or succeeding in remotely logging in to a host.

cccs:event="remote-exploitation"

Remote exploitation

A threat actor is attempting to exploit vulnerabilities remotely.

cccs:event="scan"

Scan

A threat actor is scanning the network.

cccs:event="scraping"

Scraping

Represents a collection of virtually identical scraping events within a range of time.

cccs:event="traffic-interception"

Traffic interception

Represents a collection of virtually identical traffic interception events within a range of time.

disclosure-type

Type of information being disclosed.

cccs:disclosure-type="goc-credential-disclosure"

Goc credential disclosure

Credentials for a GoC system or user were disclosed.

cccs:disclosure-type="personal-credential-disclosure"

Personal credential disclosure

Credentials not related to a GoC system or user were disclosed.

cccs:disclosure-type="personal-information-disclosure"

Personal information disclosure

Information about a person or persons was disclosed.

cccs:disclosure-type="none"

None

No information was disclosed.

cccs:disclosure-type="other"

Other

Information other than credentials and personal information was disclosed.

domain-category

The Domain Category.

cccs:domain-category="c2"

C2

Domain is being used as command-and-control infrastructure.

cccs:domain-category="proxy"

Proxy

Domain is being used as a proxy.

cccs:domain-category="seeded"

Seeded

Domain has been seeded with malware or other malicious code.

cccs:domain-category="wateringhole"

Wateringhole

Domain is being used a wateringhole.

cccs:domain-category="cloud-infrastructure"

Cloud infrastructure

Domain is hosted on cloud infrastructure.

cccs:domain-category="name-server"

Name server

Domain is a name server.

cccs:domain-category="sinkholed"

Sinkholed

Domain is being re-directed to a sinkhole.

email-type

Type of email event.

cccs:email-type="spam"

Spam

Unsolicited or junk email named after a Monty Python sketch.

cccs:email-type="content\-delivery\-attack"

Content\-delivery\-attack

Email contained malicious content or attachments.

cccs:email-type="phishing"

Phishing

Email designed to trick the recipient into providing sensitive information.

cccs:email-type="baiting"

Baiting

Email designed to trick the recipient into providing sensitive information.

cccs:email-type="unknown"

Unknown

Type of email was unknown.

exploitation-technique

The technique used to remotely exploit a GoC system.

cccs:exploitation-technique="sql-injection"

Sql injection

Exploitation occurred due to malicious SQL queries being executed against a database.

cccs:exploitation-technique="directory-traversal"

Directory traversal

Exploitation occurred through a directory traversal attack allowing access to a restricted directory.

cccs:exploitation-technique="remote-file-inclusion"

Remote file inclusion

Exploitation occurred due to vulnerabilities allowing malicious files to be sent.

cccs:exploitation-technique="code-injection"

Code injection

Exploitation occurred due to malicious code being injected.

cccs:exploitation-technique="other"

Other

Other.

ip-category

The IP Category.

cccs:ip-category="c2"

C2

IP address is a command-and-control server.

cccs:ip-category="proxy"

Proxy

IP address is a proxy server.

cccs:ip-category="seeded"

Seeded

IP address has been seeded with malware or other malicious code.

cccs:ip-category="wateringhole"

Wateringhole

IP address is a wateringhole.

cccs:ip-category="cloud-infrastructure"

Cloud infrastructure

IP address is part of cloud infrastructure.

cccs:ip-category="network-gateway"

Network gateway

IP address is a network gateway.

cccs:ip-category="server"

Server

IP address is a server of some type.

cccs:ip-category="dns-server"

Dns server

IP address is a DNS server.

cccs:ip-category="smtp-server"

Smtp server

IP address is a mail server.

cccs:ip-category="web-server"

Web server

IP address is a web server.

cccs:ip-category="file-server"

File server

IP address is a file server.

cccs:ip-category="database-server"

Database server

IP address is a database server.

cccs:ip-category="security-appliance"

Security appliance

IP address is a security appliance of some type.

cccs:ip-category="tor-node"

Tor node

IP address is a node of the TOR anonymization system.

cccs:ip-category="sinkhole"

Sinkhole

IP address is a sinkhole.

cccs:ip-category="router"

Router

IP address is a router device.

maliciousness

Level of maliciousness.

cccs:maliciousness="non-malicious"

Non-malicious

Non-malicious is not malicious or suspicious.

cccs:maliciousness="suspicious"

Suspicious

Suspicious is not non-malicious and not malicious.

cccs:maliciousness="malicious"

Malicious

Malicious is not non-malicious or suspicious.

malware-category

The Malware Category.

cccs:malware-category="exploit-kit"

Exploit kit

Toolkit used to attack vulnerabilities in systems.

cccs:malware-category="first-stage"

First stage

Malware used in the initial phase of an attack and commonly used to retrieve a second stage.

cccs:malware-category="second-stage"

Second stage

Typical more complex malware retrieved by first stage malware.

cccs:malware-category="scanner"

Scanner

Malware used to look for common vulnerabilities or running software.

cccs:malware-category="downloader"

Downloader

Malware used to retrieve additional malware or tools.

cccs:malware-category="proxy"

Proxy

Malware used to proxy traffic on an infected host.

cccs:malware-category="reverse-proxy"

Reverse proxy

If you choose this option please provide a description of what it is to the ALFRED PO.

cccs:malware-category="webshell"

Webshell

Malware uploaded to a web server allowing remote access to an attacker.

cccs:malware-category="ransomware"

Ransomware

Malware used to hold infected host's data hostage, typically through encryption until a payment is made to the attackers.

cccs:malware-category="adware"

Adware

Malware used to display ads to the infected host.

cccs:malware-category="spyware"

Spyware

Malware used to collect information from the infected host, such as credentials.

cccs:malware-category="virus"

Virus

Malware that propogates by inserting a copy of itself into another program.

cccs:malware-category="worm"

Worm

Standalone malware that propogates by copying itself..

cccs:malware-category="trojan"

Trojan

Malware that looks like legitimate software but hides malicious code.

cccs:malware-category="rootkit"

Rootkit

Malware that can hide the existance of other malware by modifying operating system functions.

cccs:malware-category="keylogger"

Keylogger

Malware that runs in the background, capturing keystrokes from a user unknowingly for exfiltration.

cccs:malware-category="browser-hijacker"

Browser hijacker

Malware that re-directs or otherwise intercepts Internet browsing by the user.

misusage-type

The type of misusage.

cccs:misusage-type="unauthorized-usage"

Unauthorized usage

Usage of the system or resource was without appropriate permission or authorization.

cccs:misusage-type="misconfiguration"

Misconfiguration

System or resource is misconfigured.

cccs:misusage-type="lack-of-encryption"

Lack of encryption

System or resources has insufficient encryption or no encryption.

cccs:misusage-type="vulnerable-software"

Vulnerable software

System or resource has software with known vulnerabilities.

cccs:misusage-type="privilege-escalation"

Privilege escalation

System or resource was exploited to gain higher privilege level.

cccs:misusage-type="other"

Other

Other.

mitigation-type

The type of mitigation.

cccs:mitigation-type="anti-virus"

Anti-virus

Anti-Virus

cccs:mitigation-type="content-filtering-system"

Content filtering system

Content Filtering System

cccs:mitigation-type="dynamic-defense"

Dynamic defense

Dynamic Defense

cccs:mitigation-type="insufficient-privileges"

Insufficient privileges

Insufficient Privileges

cccs:mitigation-type="ids"

Ids

Intrusion Detection System

cccs:mitigation-type="sink-hole-/-take-down-by-third-party"

Sink hole / take down by third party

Sink Hole / Take Down by Third Party

cccs:mitigation-type="isp"

Isp

Internet Service Provider

cccs:mitigation-type="invalid-credentials"

Invalid credentials

Invalid Credentials

cccs:mitigation-type="not-vulnerable"

Not vulnerable

No mitigation was required because the system was not vulnerable to the attack.

cccs:mitigation-type="other"

Other

Other

cccs:mitigation-type="unknown"

Unknown

Unknown

cccs:mitigation-type="user"

User

User

origin

Where the request originated from.

cccs:origin="subscriber"

Subscriber

Subscriber.

cccs:origin="internet"

Internet

Internet.

originating-organization

Origin of a signature.

cccs:originating-organization="cse"

Cse

Communications Security Establishment.

cccs:originating-organization="nsa"

Nsa

National Security Agency.

cccs:originating-organization="gchq"

Gchq

Government Communications Headquarters.

cccs:originating-organization="asd"

Asd

Australian Signals Directorate.

cccs:originating-organization="gcsb"

Gcsb

Government Communications Security Bureau.

cccs:originating-organization="open-source"

Open source

Originated from publically available information.

cccs:originating-organization="3rd-party"

3rd party

Originated from a 3rd party organization.

cccs:originating-organization="other"

Other

Other.

scan-type

The type of scan event.

cccs:scan-type="open-port"

Open port

Scan was looking for open ports corresponding to common applications or protocols.

cccs:scan-type="icmp"

Icmp

Scan was attempting to enumerate devices through the ICMP protocol.

cccs:scan-type="os-fingerprinting"

Os fingerprinting

Scan was looking for operating system information through unique characteristics in responses.

cccs:scan-type="web"

Web

Scan was enumerating or otherwise traversing web hosts.

cccs:scan-type="other"

Other

Other.

severity

Severity of the event.

cccs:severity="reconnaissance"

Reconnaissance

An actor attempted or succeeded in gaining information that may be used to identify and/or compromise systems or data.

cccs:severity="attempted-compromise"

Attempted compromise

An actor attempted affecting the confidentiality, integrity or availability of a system.

cccs:severity="exploited"

Exploited

A vulnerability was successfully exploited.

threat-vector

Specifies how the threat actor gained or attempted to gain initial access to the target GoC host.

cccs:threat-vector="application:cms"

Application:cms

Content Management System.

cccs:threat-vector="application:bash"

Application:bash

BASH script.

cccs:threat-vector="application:acrobat-reader"

Application:acrobat reader

Adobe Acrobat Reader.

cccs:threat-vector="application:ms-excel"

Application:ms excel

Microsoft Excel.

cccs:threat-vector="application:other"

Application:other

Other Application.

cccs:threat-vector="language:sql"

Language:sql

Structured Query Language.

cccs:threat-vector="language:php"

Language:php

PHP: Hypertext Preprocessor.

cccs:threat-vector="language:javascript"

Language:javascript

JavaScript.

cccs:threat-vector="language:other"

Language:other

Other Language.

cccs:threat-vector="protocol:dns"

Protocol:dns

Domain Name System.

cccs:threat-vector="protocol:ftp"

Protocol:ftp

File Transfer Protocol.

cccs:threat-vector="protocol:http"

Protocol:http

Hyper Text Transfer Protocol.

cccs:threat-vector="protocol:icmp"

Protocol:icmp

Internet Control Message Protocol.

cccs:threat-vector="protocol:ntp"

Protocol:ntp

Network Time Protocol.

cccs:threat-vector="protocol:rdp"

Protocol:rdp

Remote Desktop Protocol.

cccs:threat-vector="protocol:smb"

Protocol:smb

Server Message Block.

cccs:threat-vector="protocol:snmp"

Protocol:snmp

Simple Network Management Protocol.

cccs:threat-vector="protocol:ssl"

Protocol:ssl

Secure Sockets Layer.

cccs:threat-vector="protocol:telnet"

Protocol:telnet

Network Virtual Terminal Protocol.

cccs:threat-vector="protocol:sip"

Protocol:sip

Session Initiation Protocol.

circl

circl namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

CIRCL Taxonomy - Schemes of Classification in Incident Response and Detection

incident-classification

circl:incident-classification="spam"

Spam

circl:incident-classification="system-compromise"

System compromise

circl:incident-classification="sabotage"

Sabotage

circl:incident-classification="privacy-violation"

Privacy violation

circl:incident-classification="scan"

Scan

circl:incident-classification="denial-of-service"

Denial of Service

circl:incident-classification="copyright-issue"

Copyright issue

circl:incident-classification="phishing"

Phishing

circl:incident-classification="whaling"

Whaling

circl:incident-classification="smishing"

SMS Phishing

circl:incident-classification="malware"

Malware

circl:incident-classification="XSS"

XSS

circl:incident-classification="vulnerability"

Vulnerability

circl:incident-classification="fastflux"

Fastflux

circl:incident-classification="domain-fronting"

Domain Fronting

circl:incident-classification="sql-injection"

SQL Injection

circl:incident-classification="information-leak"

Information leak

circl:incident-classification="scam"

Scam

circl:incident-classification="cryptojacking"

Cryptojacking

circl:incident-classification="locker"

Locker

circl:incident-classification="screenlocker"

Screenlocker

circl:incident-classification="wiper"

Wiper

circl:incident-classification="ransomware"

ransomware

circl:incident-classification="sextortion"

sextortion

circl:incident-classification="social-engineering"

Social Engineering

circl:incident-classification="gdpr-violation"

GDPR Violation

circl:incident-classification="covid-19"

covid-19

topic

circl:topic="finance"

Finance

circl:topic="ict"

ICT

circl:topic="individual"

Individual

circl:topic="industry"

Industry

circl:topic="medical"

Medical

circl:topic="services"

Services

circl:topic="undefined"

Undefined

coa

coa namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Course of action taken within organization to discover, detect, deny, disrupt, degrade, deceive and/or destroy an attack.

discover

coa:discover="proxy"

Searched historical proxy logs.

coa:discover="ids"

Searched historical IDS logs.

coa:discover="firewall"

Searched historical firewall logs.

coa:discover="pcap"

Discovered in packet-capture logs

coa:discover="remote-access"

Searched historical remote access logs.

coa:discover="authentication"

Searched historical authentication logs.

coa:discover="honeypot"

Searched historical honeypot data.

coa:discover="syslog"

Searched historical system logs.

coa:discover="web"

Searched historical WAF and web application logs.

coa:discover="database"

Searched historcial database logs.

coa:discover="mail"

Searched historical mail logs.

coa:discover="antivirus"

Searched historical antivirus alerts.

coa:discover="malware-collection"

Retro hunted in a malware collection.

coa:discover="other"

Searched other historical data.

coa:discover="unspecified"

Unspecified information.

detect

coa:detect="proxy"

Detect by Proxy infrastructure

coa:detect="nids"

Detect by Network Intrusion detection system.

coa:detect="hids"

Detect by Host Intrusion detection system.

coa:detect="other"

Detect by other tools.

coa:detect="syslog"

Detect in system logs.

coa:detect="firewall"

Detect by firewall.

coa:detect="email"

Detect by MTA.

coa:detect="web"

Detect by web infrastructure including WAF.

coa:detect="database"

Detect in database.

coa:detect="remote-access"

Detect in remote-access logs.

coa:detect="malware-collection"

Detect in malware-collection.

coa:detect="antivirus"

Detect with antivirus.

coa:detect="unspecified"

Unspecified information.

deny

coa:deny="proxy"

Implemented a proxy filter.

coa:deny="firewall"

Implemented a block rule on a firewall.

coa:deny="waf"

Implemented a block rule on a web application firewall.

coa:deny="email"

Implemented a filter on a mail transfer agent.

coa:deny="chroot"

Implemented a chroot jail.

coa:deny="remote-access"

Blocked an account for remote access.

coa:deny="other"

Denied an action by other means.

coa:deny="unspecified"

Unspecified information.

disrupt

coa:disrupt="nips"

Implemented a rule on a network IPS.

coa:disrupt="hips"

Implemented a rule on a host-based IPS.

coa:disrupt="other"

Disrupted an action by other means.

coa:disrupt="email"

Quarantined an email.

coa:disrupt="memory-protection"

Implemented memory protection like DEP and/or ASLR.

coa:disrupt="sandboxing"

Exploded in a sandbox.

coa:disrupt="antivirus"

Activated an antivirus signature.

coa:disrupt="unspecified"

Unspecified information.

degrade

coa:degrade="bandwidth"

Throttled the bandwidth.

coa:degrade="tarpit"

Implement a network tarpit.

coa:degrade="other"

Degraded an action by other means.

coa:degrade="email"

Queued an email.

coa:degrade="unspecified"

Unspecified information.

deceive

coa:deceive="honeypot"

Implemented an interactive honeypot.

coa:deceive="DNS"

Implemented DNS redirects, e.g. a response policy zone.

coa:deceive="other"

Deceived the attacker with other technology.

coa:deceive="email"

Implemented email redirection.

coa:deceive="unspecified"

Unspecified information.

destroy

coa:destroy="arrest"

Arrested the threat actor.

coa:destroy="seize"

Seized attacker infrastructure.

coa:destroy="physical"

Physically destroyed attacker hardware.

coa:destroy="dos"

Performed a denial-of-service attack against attacker infrastructure.

coa:destroy="hack-back"

Hack back against the threat actor.

coa:destroy="other"

Carried out other offensive actions against the attacker.

coa:destroy="unspecified"

Unspecified information.

collaborative-intelligence

collaborative-intelligence namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Collaborative intelligence support language is a common language to support analysts to perform their analysis to get crowdsourced support when using threat intelligence sharing platform like MISP. The objective of this language is to advance collaborative analysis and to share earlier than later.

request

Request predicate covers all the requests which can be done by analysts or organisations willing to get additional information to support their analysis.

collaborative-intelligence:request="sample"

Request a binary sample

collaborative-intelligence:request="extracted-malware-config"

Extracted malware config

Request of the malware configuration extracted from the malware sample tagged.

collaborative-intelligence:request="deobfuscated-sample"

Request a deobfuscated sample of the shared sample

collaborative-intelligence:request="more-samples"

Request additional samples compared to the original analysis to build a competitive analysis on the reversing aspect

collaborative-intelligence:request="related-samples"

Request related samples required for further analysis

collaborative-intelligence:request="static-analysis"

Request additional static analysis or reversing on the information shared

collaborative-intelligence:request="detection-signature"

Request detection signature from

collaborative-intelligence:request="context"

Request more contextual information

collaborative-intelligence:request="abuse-contact"

Request an abuse contact to report to

collaborative-intelligence:request="historical-information"

Request more historical information from

collaborative-intelligence:request="complementary-validation"

Request complementary validation

collaborative-intelligence:request="target-information"

Request about the target(s) including field of activities or companies

collaborative-intelligence:request="request-analysis"

Request further technical or tactical analysis

collaborative-intelligence:request="more-information"

Request for generic additional information

common-taxonomy

common-taxonomy namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Common Taxonomy for Law enforcement and CSIRTs

malware

Infection of one or various systems with a specific type of malware / Connection performed by/from/to (a) suspicious system(s)

common-taxonomy:malware="infection"

Infection

Malware detected in a system.

common-taxonomy:malware="distribution"

Distribution

Malware attached to a message or email message containing link to malicious URL or IP.

common-taxonomy:malware="command-and-control"

Command & Control (C&C)

System used as a command-and-control point by a botnet. Also included in this field are systems serving as a point for gathering information stolen by botnets.

common-taxonomy:malware="malicious-connection"

Malicious connection

System attempting to gain access to a port normally linked to a specific type of malware / System attempting to gain access to an IP address or URL normally linked to a specific type of malware, e.g. C&C or a distribution page for components linked to a specific botnet.

availability

Disruption of the processing and response capacity of systems and networks in order to render them inoperative / Premeditated action to damage a system, interrupt a process, change or delete information, etc.

common-taxonomy:availability="dos-ddos"

Denial of Service (DoS) / Distributed Denial of Service (DDoS)

Single source using specially designed software to affect the normal functioning of a specific service, by exploiting vulnerability / Mass mailing of requests (network packets, emails, etc.) from one single source to a specific service, aimed at affecting its normal functioning.

common-taxonomy:availability="sabotage"

Sabotage

Logical and physical activities which – although they are not aimed at causing damage to information or at preventing its transmission among systems – have this effect.

information-gathering

Active and passive gathering of information on systems or networks / Unauthorised monitoring and reading of network traffic / Attempt to gather information on a user or a system through phishing methods.

common-taxonomy:information-gathering="scanning"

Scanning

Single system scan searching for open ports or services using these ports for responding / Scanning a network aimed at identifying systems which are active in the same network / Transfer of a specific DNS zone.

common-taxonomy:information-gathering="sniffing"

Sniffing

Logical or physical interception of communications.

common-taxonomy:information-gathering="phishing"

Phishing

Mass emailing aimed at collecting data for phishing purposes with regard to the victims / Hosting web sites for phishing purposes.

intrusion-attempt

Attempt to intrude by exploiting vulnerability in a system, component or network / Attempt to log in to services or authentication/access control mechanisms.

common-taxonomy:intrusion-attempt="vulnerability-exploitation-attempt"

Exploitation of vulnerability attempt

Unsuccessful use of a tool exploiting a specific vulnerability of the system / Unsuccessful attempt to manipulate or read the information of a database by using the SQL injection technique / Unsuccessful attempts to perform attacks by using cross-site scripting techniques / Unsuccessful attempt to include files in the system under attack by using file inclusion techniques / Unauthorised access to a system or component by bypassing an access control system in place.

common-taxonomy:intrusion-attempt="login-attempt"

Login attempt

Unsuccessful login by using sequential credentials for gaining access to the system / Unsuccessful acquisition of access credentials by breaking the protective cryptographic keys / Unsuccessful login by using system access credentials previously loaded into a dictionary.

intrusion

Actual intrusion by exploiting vulnerability in the system, component or network / Actual intrusion in a system, component or network by compromising a user or administrator account.

common-taxonomy:intrusion="vulnerability-exploitation"

(Successful) Exploitation of vulnerability

Unauthorised use of a tool exploiting a specific vulnerability of the system / Unauthorised manipulation or reading of information contained in a database by using the SQL injection technique / Attack performed with the use of cross-site scripting techniques / Unauthorised inclusion of files into a system under attack with the use of file inclusion techniques / Unauthorised

access to a system or component by bypassing an access control system in place.

common-taxonomy:intrusion="account-compromise"

Compromising an account

Unauthorised access to a system or component by using stolen access credentials.

information-security

Unauthorised access to a particular set of information / Unauthorised change or elimination of a particular set of information.

common-taxonomy:information-security="unauthorised-access"

Unauthorised access

Unauthorised access to a system or component / Unauthorised access to a set of information / Unauthorised access to and sharing of a specific set of information.

common-taxonomy:information-security="unauthorised-modification-or-deletion"

Unauthorised modification / deletion

Unauthorised changes to a specific set of information / Unauthorised deleting of a specific set of information.

fraud

Loss of property caused with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

common-taxonomy:fraud="resources-misuse"

Misuse or unauthorised use of resources

Use of institutional resources for purposes other than those intended.

common-taxonomy:fraud="false-representation"

False representation

Unauthorised use of the name of an institution.

abusive-content

Sending SPAM messages / Distribution and sharing of copyright protected content / Dissemination

of content forbidden by law.

common-taxonomy:abusive-content="spam"

SPAM

Sending an unusually large quantity of email messages / Unsolicited or unwanted email message sent to the recipient.

common-taxonomy:abusive-content="copyright"

Copyright

Unauthorised distribution or sharing of content protected by Copyright and related rights.

common-taxonomy:abusive-content="cse-racism-violence-incitement"

Child Sexual Exploitation, racism or incitement to violence

Distribution or sharing of illegal content such as child sexual exploitation material, racism, xenophobia, etc.

other

Incidents not classified in the existing classification.

common-taxonomy:other="unclassified-incident"

Unclassified incident

Incidents which do not fit the existing classification, acting as an indicator for the classification's update.

common-taxonomy:other="undetermined-incident"

Undetermined incident

Unprocessed incidents which have remained undetermined from the beginning.

copine-scale

copine-scale namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The COPINE Scale is a rating system created in Ireland and used in the United Kingdom to categorise the severity of images of child sex abuse. The scale was developed by staff at the COPINE (Combating Paedophile Information Networks in Europe) project. The COPINE Project was founded

in 1997, and is based in the Department of Applied Psychology, University College Cork, Ireland.

Exclusive flag set which means the values or predicate below must be set exclusively.

level-10

copine-scale:level-10

Sadistic/bestiality: (a) Pictures showing a child being tied, bound, beaten, whipped, or otherwise subjected to something that implies pain; (b) Pictures where an animal is involved in some form of sexual behavior with a child

100

level-9

copine-scale:level-9

Gross assault: Grossly obscene pictures of sexual assault, involving penetrative sex, masturbation, or oral sex involving an adult

90

level-8

copine-scale:level-8

Assault: Pictures of children being subjected to a sexual assault, involving digital touching, involving an adult

80

level-7

copine-scale:level-7

Explicit sexual activity: Involves touching, mutual and self-masturbation, oral sex, and intercourse by child, not involving an adult

70

level-6

copine-scale:level-6

Explicit erotic posing: Emphasizing genital areas where the child is posing either naked, partially clothed, or fully clothed

60

level-5

copine-scale:level-5

Erotic posing: Deliberately posed pictures of fully or partially clothed or naked children in sexualized or provocative poses

50

level-4

copine-scale:level-4

Posing: Deliberately posed pictures of children fully or partially clothed or naked (where the amount, context, and organization suggests sexual interest)

40

level-3

copine-scale:level-3

Erotica: Surreptitiously taken photographs of children in play areas or other safe environments showing either underwear or varying degrees of nakedness

30

level-2

copine-scale:level-2

Nudist: Pictures of naked or seminaked children in appropriate nudist settings, and from legitimate sources

20

level-1

copine-scale:level-1

Indicative: Nonerotic and nonsexualized pictures showing children in their underwear, swimming costumes, and so on, from either commercial sources or family albums; pictures of children playing in normal settings, in which the context or organization of pictures by the collector indicates inappropriateness

10

course-of-action

course-of-action namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A Course Of Action analysis considers six potential courses of action for the development of a cyber security capability.

passive

course-of-action:passive="discover"

The discover action is a 'historical look at the data'. This action heavily relies on your capability to store logs for a reasonable amount of time and have them accessible for searching. Typically, this type of action is applied against security information and event management (SIEM) or stored network data. The goal is to determine whether you have seen a specific indicator in the past.

course-of-action:passive="detect"

The passive action is setting up detection rules of an indicator for future traffic. These actions are most often executed via an intrusion detection system (IDS) or a specific logging rule on your firewall or application. It can also be configured as an alert in a SIEM when a specific condition is triggered.

active

course-of-action:active="deny"

The deny action prevents the event from taking place. Common examples include a firewall block or a proxy filter.

course-of-action:active="disrupt"

Disruption makes the event fail as it is occurring. Examples include quarantining or memory protection measures.

course-of-action:active="degrade"

Degrading will not immediately fail an event, but it will slow down the further actions of the attacker. This tactic allows you to catch up during an incident response process, but you have to consider that the attackers may eventually succeed in achieving their objectives. Throttling bandwidth is one way to degrade an intrusion.

course-of-action:active="deceive"

Deception allows you to learn more about the intentions of the attacker by making them think the action was successful. One way to do this is to put a honeypot in place and redirect the traffic, based on an indicator, towards the honeypot.

course-of-action:active="destroy"

The destroy action is rarely for 'usual' defenders, as this is an offensive action against the attacker. These actions, including physical destructive actions and arresting the attackers, are usually left to law enforcement agencies.

cryptocurrency-threat

cryptocurrency-threat namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Threats targetting cryptocurrency, based on CipherTrace report.

SIM Swapping

cryptocurrency-threat:SIM Swapping

An identity theft technique that takes over a victim’s mobile device to steal credentials and break into wallets or exchange accounts to steal cryptocurrency.

Crypto Dusting

cryptocurrency-threat:Crypto Dusting

A new form of blockchain spam that erodes the recipient’s reputation by sending cryptocurrency from known money mixers.

Sanction Evasion

cryptocurrency-threat:Sanction Evasion

Nation states using cryptocurrencies has been promoted by the Iranian and Venezuelan

governments.

Next-Generation Crypto Mixers

cryptocurrency-threat:Next-Generation Crypto Mixers

Money laundering services that promise to exchange tainted tokens for freshly mined crypto, but in reality, cleanse cryptocurrency through exchanges.

Shadow Money Service Businesses

cryptocurrency-threat:Shadow Money Service Businesses

Unlicensed Money Service Businesses (MSBs) banking cryptocurrency without the knowledge of host financial institutions, and thus exposing banks to unknown risk.

Datacenter-Scale Crypto Jacking:

cryptocurrency-threat:Datacenter-Scale Crypto Jacking:

Takeover attacks that mine for cryptocurrency at a massive scale have been discovered in datacenters, including AWS.

Lightning Network Transactions

cryptocurrency-threat:Lightning Network Transactions

Enable anonymous bitcoin transactions by going "off-chain," and cannow scale to $2,150,000.

Decentralized Stable Coins

cryptocurrency-threat:Decentralized Stable Coins

Stabilized tokens that can be designed for use as private coins.

Email Extortion and Bomb Threats

cryptocurrency-threat:Email Extortion and Bomb Threats

Cyber-extortionists stepped up mass-customized phishing emails campaigns using old passwords and spouse names in 2018. Bomb threat extortion scams demanding bitcoin spiked in December.

Crypto Robbing Ransomware

cryptocurrency-threat:Crypto Robbing Ransomware

Cyber-extortionists began distributing new malware that empties cryptocurrency wallets and steals private keys while holding user data hostage.

csirt-americas

csirt-americas namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Taxonomía CSIRT Américas.

defacement

csirt-americas:defacement

Defacement

malware

csirt-americas:malware

Malware

ddos

csirt-americas:ddos

DDoS

phishing

csirt-americas:phishing

Phishing

spam

csirt-americas:spam

Spam

botnet

csirt-americas:botnet

Botnet

fastflux

csirt-americas:fastflux

Fastflux

cryptojacking

csirt-americas:cryptojacking

Cryptojacking

xss

csirt-americas:xss

XSS

sqli

csirt-americas:sqli

SQL Injection

vulnerability

csirt-americas:vulnerability

Vulnerability

infoleak

csirt-americas:infoleak

Information leak

compromise

csirt-americas:compromise

System compromise

other

csirt-americas:other

Other

csirt_case_classification

csirt_case_classification namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

It is critical that the CSIRT provide consistent and timely response to the customer, and that sensitive information is handled appropriately. This document provides the guidelines needed for CSIRT Incident Managers (IM) to classify the case category, criticality level, and sensitivity level for each CSIRT case. This information will be entered into the Incident Tracking System (ITS) when a case is created. Consistent case classification is required for the CSIRT to provide accurate reporting to management on a regular basis. In addition, the classifications will provide CSIRT IM's with proper case handling procedures and will form the basis of SLA's between the CSIRT and other Company departments.

incident-category

csirt_case_classification:incident-category="DOS"

Denial of service / Distributed Denial of service

csirt_case_classification:incident-category="forensics"

Forensics work

csirt_case_classification:incident-category="compromised-information"

Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property

csirt_case_classification:incident-category="compromised-asset"

Compromised host (root account, Trojan, rootkit), network device, application, user account.

csirt_case_classification:incident-category="unlawful-activity"

Theft / Fraud / Human Safety / Child Porn

csirt_case_classification:incident-category="internal-hacking"

Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware

csirt_case_classification:incident-category="external-hacking"

Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.

csirt_case_classification:incident-category="malware"

A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan.

csirt_case_classification:incident-category="email"

Spoofed email, SPAM, and other email security-related events.

csirt_case_classification:incident-category="consulting"

Security consulting unrelated to any confirmed incident

csirt_case_classification:incident-category="policy-violation"

Violation of various policies

criticality-classification

csirt_case_classification:criticality-classification="1"

Incident affecting critical systems or information with potential to be revenue or customer impacting.

csirt_case_classification:criticality-classification="2"

Incident affecting non-critical systems or information, not revenue or customer impacting. Employee investigations that are time sensitive should typically be classified at this level.

csirt_case_classification:criticality-classification="3"

Possible incident, non-critical systems. Incident or employee investigations that are not time sensitive. Long-term investigations involving extensive research and/or detailed forensic work.

sensitivity-classification

csirt_case_classification:sensitivity-classification="1"

Extremely Sensitive

csirt_case_classification:sensitivity-classification="2"

Sensitive

csirt_case_classification:sensitivity-classification="3"

Not Sensitive

cssa

cssa namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The CSSA agreed sharing taxonomy.

sharing-class

cssa:sharing-class="high_profile"

Generated within the company during incident/case related investigations or forensic analysis or via malware reversing, validated by humans and highly contextualized.

Associated numerical value="95"

cssa:sharing-class="vetted"

Generated within the company, validated by a human prior to sharing, data points have been contextualized (to a degree) e.g. IPs are related to C2 or drop site.

Associated numerical value="50"

cssa:sharing-class="unvetted"

Generated within the company by automated means without human interaction e.g., by malware sandbox, honeypots, IDS, etc.

Associated numerical value="10"

report

cssa:report="details"

Description of the incidence.

cssa:report="link"

Link to the original report location.

cssa:report="attached"

Attached report.

origin

cssa:origin="manual_investigation"

Information gathered by an analyst/incident responder/forensic expert/etc.

cssa:origin="honeypot"

Information coming out of honeypots.

cssa:origin="sandbox"

Information coming out of sandboxes.

cssa:origin="email"

Information coming out of email infrastructure.

cssa:origin="3rd-party"

Information from outside the company.

cssa:origin="report"

Information coming from a report.

cssa:origin="other"

If none of the other origins applies.

cssa:origin="unknown"

Origin of the data unknown.

analyse

cti

cti namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Cyber Threat Intelligence cycle to control workflow state of your process.

planning

CTI requirementes being generated.

cti:planning

Phase

CTI requirementes being generated.

collection

Data collection initiated.

cti:collection

Phase

Data collection initiated.

processing-and-analysis

Data is being processed and analyzed

cti:processing-and-analysis

Phase

Data is being processed and analyzed

dissemination-done

CTI product created and delivered to stakeholders.

cti:dissemination-done

Phase

CTI product created and delivered to stakeholders.

feedback-received

Feedback received by stakeholders.

cti:feedback-received

Phase

Feedback received by stakeholders.

feedback-pending

Feedback pending by stakeholders.

cti:feedback-pending

Phase

Feedback pending by stakeholders.

current-event

current-event namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Current events - Schemes of Classification in Incident Response and Detection

pandemic

current-event:pandemic="sars-cov"

SARS-CoV 2003

current-event:pandemic="covid-19"

COVID-19

election

current-event:election="eu-par-2019"

European Parliament election, 2019

current-event:election="us-pres-2020"

United States Presidential election, 2020

cyber-threat-framework

cyber-threat-framework namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Cyber Threat Framework was developed by the US Government to enable consistent characterization and categorization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries. https://www.dni.gov/index.php/cyber-threat-framework

Preparation

cyber-threat-framework:Preparation="plan-activity"

Plan activity

Associated numerical value="10"

cyber-threat-framework:Preparation="conduct-research-and-analysis"

Conduct research & analysis

Associated numerical value="11"

cyber-threat-framework:Preparation="develop-resource-and-capabilities"

Develop resources & capabilities

Associated numerical value="12"

cyber-threat-framework:Preparation="acquire-victim-and-specific-knowledge"

Acquire victim & specific knowledge

Associated numerical value="13"

cyber-threat-framework:Preparation="complete-preparations"

Complete preparations

Associated numerical value="14"

Engagement

cyber-threat-framework:Engagement="deploy-capability"

Deploy capability

Associated numerical value="20"

cyber-threat-framework:Engagement="interact-with-intended-victim"

Interact with intended victim

Associated numerical value="21"

cyber-threat-framework:Engagement="exploit-vulnerabilities"

Exploit vulnerabilities

Associated numerical value="22"

cyber-threat-framework:Engagement="deliver-malicious-capabilities"

Deliver malicious capabilities

Associated numerical value="23"

Presence

cyber-threat-framework:Presence="establish-controlled-access"

Establish controlled access

Associated numerical value="30"

cyber-threat-framework:Presence="hide"

Hide

Associated numerical value="31"

cyber-threat-framework:Presence="expand-presence"

Expand presence

Associated numerical value="32"

cyber-threat-framework:Presence="refine-focus-of-activity"

Refine focus of activity

Associated numerical value="33"

cyber-threat-framework:Presence="establish-persistence"

Establish persistence

Associated numerical value="34"

Effect/Consequence

cyber-threat-framework:Effect/Consequence="enable-other-operations"

Enable other operations

Associated numerical value="40"

cyber-threat-framework:Effect/Consequence="deny-access"

Deny access

Associated numerical value="41"

cyber-threat-framework:Effect/Consequence="extract-data"

Extract data

Associated numerical value="42"

cyber-threat-framework:Effect/Consequence="alter-data-and-or-computer-network-or-system-behavior"

Alter data and/or computer, network or system behavior

Associated numerical value="43"

cyber-threat-framework:Effect/Consequence="destroy-hardware-software-or-data"

Destroy HW/SW/data

Associated numerical value="44"

cycat

cycat namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Taxonomy used by CyCAT, the Universal Cybersecurity Resource Catalogue, to categorize the

namespaces it supports and uses.

type

Type of entry in the catalogue.

cycat:type="tool"

Tool

Open source or proprietary tool used in cybersecurity.

cycat:type="playbook"

Playbook

Playbook, such as a defined set of rules with one or more actions triggered by different events to respond to, orchestrate or automate cybersecurity related actions.

cycat:type="taxonomy"

Taxonomy

Cybersecurity taxonomy is a set of labels used to classify (in both terms - arrange in classes or/and design to national classification) cybersecurity related information.

cycat:type="rule"

Rule

Detection rule or set of detection rules used in the cybersecurity field. Rulesets can be in different formats for (N/L)IDS/SIEM (such as Snort, Suricata, Zeek, SIGMA or YARA) or any other tool capable of parsing them.

cycat:type="notebook"

Notebook

Interactive document to code, experiment, train or visualize cybersecurity-related information. A notebook can be transcribed in a format such as Jupyter Notebooks, Apache Zeppelin, Pluton or Google Colab.

cycat:type="vulnerability"

Vulnerability

Public or non-public information about a security vulnerability in a specific software, hardware or service.

cycat:type="proof-of-concept"

Proof-of-concept

Code to validate a known vulnerability.

cycat:type="fingerprint"

Fingerprint

Code to uniquely identify specific cybersecurity-relevant patterns. Fingerprints can be expressed in different formats such as ja3, ja3s, hassh, jarm or favicon-mmh3.

cycat:type="mitigation"

Mitigation

Mitigating control to prevent unwanted activity from happening, like a specific configuration of the operating system/tools or an implementation policy.

cycat:type="dataset"

Dataset

Dataset for validation of detections and tool stacks,

scope

Scope of usage for the entry in the catalogue.

cycat:scope="identify"

Identify

cycat:scope="protect"

Protect

cycat:scope="detect"

Detect

cycat:scope="respond"

Respond

cycat:scope="recover"

Recover

cycat:scope="exploit"

Exploit

cycat:scope="investigate"

Investigate

cycat:scope="train"

Train

cycat:scope="test"

Test

cytomic-orion

cytomic-orion namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Taxonomy to describe desired actions for Cytomic Orion

action

Desired action of background jobs with the API

Exclusive flag set which means the values or predicate below must be set exclusively.

cytomic-orion:action="upload"

upload

Upload IOC to Cytomic Orion

cytomic-orion:action="delete"

delete

Delete IOC from Cytomic Orion

dark-web

dark-web namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Criminal motivation on the dark web: A categorisation model for law enforcement. ref: Janis Dalins, Campbell Wilson, Mark Carman. Taxonomy updated by MISP Project

topic

Topic associated with the materials tagged

dark-web:topic="drugs-narcotics"

Drugs/Narcotics

Illegal drugs/chemical compounds for consumption/ingestion - either via blanket unlawfulness (e.g. proscribed drugs) or via unlawful access (e.g. prescription-only/restricted medications sold without lawful accessibility).

dark-web:topic="electronics"

Electronics

Electronics and high tech materials, described or to sell for example.

dark-web:topic="finance"

Finance

Any monetary/currency/exchangeable materials. Includes carding, Paypal etc.

dark-web:topic="finance-crypto"

CryptoFinance

Any monetary/currency/exchangeable materials based on cryptocurrencies. Includes Bitcoin, Litecoin etc.

dark-web:topic="credit-card"

Credit-Card

Credit cards and payments materials

dark-web:topic="cash-in"

Cash-in

Buying parts of assets, conversion from liquid assets, currency, etc.

dark-web:topic="cash-out"

Cash-out

Selling parts of assets, conversion to liquid assets, currency, etc.

dark-web:topic="escrow"

Escrow

Third party keeping assets in behalf of two other parties making a transactions.

dark-web:topic="hacking"

Hacking

Materials relating to the illegal access to or alteration of data and/or electronic services.

dark-web:topic="identification-credentials"

Identification/Credentials

Materials used for providing/establishing identification with third parties. Examples include passports, driver licenses and login credentials.

dark-web:topic="intellectual-property-copyright-materials"

Intellectual Property/Copyright Materials

Otherwise lawful materials stored, transferred or made available without consent of their legal rights holders.

dark-web:topic="pornography-adult"

Pornography - Adult

Lawful, ethical pornography (i.e. involving only consenting adults).

dark-web:topic="pornography-child-exploitation"

Pornography - Child (Child Exploitation)

Child abuse materials (aka child pornography), including 'fantasy' fiction materials, CGI. Also includes the provision/offering of child abuse materials and/or activities

dark-web:topic="pornography-illicit-or-illegal"

Pornography - Illicit or Illegal

Illegal pornography NOT including children/child abuse. Includes bestiality, stolen/revenge porn, hidden cameras etc.

dark-web:topic="search-engine-index"

Search Engine/Index

Site providing links/references to other sites/services. Referred to as a ‘nexus’ by (Moore and Rid, 2016)

dark-web:topic="unclear"

Unclear

Unable to completely establish topic of material.

dark-web:topic="extremism"

Extremism

Illegal or ‘of concern’ levels of extremist ideology. Note this does not provide blanket coverage of fundamentalist ideologies and dogma - only those associated with illegal acts. Socialist/anarchist/religious materials (for example) will not be included unless inclusive or indicative of associated illegal conduct, such as hate crimes.

dark-web:topic="violence"

Violence

Materials relating to violence against persons or property.

dark-web:topic="weapons"

Weapons

Materials specifically associated with materials and/or items for use in violent acts against persons or property. Examples include firearms and bomb-making ingredients.

dark-web:topic="softwares"

Softwares

Illegal or armful software distribution

dark-web:topic="counteir-feit-materials"

Counter-feit materials

Fake identification papers.

dark-web:topic="gambling"

Gambling

Games involving money

dark-web:topic="library"

Library

Library or list of books

dark-web:topic="other-not-illegal"

Other not illegal

Material not of interest to law enforcement - e.g. personal sites, Facebook mirrors.

dark-web:topic="legitimate"

Legitimate

Legitimate websites

dark-web:topic="chat"

Chats platforms

Chats space or equivalent, which are not forums

dark-web:topic="mixer"

Mixer

Anonymization tools for crypto-currencies transactions

dark-web:topic="mystery-box"

Mystery-Box

Mystery Box seller

dark-web:topic="anonymizer"

Anonymizer

Anonymization tools

dark-web:topic="vpn-provider"

VPN-Provider

Provides VPN services and related

dark-web:topic="email-provider"

EMail-Provider

Provides e-mail services and related

dark-web:topic="ponies"

Ponies

self-explanatory. It’s ponies

dark-web:topic="games"

Games

Flash or online games

dark-web:topic="parody"

Parody or Joke

Meme, Parody, Jokes, Trolling, …

dark-web:topic="whistleblower"

Whistleblower

Exposition and sharing of confidential information with protection of the witness in mind

dark-web:topic="ransomware-group"

Ransomware Group

Ransomware group PR or leak website

motivation

Motivation with the materials tagged

dark-web:motivation="education-training"

Education & Training

Materials providing instruction - e.g. ‘how to’ guides

dark-web:motivation="wiki"

Wiki

Wiki pages, documentation and information display

dark-web:motivation="forum"

Forum

Sites specifically designed for multiple users to communicate as peers

dark-web:motivation="file-sharing"

File Sharing

General file sharing, typically (but not limited to) movie/image sharing

dark-web:motivation="hosting"

Hosting

Hosting providers, e-mails, websites, file-storage etc.

dark-web:motivation="ddos-services"

DDoS-Services

Stresser, Booter, DDoSer, DDoS as a Service provider, DDoS tools, etc.

dark-web:motivation="general"

General

Materials not covered by the other motivations. Typically, materials of a nature not of interest to law enforcement. For example, personal biography sites.

dark-web:motivation="information-sharing-reportage"

Information Sharing/Reportage

Journalism/reporting on topics. Can include biased coverage, but obvious propaganda materials are covered by Recruitment/Advocacy.

dark-web:motivation="scam"

Scam

Intentional confidence trick to fraud people or group of people

dark-web:motivation="political-speech"

Political-Speech

Political, activism, without extremism.

dark-web:motivation="conspirationist"

Conspirationist

Conspirationist content, fake news, etc.

dark-web:motivation="hate-speech"

Hate-Speech

Racism, violent, hate… speech.

dark-web:motivation="religious"

Religious

Religious, faith, doctrinal related content.

dark-web:motivation="marketplace-for-sale"

Marketplace/For Sale

Services/goods for sale, regardless of means of payment.

dark-web:motivation="smuggling"

Smuggling

Information or trading of wild animals, prohibited goods, …

dark-web:motivation="recruitment-advocacy"

Recruitment/Advocacy

Propaganda

dark-web:motivation="system-placeholder"

System/Placeholder

Automatically generated content, not designed for any identifiable purpose other than diagnostics - e.g. “It Works” message provided by default by Apache2

dark-web:motivation="unclear"

Unclear

Unable to completely establish motivation of material.

structure

Structure of the materials tagged

dark-web:structure="incomplete"

Incomplete websites or information

Websites and pages that are unable to load completely properly

dark-web:structure="captcha"

Captcha and Solvers

Captchas and solvers elements

dark-web:structure="login-forms"

Logins forms and gates

Authentication pages, login page, login forms that block access to an internal part of a website.

dark-web:structure="contact-forms"

Contact forms and gates

Forms to perform a contact request, send an e-mail, fill information, enter a password, ...

dark-web:structure="encryption-keys"

Encryption and decryption keys

e.g. PGP Keys, passwords, ...

dark-web:structure="police-notice"

Police Notice

Closed websites, with police-equivalent banners

dark-web:structure="legal-statement"

Legal-Statement

RGPD statement, Privacy-policy, guidelines of a websites or forum...

dark-web:structure="test"

Test

Test websites without any real consequences or effects

dark-web:structure="videos"

Videos

Videos and streaming

dark-web:structure="unclear"

Unclear

Unable to completely establish structure of material.

data-classification

data-classification namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Data classification for data potentially at risk of exfiltration based on table 2.1 of Solving Cyber Risk book.

regulated-data

Data which is regulated under a specific regulation or law such as PII, SPD, PCI or PHI.

data-classification:regulated-data

Regulated data

Data which is regulated under a specific regulation or law such as PII, SPD, PCI or PHI.

commercially-confidential-information

Data which represents a specific commercial value and is confidential to an organisation such as trade secrets, customer accounts.

data-classification:commercially-confidential-information

Commercially confidential information (CCI)

Data which represents a specific commercial value and is confidential to an organisation such as trade secrets, customer accounts.

financially-sensitive-information

Data which represents a specific financial value to an organisation such as payroll, investment information.

data-classification:financially-sensitive-information

Financially sensitive information (FSI)

Data which represents a specific financial value to an organisation such as payroll, investment information.

valuation-sensitive-information

Data which is sensitive to the valuation of an organisation such as inside information (as defined by a Financial Services Authority).

data-classification:valuation-sensitive-information

Valuation sensitive information (VSI)

Data which is sensitive to the valuation of an organisation such as inside information (as defined by a Financial Services Authority).

sensitive-information

Data which is sensitive such as email or letters.

data-classification:sensitive-information

Sensitive information

Data which is sensitive such as email or letters.

dcso-sharing

dcso-sharing namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Taxonomy defined in the DCSO MISP Event Guide. It provides guidance for the creation and consumption of MISP events in a way that minimises the extra effort for the sending party, while enhancing the usefulness for receiving parties.

event-type

dcso-sharing:event-type="Observation"

This event describes traits and indicators closely related to a single entity, like an email campaign or sighting of a reference sample on VirusTotal. Events of this type are typically created by CSOC staff and may be verified by analysts. Observed and verified indicators would be consumed by automated filtering systems in order to support near-time threat prevention. In retrospect, observations could be correlated with reports and analysis events in order to help understand the motivation for an attack and to reassess the associated risk.

dcso-sharing:event-type="Incident"

This event describes traits and indicators related to a security incident. As such, the event may refer to multiple entities like organizations, bank account numbers, files, and URLs. Events of this type contain first-hand information, that is, the reporting organization took part in the analysis of the incident. Use event type "Report" for second-hand information. Events of this type are typically created and consumed by analysts.

dcso-sharing:event-type="Report"

Traceability of indicators can be essential to document compliance of processes with legal obligations or company regulations. This event preserves a report to document the origin and context of indicators. Events of this type need to be checked by a human to ensure correct reproduction of indicators and context. Intended consumers are automated processes. Events may also serve as a basis for analysis reports or to justify preventive measures. If your organization is or was directly involved in an incident and you want to provide a first-hand account, then please use event type "Incident" instead.

dcso-sharing:event-type="Analysis"

This event builds on "observation", "incident", and "report" events; adds enrichments; and provides context. Events of this type will be created by analysts with support by automated tools. Analysts are also the main consumers.

dcso-sharing:event-type="Collection"

This event collects unrelated IoCs. For example, an event could combine all network IoCs that were learned of during a day or a week from events of other types.

ddos

ddos namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Distributed Denial of Service - or short: DDoS - taxonomy supports the description of Denial of Service attacks and especially the types they belong too.

type

Types and techniques described the way that the attack is performed to launch the Denial of Service attacks. A combination of type values can be used to explain combined techniques and methods.

ddos:type="amplification-attack"

Amplification attack

ddos:type="reflected-spoofed-attack"

Reflected and Spoofed attack

ddos:type="slow-read-attack"

Slow Read attack

ddos:type="flooding-attack"

Flooding attack

ddos:type="post-attack"

Large POST HTTP attack

de-vs

de-vs namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

German (DE) Government classification markings (VS).

Einstufung

de-vs:Einstufung="STRENG GEHEIM"

STRENG GEHEIM

Kenntnisnahme durch Unbefugte kann den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden.

de-vs:Einstufung="GEHEIM"

GEHEIM

Kenntnisnahme durch Unbefugte kann die Sicherheit der Bundesrepublik Deutschland oder eines

ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen.

de-vs:Einstufung="VS-VERTRAULICH"

VS-VERTRAULICH

Kenntnisnahme durch Unbefugte kann für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein.

de-vs:Einstufung="VS-NfD"

VS-NUR FÜR DEN DIENSTGEBRAUCH

Kenntnisnahme durch Unbefugte kann für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein.

Schutzwort

de-vs:Schutzwort="Dummy"

Dummy

Platzhalter.

deception

deception namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Deception is an important component of information operations, valuable for both offense and defense.

space

Actions have associated locations, and deception can apply to those references.

deception:space="direction"

Direction

direction of the action. Direction cases can arise with some actions that are supposedly one-way like file transfers.

deception:space="location-at"

Location at

Location where something occured

deception:space="location-from"

Location from

Location where something started

deception:space="location-to"

Location to

Location where something finished

deception:space="location-through"

Location through

Location where some action passed through

deception:space="orientation"

Orientation

Orientation (in some space). Orientation cases can arise with some actions that are supposedly one-way like file transfers.

time

Many actions on computer are timestamped, and attackers and defenders can deceive in regard to those times. An attacker could change the times of events recorded in a log file or the directory information about files to conceal records of their activities.

deception:time="frequency"

Frequency

Frequency of occurrence of a repeated action. Frequency is an excellent case for deception, as in denial-of-service attacks that greatly increase the frequency of requests or transactions to tie up computer resources.

deception:time="time-at"

Time at

Time at which something occurred

deception:time="time-from"

Time from

Time at which something started

deception:time="time-to"

Time to

Time at which something ended

deception:time="time-through"

Time through

Time through which something occurred

participant

Actions have associated participants and the tools or objects by actions are accomplished.

deception:participant="agent"

Agent

Who initiates the action.Identification of participants responsible for actions ("agents") is a key problem in cyberspace, and is an easy target for deception.

deception:participant="beneficiary"

Beneficiary

Who benefits. Deceptions involving the beneficiary of an action occur with phishing and other email scams.

deception:participant="experiencer"

Experiencer

Who senses, experiences the action. Deception in the "experiencer" case occurs with secret monitoring of adversary activities.

deception:participant="instrument"

Instrument

What helps accomplish the action. Deception is easy with the instrument case because details of how software accomplishes things are often hidden in cyberspace.

deception:participant="object"

Object

What the action is done for. Deception in objects of the action is easy: Honeypots deceive as to the hardware and software objects of an attack, and "bait" data such as credit-card numbers can also be deceptive objects.

deception:participant="recipient"

Recipient

Who receives the action. The recipient of an action in cyberspace is usually the object.

causality

Deception in cause, purpose, and effect is important in many kinds of social-engineering attacks where false reasons like "I have a deadline" or "It didn't work" are given for requests for actions or information that aid the adversary. Deception in a contradiction action is not possible in cyberspace because commands do not generally relate actions.

deception:causality="cause"

Cause

Cause of the action

deception:causality="contradiction"

Contradiction

What this action opposes if anything

deception:causality="effect"

Effect

Effect of the action

deception:causality="purpose"

Purpose

Purpose of the action

quality

The "quality" semantic cases cover the manner in which actions are performed.

deception:quality="accompaniment"

Accompaniment

An additionnal object associated with the action

deception:quality="content"

Content

What is contained by th eaction object

deception:quality="manner"

Manner

The way in which action is done. (Deception in manner does not generally apply because the manner in which a command is issued or executed should not affect the outcome.)

deception:quality="material"

Material

The atomic units out of which the action is composed. Deception in material does not apply much because everything is represented as bits in cyberspace, though defenders can deceive this way by simulating commands rather than executing them.

deception:quality="measure"

Measure

The mesurement associated with the action. Deception in measure (the amount of data) is important in denial-of-service attacks and can also done defensively by swamping the attacker with data.

deception:quality="order"

Order

With respect to other actions

deception:quality="value"

Value

The data transmitted by the action (the software sense of the term). Deception in value (or subroutine "argument") can occur defensively as in a ploy of misunderstanding attacker commands.

essence

Deception can occur in the ontological features of an action, its type and the context to which is belongs.

deception:essence="supertype"

Supertype

a generalization of the action type. Phishing email is an example of deception in supertype.

deception:essence="whole"

Whole

of which the action is a part

speech-act-theory

Deception can involve semantic cases related to communication. Both internal and external preconditions provide useful deceptions by defenders since it is often hard to confirm deception in such conditions in cyberspace.

deception:speech-act-theory="external-precondition"

External precondition

external precondition on the action. External preconditions are on the rest of the world such as the ability of a site to accept a particular user-supplied password.

deception:speech-act-theory="internal-precondition"

Internal precondition

internal precondition, on the ability of the agent to perform the action. Internal preconditions are on the agent of the action, such as ability of a user to change their password.

dhs-ciip-sectors

dhs-ciip-sectors namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

DHS critical sectors as in https://www.dhs.gov/critical-infrastructure-sectors

DHS-critical-sectors

dhs-ciip-sectors:DHS-critical-sectors="chemical"

Chemical

dhs-ciip-sectors:DHS-critical-sectors="commercial-facilities"

Commercial Facilities

dhs-ciip-sectors:DHS-critical-sectors="communications"

Communications

dhs-ciip-sectors:DHS-critical-sectors="critical-manufacturing"

Critical Manufacturing

dhs-ciip-sectors:DHS-critical-sectors="dams"

Dams

dhs-ciip-sectors:DHS-critical-sectors="dib"

Defense Industrial Base

dhs-ciip-sectors:DHS-critical-sectors="emergency-services"

Emergency services

dhs-ciip-sectors:DHS-critical-sectors="energy"

energy

dhs-ciip-sectors:DHS-critical-sectors="financial-services"

Financial Services

dhs-ciip-sectors:DHS-critical-sectors="food-agriculture"

Food and Agriculture

dhs-ciip-sectors:DHS-critical-sectors="government-facilities"

Government Facilities

dhs-ciip-sectors:DHS-critical-sectors="healthcare-public"

Healthcare and Public Health

dhs-ciip-sectors:DHS-critical-sectors="it"

Information Technology

dhs-ciip-sectors:DHS-critical-sectors="nuclear"

Nuclear

dhs-ciip-sectors:DHS-critical-sectors="transport"

Transportation Systems

dhs-ciip-sectors:DHS-critical-sectors="water"

Water and water systems

sector

diamond-model

diamond-model namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Diamond Model for Intrusion Analysis establishes the basic atomic element of any intrusion activity, the event, composed of four core features: adversary, infrastructure, capability, and victim.

Adversary

diamond-model:Adversary

An adversary is the actor/organization responsible for utilizing a capability against the victim to achieve their intent.

Capability

diamond-model:Capability

The capability describes the tools and/or techniques of the adversary used in the event. It includes all means to affect the victim from the most manual “unsophisticated” methods (e.g., manual password guessing) to the most sophisticated automated techniques.

Infrastructure

diamond-model:Infrastructure

The infrastructure feature describes the physical and/or logical communication structures the adversary uses to deliver a capability, maintain control of capabilities (e.g., commandand-control/C2), and effect results from the victim (e.g., exfiltrate data). As with the other features, the infrastructure can be as specific or broad as necessary. Examples include: Internet Protocol (IP) addresses, domain names, e-mail addresses, Morse code flashes from a phone's voice-mail light watched from across a street, USB devices found in a parking lot and inserted into a workstation, or the compromising emanations from hardware (e.g., Van Eck Phreaking) being collected by a nearby listening post.

Victim

diamond-model:Victim

A victim is the target of the adversary and against whom vulnerabilities and exposures are exploited and capabilities used. A victim can be described in whichever way necessary and appropriate: organization, person, target email address, IP address, domain, etc. However, it is useful to define the victim persona and their assets separately as they serve different analytic functions. Victim personae are useful in non-technical analysis such as cyber-victimology and social-political centered approaches whereas victim assets are associated with common technical approaches such as vulnerability analysis..

dni-ism

dni-ism namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A subset of Information Security Marking Metadata ISM as required by Executive Order (EO) 13526. As described by DNI.gov as Data Encoding Specifications for Information Security Marking Metadata in Controlled Vocabulary Enumeration Values for ISM

classification:all

dni-ism:classification:all="R"

RESTRICTED

dni-ism:classification:all="C"

CONFIDENTIAL

dni-ism:classification:all="S"

SECRET

dni-ism:classification:all="TS"

TOP SECRET

dni-ism:classification:all="U"

UNCLASSIFIED

classification:us

dni-ism:classification:us="C"

CONFIDENTIAL

dni-ism:classification:us="S"

SECRET

dni-ism:classification:us="TS"

TOP SECRET

dni-ism:classification:us="U"

UNCLASSIFIED

scicontrols

dni-ism:scicontrols="EL"

ENDSEAL

dni-ism:scicontrols="EL-EU"

ECRU

dni-ism:scicontrols="EL-NK"

NONBOOK

dni-ism:scicontrols="HCS"

HCS

dni-ism:scicontrols="HCS-O"

HCS-O

dni-ism:scicontrols="HCS-P"

HCS-P

dni-ism:scicontrols="KDK"

KLONDIKE

dni-ism:scicontrols="KDK-BLFH"

KDK BLUEFISH

dni-ism:scicontrols="KDK-IDIT"

KDK IDITAROD

dni-ism:scicontrols="KDK-KAND"

KDK KANDIK

dni-ism:scicontrols="RSV"

RESERVE

dni-ism:scicontrols="SI"

SPECIAL INTELLIGENCE

dni-ism:scicontrols="SI-G"

SI-GAMMA

dni-ism:scicontrols="TK"

TALENT KEYHOLE

complies:with

dni-ism:complies:with="USGov"

Document claims compliance with all rules encoded in ISM for documents produced by the US Federal Government. This is the minimum set of rules for US documents to adhere to, and all US documents should claim compliance with USGov.

dni-ism:complies:with="USIC"

Document claims compliance with all rules encoded in ISM for documents produced by the US Intelligence Community. Documents that claim compliance with USIC MUST also claim compliance with USGov.

dni-ism:complies:with="USDOD"

Document claims compliance with all rules encoded in ISM for documents produced by the US Department of Defense. Documents that claim compliance with USDOD MUST also claim compliance with USGov.

dni-ism:complies:with="OtherAuthority"

Document claims compliance with an authority other than the USGov, USIC, or USDOD.

atomicenergymarkings

dni-ism:atomicenergymarkings="RD"

RESTRICTED DATA

dni-ism:atomicenergymarkings="RD-CNWDI"

RD-CRITICAL NUCLEAR WEAPON DESIGN INFORMATION

dni-ism:atomicenergymarkings="FRD"

FORMERLY RESTRICTED DATA

dni-ism:atomicenergymarkings="DCNI"

DoD CONTROLLED NUCLEAR INFORMATION

dni-ism:atomicenergymarkings="UCNI"

DoE CONTROLLED NUCLEAR INFORMATION

dni-ism:atomicenergymarkings="TFNI"

TRANSCLASSIFIED FOREIGN NUCLEAR INFORMATION

notice

dni-ism:notice="FISA"

FISA Warning statement

dni-ism:notice="IMC"

IMCON Warning statement

dni-ism:notice="CNWDI"

Controled Nuclear Weapon Design Information Warning statement

dni-ism:notice="RD"

RD Warning statement

dni-ism:notice="FRD"

FRD Warning statement

dni-ism:notice="DS"

LIMDIS caveat

dni-ism:notice="LES"

LES Notice

dni-ism:notice="LES-NF"

LES-NF Notice

dni-ism:notice="DSEN"

DSEN Notice

dni-ism:notice="DoD-Dist-A"

DoD Distribution statement A from DoD Directive 5230.24

dni-ism:notice="DoD-Dist-B"

DoD Distribution statement B from DoD Directive 5230.24

dni-ism:notice="DoD-Dist-C"

DoD Distribution statement C from DoD Directive 5230.24

dni-ism:notice="DoD-Dist-D"

DoD Distribution statement D from DoD Directive 5230.24

dni-ism:notice="DoD-Dist-E"

DoD Distribution statement E from DoD Directive 5230.24

dni-ism:notice="DoD-Dist-F"

DoD Distribution statement F from DoD Directive 5230.24

dni-ism:notice="DoD-Dist-X"

DoD Distribution statement X from DoD Directive 5230.24

dni-ism:notice="US-Person"

US Person info Notice

dni-ism:notice="pre13526ORCON"

Indicates that an instance document must abide by rules pertaining to ORIGINATOR CONTROLLED data issued prior to Executive Order 13526.

dni-ism:notice="POC"

Indicates that the contents of this notice specify the contact information for a required point-of-contact.

dni-ism:notice="COMSEC"

COMSEC Notice

nonic

dni-ism:nonic="NNPI"

NAVAL NUCLEAR PROPULSION INFORMATION

dni-ism:nonic="DS"

LIMITED DISTRIBUTION

dni-ism:nonic="XD"

EXCLUSIVE DISTRIBUTION

dni-ism:nonic="ND"

NO DISTRIBUTION

dni-ism:nonic="SBU"

SENSITIVE BUT UNCLASSIFIED

dni-ism:nonic="SBU-NF"

SENSITIVE BUT UNCLASSIFIED NOFORN

dni-ism:nonic="LES"

LAW ENFORCEMENT SENSITIVE

dni-ism:nonic="LES-NF"

LAW ENFORCEMENT SENSITIVE NOFORN

dni-ism:nonic="SSI"

SENSITIVE SECURITY INFORMATION

nonuscontrols

dni-ism:nonuscontrols="ATOMAL"

NATO Atomal mark

dni-ism:nonuscontrols="BOHEMIA"

NATO Bohemia mark

dni-ism:nonuscontrols="BALK"

NATO Balk mark

dissem

dni-ism:dissem="RS"

RISK SENSITIVE

dni-ism:dissem="FOUO"

FOR OFFICIAL USE ONLY

dni-ism:dissem="OC"

ORIGINATOR CONTROLLED

dni-ism:dissem="OC-USGOV"

ORIGINATOR CONTROLLED US GOVERNMENT

dni-ism:dissem="IMC"

CONTROLLED IMAGERY

dni-ism:dissem="NF"

NOT RELEASABLE TO FOREIGN NATIONALS

dni-ism:dissem="PR"

CAUTION-PROPRIETARY INFORMATION INVOLVED

dni-ism:dissem="REL"

AUTHORIZED FOR RELEASE TO

dni-ism:dissem="RELIDO"

RELEASABLE BY INFORMATION DISCLOSURE OFFICIAL

dni-ism:dissem="DSEN"

DEA SENSITIVE

dni-ism:dissem="FISA"

FOREIGN INTELLIGENCE SURVEILLANCE ACT

dni-ism:dissem="DISPLAYONLY"

AUTHORIZED FOR DISPLAY BUT NOT RELEASE TO

domain-abuse

domain-abuse namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Domain Name Abuse - taxonomy to tag domain names used for cybercrime.

domain-status

Domain status - describes the registration status of the domain name

domain-abuse:domain-status="active"

Registered & active

Domain name is registered and DNS is delegated

domain-abuse:domain-status="inactive"

Registered & inactive

Domain name is registered and DNS is not delegated

domain-abuse:domain-status="suspended"

Registered & suspended

Domain name is registered & DNS delegation is temporarily removed by the registry

domain-abuse:domain-status="not-registered"

Not registered

Domain name is not registered and open for registration

domain-abuse:domain-status="not-registrable"

Not registrable

Domain is not registered and cannot be registered

domain-abuse:domain-status="grace-period"

Grace period

Domain is deleted and still reserved for previous owner

domain-access-method

Domain Access - describes how the adversary has gained access to the domain name

domain-abuse:domain-access-method="criminal-registration"

Criminal registration

Domain name is registered for criminal purposes

domain-abuse:domain-access-method="compromised-webserver"

Compromised webserver

Webserver is compromised for criminal purposes

domain-abuse:domain-access-method="compromised-dns"

Compromised DNS

Compromised authoritative DNS or compromised delegation

domain-abuse:domain-access-method="sinkhole"

Sinkhole

Domain Name is sinkholed for research, detection, LE

domain-abuse:domain-access-method="compromised-domain-name-registrar"

Compromised domain name registrar

Domain name is compromised due to an incident at the registrar

domain-abuse:domain-access-method="compromised-domain-name-registry"

Compromised domain name registry

Domain name is compromised due to an incident at the registry

drugs

drugs namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A taxonomy based on the superclass and class of drugs. Based on https://www.drugbank.ca/releases/latest

alkaloids-and-derivatives

drugs:alkaloids-and-derivatives="ajmaline-sarpagine-alkaloids"

Ajmaline-sarpagine alkaloids

drugs:alkaloids-and-derivatives=" allocolchicine-alkaloids"

```
Allocolchicine alkaloids
```

drugs:alkaloids-and-derivatives=" Amaryllidaceae alkaloids"

```
Amaryllidaceae alkaloids
```

drugs:alkaloids-and-derivatives="aporphines"

Aporphines

drugs:alkaloids-and-derivatives="camptothecins"

Camptothecins

drugs:alkaloids-and-derivatives="cephalotaxus-alkaloids"

Cephalotaxus alkaloids

drugs:alkaloids-and-derivatives="cinchona-alkaloids"

Cinchona alkaloids

drugs:alkaloids-and-derivatives="eburnan-type-alkaloids"

Eburnan-type alkaloids

drugs:alkaloids-and-derivatives="epibatidine-analogues"

Epibatidine analogues

drugs:alkaloids-and-derivatives="ergoline-and-derivatives"

Ergoline and derivatives

drugs:alkaloids-and-derivatives="harmala-alkaloids"

Harmala alkaloids

drugs:alkaloids-and-derivatives="ibogan-type-alkaloids"

Ibogan-type alkaloids

drugs:alkaloids-and-derivatives="lupin-alkaloids"

Lupin alkaloids

drugs:alkaloids-and-derivatives="morphinans"

Morphinans

drugs:alkaloids-and-derivatives="phthalide-isoquinolines"

Phthalide isoquinolines

drugs:alkaloids-and-derivatives="protoberberine-alkaloids-and-derivatives"

Protoberberine alkaloids and derivatives

drugs:alkaloids-and-derivatives="tropane-alkaloids"

Tropane alkaloids

drugs:alkaloids-and-derivatives="vinca-alkaloids"

Vinca alkaloids

drugs:alkaloids-and-derivatives="yohimbine-alkaloids"

Yohimbine alkaloids

benzenoids

drugs:benzenoids="anthracenes"

Anthracenes

drugs:benzenoids="benzene-and-substituted-derivatives"

Benzene and substituted derivatives

drugs:benzenoids="dibenzocycloheptenes"

Dibenzocycloheptenes

drugs:benzenoids="fluorenes"

Fluorenes

drugs:benzenoids="indanes"

Indanes

drugs:benzenoids="indenes-and-isoindenes"

Indenes and isoindenes

drugs:benzenoids="naphthacenes"

Naphthacenes

drugs:benzenoids="phenanthrenes-and-derivatives"

Phenanthrenes and derivatives

drugs:benzenoids="phenol-esters"

Phenol esters

drugs:benzenoids="phenol-ethers"

Phenol ethers

drugs:benzenoids="phenols"

Phenols

drugs:benzenoids="pyrenes"

Pyrenes

drugs:benzenoids="tetralins"

Tetralins

drugs:benzenoids="triphenyl-compounds"

Triphenyl compounds

homogeneous-metal-compounds

drugs:homogeneous-metal-compounds="homogeneous-actinide-compounds"

Homogeneous actinide compounds

drugs:homogeneous-metal-compounds="homogeneous-alkali-metal-compounds"

Homogeneous alkali metal compounds

drugs:homogeneous-metal-compounds="homogeneous-alkaline-earth-metal-compounds"

Homogeneous alkaline earth metal compounds

drugs:homogeneous-metal-compounds="homogeneous-lanthanide-compounds"

Homogeneous lanthanide compounds

drugs:homogeneous-metal-compounds="homogeneous-metalloid-compounds"

Homogeneous metalloid compounds

drugs:homogeneous-metal-compounds="homogeneous-post-transition-metal-compounds"

Homogeneous post-transition metal compounds

drugs:homogeneous-metal-compounds="homogeneous-transition-metal-compounds"

Homogeneous transition metal compounds

homogeneous-non-metal-compounds

drugs:homogeneous-non-metal-compounds="halogen-organides"

Halogen organides

drugs:homogeneous-non-metal-compounds="homogeneous-halogens"

Homogeneous halogens

drugs:homogeneous-non-metal-compounds="homogeneous-noble-gases"

Homogeneous noble gases

drugs:homogeneous-non-metal-compounds="homogeneous-other-non-metal-compounds"

Homogeneous other non-metal compounds

drugs:homogeneous-non-metal-compounds="non-metal-oxoanionic-compounds"

Non-metal oxoanionic compounds

drugs:homogeneous-non-metal-compounds="other-non-metal-halides"

Other non-metal halides

drugs:homogeneous-non-metal-compounds="other-non-metal-organides"

Other non-metal organides

hydrocarbons

drugs:hydrocarbons="polycyclic-hydrocarbons"

Polycyclic hydrocarbons

hydrocarbon-derivatives

drugs:hydrocarbon-derivatives="tropones"

Tropones

lignans,-neolignans-and-related-compounds

drugs:lignans,-neolignans-and-related-compounds="aryltetralin-lignans"

Aryltetralin lignans

drugs:lignans,-neolignans-and-related-compounds="dibenzylbutane-lignans"

Dibenzylbutane lignans

drugs:lignans,-neolignans-and-related-compounds="flavonolignans"

Flavonolignans

drugs:lignans,-neolignans-and-related-compounds="furanoid-lignans"

Furanoid lignans

drugs:lignans,-neolignans-and-related-compounds="lignan-lactones"

Lignan lactones

lipids-and-lipid-like-molecules

drugs:lipids-and-lipid-like-molecules="fatty-acyls"

Fatty Acyls

drugs:lipids-and-lipid-like-molecules="glycero-3-dithiophosphocholines"

Glycero-3-dithiophosphocholines

drugs:lipids-and-lipid-like-molecules="glycerolipids"

Glycerolipids

drugs:lipids-and-lipid-like-molecules="glycerophospholipids"

Glycerophospholipids

drugs:lipids-and-lipid-like-molecules="prenol-lipids"

Prenol lipids

drugs:lipids-and-lipid-like-molecules="saccharolipids"

Saccharolipids

drugs:lipids-and-lipid-like-molecules="s-alkyl-coas"

S-alkyl-CoAs

drugs:lipids-and-lipid-like-molecules="sphingolipids"

Sphingolipids

drugs:lipids-and-lipid-like-molecules="steroids-and-steroid-derivatives"

Steroids and steroid derivatives

mixed-metal/non-metal-compounds

drugs:mixed-metal/non-metal-compounds="alkali-metal-organides"

Alkali metal organides

drugs:mixed-metal/non-metal-compounds="alkali-metal-oxoanionic-compounds"

Alkali metal oxoanionic compounds

drugs:mixed-metal/non-metal-compounds="alkali-metal-salts"

Alkali metal salts

drugs:mixed-metal/non-metal-compounds="alkaline-earth-metal-organides"

Alkaline earth metal organides

drugs:mixed-metal/non-metal-compounds="alkaline-earth-metal-oxoanionic-compounds"

Alkaline earth metal oxoanionic compounds

drugs:mixed-metal/non-metal-compounds="alkaline-earth-metal-salts"

Alkaline earth metal salts

drugs:mixed-metal/non-metal-compounds="metalloid-organides"

Metalloid organides

drugs:mixed-metal/non-metal-compounds="metalloid-oxoanionic-compounds"

Metalloid oxoanionic compounds

drugs:mixed-metal/non-metal-compounds="miscellaneous-mixed-metal/non-metals"

Miscellaneous mixed metal/non-metals

drugs:mixed-metal/non-metal-compounds="other-mixed-metal/non-metal-oxoanionic-compounds"

Other mixed metal/non-metal oxoanionic compounds

drugs:mixed-metal/non-metal-compounds="post-transition-metal-organides"

Post-transition metal organides

drugs:mixed-metal/non-metal-compounds="post-transition-metal-oxoanionic-compounds"

Post-transition metal oxoanionic compounds

drugs:mixed-metal/non-metal-compounds="post-transition-metal-salts"

Post-transition metal salts

drugs:mixed-metal/non-metal-compounds="transition-metal-organides"

Transition metal organides

drugs:mixed-metal/non-metal-compounds="transition-metal-oxoanionic-compounds"

Transition metal oxoanionic compounds

drugs:mixed-metal/non-metal-compounds="transition-metal-salts"

Transition metal salts

nucleosides,-nucleotides,-and-analogues

drugs:nucleosides,-nucleotides,-and-analogues="2',3'-dideoxy-3'-thionucleoside-monophosphates"

2',3'-dideoxy-3'-thionucleoside monophosphates

drugs:nucleosides,-nucleotides,-and-analogues="2',5'-dideoxyribonucleosides"

2',5'-dideoxyribonucleosides

drugs:nucleosides,-nucleotides,-and-analogues="(3'->5')-dinucleotides-and-analogues"

(3'->5')-dinucleotides and analogues

drugs:nucleosides,-nucleotides,-and-analogues="5'-deoxyribonucleosides"

5'-deoxyribonucleosides

drugs:nucleosides,-nucleotides,-and-analogues="(5'->5')-dinucleotides"

(5'->5')-dinucleotides

drugs:nucleosides,-nucleotides,-and-analogues="benzimidazole-ribonucleosides-and-ribonucleotides"

Benzimidazole ribonucleosides and ribonucleotides

drugs:nucleosides,-nucleotides,-and-analogues="flavin-nucleotides"

Flavin nucleotides

drugs:nucleosides,-nucleotides,-and-analogues="glycinamide-ribonucleotides"

Glycinamide ribonucleotides

drugs:nucleosides,-nucleotides,-and-analogues="imidazole[4,5-c]pyridine-ribonucleosides-and-ribonucleotides"

Imidazole[4,5-c]pyridine ribonucleosides and ribonucleotides

drugs:nucleosides,-nucleotides,-and-analogues="imidazole-ribonucleosides-and-ribonucleotides"

Imidazole ribonucleosides and ribonucleotides

drugs:nucleosides,-nucleotides,-and-analogues="molybdopterin-dinucleotides"

Molybdopterin dinucleotides

drugs:nucleosides,-nucleotides,-and-analogues="nucleoside-and-nucleotide-analogues"

Nucleoside and nucleotide analogues

drugs:nucleosides,-nucleotides,-and-analogues="purine-nucleosides"

Purine nucleosides

drugs:nucleosides,-nucleotides,-and-analogues="pyrazolo[3,4-d]pyrimidine-glycosides"

Pyrazolo[3,4-d]pyrimidine glycosides

drugs:nucleosides,-nucleotides,-and-analogues="pyridine-nucleotides"

Pyridine nucleotides

drugs:nucleosides,-nucleotides,-and-analogues="pyrimidine-nucleosides"

Pyrimidine nucleosides

drugs:nucleosides,-nucleotides,-and-analogues="pyrimidine-nucleotides"

Pyrimidine nucleotides

drugs:nucleosides,-nucleotides,-and-analogues="pyrrolopyrimidine-nucleosides-and-nucleotides"

Pyrrolopyrimidine nucleosides and nucleotides

drugs:nucleosides,-nucleotides,-and-analogues="ribonucleoside-3'-phosphates"

Ribonucleoside 3'-phosphates

drugs:nucleosides,-nucleotides,-and-analogues="triazole-ribonucleosides-and-ribonucleotides"

Triazole ribonucleosides and ribonucleotides

organic-1,3-dipolar-compounds

drugs:organic-1,3-dipolar-compounds="allyl-type-1,3-dipolar-organic-compounds"

Allyl-type 1,3-dipolar organic compounds

organic-acids-and-derivatives

drugs:organic-acids-and-derivatives="boronic-acid-derivatives"

Boronic acid derivatives

drugs:organic-acids-and-derivatives="carboximidic-acids-and-derivatives"

Carboximidic acids and derivatives

drugs:organic-acids-and-derivatives="carboxylic-acids-and-derivatives"

Carboxylic acids and derivatives

drugs:organic-acids-and-derivatives="hydroxy-acids-and-derivatives"

Hydroxy acids and derivatives

drugs:organic-acids-and-derivatives="keto-acids-and-derivatives"

Keto acids and derivatives

drugs:organic-acids-and-derivatives="organic-carbonic-acids-and-derivatives"

Organic carbonic acids and derivatives

drugs:organic-acids-and-derivatives="organic-phosphonic-acids-and-derivatives"

Organic phosphonic acids and derivatives

drugs:organic-acids-and-derivatives="organic-phosphoric-acids-and-derivatives"

Organic phosphoric acids and derivatives

drugs:organic-acids-and-derivatives="organic-sulfonic-acids-and-derivatives"

Organic sulfonic acids and derivatives

drugs:organic-acids-and-derivatives="organic-sulfuric-acids-and-derivatives"

Organic sulfuric acids and derivatives

drugs:organic-acids-and-derivatives="organic-thiophosphoric-acids-and-derivatives"

Organic thiophosphoric acids and derivatives

drugs:organic-acids-and-derivatives="orthocarboxylic-acid-derivatives"

Orthocarboxylic acid derivatives

drugs:organic-acids-and-derivatives="peptidomimetics"

Peptidomimetics

drugs:organic-acids-and-derivatives="thiosulfinic-acid-esters"

Thiosulfinic acid esters

organic-acids

drugs:organic-acids="carboxylic-acids-and-derivatives"

Carboxylic Acids and Derivatives

organic-nitrogen-compounds

drugs:organic-nitrogen-compounds="organonitrogen-compounds"

Organonitrogen compounds

organic-oxygen-compounds

drugs:organic-oxygen-compounds="organic-oxides"

Organic oxides

drugs:organic-oxygen-compounds="organic-oxoanionic-compounds"

Organic oxoanionic compounds

drugs:organic-oxygen-compounds="organooxygen-compounds"

Organooxygen compounds

organic-polymers

drugs:organic-polymers="phosphorothioate-polynucleotides"

Phosphorothioate polynucleotides

drugs:organic-polymers="polypeptides"

Polypeptides

drugs:organic-polymers="polysaccharides"

Polysaccharides

organic-salts

drugs:organic-salts="organic-metal-salts"

Organic metal salts

organohalogen-compounds

drugs:organohalogen-compounds="acyl-halides"

Acyl halides

drugs:organohalogen-compounds="alkyl-halides"

Alkyl halides

drugs:organohalogen-compounds="aryl-halides"

Aryl halides

drugs:organohalogen-compounds="halohydrins"

Halohydrins

drugs:organohalogen-compounds="organochlorides"

Organochlorides

drugs:organohalogen-compounds="organofluorides"

Organofluorides

drugs:organohalogen-compounds="sulfonyl-halides"

Sulfonyl halides

drugs:organohalogen-compounds="vinyl-halides"

Vinyl halides

organoheterocyclic-compounds

drugs:organoheterocyclic-compounds="azaspirodecane-derivatives"

Azaspirodecane derivatives

drugs:organoheterocyclic-compounds="azepanes"

Azepanes

drugs:organoheterocyclic-compounds="azobenzenes"

Azobenzenes

drugs:organoheterocyclic-compounds="azoles"

Azoles

drugs:organoheterocyclic-compounds="azolidines"

Azolidines

drugs:organoheterocyclic-compounds="azolines"

Azolines

drugs:organoheterocyclic-compounds="benzazepines"

Benzazepines

drugs:organoheterocyclic-compounds="benzimidazoles"

Benzimidazoles

drugs:organoheterocyclic-compounds="benzisoxazoles"

Benzisoxazoles

drugs:organoheterocyclic-compounds="benzocycloheptapyridines"

Benzocycloheptapyridines

drugs:organoheterocyclic-compounds="benzodiazepines"

Benzodiazepines

drugs:organoheterocyclic-compounds="benzodioxanes"

Benzodioxanes

drugs:organoheterocyclic-compounds="benzodioxoles"

Benzodioxoles

drugs:organoheterocyclic-compounds="benzofurans"

Benzofurans

drugs:organoheterocyclic-compounds="benzopyrans"

Benzopyrans

drugs:organoheterocyclic-compounds="benzopyrazoles"

Benzopyrazoles

drugs:organoheterocyclic-compounds="benzothiadiazoles"

Benzothiadiazoles

drugs:organoheterocyclic-compounds="benzothiazepines"

Benzothiazepines

drugs:organoheterocyclic-compounds="benzothiazines"

Benzothiazines

drugs:organoheterocyclic-compounds="benzothiazoles"

Benzothiazoles

drugs:organoheterocyclic-compounds="benzothiepins"

Benzothiepins

drugs:organoheterocyclic-compounds="benzothiophenes"

Benzothiophenes

drugs:organoheterocyclic-compounds="benzothiopyrans"

Benzothiopyrans

drugs:organoheterocyclic-compounds="benzotriazoles"

Benzotriazoles

drugs:organoheterocyclic-compounds="benzoxadiazoles"

Benzoxadiazoles

drugs:organoheterocyclic-compounds="benzoxazepines"

Benzoxazepines

drugs:organoheterocyclic-compounds="benzoxazines"

Benzoxazines

drugs:organoheterocyclic-compounds="benzoxazoles"

Benzoxazoles

drugs:organoheterocyclic-compounds="benzoxepines"

Benzoxepines

drugs:organoheterocyclic-compounds="bi—and-oligothiophenes"

Bi- and oligothiophenes

drugs:organoheterocyclic-compounds="biotin-and-derivatives"

Biotin and derivatives

drugs:organoheterocyclic-compounds="coumarans"

Coumarans

drugs:organoheterocyclic-compounds="cycloheptapyrans"

Cycloheptapyrans

drugs:organoheterocyclic-compounds="cycloheptathiophenes"

Cycloheptathiophenes

drugs:organoheterocyclic-compounds="diazanaphthalenes"

Diazanaphthalenes

drugs:organoheterocyclic-compounds="diazepanes"

Diazepanes

drugs:organoheterocyclic-compounds="diazinanes"

Diazinanes

drugs:organoheterocyclic-compounds="diazines"

Diazines

drugs:organoheterocyclic-compounds="dihydrofurans"

Dihydrofurans

drugs:organoheterocyclic-compounds="dihydroisoquinolines"

Dihydroisoquinolines

drugs:organoheterocyclic-compounds="dihydrothiophenes"

Dihydrothiophenes

drugs:organoheterocyclic-compounds="dioxaborolanes"

Dioxaborolanes

drugs:organoheterocyclic-compounds="dioxanes"

Dioxanes

drugs:organoheterocyclic-compounds="dioxolopyrans"

Dioxolopyrans

drugs:organoheterocyclic-compounds="dithianes"

Dithianes

drugs:organoheterocyclic-compounds="dithiolanes"

Dithiolanes

drugs:organoheterocyclic-compounds="epoxides"

Epoxides

drugs:organoheterocyclic-compounds="furans"

Furans

drugs:organoheterocyclic-compounds="furofurans"

Furofurans

drugs:organoheterocyclic-compounds="furopyrans"

Furopyrans

drugs:organoheterocyclic-compounds="furopyridines"

Furopyridines

drugs:organoheterocyclic-compounds="furopyrroles"

Furopyrroles

drugs:organoheterocyclic-compounds="heteroaromatic-compounds"

Heteroaromatic compounds

drugs:organoheterocyclic-compounds="imidazo[1,5-a]pyrazines"

Imidazo[1,5-a]pyrazines

drugs:organoheterocyclic-compounds="imidazodiazepines"

Imidazodiazepines

drugs:organoheterocyclic-compounds="imidazopyrazines"

Imidazopyrazines

drugs:organoheterocyclic-compounds="imidazopyridines"

Imidazopyridines

drugs:organoheterocyclic-compounds="imidazopyrimidines"

Imidazopyrimidines

drugs:organoheterocyclic-compounds="imidazotetrazines"

Imidazotetrazines

drugs:organoheterocyclic-compounds="imidazothiazoles"

Imidazothiazoles

drugs:organoheterocyclic-compounds="indoles-and-derivatives"

Indoles and derivatives

drugs:organoheterocyclic-compounds="indolizidines"

Indolizidines

drugs:organoheterocyclic-compounds="isocoumarans"

Isocoumarans

drugs:organoheterocyclic-compounds="isoindoles-and-derivatives"

Isoindoles and derivatives

drugs:organoheterocyclic-compounds="isoquinolines-and-derivatives"

Isoquinolines and derivatives

drugs:organoheterocyclic-compounds="isoxazolopyridines"

Isoxazolopyridines

drugs:organoheterocyclic-compounds="lactams"

Lactams

drugs:organoheterocyclic-compounds="lactones"

Lactones

drugs:organoheterocyclic-compounds="metalloheterocyclic-compounds"

Metalloheterocyclic compounds

drugs:organoheterocyclic-compounds="naphthofurans"

Naphthofurans

drugs:organoheterocyclic-compounds="naphthopyrans"

Naphthopyrans

drugs:organoheterocyclic-compounds="oxanes"

Oxanes

drugs:organoheterocyclic-compounds="oxazaphosphinanes"

Oxazaphosphinanes

drugs:organoheterocyclic-compounds="oxazinanes"

Oxazinanes

drugs:organoheterocyclic-compounds="oxepanes"

Oxepanes

drugs:organoheterocyclic-compounds="phenanthrolines"

Phenanthrolines

drugs:organoheterocyclic-compounds="piperazinoazepines"

Piperazinoazepines

drugs:organoheterocyclic-compounds="piperidines"

Piperidines

drugs:organoheterocyclic-compounds="pteridines-and-derivatives"

Pteridines and derivatives

drugs:organoheterocyclic-compounds="pyranodioxins"

Pyranodioxins

drugs:organoheterocyclic-compounds="pyranopyridines"

Pyranopyridines

drugs:organoheterocyclic-compounds="pyranopyrimidines"

Pyranopyrimidines

drugs:organoheterocyclic-compounds="pyrans"

Pyrans

drugs:organoheterocyclic-compounds="pyrazolopyridines"

Pyrazolopyridines

drugs:organoheterocyclic-compounds="pyrazolopyrimidines"

Pyrazolopyrimidines

drugs:organoheterocyclic-compounds="pyrazolotriazines"

Pyrazolotriazines

drugs:organoheterocyclic-compounds="pyridines-and-derivatives"

Pyridines and derivatives

drugs:organoheterocyclic-compounds="pyridopyrimidines"

Pyridopyrimidines

drugs:organoheterocyclic-compounds="pyrroles"

Pyrroles

drugs:organoheterocyclic-compounds="pyrrolidines"

Pyrrolidines

drugs:organoheterocyclic-compounds="pyrrolines"

Pyrrolines

drugs:organoheterocyclic-compounds="pyrrolizines"

Pyrrolizines

drugs:organoheterocyclic-compounds="pyrroloazepines"

Pyrroloazepines

drugs:organoheterocyclic-compounds="pyrrolopyrazines"

Pyrrolopyrazines

drugs:organoheterocyclic-compounds="pyrrolopyrazoles"

Pyrrolopyrazoles

drugs:organoheterocyclic-compounds="pyrrolopyridines"

Pyrrolopyridines

drugs:organoheterocyclic-compounds="pyrrolopyrimidines"

Pyrrolopyrimidines

drugs:organoheterocyclic-compounds="pyrrolotriazines"

Pyrrolotriazines

drugs:organoheterocyclic-compounds="quinolines-and-derivatives"

Quinolines and derivatives

drugs:organoheterocyclic-compounds="quinuclidines"

Quinuclidines

drugs:organoheterocyclic-compounds="selenazoles"

Selenazoles

drugs:organoheterocyclic-compounds="tetrahydrofurans"

Tetrahydrofurans

drugs:organoheterocyclic-compounds="tetrahydroisoquinolines"

Tetrahydroisoquinolines

drugs:organoheterocyclic-compounds="tetrapyrroles-and-derivatives"

Tetrapyrroles and derivatives

drugs:organoheterocyclic-compounds="thiadiazinanes"

Thiadiazinanes

drugs:organoheterocyclic-compounds="thiadiazines"

Thiadiazines

drugs:organoheterocyclic-compounds="thianes"

Thianes

drugs:organoheterocyclic-compounds="thiazepines"

Thiazepines

drugs:organoheterocyclic-compounds="thiazinanes"

Thiazinanes

drugs:organoheterocyclic-compounds="thiazines"

Thiazines

drugs:organoheterocyclic-compounds="thienodiazepines"

Thienodiazepines

drugs:organoheterocyclic-compounds="thienoimidazolidines"

Thienoimidazolidines

drugs:organoheterocyclic-compounds="thienopyridines"

Thienopyridines

drugs:organoheterocyclic-compounds="thienopyrimidines"

Thienopyrimidines

drugs:organoheterocyclic-compounds="thienopyrroles"

Thienopyrroles

drugs:organoheterocyclic-compounds="thienothiazines"

Thienothiazines

drugs:organoheterocyclic-compounds="thiochromanes"

Thiochromanes

drugs:organoheterocyclic-compounds="thiochromenes"

Thiochromenes

drugs:organoheterocyclic-compounds="thiolanes"

Thiolanes

drugs:organoheterocyclic-compounds="thiophenes"

Thiophenes

drugs:organoheterocyclic-compounds="triazinanes"

Triazinanes

drugs:organoheterocyclic-compounds="triazines"

Triazines

drugs:organoheterocyclic-compounds="triazolopyrazines"

Triazolopyrazines

drugs:organoheterocyclic-compounds="triazolopyridines"

Triazolopyridines

drugs:organoheterocyclic-compounds="triazolopyrimidines"

Triazolopyrimidines

drugs:organoheterocyclic-compounds="trioxanes"

Trioxanes

organometallic-compounds

drugs:organometallic-compounds="organometalloid-compounds"

Organometalloid compounds

drugs:organometallic-compounds="organo-post-transition-metal-compounds"

Organo-post-transition metal compounds

organophosphorus-compounds

drugs:organophosphorus-compounds="organic-phosphines-and-derivatives"

Organic phosphines and derivatives

drugs:organophosphorus-compounds="organophosphinic-acids-and-derivatives"

Organophosphinic acids and derivatives

drugs:organophosphorus-compounds="organothiophosphorus-compounds"

Organothiophosphorus compounds

organosulfur-compounds

drugs:organosulfur-compounds="isothioureas"

Isothioureas

drugs:organosulfur-compounds="organic-disulfides"

Organic disulfides

drugs:organosulfur-compounds="sulfonyls"

Sulfonyls

drugs:organosulfur-compounds="sulfoxides"

Sulfoxides

drugs:organosulfur-compounds="thiocarbonyl-compounds"

Thiocarbonyl compounds

drugs:organosulfur-compounds="thioethers"

Thioethers

drugs:organosulfur-compounds="thiols"

Thiols

drugs:organosulfur-compounds="thioureas"

Thioureas

phenylpropanoids-and-polyketides

drugs:phenylpropanoids-and-polyketides="2-arylbenzofuran-flavonoids"

2-arylbenzofuran flavonoids

drugs:phenylpropanoids-and-polyketides="anthracyclines"

Anthracyclines

drugs:phenylpropanoids-and-polyketides="aurone-flavonoids"

Aurone flavonoids

drugs:phenylpropanoids-and-polyketides="cinnamic-acids-and-derivatives"

Cinnamic acids and derivatives

drugs:phenylpropanoids-and-polyketides="cinnamyl-alcohols"

Cinnamyl alcohols

drugs:phenylpropanoids-and-polyketides="coumarins-and-derivatives"

Coumarins and derivatives

drugs:phenylpropanoids-and-polyketides="depsides-and-depsidones"

Depsides and depsidones

drugs:phenylpropanoids-and-polyketides="diarylheptanoids"

Diarylheptanoids

drugs:phenylpropanoids-and-polyketides="flavonoids"

Flavonoids

drugs:phenylpropanoids-and-polyketides="isochromanequinones"

Isochromanequinones

drugs:phenylpropanoids-and-polyketides="isocoumarins-and-derivatives"

Isocoumarins and derivatives

drugs:phenylpropanoids-and-polyketides="isoflavonoids"

Isoflavonoids

drugs:phenylpropanoids-and-polyketides="linear-1,3-diarylpropanoids"

Linear 1,3-diarylpropanoids

drugs:phenylpropanoids-and-polyketides="macrolactams"

Macrolactams

drugs:phenylpropanoids-and-polyketides="macrolide-lactams"

Macrolide lactams

drugs:phenylpropanoids-and-polyketides="macrolides-and-analogues"

Macrolides and analogues

drugs:phenylpropanoids-and-polyketides="neoflavonoids"

Neoflavonoids

drugs:phenylpropanoids-and-polyketides="phenylpropanoic-acids"

Phenylpropanoic acids

drugs:phenylpropanoids-and-polyketides="saxitoxins,-gonyautoxins,-and-derivatives"

Saxitoxins, gonyautoxins, and derivatives

drugs:phenylpropanoids-and-polyketides="stilbenes"

Stilbenes

drugs:phenylpropanoids-and-polyketides="tannins"

Tannins

drugs:phenylpropanoids-and-polyketides="tetracyclines"

Tetracyclines

economical-impact

economical-impact namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Economical impact is a taxonomy to describe the financial impact as positive or negative gain to the tagged information (e.g. data exfiltration loss, a positive gain for an adversary).

loss

A financial impact evaluated as a casuality.

Exclusive flag set which means the values or predicate below must be set exclusively.

economical-impact:loss="none"

No loss

economical-impact:loss="less-than-25k-eur"

Less than 25K EUR

Associated numerical value="10"

economical-impact:loss="less-than-50k-euro"

Less than 50K EUR

Associated numerical value="20"

economical-impact:loss="less-than-100k-euro"

Less than 100K EUR

Associated numerical value="30"

economical-impact:loss="less-than-1M-euro"

Less than 1 million EUR

Associated numerical value="40"

economical-impact:loss="less-than-10M-euro"

Less than 10 million EUR

Associated numerical value="50"

economical-impact:loss="less-than-100M-euro"

Less than 100 million EUR

Associated numerical value="60"

economical-impact:loss="less-than-1B-euro"

Less than 1 billion EUR

Associated numerical value="70"

economical-impact:loss="more-than-1B-euro"

More than 1 billion EUR

Associated numerical value="80"

gain

A financial impact evaluated as a benefit.

Exclusive flag set which means the values or predicate below must be set exclusively.

economical-impact:gain="none"

No gain

economical-impact:gain="less-than-25k-eur"

Less than 25K EUR

Associated numerical value="10"

economical-impact:gain="less-than-50k-euro"

Less than 50K EUR

Associated numerical value="20"

economical-impact:gain="less-than-100k-euro"

Less than 100K EUR

Associated numerical value="30"

economical-impact:gain="less-than-1M-euro"

Less than 1 million EUR

Associated numerical value="40"

economical-impact:gain="less-than-10M-euro"

Less than 10 million EUR

Associated numerical value="50"

economical-impact:gain="less-than-100M-euro"

Less than 100 million EUR

Associated numerical value="60"

economical-impact:gain="less-than-1B-euro"

Less than 1 billion EUR

Associated numerical value="70"

economical-impact:gain="more-than-1B-euro"

More than 1 billion EUR

Associated numerical value="80"

ecsirt

ecsirt namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Incident Classification by the ecsirt.net version mkVI of 31 March 2015 enriched with IntelMQ taxonomy-type mapping.

abusive-content

Abusive Content.

ecsirt:abusive-content="spam"

spam

Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content.

ecsirt:abusive-content="harmful-speech"

Harmful Speech

Discreditation or discrimination of somebody e.g. cyber stalking, racism and threats against one or more individuals).

ecsirt:abusive-content="violence"

Child/Sexual/Violence/...

Child Pornography, glorification of violence, ...

malicious-code

Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.

ecsirt:malicious-code="virus"

Virus

ecsirt:malicious-code="worm"

Worm

ecsirt:malicious-code="trojan"

Trojan

ecsirt:malicious-code="spyware"

Spyware

ecsirt:malicious-code="dialer"

Dialer

ecsirt:malicious-code="rootkit"

Rootkit

ecsirt:malicious-code="malware"

Malware

ecsirt:malicious-code="botnet-drone"

Botnet drone

ecsirt:malicious-code="ransomware"

Ransomware

ecsirt:malicious-code="malware-configuration"

Malware configuration

ecsirt:malicious-code="c&c"

C&C

information-gathering

Information Gathering.

ecsirt:information-gathering="scanner"

Scanning

Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.

ecsirt:information-gathering="sniffing"

Sniffing

Observing and recording of network traffic (wiretapping).

ecsirt:information-gathering="social-engineering"

Social Engineering

Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).

intrusion-attempts

Intrusion Attempts.

ecsirt:intrusion-attempts="ids-alert"

Exploiting of known Vulnerabilities

An attempt to compromise a system or to disrupt any service by exploiting vunerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.)

ecsirt:intrusion-attempts="brute-force"

Login attempts

Multiple login attempts (Guessing / cracking of passwords, brute force).

ecsirt:intrusion-attempts="exploit"

New attack signature

An attempt using an unknown exploit.

intrusions

A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access. Also includes being part of a botnet.

ecsirt:intrusions="privileged-account-compromise"

Privileged Account Compromise

ecsirt:intrusions="unprivileged-account-compromise"

Unprivileged Account Compromise

ecsirt:intrusions="application-compromise"

Application Compromise

ecsirt:intrusions="bot"

Bot

ecsirt:intrusions="defacement"

defacement

ecsirt:intrusions="compromised"

compromised

ecsirt:intrusions="backdoor"

backdoor

availability

By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) – or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.

ecsirt:availability="dos"

DoS

Denial of Service.

ecsirt:availability="ddos"

DDoS

Distributed Denial of Service.

ecsirt:availability="sabotage"

Sabotage

Sabotage.

ecsirt:availability="outage"

Outage (no malice)

Outage (no malice).

information-content-security

Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/software error can also be the cause.

ecsirt:information-content-security="Unauthorised-information-access"

Unauthorised access to information

ecsirt:information-content-security="Unauthorised-information-modification"

Unauthorised modification of information

ecsirt:information-content-security="dropzone"

dropzone

fraud

Fraud.

ecsirt:fraud="unauthorized-use-of-resources"

Unauthorized use of resources

Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).

ecsirt:fraud="copyright"

Copyright

Offering or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).

ecsirt:fraud="masquerade"

Masquerade

Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit

from it.

ecsirt:fraud="phishing"

Phishing

Masquerading as another entity in order to persuade the user to reveal a private credential.

vulnerable

Open resolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus signatures not up-to-date, etc

ecsirt:vulnerable="vulnerable-service"

Open for abuse

other

All incidents which don't fit in one of the given categories should be put into this class. If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised

ecsirt:other="blacklist"

blacklist

ecsirt:other="unknown"

unknown

ecsirt:other="other"

other

test

Meant for testing.

ecsirt:test="test"

Test

enisa

enisa namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The present threat taxonomy is an initial version that has been developed on the basis of available ENISA material. This material has been used as an ENISA-internal structuring aid for information collection and threat consolidation purposes. It emerged in the time period 2012-2015.

physical-attack

Threats of intentional, hostile human actions.

enisa:physical-attack="fraud"

Fraud

Fraud committed by humans.

enisa:physical-attack="fraud-by-employees"

Fraud committed by employees

Fraud committed by employees or others that are in relation with entities, who have access to entities' information and IT assets.

enisa:physical-attack="sabotage"

Sabotage

Intentional actions (non-fulfilment or defective fulfilment of personal duties) aimed to cause disruption or damage to IT assets.

enisa:physical-attack="vandalism"

Vandalism

Act of physically damaging IT assets.

enisa:physical-attack="theft"

Theft (of devices, storage media and documents)

Stealing information or IT assets. Robbery.

enisa:physical-attack="theft-of-mobile-devices"

Theft of mobile devices (smartphones/ tablets)

Taking away another person’s property in the form of mobile devices, for example smartphones, tablets.

enisa:physical-attack="theft-of-fixed-hardware"

Theft of fixed hardware

Taking away another person’s hardware property (except mobile devices), which often contains business-sensitive data.

enisa:physical-attack="theft-of-documents"

Theft of documents

Stealing documents from private/company archives, often for the purpose of re-sale or to achieve personal benefits.

enisa:physical-attack="theft-of-backups"

Theft of backups

Stealing media devices, on which copies of essential information are kept.

enisa:physical-attack="information-leak-or-unauthorised-sharing"

Information leak /sharing

Sharing information with unauthorised entities. Loss of information confidentiality due to intentional human actions (e.g., information leak may occur due to loss of paper copies of confidential information).

enisa:physical-attack="unauthorised-physical-access-or-unauthorised-entry-to-premises"

Unauthorized physical access / Unauthorised entry to premises

Unapproved access to facility.

enisa:physical-attack="coercion-or-extortion-or-corruption"

Coercion, extortion or corruption

Actions following acts of coercion, extortion or corruption.

enisa:physical-attack="damage-from-the-wafare"

Damage from the warfare

Threats of direct impact of warfare activities.

enisa:physical-attack="terrorist-attack"

Terrorist attack

Threats from terrorists.

unintentional-damage

Threats of unintentional human actions or errors.

enisa:unintentional-damage="information-leak-or-sharing-due-to-human-error"

Information leak /sharing due to human error

Information leak / sharing caused by humans, due to their mistakes.

enisa:unintentional-damage="accidental-leaks-or-sharing-of-data-by-employees"

Accidental leaks/sharing of data by employees

Unintentional distribution of private or sensitive data to an unauthorized entity by a staff member.

enisa:unintentional-damage="leaks-of-data-via-mobile-applications"

Leaks of data via mobile applications

Threat of leaking private data (a result of using applications for mobile devices).

enisa:unintentional-damage="leaks-of-data-via-web-applications"

Leaks of data via Web applications

Threat of leaking important information using web applications.

enisa:unintentional-damage="leaks-of-information-transferred-by-network"

Leaks of information transferred by network

Threat of eavesdropping of unsecured network traffic.

enisa:unintentional-damage="erroneous-use-or-administration-of-devices-and-systems"

Erroneous use or administration of devices and systems

Information leak / sharing / damage caused by misuse of IT assets (lack of awareness of application features) or wrong / improper IT assets configuration or management.

enisa:unintentional-damage="loss-of-information-due-to-maintenance-errors-or-operators-errors"

Loss of information due to maintenance errors / operators' errors

Threat of loss of information by incorrectly performed maintenance of devices or systems or other operator activities.

enisa:unintentional-damage="loss-of-information-due-to-configuration-or-installation error"

Loss of information due to configuration/ installation error

Threat of loss of information due to errors in installation or system configuration.

enisa:unintentional-damage="increasing-recovery-time"

Increasing recovery time

Threat of unavailability of information due to errors in the use of backup media and increasing information recovery time.

enisa:unintentional-damage="lost-of-information-due-to-user-errors"

Loss of information due to user errors

Threat of unavailability of information or damage to IT assets caused by user errors (using IT infrastructure) or IT software recovery time.

enisa:unintentional-damage="using-information-from-an-unreliable-source"

Using information from an unreliable source

Bad decisions based on unreliable sources of information or unchecked information.

enisa:unintentional-damage="unintentional-change-of-data-in-an-information-system"

Unintentional change of data in an information system

Loss of information integrity due to human error (information system user mistake).

enisa:unintentional-damage="inadequate-design-and-planning-or-improper-adaptation"

Inadequate design and planning or improper adaptation

Threats caused by improper IT assets or business processes design (inadequate specifications of IT products, inadequate usability, insecure interfaces, policy/procedure flows, design errors).

enisa:unintentional-damage="damage-caused-by-a-third-party"

Damage caused by a third party

Threats of damage to IT assets caused by third party.

enisa:unintentional-damage="security-failure-caused-by-third-party"

Security failure caused by third party

Threats of damage to IT assets caused by breach of security regulations by third party.

enisa:unintentional-damage="damages-resulting-from-penetration-testing"

Damages resulting from penetration testing

Threats to information systems caused by conducting IT penetration tests inappropriately.

enisa:unintentional-damage="loss-of-information-in-the-cloud"

Loss of information in the cloud

Threats of losing information or data stored in the cloud.

enisa:unintentional-damage="loss-of-(integrity-of)-sensitive-information"

Loss of (integrity of) sensitive information

Threats of losing information or data, or changing information classified as sensitive.

enisa:unintentional-damage="loss-of-integrity-of-certificates"

Loss of integrity of certificates

Threat of losing integrity of certificates used for authorisation services

enisa:unintentional-damage="loss-of-devices-and-storage-media-and-documents"

Loss of devices, storage media and documents

Threats of unavailability (losing) of IT assets and documents.

enisa:unintentional-damage="loss-of-devices-or-mobile-devices"

Loss of devices/ mobile devices

Threat of losing mobile devices.

enisa:unintentional-damage="loss-of-storage-media"

Loss of storage media

Threat of losing data-storage media.

enisa:unintentional-damage="loss-of-documentation-of-IT-Infrastructure"

Loss of documentation of IT Infrastructure

Threat of losing important documentation.

enisa:unintentional-damage="destruction-of-records"

Destruction of records

Threats of unavailability (destruction) of data and records (information) stored in devices and storage media.

enisa:unintentional-damage="infection-of-removable-media"

Infection of removable media

Threat of loss of important data due to using removable media, web or mail infection.

enisa:unintentional-damage="abuse-of-storage"

Abuse of storage

Threat of loss of records by improper /unauthorised use of storage devices.

disaster

Threats of damage to information assets caused by natural or environmental factors.

enisa:disaster="disaster"

Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy snowfalls, heavy winds)

Large scale natural disasters.

enisa:disaster="fire"

Fire

Threat of fire.

enisa:disaster="pollution-dust-corrosion"

Pollution, dust, corrosion

Threat of disruption of work of IT systems (hardware) due to pollution, dust or corrosion (arising from the air).

enisa:disaster="thunderstrike"

Thunderstrike

Threat of damage to IT hardware caused by thunder strike (overvoltage).

enisa:disaster="water"

Water

Threat of damage to IT hardware caused by water.

enisa:disaster="explosion"

Explosion

Threat of damage to IT hardware caused by explosion.

enisa:disaster="dangerous-radiation-leak"

Dangerous radiation leak

Threat of damage to IT hardware caused by radiation leak.

enisa:disaster="unfavourable-climatic-conditions"

Unfavourable climatic conditions

Threat of disruption of work of IT systems due to climatic conditions that have a negative effect on hardware.

enisa:disaster="loss-of-data-or-accessibility-of-IT-infrastructure-as-a-result-of-heightened-humidity"

Loss of data or accessibility of IT infrastructure as a result of heightened humidity

Threat of disruption of work of IT systems due to high humidity.

enisa:disaster="lost-of-data-or-accessibility-of-IT-infrastructure-as-a-result-of-very-high-temperature"

Lost of data or accessibility of IT infrastructure as a result of very high temperature

Threat of disruption of work of IT systems due to high or low temperature.

enisa:disaster="threats-from-space-or-electromagnetic-storm"

Threats from space / Electromagnetic storm

Threats of the negative impact of solar radiation to satellites and radio wave communication systems - electromagnetic storm.

enisa:disaster="wildlife"

Wildlife

Threat of destruction of IT assets caused by animals: mice, rats, birds.

failures-malfunction

Threat of failure/malfunction of IT supporting infrastructure (i.e. degradation of quality, improper working parameters, jamming). The cause of a failure is mostly an internal issue (e.g.. overload of the power grid in a building).

enisa:failures-malfunction="failure-of-devices-or-systems"

Failure of devices or systems

Threat of failure of IT hardware and/or software assets or its parts.

enisa:failures-malfunction="failure-of-data-media"

Failure of data media

Threat of failure of data media.

enisa:failures-malfunction="hardware-failure"

Hardware failure

Threat of failure of IT hardware.

enisa:failures-malfunction="failure-of-applications-and-services"

Failure of applications and services

Threat of failure of software/applications or services.

enisa:failures-malfunction="failure-of-parts-of-devices-connectors-plug-ins"

Failure of parts of devices (connectors, plug-ins)

Threat of failure of IT equipment or its part.

enisa:failures-malfunction="failure-or-disruption-of-communication-links-communication networks"

Failure or disruption of communication links (communication networks)

Threat of failure or malfunction of communications links.

enisa:failures-malfunction="failure-of-cable-networks"

Failure of cable networks

Threat of failure of communications links due to problems with cable network.

enisa:failures-malfunction="failure-of-wireless-networks"

Failure of wireless networks

Threat of failure of communications links due to problems with wireless networks.

enisa:failures-malfunction="failure-of-mobile-networks"

Failure of mobile networks

Threat of failure of communications links due to problems with mobile networks.

enisa:failures-malfunction="failure-or-disruption-of-main-supply"

Failure or disruption of main supply

Threat of failure or disruption of supply required for information systems.

enisa:failures-malfunction="failure-or-disruption-of-power-supply"

Failure or disruption of power supply

Threat of failure or malfunction of power supply.

enisa:failures-malfunction="failure-of-cooling-infrastructure"

Failure of cooling infrastructure

Threat of failure of IT assets due to improper work of cooling infrastructure.

enisa:failures-malfunction="failure-or-disruption-of-service-providers-supply-chain"

Failure or disruption of service providers (supply chain)

Threat of failure or disruption of third party services required for proper operation of information systems.

enisa:failures-malfunction="malfunction-of-equipment-devices-or-systems"

Malfunction of equipment (devices or systems)

Threat of malfunction of IT hardware and/or software assets or its parts (i.e. improper working parameters, jamming, rebooting).

outages

Threat of complete lack or loss of resources necessary for IT infrastructure. The cause of an outage is mostly an external issue (i.e electricity blackout in the whole city).

enisa:outages="absence-of-personnel"

Absence of personnel

Unavailability of key personnel and their competences.

enisa:outages="strike"

Strike

Unavailability of staff due to a strike (large scale absence of personnel).

enisa:outages="loss-of-support-services"

Loss of support services

Unavailability of support services required for proper operation of the information system.

enisa:outages="internet-outage"

Internet outage

Unavailability of the Internet connection.

enisa:outages="network-outage"

Network outage

Unavailability of communication links.

enisa:outages="outage-of-cable-networks"

Outage of cable networks

Threat of lack of communications links due to problems with cable network.

enisa:outages="Outage-of-short-range-wireless-networks"

Outage of short-range wireless networks

Threat of lack of communications links due to problems with wireless networks (802.11 networks, Bluetooth, NFC etc.).

enisa:outages="outages-of-long-range-wireless-networks"

Outages of long-range wireless networks

Threat of lack of communications links due to problems with mobile networks like cellular network (3G, LTE, GSM etc.) or satellite links.

eavesdropping-interception-hijacking

Threats that alter communication between two parties. These attacks do not have to install additional tools/software on a victim's site.

enisa:eavesdropping-interception-hijacking="war-driving"

War driving

Threat of locating and possibly exploiting connection to the wireless network.

enisa:eavesdropping-interception-hijacking="intercepting-compromising-emissions"

Intercepting compromising emissions

Threat of disclosure of transmitted information using interception and analysis of compromising emission.

enisa:eavesdropping-interception-hijacking="interception-of-information"

Interception of information

Threat of interception of information which is improperly secured in transmission or by improper actions of staff.

enisa:eavesdropping-interception-hijacking="corporate-espionage"

Corporate espionage

Threat of obtaining information secrets by dishonest means.

enisa:eavesdropping-interception-hijacking="nation-state-espionage"

Nation state espionage

Threats of stealing information by nation state espionage (e.g. China based governmental espionage, NSA from USA).

enisa:eavesdropping-interception-hijacking="information-leakage-due-to-unsecured-wi-fi-like-rogue-access-points"

Information leakage due to unsecured Wi-Fi, rogue access points

Threat of obtaining important information by insecure network rogue access points etc.

enisa:eavesdropping-interception-hijacking="interfering-radiation"

Interfering radiation

Threat of failure of IT hardware or transmission connection due to electromagnetic induction or electromagnetic radiation emitted by an outside source.

enisa:eavesdropping-interception-hijacking="replay-of-messages"

Replay of messages

Threat in which valid data transmission is maliciously or fraudulently repeated or delayed.

enisa:eavesdropping-interception-hijacking="network-reconnaissance-network-traffic-manipulation-and-information-gathering"

Network Reconnaissance, Network traffic manipulation and Information gathering

Threat of identifying information about a network to find security weaknesses.

enisa:eavesdropping-interception-hijacking="man-in-the-middle-session-hijacking"

Man in the middle/ Session hijacking

Threats that relay or alter communication between two parties.

legal

Threat of financial or legal penalty or loss of trust of customers and collaborators due to legislation.

enisa:legal="violation-of-rules-and-regulations-breach-of-legislation"

Violation of rules and regulations / Breach of legislation

Threat of financial or legal penalty or loss of trust of customers and collaborators due to violation of law or regulations.

enisa:legal="failure-to-meet-contractual-requirements"

Failure to meet contractual requirements

Threat of financial penalty or loss of trust of customers and collaborators due to failure to meet contractual requirements.

enisa:legal="failure-to-meet-contractual-requirements-by-third-party"

Failure to meet contractual requirements by third party

Threat of financial penalty or loss of trust of customers and collaborators due to a third party's failure to meet contractual requirements

enisa:legal="unauthorized-use-of-IPR-protected-resources"

Unauthorized use of IPR protected resources

Threat of financial or legal penalty or loss of trust of customers and collaborators due to improper/illegal use of IPR protected material (IPR- Intellectual Property Rights.

enisa:legal="illegal-usage-of-file-sharing-services"

Illegal usage of File Sharing services

Threat of financial or legal penalty or loss of trust of customers and collaborators due to improper/illegal use of file sharing services.

enisa:legal="abuse-of-personal-data"

Abuse of personal data

Threat of illegal use of personal data.

enisa:legal="judiciary-decisions-or-court-order"

Judiciary decisions/court order

Threat of financial or legal penalty or loss of trust of customers and collaborators due to judiciary decisions/court order.

nefarious-activity-abuse

Threats of nefarious activities that require use of tools by the attacker. These attacks require installation of additional tools/software or performing additional steps on the victim's IT infrastructure/software.

enisa:nefarious-activity-abuse="identity-theft-identity-fraud-account)"

Identity theft (Identity Fraud/ Account)

Threat of identity theft action.

enisa:nefarious-activity-abuse="credentials-stealing-trojans"

Credentials-stealing trojans

Threat of identity theft action by malware computer programs.

enisa:nefarious-activity-abuse="receiving-unsolicited-e-mail"

Receiving unsolicited E-mail

Threat of receiving unsolicited email which affects information security and efficiency.

enisa:nefarious-activity-abuse="spam"

SPAM

Threat of receiving unsolicited, undesired, or illegal email messages.

enisa:nefarious-activity-abuse="unsolicited-infected-e-mails"

Unsolicited infected e-mails

Threat emanating from unwanted emails that may contain infected attachments or links to malicious / infected web sites.

enisa:nefarious-activity-abuse="denial-of-service"

Denial of service

Threat of service unavailability due to massive requests for services.

enisa:nefarious-activity-abuse="distributed-denial-of-network-service-network-layer-attack"

Distributed denial of network service (DDoS) (network layer attack i.e. Protocol exploitation / Malformed packets / Flooding / Spoofing)

Threat of service unavailability due to a massive number of requests for access to network services from malicious clients.

enisa:nefarious-activity-abuse="distributed-denial-of-network-service-application-layer-attack"

Distributed denial of application service (DDoS) (application layer attack i.e. Ping of Death / XDoS /

WinNuke / HTTP Floods)

Threat of service unavailability due to massive requests sent by multiple malicious clients.

enisa:nefarious-activity-abuse="distributed-denial-of-network-service-amplification-reflection-attack"

Distributed DoS (DDoS) to both network and application services (amplification/reflection methods i.e. NTP/ DNS /…/ BitTorrent)

Threat of creating a massive number of requests, using multiplication/amplification methods.

enisa:nefarious-activity-abuse="malicious-code-software-activity"

Malicious code/ software/ activity

enisa:nefarious-activity-abuse="search-engine-poisoning"

Search Engine Poisoning

Threat of deliberate manipulation of search engine indexes.

enisa:nefarious-activity-abuse="exploitation-of-fake-trust-of-social-media"

Exploitation of fake trust of social media

Threat of malicious activities making use of trusted social media.

enisa:nefarious-activity-abuse="worms-trojans"

Worms/ Trojans

Threat of malware computer programs (trojans/worms).

enisa:nefarious-activity-abuse="rootkits"

Rootkits

Threat of stealthy types of malware software.

enisa:nefarious-activity-abuse="mobile-malware"

Mobile malware

Threat of mobile malware programs.

enisa:nefarious-activity-abuse="infected-trusted-mobile-apps"

Infected trusted mobile apps

Threat of using mobile malware software that is recognised as trusted one.

enisa:nefarious-activity-abuse="elevation-of-privileges"

Elevation of privileges

Threat of exploiting bugs, design flaws or configuration oversights in an operating system or software application to gain elevated access to resources.

enisa:nefarious-activity-abuse="web-application-attacks-injection-attacks-code-injection-SQL-XSS"

Web application attacks / injection attacks (Code injection: SQL, XSS)

Threat of utilizing custom web applications embedded within social media sites, which can lead to installation of malicious code onto computers to be used to gain unauthorized access.

enisa:nefarious-activity-abuse="spyware-or-deceptive-adware"

Spyware or deceptive adware

Threat of using software that aims to gather information about a person or organization without their knowledge.

enisa:nefarious-activity-abuse="viruses"

Viruses

Threat of infection by viruses.

enisa:nefarious-activity-abuse="rogue-security-software-rogueware-scareware"

Rogue security software/ Rogueware / Scareware

Threat of internet fraud or malicious software that mislead users into believing there is a virus on their computer, and manipulates them to pay money for fake removal tool.

enisa:nefarious-activity-abuse="ransomware"

Ransomware

Threat of infection of computer system or device by malware that restricts access to it and demands that the user pay a ransom to remove the restriction.

enisa:nefarious-activity-abuse="exploits-exploit-kits"

Exploits/Exploit Kits

Threat to IT assets due to the use of web available exploits or exploits software.

enisa:nefarious-activity-abuse="social-engineering"

Social Engineering

Threat of social engineering type attacks (target: manipulation of personnel behaviour).

enisa:nefarious-activity-abuse="phishing-attacks"

Phishing attacks

Threat of an email fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy websites.

enisa:nefarious-activity-abuse="spear-phishing-attacks"

Spear phishing attacks

Spear-phishing is a targeted e-mail message that has been crafted to create fake trust and thus lure the victim to unveil some business or personal secrets that can be abused by the adversary.

enisa:nefarious-activity-abuse="abuse-of-information-leakage"

Abuse of Information Leakage

Threat of leaking important information.

enisa:nefarious-activity-abuse="leakage-affecting-mobile-privacy-and-mobile-applications"

Leakage affecting mobile privacy and mobile applications

Threat of leaking important information due to using malware mobile applications.

enisa:nefarious-activity-abuse="leakage-affecting-web-privacy-and-web-applications"

Leakage affecting web privacy and web applications

Threat of leakage important information due to using malware web applications.

enisa:nefarious-activity-abuse="leakage-affecting-network-traffic"

Leakage affecting network traffic

Threat of leaking important information in network traffic.

enisa:nefarious-activity-abuse="leakage-affecting-cloud-computing"

Leakage affecting cloud computing

Threat of leaking important information in cloud computing.

enisa:nefarious-activity-abuse="generation-and-use-of-rogue-certificates"

Generation and use of rogue certificates

Threat of use of rogue certificates.

enisa:nefarious-activity-abuse="loss-of-integrity-of-sensitive-information"

Loss of (integrity of) sensitive information

Threat of loss of sensitive information due to loss of integrity.

enisa:nefarious-activity-abuse="man-in-the-middle-session-hijacking"

Man in the middle / Session hijacking

Threat of attack consisting in the exploitation of the web session control mechanism, which is normally managed by a session token.

enisa:nefarious-activity-abuse="social-engineering-via-signed-malware"

Social Engineering / signed malware

Threat of install fake trust signed software (malware) e.g. fake OS updates.

enisa:nefarious-activity-abuse="fake-SSL-certificates"

Fake SSL certificates

Threat of attack due to malware application signed by a certificate that is typically inherently trusted by an endpoint.

enisa:nefarious-activity-abuse="manipulation-of-hardware-and-software"

Manipulation of hardware and software

Threat of unauthorised manipulation of hardware and software.

enisa:nefarious-activity-abuse="anonymous-proxies"

Anonymous proxies

Threat of unauthorised manipulation by anonymous proxies.

enisa:nefarious-activity-abuse="abuse-of-computing-power-of-cloud-to-launch-attacks-cybercrime-as-a-service)"

Abuse of computing power of cloud to launch attacks (cybercrime as a service)

Threat of using large computing powers to generate attacks on demand.

enisa:nefarious-activity-abuse="abuse-of-vulnerabilities-0-day-vulnerabilities"

Abuse of vulnerabilities, 0-day vulnerabilities

Threat of attacks using 0-day or known IT assets vulnerabilities.

enisa:nefarious-activity-abuse="access-of-web-sites-through-chains-of-HTTP-Proxies-Obfuscation"

Access of web sites through chains of HTTP Proxies (Obfuscation)

Threat of bypassing the security mechanism using HTTP proxies (bypassing the website blacklist).

enisa:nefarious-activity-abuse="access-to-device-software"

Access to device software

Threat of unauthorised manipulation by access to device software.

enisa:nefarious-activity-abuse="alternation-of-software"

Alternation of software

Threat of unauthorized modifications to code or data, attacking its integrity.

enisa:nefarious-activity-abuse="rogue-hardware"

Rogue hardware

Threat of manipulation due to unauthorized access to hardware.

enisa:nefarious-activity-abuse="manipulation-of-information"

Manipulation of information

Threat of intentional data manipulation to mislead information systems or somebody or to cover other nefarious activities (loss of integrity of information).

enisa:nefarious-activity-abuse="repudiation-of-actions"

Repudiation of actions

Threat of intentional data manipulation to repudiate action.

enisa:nefarious-activity-abuse="address-space-hijacking-IP-prefixes"

Address space hijacking (IP prefixes)

Threat of the illegitimate takeover of groups of IP addresses.

enisa:nefarious-activity-abuse="routing-table-manipulation"

Routing table manipulation

Threat of route packets of network to IP addresses other than that was intended via sender by unauthorised manipulation of routing table.

enisa:nefarious-activity-abuse="DNS-poisoning-or-DNS-spoofing-or-DNS-Manipulations"

DNS poisoning / DNS spoofing / DNS Manipulations

Threat of falsification of DNS information.

enisa:nefarious-activity-abuse="falsification-of-record"

Falsification of record

Threat of intentional data manipulation to falsify records.

enisa:nefarious-activity-abuse="autonomous-system-hijacking"

Autonomous System hijacking

Threat of overtaking by the attacker the ownership of a whole autonomous system and its prefixes despite origin validation.

enisa:nefarious-activity-abuse="autonomous-system-manipulation"

Autonomous System manipulation

Threat of manipulation by the attacker of a whole autonomous system in order to perform malicious actions.

enisa:nefarious-activity-abuse="falsification-of-configurations"

Falsification of configurations

Threat of intentional manipulation due to falsification of configurations.

enisa:nefarious-activity-abuse="misuse-of-audit-tools"

Misuse of audit tools

Threat of nefarious actions performed using audit tools (discovery of security weaknesses in information systems)

enisa:nefarious-activity-abuse="misuse-of-information-or-information systems-including-mobile-apps"

Misuse of information/ information systems (including mobile apps)

Threat of nefarious action due to misuse of information / information systems.

enisa:nefarious-activity-abuse="unauthorized-activities"

Unauthorized activities

Threat of nefarious action due to unauthorised activities.

enisa:nefarious-activity-abuse="Unauthorised-use-or-administration-of-devices-and-systems"

Unauthorised use or administration of devices and systems

Threat of nefarious action due to unauthorised use of devices and systems.

enisa:nefarious-activity-abuse="unauthorised-use-of-software"

Unauthorised use of software

Threat of nefarious action due to unauthorised use of software.

enisa:nefarious-activity-abuse="unauthorized-access-to-the-information-systems-or-networks-like-IMPI-Protocol-DNS-Registrar-Hijacking)"

Unauthorized access to the information systems-or-networks (IMPI Protocol / DNS Registrar Hijacking)

Threat of unauthorised access to the information systems / network.

enisa:nefarious-activity-abuse="network-intrusion"

Network Intrusion

Threat of unauthorised access to network.

enisa:nefarious-activity-abuse="unauthorized-changes-of-records"

Unauthorized changes of records

Threat of unauthorised changes of information.

enisa:nefarious-activity-abuse="unauthorized-installation-of-software"

Unauthorized installation of software

Threat of unauthorised installation of software.

enisa:nefarious-activity-abuse="Web-based-attacks-drive-by-download-or-malicious-URLs-or-browser-based-attacks"

Web based attacks (Drive-by download / malicious URLs / Browser based attacks)

Threat of installation of unwanted malware software by misusing websites.

enisa:nefarious-activity-abuse="compromising-confidential-information-like-data-breaches"

Compromising confidential information (data breaches)

Threat of data breach.

enisa:nefarious-activity-abuse="hoax"

Hoax

Threat of loss of IT assets security due to cheating.

enisa:nefarious-activity-abuse="false-rumour-and-or-fake-warning"

False rumour and/or fake warning

Threat of disruption of work due to rumours and/or a fake warning.

enisa:nefarious-activity-abuse="remote-activity-execution"

Remote activity (execution)

Threat of nefarious action by attacker remote activity.

enisa:nefarious-activity-abuse="remote-command-execution"

Remote Command Execution

Threat of nefarious action due to remote command execution.

enisa:nefarious-activity-abuse="remote-access-tool"

Remote Access Tool (RAT)

Threat of infection of software that has a remote administration capabilities allowing an attacker to control the victim’s computer.

enisa:nefarious-activity-abuse="botnets-remote-activity"

Botnets / Remote activity

Threat of penetration by software from malware distribution.

enisa:nefarious-activity-abuse="targeted-attacks"

Targeted attacks (APTs etc.)

Threat of sophisticated, targeted attack which combine many attack techniques.

enisa:nefarious-activity-abuse="mobile-malware-exfiltration"

Mobile malware (exfiltration)

Threat of mobile software that aims to gather information about a person or organization without their knowledge.

enisa:nefarious-activity-abuse="spear-phishing-attacks-targeted"

Spear phishing attacks (targeted)

Threat of attack focused on a single user or department within an organization, coming from someone within the company in a position of trust and requesting information such as login, IDs and passwords.

enisa:nefarious-activity-abuse="installation-of-sophisticated-and-targeted-malware"

Installation of sophisticated and targeted malware

Threat of malware delivered by sophisticated and targeted software.

enisa:nefarious-activity-abuse="watering-hole-attacks"

Watering Hole attacks

Threat of malware residing on the websites which a group often uses.

enisa:nefarious-activity-abuse="failed-business-process"

Failed business process

Threat of damage or loss of IT assets due to improperly executed business process.

enisa:nefarious-activity-abuse="brute-force"

Brute force

Threat of unauthorised access via systematically checking all possible keys or passwords until the correct one is found.

enisa:nefarious-activity-abuse="abuse-of-authorizations"

Abuse of authorizations

Threat of using authorised access to perform illegitimate actions.

estimative-language

estimative-language namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Estimative language to describe quality and credibility of underlying sources, data, and methodologies based Intelligence Community Directive 203 (ICD 203) and JP 2-0, Joint Intelligence

likelihood-probability

Properly expresses and explains uncertainties associated with major analytic judgments: Analytic products should indicate and explain the basis for the uncertainties associated with major analytic judgments, specifically the likelihood of occurrence of an event or development, and the analyst's confidence in the basis for this judgment. Degrees of likelihood encompass a full spectrum from remote to nearly certain. Analysts' confidence in an assessment or judgment may be based on the logic and evidentiary base that underpin it, including the quantity and quality of source material, and their understanding of the topic. Analytic products should note causes of uncertainty (e.g., type, currency, and amount of information, knowledge gaps, and the nature of the issue) and explain how uncertainties affect analysis (e.g., to what degree and how a judgment depends on assumptions). As appropriate, products should identify indicators that would alter the levels of uncertainty for major analytic judgments. Consistency in the terms used and the supporting information and logic advanced is critical to success in expressing uncertainty, regardless of whether likelihood or confidence expressions are used.

Exclusive flag set which means the values or predicate below must be set exclusively.

estimative-language:likelihood-probability="almost-no-chance"

Almost no chance - remote - 01-05%

estimative-language:likelihood-probability="very-unlikely"

Very unlikely - highly improbable - 05-20%

Associated numerical value="5"

estimative-language:likelihood-probability="unlikely"

Unlikely - improbable (improbably) - 20-45%

Associated numerical value="20"

estimative-language:likelihood-probability="roughly-even-chance"

Roughly even change - roughly even odds - 45-55%

Associated numerical value="45"

estimative-language:likelihood-probability="likely"

Likely - probable (probably) - 55-80%

Associated numerical value="55"

estimative-language:likelihood-probability="very-likely"

Very likely - highly probable - 80-95%

Associated numerical value="80"

estimative-language:likelihood-probability="almost-certain"

Almost certain(ly) - nearly certain - 95-99%

Associated numerical value="95"

confidence-in-analytic-judgment

Confidence in a judgment is based on three factors: number of key assumptions required, the credibility and diversity of sourcing in the knowledge base, and the strength of argumentation. Each factor should be assessed independently and then in concert with the other factors to determine the confidence level. Multiple judgments in a product may contain varying levels of confidence. Confidence levels are stated as Low, Moderate, and High.

Exclusive flag set which means the values or predicate below must be set exclusively.

estimative-language:confidence-in-analytic-judgment="low"

Low

Uncorroborated information from good or marginal sources. Many assumptions. Mostly weak logical inferences, minimal methods application. Glaring intelligence gaps exist. Terms or expressions used: 'Possible', 'Could, may, might', 'Cannot judge, unclear.'

estimative-language:confidence-in-analytic-judgment="moderate"

Moderate

Partially corroborated information from good sources. Several assumptions. Mix of strong and weak inferences and methods. Minimum intelligence gaps exist. Terms or expressions used: 'Likely, unlikely', 'Probable, improbable' 'Anticipate, appear'.

Associated numerical value="55"

estimative-language:confidence-in-analytic-judgment="high"

High

Well-corroborated information from proven sources. Minimal assumptions. Strong logical inferences and methods. No or minor intelligence gaps exist. Terms or expressions used: 'Will, will not', 'Almost certainly, remote', 'Highly likely, highly unlikely', 'Expect, assert, affirm'.

Associated numerical value="95"

eu-marketop-and-publicadmin

eu-marketop-and-publicadmin namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Market operators and public administrations that must comply to some notifications requirements under EU NIS directive

critical-infra-operators

eu-marketop-and-publicadmin:critical-infra-operators="transport"

Transport

eu-marketop-and-publicadmin:critical-infra-operators="energy"

Energy

eu-marketop-and-publicadmin:critical-infra-operators="health"

Health

eu-marketop-and-publicadmin:critical-infra-operators="financial"

Financial market operators

eu-marketop-and-publicadmin:critical-infra-operators="banking"

Banking

info-services

eu-marketop-and-publicadmin:info-services="e-commerce"

e-commerce platforms

eu-marketop-and-publicadmin:info-services="internet-payment"

Internet payment

eu-marketop-and-publicadmin:info-services="cloud"

cloud computing

eu-marketop-and-publicadmin:info-services="search-engines"

search engines

eu-marketop-and-publicadmin:info-services="socnet"

social networks

eu-marketop-and-publicadmin:info-services="app-stores"

application stores

public-admin

eu-marketop-and-publicadmin:public-admin="public-admin"

Public Administrations

eu-nis-sector-and-subsectors

eu-nis-sector-and-subsectors namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Sectors, subsectors, and digital services as identified by the NIS Directive

eu-nis-oes

eu-nis-sector-and-subsectors:eu-nis-oes="energy"

Energy

eu-nis-sector-and-subsectors:eu-nis-oes="transport"

Transport

eu-nis-sector-and-subsectors:eu-nis-oes="banking"

Banking

eu-nis-sector-and-subsectors:eu-nis-oes="financial"

Financial Market Infrastructures

eu-nis-sector-and-subsectors:eu-nis-oes="health"

Health

eu-nis-sector-and-subsectors:eu-nis-oes="water"

Drinking Water Supply and Distribution

eu-nis-sector-and-subsectors:eu-nis-oes="digitalinfrastructure"

Digital Infrastructure

eu-nis-oes-energy

eu-nis-sector-and-subsectors:eu-nis-oes-energy="electricity-energy"

Electricity Subsector

eu-nis-sector-and-subsectors:eu-nis-oes-energy="oil-energy"

Oil Subsector

eu-nis-sector-and-subsectors:eu-nis-oes-energy="gas-energy"

Gas Subsector

eu-nis-oes-transport

eu-nis-sector-and-subsectors:eu-nis-oes-transport="air-transport"

Air Transport Subsector

eu-nis-sector-and-subsectors:eu-nis-oes-transport="rail-transport"

Rail Transport Subsector

eu-nis-sector-and-subsectors:eu-nis-oes-transport="water-transport"

Water Transport Subsector

eu-nis-sector-and-subsectors:eu-nis-oes-transport="road-transport"

Road Transport Subsector

eu-nis-oes-banking

eu-nis-oes-financial

eu-nis-oes-health

eu-nis-oes-water

eu-nis-oes-diginfra

eu-nis-dsp

eu-nis-sector-and-subsectors:eu-nis-dsp="market-dsp"

Online Marketplace Digital Service

eu-nis-sector-and-subsectors:eu-nis-dsp="search-dsp"

Online Search Engine Digital Service

eu-nis-sector-and-subsectors:eu-nis-dsp="cloud-dsp"

Cloud Computing Digital Service

euci

euci namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

EU classified information (EUCI) means any information or material designated by a EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.

Exclusive flag set which means the values or predicate below must be set exclusively.

TS-UE/EU-TS

Information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.

euci:TS-UE/EU-TS

TRES SECRET UE/EU TOP SECRET

Information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.

S-UE/EU-S

Information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.

euci:S-UE/EU-S

SECRET UE/EU SECRET

Information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.

C-UE/EU-C

Information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States.

euci:C-UE/EU-C

CONFIDENTIEL UE/EU CONFIDENTIAL

Information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States.

R-UE/EU-R

Information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

euci:R-UE/EU-R

RESTREINT UE/EU RESTRICTED

Information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

europol-event

europol-event namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

This taxonomy was designed to describe the type of events

infected-by-known-malware

The presence of any of the types of malware was detected in a system.

europol-event:infected-by-known-malware

System(s) infected by known malware

The presence of any of the types of malware was detected in a system.

dissemination-malware-email

Malware attached to a message or email message containing link to malicious URL.

europol-event:dissemination-malware-email

Dissemination of malware by email

Malware attached to a message or email message containing link to malicious URL.

hosting-malware-webpage

```
Web page disseminating one or various types of malware.
```

europol-event:hosting-malware-webpage

Hosting of malware on web page

```
Web page disseminating one or various types of malware.
```

c&c-server-hosting

Web page disseminating one or various types of malware.

europol-event:c&c-server-hosting

Hosting of malware on web page

Web page disseminating one or various types of malware.

worm-spreading

System infected by a worm trying to infect other systems.

europol-event:worm-spreading

Replication and spreading of a worm

System infected by a worm trying to infect other systems.

connection-malware-port

System attempting to gain access to a port normally linked to a specific type of malware.

europol-event:connection-malware-port

Connection to (a) suspicious port(s) linked to specific malware

System attempting to gain access to a port normally linked to a specific type of malware.

connection-malware-system

System attempting to gain access to an IP address or URL normally linked to a specific type of malware, e.g. C&C or a distribution page for components linked to a specific botnet.

europol-event:connection-malware-system

Connection to (a) suspicious system(s) linked to specific malware

System attempting to gain access to an IP address or URL normally linked to a specific type of malware, e.g. C&C or a distribution page for components linked to a specific botnet.

flood

Mass mailing of requests (network packets, emails, etc…) from one single source to a specific service, aimed at affecting its normal functioning.

europol-event:flood

Flood of requests

Mass mailing of requests (network packets, emails, etc…) from one single source to a specific

service, aimed at affecting its normal functioning.

exploit-tool-exhausting-resources

One single source using specially designed software to affect the normal functioning of a specific service, by exploiting a vulnerability.

europol-event:exploit-tool-exhausting-resources

Exploit or tool aimed at exhausting resources (network, processing capacity, sessions, etc…)

One single source using specially designed software to affect the normal functioning of a specific service, by exploiting a vulnerability.

packet-flood

Mass mailing of requests (network packets, emails, etc…) from various sources to a specific service, aimed at affecting its normal functioning.

europol-event:packet-flood

Packet flooding

Mass mailing of requests (network packets, emails, etc…) from various sources to a specific service, aimed at affecting its normal functioning.

exploit-framework-exhausting-resources

Various sources using specially designed software to affect the normal functioning of a specific service, by exploiting a vulnerability.

europol-event:exploit-framework-exhausting-resources

Exploit or tool distribution aimed at exhausting resources

Various sources using specially designed software to affect the normal functioning of a specific service, by exploiting a vulnerability.

vandalism

Logical and physical activities which – although they are not aimed at causing damage to information or at preventing its transmission among systems – have this effect.

europol-event:vandalism

Vandalism

Logical and physical activities which – although they are not aimed at causing damage to

information or at preventing its transmission among systems – have this effect.

disruption-data-transmission

Logical and physical activities aimed at causing damage to information or at preventing its transmission among systems.

europol-event:disruption-data-transmission

Intentional disruption of data transmission and processing mechanisms

Logical and physical activities aimed at causing damage to information or at preventing its transmission among systems.

system-probe

Single system scan searching for open ports or services using these ports for responding.

europol-event:system-probe

System probe

Single system scan searching for open ports or services using these ports for responding.

network-scanning

Scanning a network aimed at identifying systems which are active in the same network.

europol-event:network-scanning

Network scanning

Scanning a network aimed at identifying systems which are active in the same network.

dns-zone-transfer

Transfer of a specific DNS zone.

europol-event:dns-zone-transfer

DNS zone transfer

Transfer of a specific DNS zone.

wiretapping

Logical or physical interception of communications.

europol-event:wiretapping

Wiretapping

Logical or physical interception of communications.

dissemination-phishing-emails

Mass emailing aimed at collecting data for phishing purposes with regard to the victims.

europol-event:dissemination-phishing-emails

Dissemination of phishing emails

Mass emailing aimed at collecting data for phishing purposes with regard to the victims.

hosting-phishing-sites

Hosting web sites for phishing purposes.

europol-event:hosting-phishing-sites

Hosting phishing sites

Hosting web sites for phishing purposes.

aggregation-information-phishing-schemes

Collecting data obtained through phishing attacks on web pages, email accounts, etc…

europol-event:aggregation-information-phishing-schemes

Aggregation of information gathered through phishing schemes

Collecting data obtained through phishing attacks on web pages, email accounts, etc…

exploit-attempt

Unsuccessful use of a tool exploiting a specific vulnerability of the system.

europol-event:exploit-attempt

Exploit attempt

Unsuccessful use of a tool exploiting a specific vulnerability of the system.

sql-injection-attempt

Unsuccessful attempt to manipulate or read the information of a database by using the SQL injection technique.

europol-event:sql-injection-attempt

SQL injection attempt

Unsuccessful attempt to manipulate or read the information of a database by using the SQL injection technique.

xss-attempt

Unsuccessful attempts to perform attacks by using cross-site scripting techniques.

europol-event:xss-attempt

XSS attempt

Unsuccessful attempts to perform attacks by using cross-site scripting techniques.

file-inclusion-attempt

Unsuccessful attempt to include files in the system under attack by using file inclusion techniques.

europol-event:file-inclusion-attempt

File inclusion attempt

Unsuccessful attempt to include files in the system under attack by using file inclusion techniques.

brute-force-attempt

Unsuccessful login attempt by using sequential credentials for gaining access to the system.

europol-event:brute-force-attempt

Brute force attempt

Unsuccessful login attempt by using sequential credentials for gaining access to the system.

password-cracking-attempt

Attempt to acquire access credentials by breaking the protective cryptographic keys.

europol-event:password-cracking-attempt

Password cracking attempt

Attempt to acquire access credentials by breaking the protective cryptographic keys.

dictionary-attack-attempt

Unsuccessful login attempt by using system access credentials previously loaded into a dictionary.

europol-event:dictionary-attack-attempt

Dictionary attack attempt

Unsuccessful login attempt by using system access credentials previously loaded into a dictionary.

exploit

Successful use of a tool exploiting a specific vulnerability of the system.

europol-event:exploit

Use of a local or remote exploit

Successful use of a tool exploiting a specific vulnerability of the system.

sql-injection

Manipulation or reading of information contained in a database by using the SQL injection technique.

europol-event:sql-injection

SQL injection

Manipulation or reading of information contained in a database by using the SQL injection technique.

xss

Attacks performed with the use of cross-site scripting techniques.

europol-event:xss

XSS

Attacks performed with the use of cross-site scripting techniques.

file-inclusion

Inclusion of files into a system under attack with the use of file inclusion techniques.

europol-event:file-inclusion

File inclusion

Inclusion of files into a system under attack with the use of file inclusion techniques.

control-system-bypass

Unauthorised access to a system or component by bypassing an access control system in place.

europol-event:control-system-bypass

Control system bypass

Unauthorised access to a system or component by bypassing an access control system in place.

theft-access-credentials

Unauthorised access to a system or component by using stolen access credentials.

europol-event:theft-access-credentials

Theft of access credentials

Unauthorised access to a system or component by using stolen access credentials.

unauthorized-access-system

Unauthorised access to a system or component.

europol-event:unauthorized-access-system

Unauthorised access to a system

Unauthorised access to a system or component.

unauthorized-access-information

Unauthorised access to a set of information.

europol-event:unauthorized-access-information

Unauthorised access to information

Unauthorised access to a set of information.

data-exfiltration

Unauthorised access to and sharing of a specific set of information.

europol-event:data-exfiltration

Data exfiltration

Unauthorised access to and sharing of a specific set of information.

modification-information

Unauthorised changes to a specific set of information.

europol-event:modification-information

Modification of information

Unauthorised changes to a specific set of information.

deletion-information

Unauthorised deleting of a specific set of information.

europol-event:deletion-information

Deletion of information

Unauthorised deleting of a specific set of information.

illegitimate-use-resources

Use of institutional resources for purposes other than those intended.

europol-event:illegitimate-use-resources

Misuse or unauthorised use of resources

Use of institutional resources for purposes other than those intended.

illegitimate-use-name

Using the name of an institution without permission to do so.

europol-event:illegitimate-use-name

Illegitimate use of the name of an institution or third party

Using the name of an institution without permission to do so.

email-flooding

Sending an unusually large quantity of email messages.

europol-event:email-flooding

Email flooding

Sending an unusually large quantity of email messages.

spam

Sending an email message that was unsolicited or unwanted by the recipient.

europol-event:spam

Sending an unsolicited message

Sending an email message that was unsolicited or unwanted by the recipient.

copyrighted-content

Distribution or sharing of content protected by copyright and related rights.

europol-event:copyrighted-content

Distribution or sharing of copyright protected content

Distribution or sharing of content protected by copyright and related rights.

content-forbidden-by-law

Distribution or sharing of illegal content such as child pornography, racism, xenophobia, etc…

europol-event:content-forbidden-by-law

Dissemination of content forbidden by law (publicly prosecuted offences)

Distribution or sharing of illegal content such as child pornography, racism, xenophobia, etc…

unspecified

Other unlisted events.

europol-event:unspecified

Other unspecified event

Other unlisted events.

undetermined

Field aimed at the classification of unprocessed events, which have remained undetermined from the beginning.

europol-event:undetermined

Undetermined

Field aimed at the classification of unprocessed events, which have remained undetermined from the beginning.

europol-incident

europol-incident namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

This taxonomy was designed to describe the type of incidents by class.

malware

europol-incident:malware="infection"

Infection

Infecting one or various systems with a specific type of malware.

europol-incident:malware="distribution"

Distribution

Infecting one or various systems with a specific type of malware.

europol-incident:malware="c&c"

C&C

Infecting one or various systems with a specific type of malware.

europol-incident:malware="undetermined"

Undetermined

availability

europol-incident:availability="dos-ddos"

DoS/DDoS

Disruption of the processing and response capacity of systems and networks in order to render them inoperative.

europol-incident:availability="sabotage"

Sabotage

Premeditated action to damage a system, interrupt a process, change or delete information, etc.

information-gathering

europol-incident:information-gathering="scanning"

Scanning

Active and passive gathering of information on systems or networks.

europol-incident:information-gathering="sniffing"

Sniffing

Unauthorised monitoring and reading of network traffic.

europol-incident:information-gathering="phishing"

Phishing

Attempt to gather information on a user or a system through phishing methods.

intrusion-attempt

europol-incident:intrusion-attempt="exploitation-vulnerability"

Exploitation of vulnerability

Attempt to intrude by exploiting a vulnerability in a system, component or network.

europol-incident:intrusion-attempt="login-attempt"

Login attempt

Attempt to log in to services or authentication / access control mechanisms.

intrusion

europol-incident:intrusion="exploitation-vulnerability"

Exploitation of vulnerability

Actual intrusion by exploiting a vulnerability in the system, component or network.

europol-incident:intrusion="compromising-account"

Compromising an account

Actual intrusion in a system, component or network by compromising a user or administrator account.

information-security

europol-incident:information-security="unauthorized-access"

Unauthorised access

Unauthorised access to a particular set of information

europol-incident:information-security="unauthorized-modification"

Unauthorised modification/deletion

Unauthorised change or elimination of a particular set of information

fraud

europol-incident:fraud="illegitimate-use-resources"

Misuse or unauthorised use of resources

Use of institutional resources for purposes other than those intended.

europol-incident:fraud="illegitimate-use-name"

Illegitimate use of the name of a third party

Use of the name of an institution without permission to do so.

abusive-content

europol-incident:abusive-content="spam"

SPAM

```
Sending SPAM messages.
```

europol-incident:abusive-content="copyright"

Copyright

Distribution and sharing of copyright protected content.

europol-incident:abusive-content="content-forbidden-by-law"

Dissemination of content forbidden by law.

Child pornography, racism and apology of violence.

other

europol-incident:other="other"

Other

```
Other type of unspecified incident
```

event-assessment

event-assessment namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A series of assessment predicates describing the event assessment performed to make judgement(s) under a certain level of uncertainty.

alternative-points-of-view-process

A list of procedures or practices which describe alternative points of view to validate or rate an analysis. The list describes techniques or methods which could reinforce the estimative language in a human analysis and/or challenge the assumptions to reduce the potential bias of the analysis introduced by the analyst(s).

event-assessment:alternative-points-of-view-process="analytic-debates-within-the-organisation"

analytic debates within the organisation

event-assessment:alternative-points-of-view-process="devils-advocates-methodology"

Devil’s advocates methodology

event-assessment:alternative-points-of-view-process="competitive-analysis"

competitive analysis

event-assessment:alternative-points-of-view-process="interdisciplinary-brainstorming"

interdisciplinary brainstorming

event-assessment:alternative-points-of-view-process="intra-office-peer-review"

intra-office peer review

event-assessment:alternative-points-of-view-process="outside-expertise-review"

Outside expertise review

event-classification

event-classification namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Classification of events as seen in tools such as RT/IR, MISP and other

event-class

event-classification:event-class="incident_report"

Incident Report

event-classification:event-class="incident"

Incident

event-classification:event-class="investigation"

Investigation

event-classification:event-class="countermeasure"

Countermeasure

event-classification:event-class="general"

General

event-classification:event-class="exercise"

Exercise

exercise

exercise namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Exercise is a taxonomy to describe if the information is part of one or more cyber or crisis exercise.

cyber-europe

ENISA manages the programme of pan-European exercises CE2018 logonamed Cyber Europe. This is a series of EU-level cyber incident and crisis management exercises for both the public and private sectors from the EU and EFTA Member States. The Cyber Europe exercises are simulations of large-scale cybersecurity incidents that escalate to become cyber crises. The exercises offer opportunities to analyse advanced technical cybersecurity incidents but also to deal with complex business continuity and crisis management situations.

exercise:cyber-europe="2022"

2022

6th pan European cyber crisis exercise: Cyber Europe 2022 (CE2022)

exercise:cyber-europe="2018"

2018

5th pan European cyber crisis exercise, Cyber Europe 2018 (CE2018)

exercise:cyber-europe="2016"

2016

4th pan-European cyber exercise, Cyber Europe 2016

cyber-storm

Cyber Storm, the Department of Homeland Security’s (DHS) biennial exercise series, provides the framework for the most extensive government-sponsored cybersecurity exercise of its kind. Congress mandated the Cyber Storm exercise series to strengthen cyber preparedness in the public and private sectors. Securing cyber space is the DHS Office of Cybersecurity and Communications' top priority.

exercise:cyber-storm="spring-2018"

Spring 2018

The sixth iteration of the Cyber Storm exercise series, Cyber Storm VI, is scheduled for Spring 2018

locked-shields

Locked Shields is the world’s largest and most advanced international technical live-fire cyber defence exercise. This annual scenario-based, real-time network defence exercise, which has been organised by the NATO Cooperative Cyber Defence Centre of Excellence since 2010, focuses on training for security experts who protect national IT systems.

exercise:locked-shields="2017"

2017

Locked Shields 2017

exercise:locked-shields="2018"

2018

Locked Shields 2018

exercise:locked-shields="2019"

2019

Locked Shields 2019

exercise:locked-shields="2020"

2020

Locked Shields 2020

exercise:locked-shields="2021"

2021

Locked Shields 2021

exercise:locked-shields="2022"

2022

Locked Shields 2022

lukex

LÜKEX ist ein Kurzwort für Länderübergreifende Krisenmanagementübung (EXercise) und die Bezeichnung für regelmäßig stattfindende Übungen in der Bundesrepublik Deutschland. Ziel von Lükex ist es, das gemeinsame Management des Bundes und der Länder in nationalen Krisen aufgrund von außergewöhnlichen Gefahren- und Schadenslagen auf strategischer Ebene zu verbessern.

exercise:lukex="2020"

2020

Cyber-Angriff auf die deutsche Stromversorgung

cyber-coalition

Cyber Coalition tests and trains cyber defenders from across the Alliance in their ability to defend NATO and national networks. From defence against malware, through tackling hybrid challenges involving social media, to attacks on mobile devices, the exercise has a challenging, realistic scenario that helps prepare our cyber defenders for real-life cyber challenges. The training includes testing of operational and legal procedures, exchange of information and work with industry and partners.

exercise:cyber-coalition="2017"

2017

NATO Cyber Coalition 2017

exercise:cyber-coalition="2018"

2018

NATO Cyber Coalition 2018

exercise:cyber-coalition="2019"

2019

NATO Cyber Coalition 2019

exercise:cyber-coalition="2020"

2020

NATO Cyber Coalition 2020

exercise:cyber-coalition="2021"

2021

NATO Cyber Coalition 2021

pace

NATO-EU Parallel and Coordinated Exercise. PACE focuses on four key areas, namely situational awareness, effectiveness of our instruments to counter cyber threats at EU level, speed of reaction and appropriate reactivity of our crisis response mechanisms, as well as our capacity to communicate fast and in a coordinated way.

exercise:pace="2017"

2017

PACE17 will focus on four key areas, namely situational awareness, effectiveness of our instruments to counter cyber threats at EU level, speed of reaction and appropriate reactivity of our crisis response mechanisms, as well as our capacity to communicate fast and in a coordinated way. The exercise will be followed by an evaluation phase, to identify lessons learned and improve our toolbox.

exercise:pace="2018"

2018

cyber-sopex

Cyber SOPEx (formerly known as EuroSOPEx) is the first step in a series of ENISA exercises focusing on training the participants on situational awareness, information sharing, understanding roles and responsibilities and utilising related tools, as agreed by the CSIRTs Network

exercise:cyber-sopex="2019"

2019

exercise:cyber-sopex="2018"

2018

exercise:cyber-sopex="2020"

2020

exercise:cyber-sopex="2021"

2021

generic

Generic exercise which are not named.

exercise:generic="comcheck"

Communication check

A communication check exercise which can include digital or non-digital communication.

extended-event

extended-event namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Reasons why an event has been extended.

competitive-analysis

extended-event:competitive-analysis="devil-advocate"

Devil’s advocate

Is a competitive analysis of devil’s advocate type.

extended-event:competitive-analysis="absurd-reasoning"

Absurd reasoning

Is a competitive analysis of absurd reasoning type

extended-event:competitive-analysis="role-playing"

Role playing

Is a competitive analysis of role playing type

extended-event:competitive-analysis="crystal-ball"

Crystal ball

Is a competitive analysis of crystal ball type

extended-analysis

extended-event:extended-analysis="automatic-expansion"

Automatic expansion

This extended event is composed of elements derived from automatic expanxions services

extended-event:extended-analysis="aggressive-pivoting"

Aggressive pivoting

This extended event is composed of elements resulting of a careless pivoting

extended-event:extended-analysis="complementary-analysis"

Complementary analysis

This extended event is composed of elements gathered by a different analyst than the original one

human-readable

This extended event makes a human readable output of a machine or technical report.

chunked-event

This extended event is a part of a large event.

extended-event:chunked-event="time-based"

Time based

is an element of a serie of extended events, split by matter of time

extended-event:chunked-event="counter-based"

Counter based

is an element of a serie of extended events, split by number of elements

update

Original event is deprecated

failure-mode-in-machine-learning

failure-mode-in-machine-learning namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The purpose of this taxonomy is to jointly tabulate both the of these failure modes in a single place. Intentional failures wherein the failure is caused by an active adversary attempting to subvert the system to attain her goals – either to misclassify the result, infer private training data, or to steal the underlying algorithm. Unintentional failures wherein the failure is because an ML system produces a formally correct but completely unsafe outcome.

intentionally-motivated-failures-summary

Intentional failures wherein the failure is caused by an active adversary attempting to subvert the system to attain her goals – either to misclassify the result, infer private training data, or to steal the underlying algorithm.

failure-mode-in-machine-learning:intentionally-motivated-failures-summary="1-perturbation-attack"

Perturbation attack

Attacker modifies the query to get appropriate response. It doesn't violate traditional technological notion of access/authorization.

failure-mode-in-machine-learning:intentionally-motivated-failures-summary="2-poisoning-attack"

Poisoning attack

Attacker contaminates the training phase of ML systems to get intended result. It doesn't violate traditional technological notion of access/authorization.

failure-mode-in-machine-learning:intentionally-motivated-failures-summary="3-model-inversion"

Model Inversion

Attacker recovers the secret features used in the model by through careful queries. It doesn't violate traditional technological notion of access/authorization.

failure-mode-in-machine-learning:intentionally-motivated-failures-summary="4-membership-inference"

Membership Inference

Attacker can infer if a given data record was part of the model's training dataset or not. It doesn't violate traditional technological notion of access/authorization.

failure-mode-in-machine-learning:intentionally-motivated-failures-summary="5-model-stealing"

Model Stealing

Attacker is able to recover the model through carefully-crafted queries. It doesn't violate traditional technological notion of access/authorization.

failure-mode-in-machine-learning:intentionally-motivated-failures-summary="6-reprogramming-ML-system"

Reprogramming ML system

Repurpose the ML system to perform an activity it was not programmed for. It doesn't violate traditional technological notion of access/authorization.

failure-mode-in-machine-learning:intentionally-motivated-failures-summary="7-adversarial-example-in-physical-domain"

Adversarial Example in Physical Domain

Repurpose the ML system to perform an activity it was not programmed for. It doesn't violate traditional technological notion of access/authorization.

failure-mode-in-machine-learning:intentionally-motivated-failures-summary="8-malicious-ML-provider-recovering-training-data"

Malicious ML provider recovering training data

Malicious ML provider can query the model used by customer and recover customer's training data. It does violate traditional technological notion of access/authorization.

failure-mode-in-machine-learning:intentionally-motivated-failures-summary="9-attacking-the-ML-supply-chain"

Attacking the ML supply chain

Attacker compromises the ML models as it is being downloaded for use. It does violate traditional technological notion of access/authorization.

failure-mode-in-machine-learning:intentionally-motivated-failures-summary="10-backdoor-ML"

Backdoor ML

Malicious ML provider backdoors algorithm to activate with a specific trigger. It does violate traditional technological notion of access/authorization.

failure-mode-in-machine-learning:intentionally-motivated-failures-summary="10-exploit-software-dependencies"

Exploit Software Dependencies

Attacker uses traditional software exploits like buffer overflow to confuse/control ML systems. It does violate traditional technological notion of access/authorization.

unintended-failures-summary

Unintentional failures wherein the failure is because an ML system produces a formally correct but completely unsafe outcome.

failure-mode-in-machine-learning:unintended-failures-summary="12-reward-hacking"

Reward Hacking

Reinforcement Learning (RL) systems act in unintended ways because of mismatch between stated reward and true reward

failure-mode-in-machine-learning:unintended-failures-summary="13-side-effects"

Side Effects

RL system disrupts the environment as it tries to attain its goal

failure-mode-in-machine-learning:unintended-failures-summary="14-distributional-shifts"

Distributional shifts

The system is tested in one kind of environment, but is unable to adapt to changes in other kinds of environment

failure-mode-in-machine-learning:unintended-failures-summary="15-natural-adversarial-examples"

Natural Adversarial Examples

Without attacker perturbations, the ML system fails owing to hard negative mining

failure-mode-in-machine-learning:unintended-failures-summary="16-common-corruption"

Common Corruption

The system is not able to handle common corruptions and perturbations such as tilting, zooming, or noisy images

failure-mode-in-machine-learning:unintended-failures-summary="17-incomplete-testing"

Incomplete Testing

The ML system is not tested in the realistic conditions that it is meant to operate in

false-positive

false-positive namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

This taxonomy aims to ballpark the expected amount of false positives.

risk

Risk of having false positives in the tagged value.

Exclusive flag set which means the values or predicate below must be set exclusively.

false-positive:risk="low"

Low

The risk of having false positives in the tagged value is low.

Associated numerical value="75"

false-positive:risk="medium"

Medium

The risk of having false positives in the tagged value is medium.

Associated numerical value="50"

false-positive:risk="high"

High

The risk of having false positives in the tagged value is high.

Associated numerical value="25"

confirmed

Confirmed false positives in the tagged value.

Exclusive flag set which means the values or predicate below must be set exclusively.

false-positive:confirmed="true"

True

The false positive is confirmed.

false-positive:confirmed="false"

False

The flase positive is not confirmed.

Associated numerical value="50"

file-type

file-type namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

List of known file types.

type

file-type:type="peexe"

executable

file-type:type="pedll"

executable

file-type:type="neexe"

executable

file-type:type="nedll"

executable

file-type:type="mz"

executable

file-type:type="msi"

executable

file-type:type="com"

executable

file-type:type="coff"

executable

file-type:type="elf"

executable

file-type:type="krnl"

executable

file-type:type="rpm"

executable

file-type:type="linux"

executable

file-type:type="macho"

executable

file-type:type="elf32"

executable

file-type:type="elf64"

executable

file-type:type="elfso"

executable

file-type:type="peexe32"

executable

file-type:type="peexe64"

executable

file-type:type="assembly"

executable

file-type:type="html"

internet

file-type:type="xml"

internet

file-type:type="flash"

internet

file-type:type="fla"

internet

file-type:type="iecookie"

internet

file-type:type="bittorrent"

internet

file-type:type="email"

internet

file-type:type="outlook"

internet

file-type:type="cap"

internet

file-type:type="symbian"

phone and tablet

file-type:type="palmos"

phone and tablet

file-type:type="wince"

phone and tablet

file-type:type="android"

phone and tablet

file-type:type="iphone"

phone and tablet

file-type:type="jpeg"

image

file-type:type="emf"

image

file-type:type="tiff"

image

file-type:type="gif"

image

file-type:type="png"

image

file-type:type="bmp"

image

file-type:type="gimp"

image

file-type:type="indesign"

image

file-type:type="psd"

image

file-type:type="targa"

image

file-type:type="xws"

image

file-type:type="dib"

image

file-type:type="jng"

image

file-type:type="ico"

image

file-type:type="fpx"

image

file-type:type="eps"

image

file-type:type="svg"

image

file-type:type="ogg"

video and audio

file-type:type="flc"

video and audio

file-type:type="fli"

video and audio

file-type:type="mp3"

video and audio

file-type:type="flac"

video and audio

file-type:type="wav"

video and audio

file-type:type="midi"

video and audio

file-type:type="avi"

video and audio

file-type:type="mpeg"

video and audio

file-type:type="qt"

video and audio

file-type:type="asf"

video and audio

file-type:type="divx"

video and audio

file-type:type="flv"

video and audio

file-type:type="wma"

video and audio

file-type:type="wmv"

video and audio

file-type:type="rm"

video and audio

file-type:type="mov"

video and audio

file-type:type="mp4"

video and audio

file-type:type="3gp"

video and audio

file-type:type="text"

document

file-type:type="pdf"

document

file-type:type="ps"

document

file-type:type="doc"

document

file-type:type="docx"

document

file-type:type="rtf"

document

file-type:type="ppt"

document

file-type:type="pptx"

document

file-type:type="xls"

document

file-type:type="xlsx"

document

file-type:type="odp"

document

file-type:type="ods"

document

file-type:type="odt"

document

file-type:type="hwp"

document

file-type:type="gul"

document

file-type:type="ebook"

document

file-type:type="latex"

document

file-type:type="isoimage"

bundle

file-type:type="zip"

bundle

file-type:type="gzip"

bundle

file-type:type="bzip"

bundle

file-type:type="rzip"

bundle

file-type:type="dzip"

bundle

file-type:type="7zip"

bundle

file-type:type="cab"

bundle

file-type:type="jar"

bundle

file-type:type="rar"

bundle

file-type:type="mscompress"

bundle

file-type:type="ace"

bundle

file-type:type="arc"

bundle

file-type:type="arj"

bundle

file-type:type="asd"

bundle

file-type:type="blackhole"

bundle

file-type:type="kgb"

bundle

file-type:type="xz"

bundle

file-type:type="script"

code

file-type:type="php"

code

file-type:type="python"

code

file-type:type="perl"

code

file-type:type="ruby"

code

file-type:type="c"

code

file-type:type="cpp"

code

file-type:type="java"

code

file-type:type="shell"

code

file-type:type="pascal"

code

file-type:type="awk"

code

file-type:type="dyalog"

code

file-type:type="fortran"

code

file-type:type="java-bytecode"

code

file-type:type="apple"

apple

file-type:type="mac"

apple

file-type:type="applesingle"

apple

file-type:type="appledouble"

apple

file-type:type="machfs"

apple

file-type:type="appleplist"

apple

file-type:type="maclib"

apple

file-type:type="lnk"

miscellaneous

file-type:type="ttf"

miscellaneous

file-type:type="rom"

miscellaneous

file-type:type="data"

miscellaneous

flesch-reading-ease

flesch-reading-ease namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Flesch Reading Ease is a revised system for determining the comprehension difficulty of written material. The scoring of the flesh score can have a maximum of 121.22 and there is no limit on how low a score can be (negative score are valid).

Exclusive flag set which means the values or predicate below must be set exclusively.

score

flesch-reading-ease:score="90-100"

Very Easy

Very easy to read. Easily understood by an average 11-year-old student.

Associated numerical value="100"

flesch-reading-ease:score="80-89"

Easy

Easy to read. Conversational English for consumers.

Associated numerical value="89"

flesch-reading-ease:score="70-79"

Fairly Easy

Fairly easy to read.

Associated numerical value="79"

flesch-reading-ease:score="60-69"

Standard

Plain English. Easily understood by 13- to 15-year-old students.

Associated numerical value="69"

flesch-reading-ease:score="50-59"

Fairly Difficult

Fairly difficult to read.

Associated numerical value="59"

flesch-reading-ease:score="30-49"

Difficult

Difficult to read.

Associated numerical value="49"

flesch-reading-ease:score="0-29"

Very Confusing

Very difficult to read. Best understood by university graduates.

Associated numerical value="29"

fpf

fpf namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Future of Privacy Forum (FPF) [visual guide to practical de-identification](https://fpf.org/2016/04/25/a-visual-guide-to-practical-data-de-identification/) taxonomy is used to evaluate the degree of identifiability of personal data and the types of pseudonymous data, de-identified data and anonymous data. The work of FPF is licensed under a creative commons attribution 4.0 international license.

degrees-of-identifiability

Information containing direct and indirect identifiers.

fpf:degrees-of-identifiability="explicitly-personal"

Explicitly personal

Name, address, phone number, SSN, government-issued ID (e.g., Jane Smith, 123 Main Street, 555-555-5555)

fpf:degrees-of-identifiability="potentially-identifiable"

Potentially identifiable

Unique device ID, license plate, medical record number, cookie, IP address (e.g., MAC address 68:A8:6D:35:65:03)

fpf:degrees-of-identifiability="not-readily-identifiable"

Not readily identifiable

Same as Potentially Identifiable except data are also protected by safeguards and controls (e.g., hashed MAC addresses & legal representations)

pseudonymous-data

Information from which direct identifiers have been eliminated or transformed, but indirect entifiers remain intact.

fpf:pseudonymous-data="key-coded"

Key coded

Clinical or research datasets where only curator retains key (e.g., Jane Smith, diabetes, HgB 15.1 g/dl = Csrk123)

fpf:pseudonymous-data="pseudonymous"

Pseudonymous

Unique, artificial pseudonyms replace direct identifiers (e.g., HIPAA Limited Datasets, John Doe = 5L7T LX619Z) (unique sequence not used anywhere else)

fpf:pseudonymous-data="protected-pseudonymous"

Protected pseudonymous

Same as Pseudonymous, except data are also protected by safeguards and controls

de-identified-data

Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.

fpf:de-identified-data="de-identified"

De-identified

Data are suppressed, generalized, perturbed, swapped, etc. (e.g., GPA: 3.2 = 3.0-3.5, gender: female = gender: male)

fpf:de-identified-data="protected-de-identified"

Protected de-identified

Same as De-Identified, except data are also protected by safeguards and controls

anonymous-data

Direct and indirect identifiers have en removed or manipulated together with mathematical and technical guarantees to prevent re-identification.

fpf:anonymous-data="anonymous"

Anonymous

For example, noise is calibrated to a data set to hide whether an individual is present or not (differential privacy)

fpf:anonymous-data="aggregated-anonymous"

Aggregated anonymous

Very highly aggregated data (e.g., statistical data, census data, or population data that 52.6% of Washington, DC residents are women)

fr-classif

fr-classif namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

French gov information classification system

classifiees

Exclusive flag set which means the values or predicate below must be set exclusively.

fr-classif:classifiees="TRES_SECRET"

TRES SECRET

fr-classif:classifiees="SECRET"

SECRET

non-classifiees

Exclusive flag set which means the values or predicate below must be set exclusively.

fr-classif:non-classifiees="DIFFUSION_RESTREINTE"

DIFFUSION RESTREINTE

fr-classif:non-classifiees="NON-PROTEGE"

NON PROTEGE

special-france

fr-classif:special-france="SPECIAL_FRANCE"

SPECIAL FRANCE

gdpr

gdpr namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Taxonomy related to the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

special-categories

Special categories of personal data, refer to Art. 9 of the GDPR

gdpr:special-categories="racial-or-ethnic-origin"

Racial or ethnic origin

gdpr:special-categories="political-opinions"

Political opinions

gdpr:special-categories="religious-or-philosophical-beliefs"

Religious or philosophical beliefs

gdpr:special-categories="trade-union-membership"

Trade union membership

gdpr:special-categories="genetic-data"

Genetic data

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

gdpr:special-categories="biometric-data"

Biometric data

Biometric data for the purpose of uniquely identifying a natural person. Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

gdpr:special-categories="health"

Health

Data concerning health. Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal

information about his or her health status.

gdpr:special-categories="sex-life-or-sexual-orientation"

Sex life or sexual orientation

Data concerning a natural person's sex life or sexual orientation

gea-nz-activities

gea-nz-activities namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Information needed to track or monitor moments, periods or events that occur over time. This type of information is focused on occurrences that must be tracked for business reasons or represent a specific point in the evolution of 'The Business'.

cases-compliance

Information about an occurrence by a person or organisation that is under official investigation.

gea-nz-activities:cases-compliance="assessment"

Assessment

Detailed information related to performing an assessment, the act of assessing; appraisal; evaluation.

gea-nz-activities:cases-compliance="audit"

Audit

Detailed information related to performing an audit, to make an audit of; examine (accounts, records, etc.) for purposes of verification.

gea-nz-activities:cases-compliance="inspection"

Inspection

Detailed information related to performing an inspection or viewing.

gea-nz-activities:cases-compliance="investigation"

Investigation

Detailed information related to performing an investigation, to search out and examine the particulars of in an attempt to learn the facts about something hidden, unique, or complex,

especially in an attempt to find a motive, cause, or culprit.

gea-nz-activities:cases-compliance="review"

Review

Detailed information related to performing a review, to survey mentally; take a survey of.

cases-proceeding

Information about a case held by an organisation related to interpretation of the law.

gea-nz-activities:cases-proceeding="breach"

Breach

Detailed information related to breaches, such as breach of contract, defamation, the recovering of debts, and family disputes over care arrangements for children, and others.

gea-nz-activities:cases-proceeding="fine"

Fine

Detailed information related to fines, such as parking fine, speeding fine, and others.

gea-nz-activities:cases-proceeding="fraud"

Fraud

Detailed information related to fraud.

gea-nz-activities:cases-proceeding="offence"

Offence

Detailed information related to an offence.

cases-episode

Information focused on individual’s interactions with an agency, organisation or enterprise, which is tacked as a sequence over a period of time.

gea-nz-activities:cases-episode="defect"

Defect

Detailed information related to cases concerning defects, such as time of occurrence, a repeated defect, solution, etc.

gea-nz-activities:cases-episode="emergency"

Emergency

Detailed information related to emergency cases.

gea-nz-activities:cases-episode="error"

Error

Detailed information related to errors, a deviation from accuracy or correctness.

gea-nz-activities:cases-episode="fault"

Fault

Detailed information related to cases concerning faults, a defect or imperfection; flaw; failing.

gea-nz-activities:cases-episode="history"

History

Detailed information related to history, meaning a sequence of events, such as family history.

gea-nz-activities:cases-episode="incident"

Incident

Detailed information related to cases concerning incidents, an individual occurrence or event.

gea-nz-activities:cases-episode="issue"

Issue

Detailed information related to cases concerning issues, a point in question or a matter that is in dispute which needs a decision.

gea-nz-activities:cases-episode="problem"

Problem

Detailed information related to problems, any question or matter involving doubt, uncertainty, or difficulty.

gea-nz-activities:cases-episode="crime"

Crime

Detailed information related to cases concerning crimes, actions or instances of negligence that is deemed injurious to the public welfare or morals or to the interests of the state and that is legally prohibited.

gea-nz-activities:cases-episode="infrigement"

Infrigement

Detailed information related to cases concerning infringements, a breach or infraction, as of a law, right, or obligation; violation; transgression.

cases-commission-of-inquiry

Information relating to inquiries into various issues. Commissions report findings, give advice and make recommendations.

cases-claim

Information about claims.

gea-nz-activities:cases-claim="claim-of-definition"

Claim of Definition

Detailed information related to claims of definition.

gea-nz-activities:cases-claim="claim-of-cause"

Claim of Cause

Detailed information related to claims of cause.

gea-nz-activities:cases-claim="claim-of-value"

Claim of Value

Detailed information related to claims of value.

gea-nz-activities:cases-claim="claim-of-policy"

Claim of Policy

Detailed information related to claims of policy.

gea-nz-activities:cases-claim="claim-of-fact"

Claim of Fact

Detailed information related to claims of fact.

cases-request

Information about requests that need to be tracked.

gea-nz-activities:cases-request="request-for-information"

Request for Information

Detailed information related to requests for information.

gea-nz-activities:cases-request="request-for-proposal"

Request for proposal

Detailed information related to requests for proposals.

gea-nz-activities:cases-request="request-for-quotation"

Request for quotation

Detailed information related to requests for quotation.

gea-nz-activities:cases-request="request-for-tender"

Request for Tender

Detailed information related to requests for tender.

gea-nz-activities:cases-request="request-for-approval"

Request for Approval

Detailed information related to requests for approval.

gea-nz-activities:cases-request="request-for-comments"

Request for Comments

Detailed information related to requests for comments.

gea-nz-activities:cases-request="order"

Order

Information relating to orders and tracking of the orders.

cases-order

Information relating to orders and tracking of the orders.

events-personal

Information around personal events like birth, starting school, getting married, etc.

gea-nz-activities:events-personal="birth"

Birth

Detailed information related to giving birth.

gea-nz-activities:events-personal="starting-school"

Starting School

Detailed information related to starting school.

gea-nz-activities:events-personal="adoption"

Adoption

Detailed information related to adopting a child.

gea-nz-activities:events-personal="marriage"

Marriage

Detailed information related to get married.

gea-nz-activities:events-personal="senior-citizenship"

Senior Citizenship

Detailed information related to becoming a senior citizen.

gea-nz-activities:events-personal="care"

Care

Detailed information related to going into care.

gea-nz-activities:events-personal="death"

Death

Detailed information related to a death.

gea-nz-activities:events-personal="fostering"

Fostering

Detailed information related to fostering a child.

gea-nz-activities:events-personal="enrol-to-vote"

Enrol to Vote

Detailed information related to the event of enrolling to vote and voting.

gea-nz-activities:events-personal="volunteering"

Volunteering

Detailed information related to the event of volunteering for public services.

gea-nz-activities:events-personal="driver’s-licence"

Driver’s Licence

Detailed information related to getting a driver’s licence.

events-crisis

Information about events that describe a personal crisis.

gea-nz-activities:events-crisis="victim-of-a-crime"

Victim of a Crime

Detailed information related to the event of being a victim of a crime.

gea-nz-activities:events-crisis="witness-of-a-crime"

Witness of a Crime

Detailed information related to the event of being a witness of a crime.

gea-nz-activities:events-crisis="health"

Health

Detailed information related to a health event, such as illness and operations.

gea-nz-activities:events-crisis="emergency"

Emergency

Detailed information related to an emergency.

gea-nz-activities:events-crisis="accused"

Accused

Detailed information related to being accused of a crime.

gea-nz-activities:events-crisis="convicted"

Convicted

Detailed information related to being convicted of a crime.

events-social

Information relating to planned or spontaneous occurrences of a social nature that may require a response by an organisation.

gea-nz-activities:events-social="ceremony"

Ceremony

Detailed information related to ceremonies.

gea-nz-activities:events-social="conference"

Conference

Detailed information related to conferences.

gea-nz-activities:events-social="concert"

Concert

Detailed information related to concerts.

gea-nz-activities:events-social="sporting-event"

Spporting Event

Detailed information related to sporting events, an activity involving physical exertion and skill that is governed by a set of rules or customs and often undertaken competitively, often sports.

gea-nz-activities:events-social="protest"

Protest

Detailed information related to protests, an event at which people gather together to show strong disapproval about something.

gea-nz-activities:events-social="festival"

Festival

Detailed information related to festivals.

events-business

Information related to a type of event relating to the business of the organisation.

gea-nz-activities:events-business="seed-capital"

Seed Capital

Detailed information related to seeding a business.

gea-nz-activities:events-business="start-up"

Start-up

Detailed information related to starting up a business.

gea-nz-activities:events-business="hiring"

Hiring

Detailed information related to hiring staff.

gea-nz-activities:events-business="termination-of-employment"

Termination of Employment

Detailed information related to terminating a employment contract.

gea-nz-activities:events-business="merge"

Merge

Detailed information related to merging of two or more companies, generally by offering the stockholders of one company securities in the acquiring company in exchange for the surrender of their stock.

gea-nz-activities:events-business="demerge"

Demerge

Detailed information related to a demerger, the separation of a large company into two or more smaller organizations, particularly as the dissolution of an earlier merger.

gea-nz-activities:events-business="stock-exchange-listing"

Stock Exchange Listing

Detailed information related to listing a company on the stock exchange.

gea-nz-activities:events-business="stock-exchange-delisting"

Stock Exchange Delisting

Detailed information related to de-listing or removing a company from the stock exchange.

gea-nz-activities:events-business="change-name"

Change Name

Detailed information related to changing the name of a company.

gea-nz-activities:events-business="bankruptcy"

Bankruptcy

Detailed information related to a company going bankrupt.

gea-nz-activities:events-business="cease"

Cease

Detailed information related to closing a company.

events-trade

Information about events that hold substantial meaning for an individual but which are tracked by an organisation such as birth, deaths, health condition etc.

gea-nz-activities:events-trade="buying"

Buying

Detailed information related to buying goods or real estates.

gea-nz-activities:events-trade="selling"

Selling

Detailed information related to selling goods or real estates.

gea-nz-activities:events-trade="importing"

Importing

Detailed information related to importing goods.

gea-nz-activities:events-trade="exporting"

Exporting

Detailed information related to exporting goods.

gea-nz-activities:events-trade="renting"

Renting

Detailed information related to renting goods or real estate.

events-travel

Information related to traveling overseas or coming into France.

gea-nz-activities:events-travel="travelling-overseas"

Travelling Overseas

Detailed information related to traveling overseas.

gea-nz-activities:events-travel="extended-stay-in-france"

Extended Stay in France

Detailed information related to an extended stay in France.

events-environmental

Information held by an organisation about environmental activities such as atmospheric pressures, geological formations, rainfall etc.

gea-nz-activities:events-environmental="atmospheric"

Atmospheric

Detailed information related to atmospheric event, such as cyclone, hail, hurricane, lightning, rain, snow, typhoon, wind, pressure.

gea-nz-activities:events-environmental="elemental"

Elemental

Detailed information related to elemental event, such as avalanche, fire, flood, landslide, tsunami, etc.

gea-nz-activities:events-environmental="geological"

Geological

Detailed information related to geological event, such as earthquake, eruption, formation.

gea-nz-activities:events-environmental="seasonal"

Seasonal

Detailed information related to seasonal events.

events-uncontrolled

Information about events that occur spontaneously, but to which the organisation is required to respond.

gea-nz-activities:events-uncontrolled="accident"

Accident

Detailed information related to an accident, such as crash, explosion, implosion, spill, etc.

gea-nz-activities:events-uncontrolled="attack"

Attack

Detailed information related to attacks, such as arson, bombing, coup, kidnapping, biological attack, terrorism, uprising, and threats which lead to an offence.

gea-nz-activities:events-uncontrolled="failure"

Failure

Detailed information related to a failure, such as blackout, nuclear meltdown, etc.

gea-nz-activities:events-uncontrolled="other"

Other

Detailed information related to other uncontrolled events.

events-interaction

Information about activity that describes a relevant process or action undertaken by the enterprise.

gea-nz-activities:events-interaction="channel"

Channel

A channel or mode by which an interaction takes place. For example face-to-face, in-person or by mail etc.

gea-nz-activities:events-interaction="medium"

Medium

The format in which information content is supplied to others, provided internally to the organisation or purchased from an external provider.

gea-nz-activities:events-interaction="interaction-type"

Interaction Type

Actions represent the information about key interactions that occur. Concepts such as Operators Assisted and Self Service are just relationships from parties in their appropriate roles to an action.

services-france-society

Information related to services delivered across France individuals, communities, and businesses.

gea-nz-activities:services-france-society="border-control"

Border Control

Detailed information related to border control services.

gea-nz-activities:services-france-society="culture-and-heritage"

Culture and Heritage

Detailed information related to services to support culture and heritage.

gea-nz-activities:services-france-society="defence"

Defence

Detailed information related to services to support the defence and protection of the nation.

gea-nz-activities:services-france-society="economic-service"

Economic Service

Detailed information related to services to support the economic management of public funds and other resources.

gea-nz-activities:services-france-society="environment"

Environment

Detailed information related to services to support the management of surrounding natural and built environment.

gea-nz-activities:services-france-society="financial-transaction-with-government"

Financial Transaction with Government

Detailed information related to provisioning earned and unearned financial or monetary-like benefits to individuals, groups, or corporations.

gea-nz-activities:services-france-society="international-relationship"

International Relationship

Detailed information related to services around international relationships.

gea-nz-activities:services-france-society="justice"

Justice

Detailed information related to services to provide justice, apply legislation, etc.

gea-nz-activities:services-france-society="france-society"

France Society

Detailed information related to services to assist individuals and organisations.

gea-nz-activities:services-france-society="natural-resources"

Natural Resources

Detailed information related to services to support the sustainability use and management of energy, minerals, land, and water.

gea-nz-activities:services-france-society="open-government"

Open Government

Detailed information related to services around transparency that gives citizens oversight of the government.

gea-nz-activities:services-france-society="regulatory-compliance-and-enforcement"

Regulatory Compliance and Enforcement

Detailed information related to services to monitor and oversight of specific individuals, groups, industries, or communities participating in regulated activities.

gea-nz-activities:services-france-society="science-and-research"

Science and Research

Detailed information related to services to support and promote research and systematic studies.

gea-nz-activities:services-france-society="security"

Security

Detailed information related to services to maintain the safety of New Zealand at all levels of society.

gea-nz-activities:services-france-society="statistical-services"

Statistical Services

Detailed information related to services to provide high quality, objective and responsive statistics

services-inviduals-&-communities

Information related to services delivered specifically to France individuals and communities.

gea-nz-activities:services-inviduals-&-communities="adopting-and-fostering"

Adopting and Fostering

Detailed information related to services to support a person who wants to adopt or foster another person, usually a child.

gea-nz-activities:services-inviduals-&-communities="births-deaths-and-marriages"

Births, Deaths and Marriages

Detailed information related to these life events of France citizens, and residents.

gea-nz-activities:services-inviduals-&-communities="citizenship-and-immigration"

Citizenship and Immigration

Detailed information related to services to assist people wishing to enter France on a permanent or temporary basis

gea-nz-activities:services-inviduals-&-communities="community-support"

Community Support

Detailed information related to services to assist citizens in a particular district or those with common interests and needs.

gea-nz-activities:services-inviduals-&-communities="education-and-training"

Education and Training

Detailed information related to services to support the provisioning of skills and knowledge to citizens and the strategies to make education available to the broadest possible cross-section of the community.

gea-nz-activities:services-inviduals-&-communities="emergency-and-disaster-preparedness"

Emergency and Disaster Preparedness

Detailed information related to services to deal with and avoid both natural and manmade disasters.

gea-nz-activities:services-inviduals-&-communities="information-from-citizens"

Information from Citizens

Detailed information related to services to support avenues through which the government exchange information and explicit knowledge with individuals.

gea-nz-activities:services-inviduals-&-communities="health-care"

Health Care

Detailed information related to services to prevent, diagnose and treat diseases or injuries, to provision health care services and medical research.

gea-nz-activities:services-inviduals-&-communities="passport-travel-and-tourism"

Passport, Travel and Tourism

Detailed information related to services to support France citizens traveling or living overseas, and local and overseas tourists traveling within France.

gea-nz-activities:services-inviduals-&-communities="sport-and-recreation"

Sport and Recreation

Detailed information related to services to support, promote and encourage operating and marinating amenities or facilities for cultural, recreational and sporting activities.

gea-nz-activities:services-inviduals-&-communities="work-and-jobs"

Work and Jobs

Detailed information related to services to support employment, develop careers, and gain professional accreditation for individuals.

services-services-to-business

Information related to services delivered specifically to France businesses.

gea-nz-activities:services-services-to-business="business-development"

Business Development

Detailed information related to services to assist business growth and management, and support advocacy programs and advising on regulations surrounding business activities.

gea-nz-activities:services-services-to-business="business-support"

Business Support

Detailed information related to services to support the private sector, including small business and non-profit organisations assisting businesses to comply with reporting requirements of the government.

gea-nz-activities:services-services-to-business="commercial-sport"

Commercial Sport

Detailed information related to services to cover the commercial aspects of sport when run as a business.

gea-nz-activities:services-services-to-business="employment"

Employment

Detailed information related to services to support the employment growth and working environment.

gea-nz-activities:services-services-to-business="primal-industries"

Primal Industries

Detailed information related to services to support rural and marine industries.

gea-nz-activities:services-services-to-business="tourism"

Tourism

Detailed information related to services to encourage recreational visitors to a region, and support the tourism industry.

gea-nz-activities:services-services-to-business="trade"

Trade

Detailed information related to services to support purchase, sale or exchange of commodities and advising on trade regulations.

services-civic-infrastructure

Information related to services delivering France infrastructure.

gea-nz-activities:services-civic-infrastructure="civic-management"

Civic Management

Detailed information related to services to provision integrated support for town planning and building projects, coordinate of building projects, provide advice on building regulations and guidelines.

gea-nz-activities:services-civic-infrastructure="communications"

Communications

Detailed information related to services to support the growth of industries that enable and facilitate communication and transmission of information.

gea-nz-activities:services-civic-infrastructure="essential-services"

Essential Services

Detailed information related to services to provision essential community services, evaluate land use, town planning, etc.

gea-nz-activities:services-civic-infrastructure="maritime-services"

Maritime Services

Detailed information related to services to negotiate passage for sea transport and maritime jurisdiction, provide advice on regulations and manage maritime infrastructure.

gea-nz-activities:services-civic-infrastructure="public-housing"

Public Housing

Detailed information related to services to supply low cost accommodations, provide advice on guidelines, evaluate the need for public housing, setting construction targets, support on-going maintenance of public houses.

gea-nz-activities:services-civic-infrastructure="regional-development"

Regional Development

Detailed information related to services to support infrastructure projects, extend facilities beyond urban boundaries and support the installation of equipment to enable communications.

gea-nz-activities:services-civic-infrastructure="transport"

Transport

Detailed information related to services to support road, rail and air transportation systems.

services-government-administration

Information related to delivering France government wide operations and support services.

gea-nz-activities:services-government-administration="government-administration-management"

Government Administration Management

Detailed information related to services that involve day-to day management and maintenance of the internal administrative operations.

gea-nz-activities:services-government-administration="government-business-management"

Government Business Management

Detailed information related to services that involve activities associated with the management of how the government conduct its business.

gea-nz-activities:services-government-administration="government-credit-and-insurance"

Government Credit and Insurance

Detailed information related to services that involve the use of government funds to cover the subsidy cost of a direct loan or loan guarantee or to protect/indemnify members of the public from financial losses.

gea-nz-activities:services-government-administration="government-financial-management"

Government Financial Management

Detailed information related to services that involve agency's use of financial information to measure, operate and predict the effectiveness of efficiency of an entity's activities in relation to its objectives.

gea-nz-activities:services-government-administration="government-human-ressource-management"

Government Human Ressource Management

Detailed information related to services that involve all activities associated with the recruitment and management of personnel.

gea-nz-activities:services-government-administration="government-ict-management"

Government ICT Management

Detailed information related to services that involve the coordination of information and technology resources and solutions required to support or provide a service.

gea-nz-activities:services-government-administration="government-information-and-knowledge-management"

Government Information and Knowledge Management

Detailed information related to services that involve the ownership or custody of information and intellectual assets held by the government.

gea-nz-activities:services-government-administration="government-strategy-planning-and-budgeting"

Government Strategy, Planning and Budgeting

Detailed information related to services that involve the government activities of determining strategic direction, identifying and establishing programs, services and processes.

gea-nz-activities:services-government-administration="machinery-of-government"

Machinery of Government

Detailed information related to services that involve executing legislative processes in Houses of Parliament, assemblies or councils.

services-services-from-business

Information related to services delivered by businesses.

gea-nz-activities:services-services-from-business="advertising"

Advertising

Detailed information related to advertising services rendered by advertising establishments primarily undertaking communications to the public, declarations or announcements by all means of diffusion and concerning all kinds of goods or services.

gea-nz-activities:services-services-from-business="business-management"

Business Management

Detailed information related to services to support business management, mainly services rendered by persons or organizations principally with the object of help in the working or management of a commercial undertaking, or help in the management of the business affairs or commercial functions of an industrial or commercial enterprise.

gea-nz-activities:services-services-from-business="insurance"

Insurance

Detailed information related to services rendered in relation to insurance contracts of all kinds, such as services dealing with insurance such as services rendered by agents or brokers engaged in insurance, services rendered to insured, and insurance underwriting services.

gea-nz-activities:services-services-from-business="financial-service"

Finalcial Service

Detailed information related to services rendered in financial and monetary affairs.

gea-nz-activities:services-services-from-business="real-estate-affairs"

Real Estate Affairs

Detailed information related to services of realty administrators of buildings, i.e., services of letting or valuation, or financing.

gea-nz-activities:services-services-from-business="building-construction"

Building-Construction

Detailed information related to services rendered by contractors or subcontractors in the construction or making of permanent buildings, as well as services rendered by persons or organizations engaged in the restoration of objects to their original condition or in their preservation without altering their physical or chemical properties.

gea-nz-activities:services-services-from-business="telecommunication"

Telecommunication

Detailed information related to services allowing at least one person to communicate with another by a sensory means.

gea-nz-activities:services-services-from-business="transportation"

Transportation

Detailed information related to services rendered in transporting people or goods from one place to another (by rail, road, water, air or pipeline) and services necessarily connected with such transport.

gea-nz-activities:services-services-from-business="packaging-and-storage-of-goods"

Packaging and Storage of Goods

Detailed information related to services relating to the storing of goods in a warehouse or other building for their preservation or guarding.

gea-nz-activities:services-services-from-business="travel-arrangement"

Travel Arrangement

Detailed information related to services consisting of information about journeys by tourist agencies, information relating to tariffs, timetables and methods of travel.

gea-nz-activities:services-services-from-business="treatment-of-material"

Treatment of Material

Detailed information related to services not included in other categories, rendered by the mechanical or chemical processing or transformation of objects or inorganic or organic substances and any process involving a change in its essential properties (for example, dyeing a garment), and services of material treatment which may be present during the production of any substance or object other than a building, for example, services which involve cutting, shaping, polishing by abrasion or metal coating.

gea-nz-activities:services-services-from-business="providing-training"

Providing Training

Detailed information related to services rendered by persons or institutions in the development of the mental faculties of persons or animals.

gea-nz-activities:services-services-from-business="entertainment"

Entertainment

Detailed information related to services having the basic aim of the entertainment, amusement or recreation of people.

gea-nz-activities:services-services-from-business="scientific-service"

Scientific Service

Detailed information related to services provided by persons, individually or collectively, in relation to the theoretical and practical aspects of complex fields of activities, such services are provided by members of professions such as chemists, physicists, engineers, computer programmers, etc.

gea-nz-activities:services-services-from-business="providing-food-drink-and-accomodation"

Providing Food, Drinking and Accomodation

Detailed information related to services provided by persons or establishments whose aim is to prepare food and drink for consumption and services provided to obtain bed and board in hotels, boarding houses or other establishments providing temporary accommodation.

gea-nz-activities:services-services-from-business="medical-service"

Medical Service

Detailed information related to medical care, hygienic and beauty care given by persons or establishments to human beings and animals, it also includes services relating to the fields of agriculture, horticulture and forestry.

gea-nz-activities:services-services-from-business="legal-service"

Legal Service

Detailed information related to legal services, security services for the protection of property and individuals, personal and social services rendered by others to meet the needs of individuals.

gea-nz-entities

gea-nz-entities namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Information relating to instances of entities or things.

parties-party

Information dealing with people or organisations.

gea-nz-entities:parties-party="organisation"

Organisation

Information dealing with organisations, particularly where an information asset has no requirement to address either of these party sub-types directly.

gea-nz-entities:parties-party="individual"

Individual

Information dealing with an individual.

parties-qualification

Information which relates to persons or organisations of a qualifying nature.

gea-nz-entities:parties-qualification="competence"

Competence

Detailed information relating to party’s competencies, experience based or professional.

gea-nz-entities:parties-qualification="education"

Education

Detailed information relating to party’s education history, such as higher education, schools, vocations.

gea-nz-entities:parties-qualification="industry"

Industry

Detailed information relating to party’s (mostly of an organisation) specific industry.

gea-nz-entities:parties-qualification="occupation"

Occupation

Detailed information relating to a party’s occupation.

parties-role

Role information which relates to persons or organisations.

gea-nz-entities:parties-role="commerce"

Commerce

Detailed information relating to commercial roles.

gea-nz-entities:parties-role="legal"

Legal

Detailed information relating to legal roles, such as commissioner, counsel, defendant, investigator, offender, source, suspect, witness.

gea-nz-entities:parties-role="of-interest"

Of Interest

Detailed information relating to roles a party plays in any subject of interest.

gea-nz-entities:parties-role="social"

Social

Detailed information relating to social roles.

parties-party-relationship

Information about the relationship between two or more parties.

gea-nz-entities:parties-party-relationship="membership"

Membership

Detailed information relating to membership to groups, forums, etc.

gea-nz-entities:parties-party-relationship="employer"

Employer

Detailed information relating to relationship of an employer towards other parties, such as employee, government, industry.

gea-nz-entities:parties-party-relationship="provider"

Provider

Detailed information relating to relationship as a provider of services towards other parties.

gea-nz-entities:parties-party-relationship="delegation"

Delegation

Detailed information related to the relationship of delegation, both delegator / delegated.

places-address

Detailed information related to an address.

gea-nz-entities:places-address="electronic-address"

Electronic Address

Detailed information around an electronic address.

gea-nz-entities:places-address="physical-address"

Physical Address

Detailed information related to geographic addresses.

places-location-type

Information of a geospatial or geopolitical nature held by an organisation.

gea-nz-entities:places-location-type="geopolitical"

Geopolitical

Detailed information related to geopolitical places, such as council, country, electorate, locality, nation, region, and province.

gea-nz-entities:places-location-type="geospatial"

Geospatial

Detailed information related to geospatial places, such as area, lot, parish, statistical area, suburb, town, village, and zone.

places-address-type

Identifies the types of address.

gea-nz-entities:places-address-type="nz-standard-addresss"

NZ Standard Address

Detailed information relating to standard New Zealand addresses.

gea-nz-entities:places-address-type="po-box"

PO Box

Detailed information relating to PO Box, a numbered box in a post office assigned to a person or organization, where letters for them are kept until called for.

gea-nz-entities:places-address-type="rural-delivery-address"

Rural Delivery Address

Detailed information relating to rural delivery addresses which have no standard NZ format.

gea-nz-entities:places-address-type="ovearseas-address"

Overseas Address

Detailed information relating to addresses in other countries.

gea-nz-entities:places-address-type="location-addresss"

Location Address

Detailed information relating to physical location addresses including coordinates.

places-purpose-of-location

Information about the purpose of a given address or location.

gea-nz-entities:places-purpose-of-location="residency"

Residency

Detailed information relating to home addresses, both current and previous.

gea-nz-entities:places-purpose-of-location="delivery"

Delivery

Detailed information related to delivery addresses.

gea-nz-entities:places-purpose-of-location="billing"

Billing

Detailed information related to billing addresses.

gea-nz-entities:places-purpose-of-location="place-of-birth"

Place of Birth

Detailed information related to the place of birth.

gea-nz-entities:places-purpose-of-location="consultation"

Consultation

Detailed information related to the location of a consultation.

gea-nz-entities:places-purpose-of-location="referral"

Referral

Detailed information related to location of a referral.

gea-nz-entities:places-purpose-of-location="admission"

Admission

Detailed information related to the location of an admission.

gea-nz-entities:places-purpose-of-location="treatment"

Treatment

Detailed information related to the location of a treatment.

gea-nz-entities:places-purpose-of-location="work-place"

Work Place

Detailed information related to the workplace location or address.

gea-nz-entities:places-purpose-of-location="facility-location"

Facility Location

Detailed information related to the location of a facility.

gea-nz-entities:places-purpose-of-location="storage"

Storage

Detailed information related to the location of storage of goods or other items.

gea-nz-entities:places-purpose-of-location="place-of-event"

Place of Event

Detailed information related to the location of an event.

items-application-&-ict-services

Information about application and ICT service assets.

gea-nz-entities:items-application-&-ict-services="corporate-application"

Corporate Application

Detailed information related to corporate applications, such as applications for enterprise resource planning, financial and asset management, HR management, business continuity, etc..

gea-nz-entities:items-application-&-ict-services="common-line-of-business-application"

Common Line of Business Application

Detailed information related to common LoB application, such as applications to manage product and services, marketing, customer and partner relationships, customer accounting, etc.

gea-nz-entities:items-application-&-ict-services="end-user-computing"

End User Computing

Detailed information related to end user computing, such as applications to manage end user devices, end user tools, mobile applications, productivity suits, etc.

gea-nz-entities:items-application-&-ict-services="data-and-information-management"

Data and Information Management

Detailed information related to data and information management ICT services, such as services for interoperability, data governance, quality management, data protection etc.

gea-nz-entities:items-application-&-ict-services="identity-and-accesd-management"

Identity and Access Management

Detailed information related to identity and access management ICT services, such as services for identity governance, identity administration, authentication, authorisation, directory, etc.

gea-nz-entities:items-application-&-ict-services="security-service"

Security Service

Detailed information related to security ICT services, such as encryption, network security; public

key infrastructure, security controls, etc.

gea-nz-entities:items-application-&-ict-services="ict-components-services-and-tools"

ICT Components, Services and Tools

Detailed information related to software and ICT services for operational management and maintenance of applications, ICT components and services.

gea-nz-entities:items-application-&-ict-services="interface-and-integration"

Interface and Integration

Detailed information related to software and ICT services that support how agencies will interface and integrate both internally and externally.

items-ict-infrastructure

Information about man made surroundings that provide setting for organisational activity, such as platforms, networks, facilities, and end user equipment.

gea-nz-entities:items-ict-infrastructure="platform"

Platform

Detailed information related to platforms, such as hardware, platform operating systems, and virtualisation.

gea-nz-entities:items-ict-infrastructure="network"

Network

Detailed information related to networks, such as network types, traffic types, network infrastructure, transmission types, and network protocol layering.

gea-nz-entities:items-ict-infrastructure="facility"

Facility

Detailed information related to facilities, such as facility types, operational controls, facility physical security, and facility infrastructure.

gea-nz-entities:items-ict-infrastructure="end-user-equipment"

End User Equipment

Detailed information related to end user equipment, such as desktop equipment, mobility equipment, user peripherals, embedded technology devices, and equipment operating systems.

items-natural

Information held by organisation which relate to natural resources.

gea-nz-entities:items-natural="air"

Air

Detailed information related to air, such as condition, pollution, health.

gea-nz-entities:items-natural="fauna"

Fauna

Detailed information related to fauna.

gea-nz-entities:items-natural="flora"

Flora

Detailed information related to flora.

gea-nz-entities:items-natural="land"

Land

Detailed information related to land or earth, such as percentage of rocks, soil, mud, pollution, usage, etc.

gea-nz-entities:items-natural="minerals"

Minerals

Detailed information related to minerals.

gea-nz-entities:items-natural="water"

Water

Detailed information related to water, such as ground water, river water, sea water.

gea-nz-entities:items-natural="energy"

Energy

Detailed information related to energy.

items-financial

Information related to financial assistance products.

gea-nz-entities:items-financial="allowance"

Allowance

Detailed information related to allowances.

gea-nz-entities:items-financial="award"

Award

Detailed information related to awards.

gea-nz-entities:items-financial="benefit"

Benefit

Detailed information related to benefits.

gea-nz-entities:items-financial="bonus"

Bonus

Detailed information related to bonuses.

gea-nz-entities:items-financial="compensation"

Compensation

Detail information related to compensations.

gea-nz-entities:items-financial="concession"

Concession

Detailed information related to concessions.

gea-nz-entities:items-financial="grant"

Grant

Detailed information related to grants.

gea-nz-entities:items-financial="pension"

Pension

Detailed information related to pensions.

gea-nz-entities:items-financial="subsidy"

Subsidy

Detailed information related to subsidies.

gea-nz-entities:items-financial="wage"

Wage

Detailed information related to wages.

gea-nz-entities:items-financial="bond"

Bond

Detailed information related to bonds.

gea-nz-entities:items-financial="duty"

Duty

Detailed information related to income from duties.

gea-nz-entities:items-financial="excise"

Excise

Detailed information related to income from internal tax or duty on certain commodities, as liquor or tobacco, levied on their manufacture, sale, or consumption within the country.

gea-nz-entities:items-financial="insurance"

Insurance

Detailed information related to insurance.

gea-nz-entities:items-financial="loan"

Loan

Detailed information related to revenue from loans.

gea-nz-entities:items-financial="tax"

Tax

Detailed information related to revenue from taxes.

items-goods

Information related to goods.

gea-nz-entities:items-goods="chemical"

Chemical

Detailed information relating to chemicals used in industry, science and photography, as well as in agriculture, horticulture and forestry, unprocessed artificial resins, unprocessed plastics, manures, fire extinguishing compositions, tempering and soldering preparations, chemical substances for preserving foodstuffs, tanning substances, adhesives used in industry.

gea-nz-entities:items-goods="paint"

Paint

Detailed information relating to paints, varnishes, lacquers, preservatives against rust and against deterioration of wood, colorants, mordant, raw natural resins, metals in foil and powder form for painters, decorators, printers and artists.

gea-nz-entities:items-goods="bleach"

Bleach

Detailed information relating to bleaching preparations and other substances for laundry use, cleaning, polishing, scouring and abrasive preparations, soaps, perfumery, essential oils, cosmetics, hair lotions, dentifrices.

gea-nz-entities:items-goods="industrial-oil"

Industrial Oil

Detailed information relating to industrial oils and greases, lubricants, dust absorbing, wetting and binding compositions, fuels (including motor spirit) and illuminants, candles and wicks for lighting.

gea-nz-entities:items-goods="pharmaceutical-preparation"

Pharmaceutical Preparation

Detailed information relating to pharmaceutical and veterinary preparations, sanitary preparations for medical purposes, dietetic substances adapted for medical use, food for babies, plasters, materials for dressings, material for stopping teeth, dental wax, disinfectants, preparations for destroying vermin, fungicides, herbicides.

gea-nz-entities:items-goods="common-metal"

Common Metal

Detailed information relating to common metals and their alloys, metal building materials,

transportable buildings of metal, materials of metal for railway tracks, non-electric cables and wires of common metal, ironmongery, small items of metal hardware, pipes and tubes of metal, safes, goods of common metal not included in other classes, ores.

gea-nz-entities:items-goods="machine"

Machine

Detailed information relating to machines and machine tools, motors and engines (except for land vehicles), machine coupling and transmission components (except for land vehicles), agricultural implements other than hand-operated, incubators for eggs.

gea-nz-entities:items-goods="hand-tool"

Hand Tool

Detailed information relating to hand tools and implements (hand-operated), cutlery, side arms, razors.

gea-nz-entities:items-goods="scientific-apparatus-and-instrument"

Scientific Apparatus and Instrument

Detailed information relating to scientific, nautical, surveying, photographic, cinematographic, optical, weighing, measuring, signalling, checking (supervision), life-saving and teaching apparatus and instruments, apparatus and instruments for conducting, switching, transforming, accumulating, regulating or controlling electricity, apparatus for recording, transmission or reproduction of sound or images, magnetic data carriers, recording discs, automatic vending machines and mechanisms for coin-operated apparatus, cash registers, calculating machines, data processing equipment and computers, fire-extinguishing apparatus.

gea-nz-entities:items-goods="medical-apparatus-and-instrument"

Medical Apparatus and Instrument

Detailed information relating to surgical, medical, dental and veterinary apparatus and instruments, artificial limbs, eyes and teeth, orthopaedic articles, suture materials.

gea-nz-entities:items-goods="electrical-apparatus"

Electrical Apparatus

Detailed information relating to apparatus for lighting, heating, steam generating, cooking, refrigerating, drying, ventilating, water supply and sanitary purposes.

gea-nz-entities:items-goods="vehicle"

Vehicle

Detailed information relating to vehicles, apparatus for locomotion by land, air or water.

gea-nz-entities:items-goods="firearm"

Firearm

Detailed information relating to firearms, ammunition and projectiles, explosives, fireworks

gea-nz-entities:items-goods="precious-metal"

Precious Metal

Detailed information relating to precious metals and their alloys and goods in precious metals or coated therewith, not included in other classes, jewellery, precious stones, horologic and chronometrical instruments.

gea-nz-entities:items-goods="musical-instrument"

Musical Instrument

Detailed information relating to musical instruments.

gea-nz-entities:items-goods="paper"

Paper

Detailed information relating to paper, cardboard and goods made from these materials, not included in other classes, printed matter, bookbinding material, photographs, stationery, adhesives for stationery or household purposes, artists' materials, paint brushes, typewriters and office requisites (except furniture), instructional and teaching material (except apparatus), plastic materials for packaging (not included in other classes), printers' type, printing blocks.

gea-nz-entities:items-goods="rubber-good"

Rubber Good

Detailed information relating to rubber, gutta-percha, gum, asbestos, mica and goods made from these materials and not included in other classes, plastics in extruded form for use in manufacture, packing, stopping and insulating materials, flexible pipes, not of metal.

gea-nz-entities:items-goods="leather"

Leather

Detailed information relating to leather and imitations of leather, and goods made of these materials and not included in other classes, animal skins, hides, trunks and traveling bags, umbrellas, parasols and walking sticks, whips, harness and saddlery.

gea-nz-entities:items-goods="building-material"

Building Material

Detailed information relating to Building materials (non-metallic), non-metallic rigid pipes for building, asphalt, pitch and bitumen, non-metallic transportable buildings, monuments, not of metal.

gea-nz-entities:items-goods="furniture"

Furniture

Detailed information relating to furniture, mirrors, picture frames, goods (not included in other categories) of wood, cork, reed, cane, wicker, horn, bone, ivory, whalebone, shell, amber, mother-of-pearl, meerschaum and substitutes for all these materials, or of plastics.

gea-nz-entities:items-goods="household-utensil"

Household Utensil

Detailed information relating to Household or kitchen utensils and containers (not of precious metal or coated therewith), combs and sponges, brushes (except paint brushes), brush-making materials, articles for cleaning purposes, steel wool, unworked or semi-worked glass (except glass used in building), glassware, porcelain and earthenware not included in other classes.

gea-nz-entities:items-goods="rope"

Rope

Detailed information relating to ropes, string, nets, tents, awnings, tarpaulins, sails, sacks and bags (not included in other classes), padding and stuffing materials (except of rubber or plastics), raw fibrous textile materials.

gea-nz-entities:items-goods="yarn"

Yarn

Detailed information relating to yarns and threads, for textile use.

gea-nz-entities:items-goods="textile"

Textile

Detailed information relating to textiles and textile goods not included in other categories, like bed and table covers.

gea-nz-entities:items-goods="clothing"

Clothing

Detailed information relating to clothing, footwear, headgear.

gea-nz-entities:items-goods="lace"

Lace

Detailed information relating to lace and embroidery, ribbons and braid, buttons, hooks and eyes, pins and needles, artificial flowers.

gea-nz-entities:items-goods="carpet"

Carpet

Detailed information relating to carpets, rugs, mats and matting, linoleum and other materials for covering existing floors wall hangings (non-textile).

gea-nz-entities:items-goods="toy"

Toy

Detailed information relating to games and toys, gymnastic and sporting articles not included in other classes, decorations.

gea-nz-entities:items-goods="food"

Food

Detailed information relating to food, such as meat, fish, poultry and game, meat extracts, preserved, dried and cooked fruits and vegetables, jellies, jams, compotes, eggs, milk and milk products, edible oils and fats.

gea-nz-entities:items-goods="liquid-food"

Liquid Food

Detailed information relating to coffee, tea, cocoa, sugar, rice, tapioca, sago, artificial coffee, flour and preparations made from cereals, bread, pastry and confectionery, ices, honey, treacle, yeast, baking-powder, salt, mustard, vinegar, sauces (condiments), spices, ice.

gea-nz-entities:items-goods="agricultural-product"

Agricultural Product

Detailed information relating to agricultural, horticultural and forestry products and grains not included in other classes, live animals, fresh fruits and vegetables, seeds, natural plants and flowers, foodstuffs for animals, malt.

gea-nz-entities:items-goods="beverages"

Beverages

Detailed information relating to beers, mineral and aerated waters and other non-alcoholic drinks,

fruit drinks and fruit juices, syrups and other preparations for making beverages.

gea-nz-entities:items-goods="alcoholic-beverage"

Alcoholic Beverage

Detailed information relating to Alcoholic beverages (except beers).

gea-nz-entities:items-goods="tobacco"

Tobacco

Detailed information relating to tobacco, smokers' articles, matches.

items-regulatory

Information on regulatory products managed by an organisation.

gea-nz-entities:items-regulatory="certificate"

Certificate

Detailed information related to certificates.

gea-nz-entities:items-regulatory="license"

License

Detailed information related to licenses.

gea-nz-entities:items-regulatory="permit"

Permit

Detailed information related to permits.

gea-nz-entities:items-regulatory="registration"

Registration

Detailed information related to registrations.

gea-nz-entities:items-regulatory="declaration"

Declaration

Detailed information related to declarations.

items-urban-infrastructure

Information related to urban infrastructure.

gea-nz-entities:items-urban-infrastructure="water-supply-system"

Water Supply System

Detailed information related to a water supply system. A water supply system or water supply network is a system of engineered hydrologic and hydraulic components which provide water supply.

gea-nz-entities:items-urban-infrastructure="electric-power-system"

Electric Power System

Detailed information related to an electric power supply system. An electric power system is a network of electrical components used to supply, transmit and use electric power.

gea-nz-entities:items-urban-infrastructure="transport-network"

Transport Network

Detailed information related to transport networks.

gea-nz-entities:items-urban-infrastructure="sanitation-system"

Sanitation System

Detailed information related to sanitation systems to provide a hygienic means of promoting health through prevention of human contact with the hazards of wastes as well as the treatment and proper disposal of sewage or wastewater.

gea-nz-entities:items-urban-infrastructure="communication-system"

Communication System

Detailed information related to a communication system.

items-accommodation

Information related to short–term accommodation provided on a commercial basis, excluding long–term accommodation and accommodation that is provided on a non–commercial basis.

items-dwelling-type

Information related to occupied dwelling type is used to monitor trends and developments in housing and institutional dwellings, to plan for the future housing and service needs of the community.

items-artefact

An artefact is an item of value and manifests in a concrete form such as reports, documents, tables, books, instruction manuals, evidence, etc.

items-waste

Information related to the waste used, managed or produced by the organisation.

items-item-usage

Identifies the ways in which an organisation may use an item.

gea-nz-entities:items-item-usage="product"

Product

Information about tangible outputs of processes which an organisation can offer to other parties.

gea-nz-entities:items-item-usage="resource"

Resource

Resources are not kept or assigned to parties except to accomplish an activity within the organisation, typically during an interaction or the supply of products or delivery of services.

items-other-item

Detailed information of other items not categorised within Items.

gea-nz-motivators

gea-nz-motivators namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Information relating to authority or governance.

plans-budget

Information relating to budget direction or processes.

gea-nz-motivators:plans-budget="capital"

Capital

Detailed information relating to capital budget planning.

gea-nz-motivators:plans-budget="operating"

Operating

Detailed information relating to operational budget planning.

plans-strategy

Detailed information relating to strategic management.

gea-nz-motivators:plans-strategy="strategic-directive"

Strategic Directive

Detailed information relating to planning of strategic or organisational directives.

gea-nz-motivators:plans-strategy="strategic-goal"

Strategic Goal

Detailed information relating to strategic and organisational goals, such as key learning, key results, targets, and others.

gea-nz-motivators:plans-strategy="strategic-objective"

Strategic Objective

Detailed information relating to strategic and organisational objectives, such as KPIs.

gea-nz-motivators:plans-strategy="strategic-outcome"

Strategic Outcome

Detailed information relating to strategic business outcomes.

gea-nz-motivators:plans-strategy="road-map"

Road Map

Detailed information relating to strategic business road maps.

gea-nz-motivators:plans-strategy="challenge"

Challenge

Detailed information relating to strategic and organisational challenges.

gea-nz-motivators:plans-strategy="opportunity"

Opportunity

Detailed information relating to strategic and organisational opportunities.

plans-effort

Information relating to the required effort to achieve or fulfil a work related activity.

gea-nz-motivators:plans-effort="activity"

Activity

Detailed information relating to planning of activities.

gea-nz-motivators:plans-effort="campaign"

Campaign

Detailed information relating to planned campaigns.

gea-nz-motivators:plans-effort="care"

Care

Detailed information relating to planning of activities for an individual to achieve an outcome (PDP).

gea-nz-motivators:plans-effort="programme"

Programme

Detailed information relating to programmes plans.

gea-nz-motivators:plans-effort="project"

Project

Detailed information relating to project plans.

gea-nz-motivators:plans-effort="roster"

Roster

Detailed information relating to rosters.

gea-nz-motivators:plans-effort="schedule"

Schedule

Detailed information relating to schedules.

gea-nz-motivators:plans-effort="task"

Task

Detailed information relating to planning of tasks.

plans-measure

Information which tracks the effectiveness in relation to activities managed by the organisation (inputs/outputs) or employee performance.

gea-nz-motivators:plans-measure="input"

Input

Detailed information relating to input measurements.

gea-nz-motivators:plans-measure="output"

Output

Detailed information relating to output measurements.

gea-nz-motivators:plans-measure="performance"

Performance

Detailed information regarding the performance of an individual, group, organization, system or component.

gea-nz-motivators:plans-measure="benefit"

Benefit

Detailed information regarding the benefits of individual, group, organization, system or component.

plans-risk

Information about person(s) or thing(s) which relate to risk management within organisation.

gea-nz-motivators:plans-risk="consequence"

Consequence

Detailed information relating to consequences of a risk.

gea-nz-motivators:plans-risk="hazard"

Hazard

Detailed information relating to risk hazards.

gea-nz-motivators:plans-risk="likelihood"

Likelihood

Detailed information relating to likelihood of a risk.

gea-nz-motivators:plans-risk="mitigation"

Mitigation

Detailed information relating to risk mitigation.

gea-nz-motivators:plans-risk="influence"

Influence

Detailed information relating to influences that can impact the organisation’s operations, strategic goals, outcomes, etc.

gea-nz-motivators:plans-risk="disruption"

Disruption

Detailed information relating to disruptions that can impact the organisation’s operations, objectives, goals, outcomes, etc.

plans-specification

Information dealing with properties and constraints.

gea-nz-motivators:plans-specification="functional-requirement"

Functional Requirement

Detailed information relating to functional requirements.

gea-nz-motivators:plans-specification="non-functional-requirement"

Non-Functional Requirement

Detailed information relating to non-functional requirements.

gea-nz-motivators:plans-specification="design"

Design

Detailed information relating to solution designs.

controls-operational

Information about controls that provide the foundation for administration of an organisation.

gea-nz-motivators:controls-operational="convention"

Convention

Detailed information relating to conventions, which are general agreements about basic principles or procedures.

gea-nz-motivators:controls-operational="guideline"

Guideline

Detailed information relating to guidelines, which are principles put forward to set standards or determine a course of action. For example guidelines on tax reform.

gea-nz-motivators:controls-operational="policy"

Policy

Detailed information relating to policies. A policy is a plan or course of action intended to influence and determine decisions, actions, and other matters.

gea-nz-motivators:controls-operational="principle"

Principle

Detailed information relating to principles, which are accepted rules or actions on conduct.

gea-nz-motivators:controls-operational="standard"

Standard

Detailed information relating to standards, which are accepted or approved examples of something against which people, processes, items are measured.

gea-nz-motivators:controls-operational="procedure"

Procedure

Detailed information relating to procedures. A procedure is a series of steps taken to accomplish an end.

gea-nz-motivators:controls-operational="process"

Process

Detailed information relating to processes. A process is a series of operations performed in the making or treatment of a product.

gea-nz-motivators:controls-operational="capability"

Capability

Detailed information relating to capabilities; capacity to be used, treated, or developed for a specific purpose.

gea-nz-motivators:controls-operational="rule"

Rule

Detailed information relating to rules.

gea-nz-motivators:controls-operational="exception"

Exception

Detailed information around anything excluded from or not in conformance with a general rules, principles, regulations, etc.

gea-nz-motivators:controls-operational="scope-of-use"

Scope of Use

Detailed information around the scope of use of assets.

controls-finance

Information about the financial structures that provide management and control over the economic resources of the organisation.

gea-nz-motivators:controls-finance="financial-asset"

Financial Asset

Detailed information relating to the financial control of assets.

gea-nz-motivators:controls-finance="equity"

Equity

Detailed information relating to the financial control of equities, monetary value of a property or business beyond any amounts owed on it in mortgages, claims, liens, etc.

gea-nz-motivators:controls-finance="expense"

Expense

Detailed information relating to the financial control of expenses. An expense is a cost of something, such as time or labour, necessary for the attainment of a goal.

gea-nz-motivators:controls-finance="fee"

Fee

Detailed information relating to the financial control of fees; a fixed sum charged, as by an institution or by law, for a privilege: a license fee; tuition fees. Also a charge for professional services: a surgeon’s fee.

gea-nz-motivators:controls-finance="income"

Income

Detailed information relating to the financial control of income.

gea-nz-motivators:controls-finance="financial-liability"

Financial Liability

Detailed information relating to financial obligations entered in the balance sheet of the organisation.

gea-nz-motivators:controls-finance="acquisition-method"

Acquisition Method

Detailed information relating to acquisition methods. An acquisition method defines the method by which assets are acquired.

controls-industry

Information about industry practice issued by an industry specific regulation or professional body.

gea-nz-motivators:controls-industry="best-practice"

Best Practice

Detailed information relating to endorsed or recommended industry practices.

gea-nz-motivators:controls-industry="regulation"

Regulation

Detailed information relating to endorsed or recommended industry specific regulations, rules of

behaviour and procedure.

gea-nz-motivators:controls-industry="terminology"

Terminology

Detailed information of defined sets of concepts and related terms, including definitions and usage guidelines, and the industry-specific business context within which they are to be used.

controls-technological

Information about technical constraints.

gea-nz-motivators:controls-technological="enforced-rules"

Enforced Rules

Detailed information relating to enforced rules around chosen or legacy systems, i.e. Windows policies.

gea-nz-motivators:controls-technological="constraints"

Constraints

Detailed information relating to technical constraints imposed by a chosen or legacy technology.

controls-law

Information about controls in the form of legislation (statues, regulations, etc.).

gea-nz-motivators:controls-law="common-law"

Common Law

Detailed information relating to common laws A common law is established by court decisions rather than by statutes enacted by legislatures.

gea-nz-motivators:controls-law="legislative-instrument"

Legislative Instrument

Detailed information relating to legislation, which are laws enacted by a legislative body.

gea-nz-motivators:controls-law="act"

Act

Detailed information relating to Acts.

gea-nz-motivators:controls-law="cabinet-minute"

Cabinet Minute

Detailed information relating to Cabinet minutes.

controls-personal

Information about the constraints an individual places on interactions with the government, or agency.

gea-nz-motivators:controls-personal="personal-directive"

Personal Directive

Detailed information relating to directives of an individual, such as release of personal information, advance care directive.

controls-security

Information about the constraints security places on interactions within and across the government, agencies and 3th parties.

contracts-arrangement

Information relating to contracts, agreements or other arrangements with other agencies, governments, public or private organizations.

gea-nz-motivators:contracts-arrangement="memorandum-of-understanding"

Memorandum of Understanding

Detailed information relating to terms of agreement, not the legal instrument.

gea-nz-motivators:contracts-arrangement="offer"

Offer

Detailed information relating to offers, such as proposals, quotes, and others.

gea-nz-motivators:contracts-arrangement="order"

Order

Detailed information relating to orders, official request to be made, supplied, or served.

gea-nz-motivators:contracts-arrangement="agreement"

Agreement

Detailed information relating to Service level Agreements (SLA), Master Service Agreements (MSA), Statement of Work (SoW), Purchase Agreement (PA), etc.

gea-nz-motivators:contracts-arrangement="request"

Request

Detailed information relating to requests, such as request for information, request for assistance, etc.

gea-nz-motivators:contracts-arrangement="confidentiality"

Confidentiality

Detailed information relating to confidentiality, such as commercial-in-confidence (CIC), non-disclosure, privacy, and other

gea-nz-motivators:contracts-arrangement="employment"

Employment

Detailed information relating to employment contracts.

gea-nz-motivators:contracts-arrangement="service"

Service

Detailed information relating to service contracts.

gea-nz-motivators:contracts-arrangement="supply"

Supply

Detailed information relating to supply contracts.

contracts-rights

Information relating to moral or legal entitlement to have or do something.

gea-nz-motivators:contracts-rights="eligibility"

Eligibility

Detailed information related to eligibilities (fit or proper to be chosen; worthy of choice; desirable).

gea-nz-motivators:contracts-rights="credits"

Credits

Detailed information relating to credit rights like account receivable, e. i. a legally enforceable claim for payment held by a business against its customer/clients for goods supplied and/or services rendered in execution of the customer's order.

gea-nz-motivators:contracts-rights="access-right"

Access Right

Detailed information related to access rights to facilities, services, processes, information, etc.

gea-nz-motivators:contracts-rights="authorisation"

Authorisation

Detailed information related to authorisation, e. i. right to give orders or make decisions.

gea-nz-motivators:contracts-rights="human-right"

Human Right

Detailed information related to human rights.

gea-nz-motivators:contracts-rights="employment-right"

Employment Right

Detailed information related to employment rights. New Zealand has a comprehensive set of employment laws that help keep workplaces fair.

gea-nz-motivators:contracts-rights="property-right"

Property Right

Detailed information related to property rights.

gea-nz-motivators:contracts-rights="consumer-right"

Consumer Right

Detailed information related to consumer rights.

contracts-obligation

Information which is held by an organisation which relates to its obligations.

gea-nz-motivators:contracts-obligation="duty-of-care"

Duty of Care

Detailed information relating to the obligations of duty of care.

gea-nz-motivators:contracts-obligation="fitness-for-purpose"

Fitness for Purpose

Detailed information relating to something that is good enough to do the job it was designed to do.

gea-nz-motivators:contracts-obligation="warranty"

Warranty

Detailed information relating to warranties.

gea-nz-motivators:contracts-obligation="privacy"

Privacy

Detailed information relating to privacy obligations.

gea-nz-motivators:contracts-obligation="truthfulness"

Truthfulness

Detailed information relating to the obligation to be truthful.

gea-nz-motivators:contracts-obligation="enforce-the-law"

Enforce the Law

Detailed information relating to the obligation to enforce laws and regulations.

gea-nz-motivators:contracts-obligation="obey-the-law"

Obey the Law

Detailed information relating to the obligation to obey laws and regulations.

gea-nz-motivators:contracts-obligation="account-payable"

Account Payable

Detailed information related to account payables or billable, i.e. money which an agency owes to vendors for products and services purchased on credit.

gea-nz-motivators:contracts-obligation="enforce-rules"

Enforce Rules

Detailed information relating to the obligation to enforce rules, like organisational rules, educational rules, industrial rules, etc.

gea-nz-motivators:contracts-obligation="obey-rules"

Obey Rules

Detailed information relating to the obligation to obey rules, like organisational rules, educational rules, industrial rules, etc.

contracts-jurisdiction

nformation about political and geographical areas in which an organisation operates.

gea-nz-motivators:contracts-jurisdiction="national"

National

Detailed information relating to national jurisdictions.

gea-nz-motivators:contracts-jurisdiction="international"

International

Detailed information relating to international jurisdictions.

gea-nz-motivators:contracts-jurisdiction="local"

Local

Detailed information relating to local jurisdictions.

gea-nz-motivators:contracts-jurisdiction="political"

Political

Detailed information relating to political jurisdictions.

gea-nz-motivators:contracts-jurisdiction="regional"

Regional

Detailed information relating to regional jurisdictions.

controls-risk-governance

gea-nz-motivators:controls-risk-governance="residual"

Residual

gea-nz-motivators:controls-risk-governance="acceptance"

Acceptance

gea-nz-motivators:controls-risk-governance="analysis"

Analysis

gea-nz-motivators:controls-risk-governance="assessement"

Assessement

gea-nz-motivators:controls-risk-governance="management"

Management

gea-nz-motivators:controls-risk-governance="treatment"

Treatment

gsma-attack-category

gsma-attack-category namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Taxonomy used by GSMA for their information sharing program with telco describing the attack categories

denial-of-service

gsma-attack-category:denial-of-service

(Distributed) Denial of Service

exploit-attack

gsma-attack-category:exploit-attack

Exploit attack

information-gathering

gsma-attack-category:information-gathering

Information gathering

insider-attack

gsma-attack-category:insider-attack

Insider attack

interception-attack

gsma-attack-category:interception-attack

Interception attack

manipulation-attack

gsma-attack-category:manipulation-attack

Manipulation attack

physical-attack

gsma-attack-category:physical-attack

Physical attack

spoofing

gsma-attack-category:spoofing

Spoofing

gsma-fraud

gsma-fraud namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Taxonomy used by GSMA for their information sharing program with telco describing the various aspects of fraud

technical

gsma-fraud:technical="mailbox-hacking"

Mailbox Hacking (CLI Spoofing)

gsma-fraud:technical="imei-reprogramming"

IMEI Reprogramming

gsma-fraud:technical="call-forwarding-fraud"

Call Forwarding Fraud

gsma-fraud:technical="call-conference"

Call Conference / Multi-Party Calls

gsma-fraud:technical="hlr-tampering"

HLR Tampering / Switch Manipulation

gsma-fraud:technical="sim-card-cloning"

SIM Card Cloning

gsma-fraud:technical="false-base-station-attack"

False Base Station Attack

gsma-fraud:technical="spamming"

Spamming (SMS & IP services)

gsma-fraud:technical="phishing-pharming"

Phishing and Pharming

gsma-fraud:technical="mobile-malware"

Mobile Malware

gsma-fraud:technical="fraud-risks-associated-with-voice-over-ip-services"

Fraud Risks associated with Voice over IP Services

gsma-fraud:technical="pbx-hacking"

PBX Hacking

gsma-fraud:technical="fraud-risks-associated-with-m2m-services"

Fraud Risks Associated with M2M Services

gsma-fraud:technical="data-charing-bypass"

Data Charing Bypass

subscription

gsma-fraud:subscription="subscription-fraud"

Subscription Fraud

gsma-fraud:subscription="proxy-fraud"

Proxy Fraud

gsma-fraud:subscription="account-takeover"

Account Takeover

gsma-fraud:subscription="call-selling"

Call Selling

gsma-fraud:subscription="direct-debit-fraud"

Direct Debug Fraud

gsma-fraud:subscription="credit-card-fraud"

Credit Card Fraud (Card Present)

gsma-fraud:subscription="credit-card-not-present-transactions"

Credit Card Not Present Transactions

gsma-fraud:subscription="cheque-fraud"

Cheque Fraud

distribution

gsma-fraud:distribution="dealer-fraud"

Dealer Fraud

gsma-fraud:distribution="false-agent"

False Agent / Remote Activation Fraud

gsma-fraud:distribution="theft-and-handling-stolen-goods"

Theft and Handling Stolen Goods

gsma-fraud:distribution="handset-subsidy-loss"

Handset Subsidy Loss

gsma-fraud:distribution="remote-order-fraud"

Remote Order Fraud

business

gsma-fraud:business="premium-rate"

Premium Rate / Audiotext Services Fraud (PRS)

gsma-fraud:business="roaming-fraud"

Roaming Fraud

gsma-fraud:business="international-revenue-share-fraud"

International Revenue Share Fraud

gsma-fraud:business="inbound-roaming-fraud-risk-to-vpmn"

Inbound Roaming Fraud Risk to VPMN

gsma-fraud:business="interconnect-abuse"

Interconnect Abuse (GSM Gateways)

gsma-fraud:business="refiling"

Refiling

gsma-fraud:business="mobile-to-fixed-network-gateway-abuse"

Mobile to Fixed Network Gateways Abuse

gsma-fraud:business="false-answer-false-ring"

False Answer / False Ring

gsma-fraud:business="social-engineering"

Social Engineering

gsma-fraud:business="internal-fraud"

Internal Fraud

gsma-fraud:business="normal-business-fraud-crime"

Normal Business Fraud and Crime

gsma-fraud:business="brand-name-logo-abuse"

Brand Name / Logo Abuse

gsma-fraud:business="m-commerce-provider-content-fraud"

M-Commerce Provider Content Fraud

gsma-fraud:business="m-commerce-provider-prs-fraud"

M-Commerce Provider PRS Fraud

gsma-fraud:business="content-theft"

Content Theft

gsma-fraud:business="wangiri"

Wangiri

gsma-fraud:business="airtime-reseller-fraud"

Airtime Reseller Fraud

prepaid

gsma-fraud:prepaid="services-fraud"

Prepaid Services Fraud - General

gsma-fraud:prepaid="hlr-profile-manipulation"

HLR Profile Manipulation

gsma-fraud:prepaid="manual-recharging"

Manual Recharging

gsma-fraud:prepaid="generation-of-abusive-credits"

Generation of Abusive Calls

gsma-fraud:prepaid="scartch-card-abuse"

Scratch Card Abuse

gsma-network-technology

gsma-network-technology namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Taxonomy used by GSMA for their information sharing program with telco describing the types of infrastructure. WiP

user

applications

end-devices-and-components

gsma-network-technology:end-devices-and-components="ms"

Mobile Station

gsma-network-technology:end-devices-and-components="mobile-equipment-radio"

Mobile Equipment Radio

services

radio-access-network

support-and-provisioning-systems

interconnects

core

sim-secure-element-modules

honeypot-basic

honeypot-basic namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Updated (CIRCL, Seamus Dowling and EURECOM) from Christian Seifert, Ian Welch, Peter Komisarczuk, 'Taxonomy of Honeypots', Technical Report CS-TR-06/12, VICTORIA UNIVERSITY OF WELLINGTON, School of Mathematical and Computing Sciences, June 2006, http://www.mcs.vuw.ac.nz/comp/Publications/archive/CS-TR-06/CS-TR-06-12.pdf

interaction-level

Describes whether the exposed functionality of a honeypot is limited in some way, which is usually the case for honeypots that simulate services.

honeypot-basic:interaction-level="high"

High Interaction Level

Exposed functionality of the honeypot is not limited.

honeypot-basic:interaction-level="medium"

Medium Interaction Level

Exposed functionality of the honeypot is limited to the service without exposing the full operating system.

honeypot-basic:interaction-level="low"

low Interaction Level

Exposed functionality being limited. For example, a simulated SSH server of a honeypot is not able to authenticate against a valid login/password combination.

honeypot-basic:interaction-level="none"

No interaction capabilities

No exposed functionality in the honeypot.

honeypot-basic:interaction-level="adaptive"

Learns from attack interaction

Learns from attack interaction

data-capture

Describes the type of data a honeypot is able to capture

honeypot-basic:data-capture="network-capture"

Network capture

The honeypot collects raw network capture.

honeypot-basic:data-capture="events"

Events

The honeypot collects data about something that has happened or took place, a change in state.

honeypot-basic:data-capture="attacks"

Attacks

The honeypot collects malicious activity.

honeypot-basic:data-capture="intrusions"

Intrusions

The honeypot collects malicious activity that leads to a security failure.

honeypot-basic:data-capture="none"

None

The honeypot does not collect events, attacks, or intrusions.

containment

Classifies the measures a honeypot takes to defend against malicious activity spreading from itself.

honeypot-basic:containment="block"

Block

Attacker’s actions are identified and blocked. The attack never reaches the target.

honeypot-basic:containment="defuse"

Defuse

The attack reaches the target, but is manipulated in a way that it fails against the target.

honeypot-basic:containment="slow-down"

Slow Down

Attacker is slowed down in his actions of spreading malicious activity.

honeypot-basic:containment="none"

None

No action is taken to limit the intruder’s spread of malicious activity against other systems.

distribution-appearance

Describes whether the honeypot system appears to be confined to one system or multiple systems.

honeypot-basic:distribution-appearance="distributed"

Distributed

The honeypot is or appears to be composed of multiple systems.

honeypot-basic:distribution-appearance="stand-alone"

Stand-Alone

The honeypot is or appears to be one system.

communication-interface

Describes the interfaces one can use to interact directly with the honeypot.

honeypot-basic:communication-interface="network-interface"

Network Interface

The honeypot can be directly communicated with via a network interface.

honeypot-basic:communication-interface="hardware-interface"

Non-Network Hardware Interface

Examples: Printer port, CDROM drives, USB connections.

honeypot-basic:communication-interface="software-api"

Software API

The honeypot can be interacted with via a software API.

role

Describes in what role the honeypot acts within a multi-tier architecture.

honeypot-basic:role="server"

Server

The honeypot is passively awaiting requests from clients.

honeypot-basic:role="client"

Client

The honeypot is actively initiating requests to servers.

ics

ics namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

FIRST.ORG CTI SIG - MISP Proposal for ICS/OT Threat Attribution (IOC) Project

ot-security-issues

ics:ot-security-issues="Message Authentication"

Message Authentication

Auth in used protocols is attacked and falsification command can be sent

ics:ot-security-issues="Message Integrity Checking"

Message Integrity Checking

Message poart of the sent protocol is maliciously tampered

ics:ot-security-issues="Message Encryption"

Message Encryption

Self explanatory, i.e. Weak encryption is attacked

ics:ot-security-issues="Command Injection"

Command Injection

Either Remote Command Injection or Local. On local can be timer triggered under tampered firmware

ics:ot-security-issues="Replay Attack"

Replay Attack

Self explanatory

ics:ot-security-issues="Man in the middle (MITM) Attack"

Man in the middle (MITM) Attack

Self explanatory

ics:ot-security-issues="Undocumented instructions"

Undocumented instructions

Vendor’s left several instruction used for development or trouble shooting that is finally leaked and used to performed malicious activities on the devices.

ics:ot-security-issues="Vendor proprietary protocols"

Vendor proprietary protocols

Internal vendor protocols used for development or trouble shooting, that is being maliciously for an attack.

ot-network-data-transmission-protocols-automatic-automobile-vehicle-aviation

ics:ot-network-data-transmission-protocols-automatic-automobile-vehicle-aviation="ARINC 429"

ARINC 429

ics:ot-network-data-transmission-protocols-automatic-automobile-vehicle-aviation="CAN bus (ARINC 825 SAE J1939 NMEA 2000 FMS)"

CAN bus (ARINC 825 SAE J1939 NMEA 2000 FMS)

ics:ot-network-data-transmission-protocols-automatic-automobile-vehicle-aviation="Factory Instrumentation Protocol"

Factory Instrumentation Protocol

ics:ot-network-data-transmission-protocols-automatic-automobile-vehicle-aviation="FlexRay"

FlexRay

ics:ot-network-data-transmission-protocols-automatic-automobile-vehicle-aviation="IEBus"

IEBus

ics:ot-network-data-transmission-protocols-automatic-automobile-vehicle-aviation="J1587"

J1587

ics:ot-network-data-transmission-protocols-automatic-automobile-vehicle-aviation="J1708"

J1708

ics:ot-network-data-transmission-protocols-automatic-automobile-vehicle-aviation="Keyword Protocol 2000"

Keyword Protocol 2000

ics:ot-network-data-transmission-protocols-automatic-automobile-vehicle-aviation="Unified Diagnostic Services"

Unified Diagnostic Services

ics:ot-network-data-transmission-protocols-automatic-automobile-vehicle-aviation="LIN"

LIN

ics:ot-network-data-transmission-protocols-automatic-automobile-vehicle-aviation="MOST"

MOST

ics:ot-network-data-transmission-protocols-automatic-automobile-vehicle-aviation="VAN"

VAN

ot-network-data-transmission-protocols-automatic-meter-reading

ics:ot-network-data-transmission-protocols-automatic-meter-reading="ANSI C12.18"

ANSI C12.18

ics:ot-network-data-transmission-protocols-automatic-meter-reading="IEC 61107"

IEC 61107

ics:ot-network-data-transmission-protocols-automatic-meter-reading="DLMS/IEC 62056"

DLMS/IEC 62056

ics:ot-network-data-transmission-protocols-automatic-meter-reading="M-Bus"

M-Bus

ics:ot-network-data-transmission-protocols-automatic-meter-reading="Modbus"

Modbus

ics:ot-network-data-transmission-protocols-automatic-meter-reading="ZigBee"

ZigBee

ot-network-data-transmission-protocols-industrial-control-system

ics:ot-network-data-transmission-protocols-industrial-control-system="MTConnect"

MTConnect

ics:ot-network-data-transmission-protocols-industrial-control-system="OPC"

OPC

ics:ot-network-data-transmission-protocols-industrial-control-system="DA"

DA

ics:ot-network-data-transmission-protocols-industrial-control-system="HDA"

HDA

ics:ot-network-data-transmission-protocols-industrial-control-system="UA"

UA

ot-network-data-transmission-protocols-building-automation

ics:ot-network-data-transmission-protocols-building-automation="1-Wire"

1-Wire

ics:ot-network-data-transmission-protocols-building-automation="BACnet"

BACnet

ics:ot-network-data-transmission-protocols-building-automation="C-Bus"

C-Bus

ics:ot-network-data-transmission-protocols-building-automation="CEBus"

CEBus

ics:ot-network-data-transmission-protocols-building-automation="DALI"

DALI

ics:ot-network-data-transmission-protocols-building-automation="DSI"

DSI

ics:ot-network-data-transmission-protocols-building-automation="DyNet"

DyNet

ics:ot-network-data-transmission-protocols-building-automation="Factory Instrumentation Protocol"

Factory Instrumentation Protocol

ics:ot-network-data-transmission-protocols-building-automation="KNX"

KNX

ics:ot-network-data-transmission-protocols-building-automation="LonTalk"

LonTalk

ics:ot-network-data-transmission-protocols-building-automation="Modbus"

Modbus

ics:ot-network-data-transmission-protocols-building-automation="oBIX"

oBIX

ics:ot-network-data-transmission-protocols-building-automation="VSCP"

VSCP

ics:ot-network-data-transmission-protocols-building-automation="X10"

X10

ics:ot-network-data-transmission-protocols-building-automation="xAP"

xAP

ics:ot-network-data-transmission-protocols-building-automation="xPL"

xPL

ics:ot-network-data-transmission-protocols-building-automation="ZigBee"

ZigBee

ot-network-data-transmission-protocols-power-system-automation

ics:ot-network-data-transmission-protocols-power-system-automation="IEC 60870"

IEC 60870

ics:ot-network-data-transmission-protocols-power-system-automation="DNP3"

DNP3

ics:ot-network-data-transmission-protocols-power-system-automation="Factory Instrumentation Protocol"

Factory Instrumentation Protocol

ics:ot-network-data-transmission-protocols-power-system-automation="IEC 61850"

IEC 61850

ics:ot-network-data-transmission-protocols-power-system-automation="IEC 62351"

IEC 62351

ics:ot-network-data-transmission-protocols-power-system-automation="Modbus"

Modbus

ics:ot-network-data-transmission-protocols-power-system-automation="Profibus"

Profibus

ot-network-data-transmission-protocols-process-automation

ics:ot-network-data-transmission-protocols-process-automation="AS-i"

AS-i

ics:ot-network-data-transmission-protocols-process-automation="BSAP"

BSAP

ics:ot-network-data-transmission-protocols-process-automation="CC-Link Industrial Networks"

CC-Link Industrial Networks

ics:ot-network-data-transmission-protocols-process-automation="CIP"

CIP

ics:ot-network-data-transmission-protocols-process-automation="CAN bus"

CAN bus

ics:ot-network-data-transmission-protocols-process-automation="ControlNet"

ControlNet

ics:ot-network-data-transmission-protocols-process-automation="DF-1"

DF-1

ics:ot-network-data-transmission-protocols-process-automation="DirectNET"

DirectNET

ics:ot-network-data-transmission-protocols-process-automation="EtherCAT"

EtherCAT

ics:ot-network-data-transmission-protocols-process-automation="Ethernet Global Data (EGD)"

Ethernet Global Data (EGD)

ics:ot-network-data-transmission-protocols-process-automation="Ethernet Powerlink"

Ethernet Powerlink

ics:ot-network-data-transmission-protocols-process-automation="EtherNet/IP"

EtherNet/IP

ics:ot-network-data-transmission-protocols-process-automation="Experimental Physics and Industrial Control System (EPICS) StreamDevice protocol (i.e RF:FREQ 499.655 MHZ)"

Experimental Physics and Industrial Control System (EPICS) StreamDevice protocol (i.e RF:FREQ 499.655 MHZ)

ics:ot-network-data-transmission-protocols-process-automation="Factory Instrumentation Protocol"

Factory Instrumentation Protocol

ics:ot-network-data-transmission-protocols-process-automation="FINS"

FINS

ics:ot-network-data-transmission-protocols-process-automation="FOUNDATION fieldbus (H1 HSE)"

FOUNDATION fieldbus (H1 HSE)

ics:ot-network-data-transmission-protocols-process-automation="GE SRTP"

GE SRTP

ics:ot-network-data-transmission-protocols-process-automation="HART Protocol"

HART Protocol

ics:ot-network-data-transmission-protocols-process-automation="Honeywell SDS"

Honeywell SDS

ics:ot-network-data-transmission-protocols-process-automation="HostLink"

HostLink

ics:ot-network-data-transmission-protocols-process-automation="INTERBUS"

INTERBUS

ics:ot-network-data-transmission-protocols-process-automation="IO-Link"

IO-Link

ics:ot-network-data-transmission-protocols-process-automation="MECHATROLINK"

MECHATROLINK

ics:ot-network-data-transmission-protocols-process-automation="MelsecNet"

MelsecNet

ics:ot-network-data-transmission-protocols-process-automation="Modbus"

Modbus

ics:ot-network-data-transmission-protocols-process-automation="Optomu"

Optomu

ics:ot-network-data-transmission-protocols-process-automation="PieP"

PieP

ics:ot-network-data-transmission-protocols-process-automation="Profibus"

Profibus

ics:ot-network-data-transmission-protocols-process-automation="PROFINET IO"

PROFINET IO

ics:ot-network-data-transmission-protocols-process-automation="RAPIEnet"

RAPIEnet

ics:ot-network-data-transmission-protocols-process-automation="SERCOS interface"

SERCOS interface

ics:ot-network-data-transmission-protocols-process-automation="SERCOS III"

SERCOS III

ics:ot-network-data-transmission-protocols-process-automation="Sinec H1"

Sinec H1

ics:ot-network-data-transmission-protocols-process-automation="SynqNet"

SynqNet

ics:ot-network-data-transmission-protocols-process-automation="TTEthernet"

TTEthernet

ics:ot-network-data-transmission-protocols-process-automation="TCP/IP"

TCP/IP

ot-communication-interface

ics:ot-communication-interface="rs-232"

RS-232 (comm port)

Serial communication with an implementation comprises 2 data lines, 6 control lines and one ground.

ics:ot-communication-interface="rs-422, rs-423 or rs-485"

RS-422, RS-423 or RS-485

RS-422 is compatible to RS-232, used in situations where long distances are required, it can drive up to 1200m at 100kbit/s, and up to 1Mbit/s over short distances. RS-422 uses a differential driver, uses a four-conductor cable, and up to ten receivers can be on a multi-dropped network or bus. RS-485 is

like RS-422 but RS-422 allows just one driver with multiple receivers whereas RS-485 supports multiple drivers and receivers RS-485 also allows up to thirty two (32) multi-dropped receivers or transmitters on a multi-dropped network or bus. At 90 kbit/s, the maximum cable length is 1250 m, and at 10 Mbit/s it is 15 m. The devices are half-duplex (i.e. send or receive, but not both at the same time). For more nodes or long distances, you can use repeaters that regenerate the signals and begin a new RS-485 line.

ics:ot-communication-interface="ieee-488-gpib"

IEEE-488 (GPIB)

Known as Hewlett-Packard HP-IB but was renamed as GPIB (General Purpose Interface Bus) by the IEEE-488 (1975). IEEE-488 interface comprises 8 data lines, 8 control lines and 8 ground lines. Up to 15 devices can be interconnected on one bus. Each device is assigned a unique primary address, ranging from 4-30, by setting the address switches on the device. Devices are linked in either a daisy-chain or star (or some combination) configuration with up to 20 m of shielded 24-conductor cable. A maximum separation of 4 m is specified between any two devices, and an average of 2m over the entire bus. The data transfer rate can be up to 1 Mbyte/s. Three types of devices can be connected to an IEEE-488 bus (Listeners, Talkers, and Controllers)

ics:ot-communication-interface="ieee-1394-firewire"

IEEE-1394 (FireWire)

The IEEE-1394 defines a serial serial interface that can use the bus cable to power devices. Firewire transmits data in packets and incurs some overhead as a result. Firewire frames are 125 msec long which means that despite a 'headline' transfer speed of 400 Mbit/s Firewire can be substantially slower in responding to instruments' service requests. Firewire uses a peer-peer protocol, similar to IEEE-488. Using standard cable, the maximum length bus comprises 16 hops of 4.5m each. Each hop connects two devices, but each physical device can contain four logical nodes. A Firewire cable contains two twisted-pairs (signals and clock) and two untwisted conductors (power and ground).

ics:ot-communication-interface="usb-universal-serial-bus"

USB (Universal Serial Bus)

USB is the bus topology, and host-target protocol, mean that giving existing PC-based instruments a USB port not as trivial as it could be, but instruments with USB ports are coming onto the ICS market increasing numbers. USB 1.1 has many features as serial data transmission, device powering, data sent in 1 ms packets. USB offers 1.5- and 12-Mbit/s speeds. Individual devices can use the bus for a maximum of 50% of the time. In practice, the maximum rate is not more than 0.6 Mbyte/s. USB 2.0 specification was released in 2000. In addition to increasing the signaling rate from 12 MHz to 480 MHz, the specification describes a more advanced feature set and uses bandwidth more efficiently than 'Classic' USB. Version 2 of USB seems likely to prevent IEEE 1394 becoming widely adopted in instrument systems.

ics:ot-communication-interface="ethernet"

Ethernet

Instruments with ethernet interfaces have the great advantage that they can be accessed and controlled from a desktop anywhere in the world. A web-enabled ICS device behaves can be operated with standard browser. Systems with comm based on these interface can make use of existing Ethernet networks and connecting an instrument directly into the internet makes sharing of data easy. Fast data transfer is possible. However, when connected to the public internet it is difficult to secure or maintain its security and a full evaluation of the risks involved for this interface usage is very essential.

ics:ot-communication-interface="others"

Others

Other communication interface not listed.

ot-operating-systems

ics:ot-operating-systems="rtos"

RTOS

Please see the URL reference, there are a lot of it to be listed in here. These OS are also referred as Firmware. https://en.wikipedia.org/wiki/Comparison_of_real-time_operating_systems

ics:ot-operating-systems="linux-embedded-base-os"

Linux Embedded Base OS

Yocto\nBuildroot\nOpenWRT\nB & R Linux\n Scientific Linux\nRaspbian\nAndroid

ics:ot-operating-systems="bsd"

BSD

NetBSD (NetBSD Embedded Systems)\nFreeBSD (Modified. i.e.: Orbis OS)

ics:ot-operating-systems="microsoft"

Microsoft

Windows 10 IoT Enterprise\n Windows Embedded 8.1 Industry Professional\n Windows 7 Professional/Ultimate\n Windows Embedded Standard 7\n Windows Embedded Standard 2009\n Windows CE 6.0\n

ot-components-category

ics:ot-components-category="programmable-logic-controller"

Programmable Logic Controller (PLC)

1. Computing device with user-programmable memory to storing instructions to operate a physical process.\n\n 2.Various PLC types for different processses

ics:ot-components-category="remote-terminal-unit"

Remote Terminal Unit (RTU)

1. Data aquisitionand control unit designedto support field sites and remote stations.\n\n2. Wired and wireless communication capabilities.\n\n3. No stored program logic.

ics:ot-components-category="human-machine-interface"

Human-Machine Interface (HMI)

1. Hardware/software that operators used to interact with control system.\n\n2. From physical control panels to a complete computer systems

ics:ot-components-category="sensors"

Sensors

Pressure, Temperature, Flow, Voltage, Optical, Proximity

ics:ot-components-category="actuators"

Actuators

Variable Frequency Drive, Servo Drive, Valve, Circuit Breaker

ics:ot-components-category="communications"

Communications

Modems, Routers, Serial - Ethernet Converters, Swtiches

ics:ot-components-category="supervisory-level-devices"

Supervisory Level Devices

1. Control Server (Supervisory systems that hosts control software to manage lower level control devices like PLC).\n\n2. Data Historian (Centralized database for information about process, control activity and status record).\n\n3. Engineering workstations (Creating and revising control systems anbd programs, incl. project files).

iep

iep namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Forum of Incident Response and Security Teams (FIRST) Information Exchange Policy (IEP) framework

commercial-use

States whether Recipients are permitted to use information received in commercial products or services.

iep:commercial-use="MAY"

Recipients MAY use this information in commercial products or services.

iep:commercial-use="MUST NOT"

Recipients MUST NOT use this information in commercial products or services.

external-reference

This statement can be used to convey a description or reference to any applicable licenses, agreements, or conditions between the producer and receiver.

iep:external-reference="$text"

An external-reference value is required

encrypt-in-transit

States whether the received information has to be encrypted when it is retransmitted by the recipient.

iep:encrypt-in-transit="MUST"

Recipients MUST encrypt the information received when it is retransmitted or redistributed.

iep:encrypt-in-transit="MAY"

Recipients MAY encrypt the information received when it is retransmitted or redistributed.

encrypt-at-rest

States whether the received information has to be encrypted by the Recipient when it is stored at rest.

iep:encrypt-at-rest="MUST"

Recipients MUST encrypt the information received when it is stored at rest.

iep:encrypt-at-rest="MAY"

Recipients MAY encrypt the information received when it is stored at rest.

permitted-actions

States the permitted actions that Recipients can take upon information received.

iep:permitted-actions="NONE"

Recipients MUST contact the Providers before acting upon the information received.

iep:permitted-actions="CONTACT FOR INSTRUCTION"

Recipients MUST contact the Providers before acting upon the information received.

iep:permitted-actions="INTERNALLY VISIBLE ACTIONS"

Recipients MAY conduct actions on the information received that are only visible on the Recipients internal networks and systems, and MUST NOT conduct actions that are visible outside of the Recipients networks and systems, or visible to third parties.

iep:permitted-actions="EXTERNALLY VISIBLE INDIRECT ACTIONS"

Recipients MAY conduct indirect, or passive, actions on the information received that are externally visible and MUST NOT conduct direct, or active, actions.

iep:permitted-actions="EXTERNALLY VISIBLE DIRECT ACTIONS"

Recipients MAY conduct direct, or active, actions on the information received that are externally visible.

affected-party-notifications

Recipients are permitted notify affected third parties of a potential compromise or threat.

iep:affected-party-notifications="MAY"

Recipients MAY notify affected parties of a potential compromise or threat.

iep:affected-party-notifications="MUST NOT"

Recipients MUST NOT notify affected parties of potential compromise or threat.

traffic-light-protocol

Recipients are permitted to redistribute the information received within the redistribution scope as defined by the enumerations.

iep:traffic-light-protocol="RED"

Personal for identified recipients only.

iep:traffic-light-protocol="AMBER"

Limited sharing on the basis of need-to-know.

iep:traffic-light-protocol="GREEN"

Community wide sharing.

iep:traffic-light-protocol="WHITE"

Unlimited sharing.

provider-attribution

Recipients could be required to attribute or anonymize the Provider when redistributing the information received.

iep:provider-attribution="MAY"

Recipients MAY attribute the Provider when redistributing the information received.

iep:provider-attribution="MUST"

Recipients MUST attribute the Provider when redistributing the information received.

iep:provider-attribution="MUST NOT"

Recipients MUST NOT attribute the Provider when redistributing the information received.

obfuscate-affected-parties

Recipients could be required to obfuscate or anonymize information that could be used to identify the victims before redistributing the information received.

iep:obfuscate-affected-parties="MAY"

Recipients MAY obfuscate information about the specific affected parties.

iep:obfuscate-affected-parties="MUST"

Recipients MUST obfuscate information about the specific affected parties.

iep:obfuscate-affected-parties="MUST NOT"

Recipients MUST NOT obfuscate information about the specific affected parties.

unmodified-resale

States whether the recipient MAY or MUST NOT resell the information received unmodified or in a semantically equivalent format.

iep:unmodified-resale="MAY"

Recipients MAY resell the information received.

iep:unmodified-resale="MUST NOT"

Recipients MUST NOT resell the information received unmodified or in a semantically equivalent format.

start-date

States the UTC date that the IEP is effective from.

iep:start-date="$text"

A start-date value is required

end-date

States the UTC date that the IEP is effective until.

iep:end-date="$text"

An end-date value is required

reference

This statement can be used to provide a URL reference to the specific IEP implementation.

iep:reference="$text"

A reference value is required

name

This statement can be used to provide a name for an IEP implementation.

iep:name="$text"

A name value is required

version

States the version of the IEP framework that has been used.

iep:version="$text"

A version value is required

id

Provides a unique ID to identify a specific IEP implementation.

iep:id="$text"

An id value is required

iep2-policy

iep2-policy namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Forum of Incident Response and Security Teams (FIRST) Information Exchange Policy (IEP) v2.0 Policy

id

Provides a unique ID to identify a specific IEP policy.

iep2-policy:id="$text"

An id value is required

name

This statement can be used to provide a name for an IEP policy.

iep2-policy:name="$text"

A name value is required

description

This statement can be used to provide more details as a background for an IEP policy.

iep2-policy:description="$text"

A description value is required

iep_version

States the version of the IEP framework that has been used. Must be set to 2.0.

iep2-policy:iep_version="2.0"

The IEP version value must be 2.0

start_date

States the UTC date that the IEP is effective from.

iep2-policy:start_date="$text"

A start_date value is required. It must be a UTC date in RFC3339 format.

end_date

States the UTC date that the IEP is effective until.

iep2-policy:end_date="$text"

An end_date value is required. It must be a UTC date in RFC3339 format, or 'null'. null is used when the IEP policy never expires.

encrypt_in_transit

States whether the received information has to be encrypted when it is retransmitted by the recipient.

iep2-policy:encrypt_in_transit="must"

Recipients MUST encrypt the information received when it is retransmitted or redistributed.

iep2-policy:encrypt_in_transit="may"

Recipients MAY encrypt the information received when it is retransmitted or redistributed.

permitted_actions

States the permitted actions that Recipients can take upon information received.

iep2-policy:permitted_actions="none"

Recipients MUST contact the Providers before acting upon the information received.

iep2-policy:permitted_actions="contact-for-instruction"

Recipients MUST contact the Providers before acting upon the information received.

iep2-policy:permitted_actions="internally-visible-actions"

Recipients MAY conduct actions on the information received that are only visible on the Recipients internal networks and systems, and MUST NOT conduct actions that are visible outside of the Recipients networks and systems, or visible to third parties.

iep2-policy:permitted_actions="externally-visible-indirect-actions"

Recipients MAY conduct indirect, or passive, actions on the information received that are externally visible and MUST NOT conduct direct, or active, actions.

iep2-policy:permitted_actions="externally-visible-direct-actions"

Recipients MAY conduct direct, or active, actions on the information received that are externally visible.

affected_party_notifications

Recipients are permitted notify affected third parties of a potential compromise or threat.

iep2-policy:affected_party_notifications="may"

Recipients MAY notify affected parties of a potential compromise or threat.

iep2-policy:affected_party_notifications="must-not"

Recipients MUST NOT notify affected parties of potential compromise or threat.

tlp

Recipients are permitted to redistribute the information received within the redistribution scope as defined by the enumerations.

iep2-policy:tlp="red"

Personal for identified recipients only.

iep2-policy:tlp="amber"

Limited sharing on the basis of need-to-know.

iep2-policy:tlp="green"

Community wide sharing.

iep2-policy:tlp="white"

Unlimited sharing.

attribution

Recipients could be required to attribute or anonymize the Provider when redistributing the information received.

iep2-policy:attribution="may"

Recipients MAY attribute the Provider when redistributing the information received.

iep2-policy:attribution="must"

Recipients MUST attribute the Provider when redistributing the information received.

iep2-policy:attribution="must-not"

Recipients MUST NOT attribute the Provider when redistributing the information received.

unmodified_resale

States whether the recipient MAY or MUST NOT resell the information received unmodified or in a semantically equivalent format.

iep2-policy:unmodified_resale="may"

Recipients MAY resell the information received.

iep2-policy:unmodified_resale="must-not"

Recipients MUST NOT resell the information received unmodified or in a semantically equivalent format.

external_reference

This statement can be used to convey a description or reference to any applicable licenses, agreements, or conditions between the producer and receiver.

iep2-policy:external_reference="$text"

An external_reference value is a URL that contains information relevant for this IEP policy. The URL MUST adhere to RFC3986.

iep2-reference

iep2-reference namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Forum of Incident Response and Security Teams (FIRST) Information Exchange Policy (IEP) v2.0 Reference

id_ref

Refers to a unique IEP Policy ID to identify a specific IEP policy at a remote location.

iep2-reference:id_ref="$text"

An id_ref value is required

url

This is the remote URL specifying the IEP Policy File that contains the IEP Policy you wish to use.

iep2-reference:url="$text"

A URL value is required

iep_version

States the version of the IEP framework that has been used. Must be set to 2.0.

iep2-reference:iep_version="2.0"

The IEP version value must be 2.0

ifx-vetting

ifx-vetting namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The IFX taxonomy is used to categorise information (MISP events and attributes) to aid in the

intelligence vetting process

vetted

Exclusive flag set which means the values or predicate below must be set exclusively.

ifx-vetting:vetted="legit-but-compromised"

The attribute/event describes something that is legitly used, but seems to be compromised by 3rd parties to be used for malicious activities. Consider this if blocking is your course of action.

ifx-vetting:vetted="legit"

The attribute/event describes something legitly used, that does not show signes of compromise or misuse.

ifx-vetting:vetted="legit-uncertain"

The attribute/event describes something where it is not 100% clear if it is used only legitly.

ifx-vetting:vetted="malicious"

The attribute/event describes something that is definitly used maliciously.

ifx-vetting:vetted="malicious-uncertain"

The attribute/event describes something that seems to be used maliciously, but there is no 100% proof.

ifx-vetting:vetted="invalid"

The attribute/event is invalid or wrong in respect to the situation described by the event.

ifx-vetting:vetted="irrelevant"

The attribute/event is irrelevant to your organization or CTI process.

ifx-vetting:vetted="undetermined"

The nature of the attribute/event cannot be further determined. Use this only as a last resort.

ifx-vetting:vetted="fast-track"

The attribute/event was not vetted but passed through for operational reasons. A result might be higher false-positive rates.

score

Exclusive flag set which means the values or predicate below must be set exclusively.

ifx-vetting:score="0"

0

ifx-vetting:score="1"

1

Associated numerical value="1"

ifx-vetting:score="2"

2

Associated numerical value="2"

ifx-vetting:score="3"

3

Associated numerical value="3"

ifx-vetting:score="4"

4

Associated numerical value="4"

ifx-vetting:score="5"

5

Associated numerical value="5"

ifx-vetting:score="6"

6

Associated numerical value="6"

ifx-vetting:score="7"

7

Associated numerical value="7"

ifx-vetting:score="8"

8

Associated numerical value="8"

ifx-vetting:score="9"

9

Associated numerical value="9"

ifx-vetting:score="10"

10

Associated numerical value="10"

ifx-vetting:score="11"

11

Associated numerical value="11"

ifx-vetting:score="12"

12

Associated numerical value="12"

ifx-vetting:score="13"

13

Associated numerical value="13"

ifx-vetting:score="14"

14

Associated numerical value="14"

ifx-vetting:score="15"

15

Associated numerical value="15"

ifx-vetting:score="16"

16

Associated numerical value="16"

ifx-vetting:score="17"

17

Associated numerical value="17"

ifx-vetting:score="18"

18

Associated numerical value="18"

ifx-vetting:score="19"

19

Associated numerical value="19"

ifx-vetting:score="20"

20

Associated numerical value="20"

ifx-vetting:score="21"

21

Associated numerical value="21"

ifx-vetting:score="22"

22

Associated numerical value="22"

ifx-vetting:score="23"

23

Associated numerical value="23"

ifx-vetting:score="24"

24

Associated numerical value="24"

ifx-vetting:score="25"

25

Associated numerical value="25"

ifx-vetting:score="26"

26

Associated numerical value="26"

ifx-vetting:score="27"

27

Associated numerical value="27"

ifx-vetting:score="28"

28

Associated numerical value="28"

ifx-vetting:score="29"

29

Associated numerical value="29"

ifx-vetting:score="30"

30

Associated numerical value="30"

ifx-vetting:score="31"

31

Associated numerical value="31"

ifx-vetting:score="32"

32

Associated numerical value="32"

ifx-vetting:score="33"

33

Associated numerical value="33"

ifx-vetting:score="34"

34

Associated numerical value="34"

ifx-vetting:score="35"

35

Associated numerical value="35"

ifx-vetting:score="36"

36

Associated numerical value="36"

ifx-vetting:score="37"

37

Associated numerical value="37"

ifx-vetting:score="38"

38

Associated numerical value="38"

ifx-vetting:score="39"

39

Associated numerical value="39"

ifx-vetting:score="40"

40

Associated numerical value="40"

ifx-vetting:score="41"

41

Associated numerical value="41"

ifx-vetting:score="42"

42

Associated numerical value="42"

ifx-vetting:score="43"

43

Associated numerical value="43"

ifx-vetting:score="44"

44

Associated numerical value="44"

ifx-vetting:score="45"

45

Associated numerical value="45"

ifx-vetting:score="46"

46

Associated numerical value="46"

ifx-vetting:score="47"

47

Associated numerical value="47"

ifx-vetting:score="48"

48

Associated numerical value="48"

ifx-vetting:score="49"

49

Associated numerical value="49"

ifx-vetting:score="50"

50

Associated numerical value="50"

ifx-vetting:score="51"

51

Associated numerical value="51"

ifx-vetting:score="52"

52

Associated numerical value="52"

ifx-vetting:score="53"

53

Associated numerical value="53"

ifx-vetting:score="54"

54

Associated numerical value="54"

ifx-vetting:score="55"

55

Associated numerical value="55"

ifx-vetting:score="56"

56

Associated numerical value="56"

ifx-vetting:score="57"

57

Associated numerical value="57"

ifx-vetting:score="58"

58

Associated numerical value="58"

ifx-vetting:score="59"

59

Associated numerical value="59"

ifx-vetting:score="60"

60

Associated numerical value="60"

ifx-vetting:score="61"

61

Associated numerical value="61"

ifx-vetting:score="62"

62

Associated numerical value="62"

ifx-vetting:score="63"

63

Associated numerical value="63"

ifx-vetting:score="64"

64

Associated numerical value="64"

ifx-vetting:score="65"

65

Associated numerical value="65"

ifx-vetting:score="66"

66

Associated numerical value="66"

ifx-vetting:score="67"

67

Associated numerical value="67"

ifx-vetting:score="68"

68

Associated numerical value="68"

ifx-vetting:score="69"

69

Associated numerical value="69"

ifx-vetting:score="70"

70

Associated numerical value="70"

ifx-vetting:score="71"

71

Associated numerical value="71"

ifx-vetting:score="72"

72

Associated numerical value="72"

ifx-vetting:score="73"

73

Associated numerical value="73"

ifx-vetting:score="74"

74

Associated numerical value="74"

ifx-vetting:score="75"

75

Associated numerical value="75"

ifx-vetting:score="76"

76

Associated numerical value="76"

ifx-vetting:score="77"

77

Associated numerical value="77"

ifx-vetting:score="78"

78

Associated numerical value="78"

ifx-vetting:score="79"

79

Associated numerical value="79"

ifx-vetting:score="80"

80

Associated numerical value="80"

ifx-vetting:score="81"

81

Associated numerical value="81"

ifx-vetting:score="82"

82

Associated numerical value="82"

ifx-vetting:score="83"

83

Associated numerical value="83"

ifx-vetting:score="84"

84

Associated numerical value="84"

ifx-vetting:score="85"

85

Associated numerical value="85"

ifx-vetting:score="86"

86

Associated numerical value="86"

ifx-vetting:score="87"

87

Associated numerical value="87"

ifx-vetting:score="88"

88

Associated numerical value="88"

ifx-vetting:score="89"

89

Associated numerical value="89"

ifx-vetting:score="90"

90

Associated numerical value="90"

ifx-vetting:score="91"

91

Associated numerical value="91"

ifx-vetting:score="92"

92

Associated numerical value="92"

ifx-vetting:score="93"

93

Associated numerical value="93"

ifx-vetting:score="94"

94

Associated numerical value="94"

ifx-vetting:score="95"

95

Associated numerical value="95"

ifx-vetting:score="96"

96

Associated numerical value="96"

ifx-vetting:score="97"

97

Associated numerical value="97"

ifx-vetting:score="98"

98

Associated numerical value="98"

ifx-vetting:score="99"

99

Associated numerical value="99"

ifx-vetting:score="100"

100

Associated numerical value="100"

incident-disposition

incident-disposition namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

How an incident is classified in its process to be resolved. The taxonomy is inspired from NASA Incident Response and Management Handbook. https://www.nasa.gov/pdf/589502main_ITS-HBK-2810.09-02%20%5bNASA%20Information%20Security%20Incident%20Management%5d.pdf#page=9

incident

incident-disposition:incident="confirmed"

Confirmed

The incident is confirmed and response is underway following incident response procedure of the organisation.

incident-disposition:incident="deferred"

Deferred

The incident is deferred due to resource constraints, information type or external reasons.

incident-disposition:incident="unidentified"

Unidentified

The incident is unidentified because some assets, ressources or context is missing to go a state which can be handled following the incident response response procedure.

incident-disposition:incident="transferred"

Transferred

The incident is transferred to another organisations for further processing or incident handling.

incident-disposition:incident="discarded"

Discarded

The incident is discarded due to resource constraints, information type or external reasons.

incident-disposition:incident="silently-discarded"

Silently discarded

The incident is silently discarded due to resource constraints, information type or external reasons.

not-an-incident

incident-disposition:not-an-incident="insufficient-data"

Insufficient data

When insufficient data is available to explain an ambiguous (i.e., not definitively hostile or benign) indicator, the incident may be dispositioned as Insufficient Data.

incident-disposition:not-an-incident="faulty-indicator"

Faulty indicator

A false positive where an investigation reveals that the source indicator used as the basis for incident detection was a Faulty Indicator.

incident-disposition:not-an-incident="misconfiguration"

Misconfiguration

A false positive where an event that appeared to be malicious activity was subsequently disproven and determined to be a Misconfiguration (malfunction) of a system.

incident-disposition:not-an-incident="scan-probe"

Scan or Probe

Reconnaissance activity which Scanned or Probed for the presence of a vulnerability which may be later exploited to gain unauthorized access.

incident-disposition:not-an-incident="failed"

Failed

A Failed attempt to gain unauthorized access, conduct a denial of service, install malicious code, or misuse an IT resource, typically because a security control prevented it from succeeding.

incident-disposition:not-an-incident="refuted"

Refuted

Any other circumstance where a suspected incident was determined to not be an incident and was Refuted.

duplicate

incident-disposition:duplicate="duplicate"

Duplicate

An incident may be a Duplicate of another record in the Incident Management System, and should be merged with the existing workflow.

infoleak

infoleak namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A taxonomy describing information leaks and especially information classified as being potentially leaked. The taxonomy is based on the work by CIRCL on the AIL framework. The taxonomy aim is to be used at large to improve classification of leaked information.

automatic-detection

infoleak:automatic-detection="credential"

Credential

infoleak:automatic-detection="credit-card"

Credit card

infoleak:automatic-detection="iban"

IBAN

infoleak:automatic-detection="ip"

IP address

infoleak:automatic-detection="mail"

Mail

infoleak:automatic-detection="phone-number"

Phone number

infoleak:automatic-detection="api-key"

API key

infoleak:automatic-detection="google-api-key"

Google API key

infoleak:automatic-detection="aws-key"

AWS key

infoleak:automatic-detection="private-key"

Private key at large

infoleak:automatic-detection="encrypted-private-key"

Encrypted private key at large

infoleak:automatic-detection="private-ssh-key"

Private SSH key

infoleak:automatic-detection="private-static-key"

Private state key

infoleak:automatic-detection="vpn-static-key"

VPN static key

infoleak:automatic-detection="pgp-message"

PGP message

infoleak:automatic-detection="pgp-public-key-block"

PGP public key block

infoleak:automatic-detection="pgp-signature"

PGP signature

infoleak:automatic-detection="pgp-private-key"

PGP private key

infoleak:automatic-detection="certificate"

Certificate

infoleak:automatic-detection="rsa-private-key"

RSA private key

infoleak:automatic-detection="dsa-private-key"

DSA private key

infoleak:automatic-detection="ec-private-key"

EC private key

infoleak:automatic-detection="public-key"

Public key

infoleak:automatic-detection="base64"

Base64

infoleak:automatic-detection="binary"

Binary

infoleak:automatic-detection="hexadecimal"

Hexadecimal

infoleak:automatic-detection="bitcoin-address"

Bitcoin address

infoleak:automatic-detection="bitcoin-private-key"

Bitcoin private key

infoleak:automatic-detection="cve"

CVE

infoleak:automatic-detection="onion"

Onion link

infoleak:automatic-detection="sql-injection"

SQL injection

analyst-detection

infoleak:analyst-detection="credential"

Credential

infoleak:analyst-detection="credit-card"

Credit card

infoleak:analyst-detection="iban"

IBAN

infoleak:analyst-detection="ip"

IP address

infoleak:analyst-detection="mail"

Mail

infoleak:analyst-detection="phone-number"

Phone number

infoleak:analyst-detection="api-key"

API key

infoleak:analyst-detection="google-api-key"

Google API key

infoleak:analyst-detection="aws-key"

AWS key

infoleak:analyst-detection="private-key"

Private key at large

infoleak:analyst-detection="encrypted-private-key"

Encrypted private key at large

infoleak:analyst-detection="private-ssh-key"

Private SSH key

infoleak:analyst-detection="private-static-key"

Private state key

infoleak:analyst-detection="vpn-static-key"

VPN static key

infoleak:analyst-detection="pgp-message"

PGP message

infoleak:analyst-detection="pgp-public-key-block"

PGP public key block

infoleak:analyst-detection="pgp-signature"

PGP signature

infoleak:analyst-detection="pgp-private-key"

PGP private key

infoleak:analyst-detection="certificate"

Certificate

infoleak:analyst-detection="rsa-private-key"

RSA private key

infoleak:analyst-detection="dsa-private-key"

DSA private key

infoleak:analyst-detection="ec-private-key"

EC private key

infoleak:analyst-detection="public-key"

Public key

infoleak:analyst-detection="base64"

Base64

infoleak:analyst-detection="binary"

Binary

infoleak:analyst-detection="hexadecimal"

Hexadecimal

infoleak:analyst-detection="bitcoin-address"

Bitcoin address

infoleak:analyst-detection="bitcoin-private-key"

Bitcoin private key

infoleak:analyst-detection="cve"

CVE

infoleak:analyst-detection="onion"

Onion link

infoleak:analyst-detection="sql-injection"

SQL injection

confirmed

Exclusive flag set which means the values or predicate below must be set exclusively.

infoleak:confirmed="false-positive"

False positive

infoleak:confirmed="false-negative"

False negative

infoleak:confirmed="true-positive"

True positive

infoleak:confirmed="true-negative"

True negative

source

infoleak:source="public-website"

Public website

infoleak:source="pastie-website"

Pastie-like website

infoleak:source="electronic-forum"

Electronic forum

infoleak:source="mailing-list"

Mailing-list

infoleak:source="source-code-repository"

Source code repository

infoleak:source="automatic-collection"

Automatic collection including honeypots, spamtramps or equivalent technologies

infoleak:source="manual-analysis"

Manual analysis or investigation where detection took place

infoleak:source="unknown"

Unknown

infoleak:source="other"

Other source not specified in this list

submission

infoleak:submission="manual"

Manual

infoleak:submission="automatic"

Automatic

infoleak:submission="crawler"

Crawler

output-format

Exclusive flag set which means the values or predicate below must be set exclusively.

infoleak:output-format="ail-daily"

Daily event

infoleak:output-format="ail-weekly"

Weekly event

infoleak:output-format="ail-monthly"

Monthly event

certainty

Exclusive flag set which means the values or predicate below must be set exclusively.

infoleak:certainty="100"

Certainty (probability equals 1 - 100%)

Certainty

Associated numerical value="100"

infoleak:certainty="93"

Almost certain (probability equals 0.93 - 93%)

Almost certain

Associated numerical value="93"

infoleak:certainty="75"

Probable (probability equals 0.75 - 75%)

Probable

Associated numerical value="75"

infoleak:certainty="50"

Chances about even (probability equals 0.50 - 50%)

Chances about even

Associated numerical value="50"

infoleak:certainty="30"

Probably not (probability equals 0.30 - 30%)

Probably not

Associated numerical value="30"

infoleak:certainty="7"

Almost certainly not (probability equals 0.07 - 7%)

Almost certainly not

Associated numerical value="7"

infoleak:certainty="0"

Impossibility (probability equals 0 - 0%)

Impossibility

information-security-data-source

information-security-data-source namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Taxonomy to classify the information security data sources.

type-of-information

Type of provided information

information-security-data-source:type-of-information="vulnerability"

Vulnerability

Information regarding a weakness of an asset which might be exploited by a threat

information-security-data-source:type-of-information="threat"

Threat

Information regarding the potential cause on an unwanted incident

information-security-data-source:type-of-information="countermeasure"

Countermeasure

Information regarding any administrative, managerial, technical or legal control that is used to counteract an information security risk

information-security-data-source:type-of-information="attack"

Attack

Information regarding any unauthorized attempt to access, alter or destroy an asset

information-security-data-source:type-of-information="risk"

Risk

Information describing the consequences of a potential event, such as an attack

information-security-data-source:type-of-information="asset"

Asset

Information regarding any object or characteristic that has value to an organization

originality

Originality and novelty of the provided information

information-security-data-source:originality="original-source"

Original source

Information originates from the data sources which publish their own information

information-security-data-source:originality="secondary-source"

Secondary source

Information is integrated or copied from another information security data source

timeliness-sharing-behavior

Timeliness of the provided information

information-security-data-source:timeliness-sharing-behavior="routine-sharing"

Routine sharing

Information is published at a specific point in time on a regular basis, such as daily, weakly or monthly reports

information-security-data-source:timeliness-sharing-behavior="incident-specific"

Incident specific

Information is published whenever news are available or a new incident occurs

integrability-format

Level of integrability format for the provided information

information-security-data-source:integrability-format="structured"

Structured

The provided security information is available in an standardized and structured data format such as MISP core format

information-security-data-source:integrability-format="unstructured"

Unstructured

The provided security information is available in unstructured form without following a common data representation format

integrability-interface

Level of integrability interface for the provided information

information-security-data-source:integrability-interface="no-interface"

No interface

The information security data source doesn’t provide any interface to access the information

information-security-data-source:integrability-interface="api"

API

The information security data source provides an application programming interface (APIs) to obtain the provided information

information-security-data-source:integrability-interface="rss-feeds"

RSS Feeds

The information security data source provides an RSS Feed to keep track of the provided information

information-security-data-source:integrability-interface="export"

Export

The information security data source provides an interface to export contents as XML, JSON or plain text

trustworthiness-creditabilily

Source of the creditability

information-security-data-source:trustworthiness-creditabilily="vendor"

Vendor

The publisher of the information is a vendor

information-security-data-source:trustworthiness-creditabilily="government"

Government

The publisher of the information is a government

information-security-data-source:trustworthiness-creditabilily="security-expert"

Security expert

The publisher of the information is a security expert

information-security-data-source:trustworthiness-creditabilily="normal-user"

Normal user

The publisher of the information is a normal user

trustworthiness-traceability

Traceability of the provided information

information-security-data-source:trustworthiness-traceability="yes"

Yes

The provided information is classified as traceable if it can be traced back, based on meta-data, to a specific publisher and a publishing date

information-security-data-source:trustworthiness-traceability="no"

No

The provided information cannot be traced back (meta-data are not provided)

trustworthiness-feedback-mechanism

Feedback such as user ratings or comments regarding the usefulness of the provided information

information-security-data-source:trustworthiness-feedback-mechanism="yes"

Yes

The provided information is validated by including user rating, comments or additional analysis

information-security-data-source:trustworthiness-feedback-mechanism="no"

No

The provided information is not validated (a user rating, comments is not available)

type-of-source

Types of information security data source

information-security-data-source:type-of-source="news-website"

News website

information-security-data-source:type-of-source="expert-blog"

Expert blog

information-security-data-source:type-of-source="security-product-vendor-website"

(Security product) vendor website

information-security-data-source:type-of-source="vulnerability-database"

Vulnerability database

information-security-data-source:type-of-source="mailing-list-archive"

Mailing list archive

information-security-data-source:type-of-source="social-network"

Social network

information-security-data-source:type-of-source="streaming-portal"

Streaming portal

information-security-data-source:type-of-source="forum"

Forum

information-security-data-source:type-of-source="other"

Other

information-security-indicators

information-security-indicators namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A full set of operational indicators for organizations to use to benchmark their security posture.

IEX

Indicators of this category give information on the occurrence of incidents caused by external malicious threat sources.

information-security-indicators:IEX="FGY.1"

Forged domain or brand names impersonating or imitating legitimate and genuine names

Forged domains are addresses very close to the domain names legitimately filed with registration companies or organizations (forged domains are harmful only when actively used to entice

customers to the website for fraudulent purposes). It also includes domain names that imitate another domain name or a brand.

information-security-indicators:IEX="FGY.2"

Wholly or partly forged websites (excluding parking pages) spoiling company’s image or business

Forged websites correspond to two main threats (forgery of sites in order to steal personal data such as account identifiers and passwords, forgery of services in order to capitalize on a brand and to generate turnover that creates unfair competition). In this case, reference is often made to phishing (1st usage) or pharming.

information-security-indicators:IEX="SPM.1"

Not requested received bulk messages (spam) targeting organization’s registered users

Spam are messages received in company’s or organization’s messaging systems in the framework of mass and not individualized campaigns, luring into clicking dangerous URLs (possibly Trojan laden) or enticing to carry out harmful to concerned individual actions.

information-security-indicators:IEX="PHI.1"

Phishing targeting company’s customers' workstations spoiling company’s image or business

Phishing involves a growing number of business sectors (financial organizations, e-commerce sites, online games, social sites etc.). It includes attacks via e-mail with messages that contain either malicious URL links (to forged websites) or malicious URL links (to malware laden genuine websites).

information-security-indicators:IEX="PHI.2"

Spear phishing or whaling carried out using social engineering and targeting organization’s specific registered users

Spear phishing are "spoofed" and customized messages looking like a usual professional relationship or an authority, and asking to click on or open dangerous URL links or dangerous attachments (malware laden).

information-security-indicators:IEX="INT.1"

Intrusion attempts on externally accessible servers

Attempts are here systematic scans (excluding network reconnaissance) and abnormal and suspicious requests on externally accessible servers, detected by an IDS/IPS or not.

information-security-indicators:IEX="INT.2"

Intrusion on externally accessible servers

Intrusion usually targets servers that host personal data (including data subject to regulations such

as PCI DSS, for example). 3 objectives or motivations can be found wherever an intrusion exists: data theft (see before), installation of transfer links towards unlawful and rogue websites, getting a permanent internal access by installation of a backdoor for further purposes. This indicator does not include the figures from the Defacement and Misappropriation indicators, both of which however starting with an intrusion. However, it includes all means and methods to get access to servers, i.e. purely technical means (such as Command execution/injection attack) or identity usurpation to log on an admin or user account (see ETSI GS ISI 002 [4] specifications).

information-security-indicators:IEX="INT.3"

Intrusions on internal servers

This kind of incident typically comes after a PC malware installation or an intrusion on an externally accessible server often followed by a lateral movement. This indicator does not include the figures from the Misappropriation indicator which may however start with an intrusion on an internal server. This indicator includes the so-called APTs (Advanced Persistent Threats), which constitute however only a small part of this indicator. APTs are long lasting and stealthy incidents with large compromises of data through outbound links, which is not the case of most incidents of the IEX_INT.3 type. This type of incident is often the result of targeted attacks.

information-security-indicators:IEX="DFC.1"

Obvious and visible websites defacements

Obvious defacements measures the defacement of homepages and of the most consulted pages of sites.

information-security-indicators:IEX="MIS.1"

Servers resources misappropriation by external attackers

This indicator measures the amount of resources of servers misappropriated by an external attacker after a successful intrusion (on an externally accessible or an internal server).

information-security-indicators:IEX="DOS.1"

Denial of service attacks on websites

This indicator measures denial-of-service attacks against websites, carried out either by sending of harmful requests (DoS), by sending a massive flow coming from multiple distributed sites (DDoS) or via other techniques. Due to the current state of the art of attack detection, the indicator is limited to DDoS attacks.

information-security-indicators:IEX="MLW.1"

Attempts to install malware on workstations

Malware installation attempts are detected by current conventional means (Antivirus and base IPS) and blocked by the same means. This indicator (which includes desktop and laptop PC based

workstations, but does not include the different types of other workstations and mobile smart devices) provides an approximate insight into the malicious external pressure suffered in this regard. This indicator should be associated with indicator on successful malware installation in order to assess the actual effectiveness of conventional detection and blockage means in the fight against malware.

information-security-indicators:IEX="MLW.2"

Attempts to install malware on servers

Malware installation attempts are detected by current conventional means (antivirus and base IPS) and blocked by the same means. This indicator gives an approximate insight into the malicious external pressure suffered in this regard. This indicator should be associated with indicator on successful malware installation in order to assess the actual effectiveness of conventional detection and blockage means in the fight against malware.

information-security-indicators:IEX="MLW.3"

Malware installed on workstations

Malware could be not detected by conventional means (lack of activation or appropriate update), or noninventoried and/or specific very stealthy incidents, most of the time not detectable by conventional means (AV and standard IPS), consequently requiring other supplementary detection means (network or WS load, outbound links, advanced network devices as DPI tools, users themselves reporting to help desks). This indicator (which includes desktop and laptop Windows-based workstations, but does not include the different types of other workstations and mobile smart devices) therefore applies to both classical viruses and worms, as well as all new malware such as Trojan horses (which are defined as malware meant to data theft or malicious transactions) or bots (which are defined here as vectors for spam or DDoS attacks).

information-security-indicators:IEX="MLW.4"

Malware installed on internal servers

Malware could be not detected by conventional means (lack of activation or of appropriate update), or noninventoried and/or specific very stealthy incidents, most of the time not detectable by conventional means (AV and standard IPS), consequently requiring other supplementary detection means (network or server load, outbound links, advanced network devices as DPI tools, administrators themselves). This indicator therefore applies to both classical viruses and worms, as well as all new malware such as Trojan horses (which are defined as malware meant to data theft or malicious transactions)

information-security-indicators:IEX="PHY.1"

Human intrusion into the organization’s perimeter

This indicator measures illicit entrance of individuals into security perimeter.

IMF

Indicators of this category provides information on the occurrence of incidents caused by malfunctions, breakdowns or human errors.

information-security-indicators:IMF="BRE.1"

Workstations accidental breakdowns or malfunctions

Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).

information-security-indicators:IMF="BRE.2"

Servers accidental breakdowns or malfunctions

Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).

information-security-indicators:IMF="BRE.3"

Mainframes accidental breakdowns or malfunctions

Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).

information-security-indicators:IMF="BRE.4"

Networks accidental breakdowns or malfunctions

Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).

information-security-indicators:IMF="MDL.1"

Delivery of email to wrong recipient

This indicator measures errors from the sender when selecting or typing email addresses leading to misdelivery incidents. Consequences may be very serious when confidentiality is critical.

information-security-indicators:IMF="LOM.1"

Loss (or theft) of mobile devices belonging to the organization

This indicator measures the loss of all types of systems containing sensitive or not information belonging to the organization, whether encrypted or not (laptop computers, USB tokens, CD-ROMs, diskettes, magnetic tapes, smartphones, tablets, etc.). In some cases, it could be difficult to differentiate losses from thefts.

information-security-indicators:IMF="LOG.1"

Downtime or malfunction of the log production function with possible legal impact

This type of event could have two main causes: an accidental system malfunction or a system manipulation error by an administrator. Logs taken into account here are systems logs and applications logs of all servers.

information-security-indicators:IMF="LOG.2"

Absence of possible tracking of the person involved in a security event with possible legal impact

Concerns unique data related to a given and known to organization user (identifier tied to application software or directory). This indicator is a sub-set of indicator IMF_LOG.1.

information-security-indicators:IMF="LOG.3"

Downtime or malfunction of the log production function for recordings with evidential value for access to or handling of information that, at this level, is subject to law or regulatory requirements

This indicator primarily relates to Personal Identifiable Information (PII) protected by privacy laws, to information falling under the PCI-DSS regulation, to information falling under European regulation in the area of breach notification (Telcos and ISPs to begin with), and to information about electronic exchanges between employees and the exterior (electronic messaging and Internet connection). This indicator does not include possible difficulties pertaining to proof forwarding from field operations to governance (state-of-the-art unavailable). This indicator is a sub-set of indicator IMF_LOG.1, but can be identical to this one in advanced organizations.

IDB

Indicators of this category provide information on the occurrence of incidents regarding internal deviant behaviours (including especially usurpation of rights or of identity).

information-security-indicators:IDB="UID.1"

User impersonation

A person within the organization impersonates a registered user (employee, partner, contractor, external service provider) using identifier, passwords or authentication devices that had previously been obtained in an illicit manner (using a social engineering technique or not). This measures cases of usurpation for malicious purposes, and not ones that relate to user-friendly usage. Moreover, assumption is made that ID/Password is the main way of authentication

information-security-indicators:IDB="RGH.1"

Privilege escalation by exploitation of software or configuration vulnerability on an externally accessible server

Exploited vulnerabilities are typically tied to the underlying OS that supports the Web application,

exploited notably through injection of additional characters in URL links. This behaviour specifically involves external service providers and company's business partners that wish to access additional information or to launch unlawful actions (for example, service providers seeking information about their competitors). This type of behaviour is less frequent amongst employees, since it is often easier to get the same results by means of social engineering methods.

information-security-indicators:IDB="RGH.2"

Privilege escalation on a server or central application by social engineering

It is often easier to get the same results by means of social engineering methods than with technical means. Help desk teams are often involved in this kind of behaviour.

information-security-indicators:IDB="RGH.3"

```
Use on a server or central application of administrator rights illicitly granted by an
administrator
```

Illicitly granting administrator privileges generally comes from simple errors or more worrisome negligence on the part of the administrators (malicious action is rarer). The case of forgotten temporary rights (see next indicator), is not included in this indicator.

information-security-indicators:IDB="RGH.4"

Use on a server or central application of time-limited granted rights after the planned period

This indicator measures situations where time-limited user accounts (created for training, problem resolution, emergency access, test, etc.) are still in use after the initial planned period.

information-security-indicators:IDB="RGH.5"

Abuse of privileges by an administrator on a server or central application

The motivation of rights usurpation by an administrator is often the desire to breach the confidentiality of sensitive data (for example, human resources data). This indicator is similar to the indicator IDB_RGH.6 (but with consequences that may be however often potentially more serious).

information-security-indicators:IDB="RGH.6"

Abuse of privileges by an operator or a plain user on a server or central application

This indicator applies for example to authorized users having access to personal identifiable information aboutcelebrities with no real need for their job (thereby violating the "right to know").

information-security-indicators:IDB="RGH.7"

Illicit use on a server or central application of rights not removed after departure or position

change within the organization

This indicator also takes into account the problem of generic accounts (whose password might have been changed each time a user knowing this password is leaving organization).

information-security-indicators:IDB="MIS.1"

Server resources misappropriation by an internal source

This indicators measures misappropriation of on-line IT resources for one's own use (personal, association etc.).

information-security-indicators:IDB="IAC.1"

Access to hacking Website

This indicator measures unauthorized access to a hacking Website from an internal workstation

information-security-indicators:IDB="LOG.1"

Deactivating of logs recording by an administrator

This event is generally decided and deployed by an administrator in order to improve performance of the system under his/her responsibility (illicit voluntary stoppage). This indicator is a reduced subset of indicator IUS_RGH.5

IWH

Indicators of this category are indicators that concern all categories of incidents.

information-security-indicators:IWH="VNP.1"

Exploitation of a software vulnerability without available patch

This indicators measures security incidents that are the result of an exploitation of a disclosed software vulnerability that has no available patch (with or without an applied workaround measure). It is used to assess the intensity of the exploitation of recently disclosed software vulnerabilities (zero day or not). Patching here applies only to standard software (excluding bespoke software), and the scope is limited to workstations (OS, browsers and various add-ons and plug-ins, office automation standard software).

information-security-indicators:IWH="VNP.2"

Exploitation of a non-patched software vulnerability

This indicators measures security incidents that are the result of the exploitation of a non-patched software vulnerability though a patch exists. It is used to assess effectiveness or application of patching-related organization and processes and tools (patching not launched). It is linked with indicator VOR_VNP.2 that is intended to assess problems of exceeding the "time limit for the

window of exposure to risks". It has the same limitations as IWH_VNP.1 regarding scope.

information-security-indicators:IWH="VNP.3"

Exploitation of a poorly-patched software vulnerability

This indicator measures security incidents that are the result of the exploitation of a poorly patched software vulnerability. It is used to assess effectiveness of patching-related organization and processes and tools (process launched but patch not operational - Cf. no reboot, etc.). It is linked with indicator VOR_VNP.1, IWH_VNP.1 and IWH_VNP.2. It has the same limitations as IWH_VNP.1 regarding scope.

information-security-indicators:IWH="VCN.1"

Exploitation of a configuration flaw

This indicator measures security incidents that are the result of the exploitation of a configuration flaw on servers or workstations. A configuration flaw should be considered as a nonconformity against state-of-the-art security policy.

information-security-indicators:IWH="UKN.1"

Not categorized security incidents

This indicator measures all types of incidents that are new and/or a complex combination of more basic incidents and cannot be fully qualified and therefore precisely categorized.

information-security-indicators:IWH="UNA.1"

Security incidents on non-inventoried and/or not managed assets

This indicator measures security incidents tied to assets (on servers) non-inventoried and not managed by appointed teams. It is a key indicator insofar as a high percentage of incidents corresponds with this indicator on average in the profession (according to some public surveys).

VBH

Indicators of this category apply to the existence of abnormal behaviours that could lead to security incidents.

information-security-indicators:VBH="PRC.1"

Server accessed by an administrator with unsecure protocols

This indicator measures the use of insecure protocols set up by an administrator to get access to organizationbased externally accessible servers making an external intrusion possible. Insecure protocol means unencrypted, without time-out, with poor authentication means etc. (for example Telnet).

information-security-indicators:VBH="PRC.2"

P2P client in a workstation

This indicator measures the installation of P2P clients set up by a user on its professional workstation with the risk of partial or full sharing of the workstation content. It applies to workstations that are either connected to the organization's network from within the organization or directly connected to the public network from outside (notably home). There is a high risk of accidental sharing (in one quarter of all cases) of files that may host confidential company data. It is most often carried out through HTTP channel (proposed on all of these services).

information-security-indicators:VBH="PRC.3"

VoIP clients in a workstation

This indicator measures VoIP clients installed by a user on his/hers own workstation in order to use a peer-to-peer service. It applies to workstations connected to an organization's network from within the organization or directly connected to the public network from outside (notably home). The associated risk is to exchange dangerous Office documents. It is most often carried out through HTTP channel (proposed on all of these services).

information-security-indicators:VBH="PRC.4"

Outbound connection dangerously set up

This indicator measures outbound connection dangerously set up to get remote access to the company's internal network without using an inbound VPN link and a focal access point with possible exploitation by an external intruder. The outbound connection method consists for example in using a GoToMyPC™ software or a LogMeIn® software or a computer to computer connection in tunnel mode.

information-security-indicators:VBH="PRC.5"

Not compliant laptop computer used to establish a connection

This indicator measures remote or local connection to the organization's internal network from a roaming laptop computer that is organization-owned and is configured with weak parameters. In this situation and in case of the existence of a software to check compliance of roaming computers, another related software blocks the connection in principle and prevents its continuation.

information-security-indicators:VBH="PRC.6"

Other unsecure protocols used

This indicator measures other unsecure or dangerous protocols set up with similar behaviours. The other cases are the other than the 5 previous ones (VBH_PRC.1 to VBH_PRC.5). It relates to dangerous or abusive usages, i.e. situations where usages are not required and where other more secure solutions exist.

information-security-indicators:VBH="IAC.1"

Outbound controls bypassed to access Internet

This indicator measures the detection of Internet access from the internal network by means that bypass the outbound security devices. It primarily relates to Internet accesses from a perimeter area or to tunnelling (SSL port 443) or to straight accesses (via an ADSL link or public Wi-Fi access points and the telephone network) or to accesses via Smartphones connected to the workstation. The main underlying motivation is to prevent user tracking.

information-security-indicators:VBH="IAC.2"

Anonymization site used to access Internet

This indicator measures the detection of anonymous Internet access from an internal workstation through an anonymization site. The goal is to maintain free access and to avoid organization's filtering of accesses to forbidden websites.

information-security-indicators:VBH="FTR.1"

Files recklessly downloaded

This indicator measures the download of files from an external website that is not known (no reputation) within the profession to an internal workstation. "No reputation" can be assessed by information provided by URL outbound filtering devices.

information-security-indicators:VBH="FTR.2"

Personal public instant messaging account used for business file exchanges

This indicator measures the use of personal public instant messaging accounts for business exchanges with outside. This file exchange method has to be avoided due to network AV software bypassing and to identify lesser effectiveness of AV software.

information-security-indicators:VBH="FTR.3"

Personal public messaging account used for business file exchanges

This indicator measures the use of personal public messaging accounts for business file exchanges with the exterior. The risk is to expose information to external attackers.

information-security-indicators:VBH="WTI.1"

Workstations accessed in administrator mode

This indicator measures access to workstations in administrator mode without authorization.

information-security-indicators:VBH="WTI.2"

Personal storage devices used

This indicator measures the use personal storage devices on a professional workstation to input or output information or software. Mobile or removable personal storage devices include USB tokens, smartphones, tablets, etc. It is not applicable to personal devices authorized by security policy (Cf. VBH_WTI.3 and BYOD).

information-security-indicators:VBH="WTI.3"

Personal devices used without compartmentalization (BYOD)

This indicator measures the lack of or the removal of basic security measures meant to compartmentalize professional activities on personal devices. Personal devices (BYOD) include PCs, tablets, smartphones, etc.

information-security-indicators:VBH="WTI.4"

Not encrypted sensitive files exported

This indicator measures the lack of encryption of sensitive files uploaded from a professional workstation to professional mobile or removable storage devices.

information-security-indicators:VBH="WTI.5"

Personal software used

This indicator measures the presence of personal software on a professional workstation that does not comply with the corporate security policy. It corresponds with all types of local unauthorized software (with a user licence or not), such as common personal software (games, office automation etc.) or more dangerous ones (hacking etc.). It should be added that VBH_PRC.2 and VBH_PRC.3 are a share of this indicator, and that this indicator is a subset of VBH_WTI.1.

information-security-indicators:VBH="WTI.6"

Mailbox or Internet access with admin mode

This indicator applies to users using their admin account on a workstation.to access their own mailbox or Internet. This behaviour is particularly dangerous since malware (through attached pieces on email or drive-by download on Web browser) are far easier to install on the workstation in this case.

information-security-indicators:VBH="PSW.1"

Weak passwords used

The required strength of passwords depends on the organization’s security policy, but usable general recommendations in ISO/IEC 27002 [2].

information-security-indicators:VBH="PSW.2"

Passwords not changed

This indicators measures password not changed in due periodic time (case of changes not periodically imposed). Situations in which changes are not periodically imposed by accessed systems themselves remain fairly frequent within organizations (apart from Active Directory), the figure being around 25 % of the cases on average.

information-security-indicators:VBH="PSW.3"

Administrator passwords not changed

This indicators measures password not changed in due periodic time by an administrator in charge of an account used by automated applications and processes (case of changes not periodically imposed). Situations in which changes are not periodically imposed by accessed systems themselves remain fairly frequent within organizations (apart from Active Directory), the figure being around 25 % of the cases on average.

information-security-indicators:VBH="RGH.1"

Not compliant user rights granted illicitly by an administrator

This indicator measures the granting of not compliant user rights by an administrator outside any official procedure. This vulnerability may originate with an error, negligence or malice.

information-security-indicators:VBH="HUW.1"

Human weakness exploited by a spear phishing message meant to entice or appeal to do something possibly harmful to the organization

This vulnerability typically includes clicking on an Internet link or opening an attached document

information-security-indicators:VBH="HUW.2"

```
Human weakness exploited by exchanges meant to entice or appeal to tell some secrets
to be used later
```

This vulnerability applies to discussions through on-line media leading to leakage of personal identifiable information (PII) or various business details to be used later (notably for identity usurpation)

VSW

Indicators of this category apply to the existence of weaknesses in software that could be exploited and lead to security incidents.

information-security-indicators:VSW="WSR.1"

Web applications software vulnerabilities

This indicators measures software vulnerabilities detected in Web applications running on

externally accessible servers.

information-security-indicators:VSW="OSW.1"

OS software vulnerabilities regarding servers

This indicators measures software vulnerabilities detected in OS running on externally accessible servers.

information-security-indicators:VSW="WBR.1"

Web browsers software vulnerabilities

This indicators measures software vulnerabilities detected in Web browsers running on workstations.

VCF

Indicators of this category apply to the existence of weaknesses in the configuration of IT devices that could be exploited and lead to security incidents.

information-security-indicators:VCF="DIS.1"

Dangerous or illicit services on externally accessible servers

This indicator measures the presence of illicit and dangerous system services running on an externally accessible server.

information-security-indicators:VCF="LOG.1"

Insufficient size of the space allocated for logs

Such event could cause an overflow in case of quick series of unusual actions.

information-security-indicators:VCF="FWR.1"

Weak firewall filtering rules

This indicator measures the gaps between the active firewall filtering rules and the security policy.

information-security-indicators:VCF="WTI.1"

Workstation wrongly configured

This indicator measures the use of workstation with a disabled or lacking update AV and/or FW. The lack of update includes signature file older than x days (generally at least 6 days).

information-security-indicators:VCF="WTI.2"

Autorun feature enabled on workstations

This indicator measures the presence of Autorun feature enabled on workstations.

information-security-indicators:VCF="UAC.1"

Access rights configuration not compliant with the security policy

This indicator measures access rights configuration that are not compliant with corporate security policy. This indicator is more reliable in case of existence of a central repository of user rights within organization (and of an IAM achievement)

information-security-indicators:VCF="UAC.2"

Not compliant access rights on logs

This indicator measures non-compliant access rights on logs in servers which are sensitive and/or subject to regulations. This situation representing a key weakness since the necessary high confidence in the produced logs has been reduced to nothing. This indicator is a subset of VCF_UAC.1.

information-security-indicators:VCF="UAC.3"

Generic and shared administrator accounts

This indicator measures generic and shared administration accounts that are unnecessary or accounts that are necessary but without patronage. It concerns operating systems, databases and applications.

information-security-indicators:VCF="UAC.4"

Accounts without owners

This indicator measures accounts without owners that have not been erased. These are accounts that have no more assigned users (for example after internal transfer or departure of the users from organization).

information-security-indicators:VCF="UAC.5"

Inactive accounts

This indicator measures accounts inactive for at least 2 months that have not been disabled. These accounts are not used by their users due to prolonged but not definitive absence (long term illness, maternity, etc.), with the exclusion of messaging accounts (which should remain accessible to users from their home).

VTC

Indicators of this category measure the existence of weaknesses in the IT and physical architecture that could be exploited and lead to security incidents.

information-security-indicators:VTC="BKP.1"

Malfunction of server-hosted sensitive data safeguards

On servers hosting sensitive data with respect to availability, it concerns malfunctions of safeguards due to lack of periodic testing. This kind of event may be very serious since usually put trust is betrayed in a critical function.

information-security-indicators:VTC="IDS.1"

Full unavailability of IDS/IPS

Many causes are possible, including deliberate disconnection by a network administrator (to streamline operations or since IDS/IPS output is deemed too difficult to use), unwitting disconnection (error by a network administrator), breakdown, software malfunction, etc.

information-security-indicators:VTC="WFI.1"

Wi-Fi devices installed on the network without any official authorization

Many causes are possible, including for example local decisions for easier access of mobile users, rogue user behaviours or workstations configured as access points.

information-security-indicators:VTC="RAP.1"

Remote access points used to gain unauthorized access

This indicator is interesting to assess whether such accesses are localized (local areas, countries, etc.) or involve the whole organization or are increasing and spreading to whole organization.

information-security-indicators:VTC="NRG.1"

Devices or servers connected to the organization’s network without being registered and managed

According to some convergent studies, this event may be at the origin of some 70 % of all security incidents associated to malice.

information-security-indicators:VTC="PHY.1"

Not operational physical access control means

This indicator includes access to protected internal areas. The 1st cause is the lack of effective control of users at software level. The 2nd cause is hardware breakdown of a component in the chain.

VOR

Indicators of this category measure the existence of weaknesses in the organization that could be exploited and lead to security incidents.

information-security-indicators:VOR="DSC.1"

Discovery of attacks

This indicator measures stealthy security incidents difficult to detect. As most studies show, the time to discovery is often several months, time frame especially used to steal sensitive data. Incidents taken into account here are IEX_INT.3, IEX_MLW.3 and IEX_MLW.4. This indicator give landmarks regarding what may be deemed excessive, i.e. with an assumption which is above one week.

information-security-indicators:VOR="VNP.1"

Excessive time of window of risk exposure

This indicator measures situations in which the time of the window of risk exposure exceeds the time limit expressed in security policy. The window of risks exposure is the period of time between the public disclosure of a software vulnerability and the actual and checked application of a patch that corresponds with the vulnerability's remediation (independently of the time needed for the vendor to provide the patch). This indicator only applies to workstations (OS, application software and browsers), and to critical vulnerabilities (as publicly determined via the CVSS scale) that require an action as quickly as possible.

information-security-indicators:VOR="VNP.2"

Rate of not patched systems

This indicator measures the rate of not patched systems for detected critical software vulnerabilities (see VOR_VNP.1 for criticality definition). Not patched systems to be taken into account are the ones which are not patched beyond the time limit defined in security policy. This indicator only applies to workstations (OS, application software and browsers).

information-security-indicators:VOR="VNR.1"

Rate of not reconfigured systems

This indicator measures the rate of not reconfigured systems for detected critical configuration vulnerabilities. Configuration vulnerabilities are either non-conformities relative to a level 3 security policy, or discrepancies relative to a state-of-the-art available within the profession (and that can correspond with a configuration master produced by a vendor and applied within the organization). This indicator only applies to workstations (OS, application software and browsers). Not reconfigured systems to be taken into account are the ones which are not reconfigured beyond the time limit defined in security policy.

information-security-indicators:VOR="RCT.1"

Reaction plans launched without experience feedback

This indicator applies to plans for responding to incidents formalized in security policy launched without experience feedback.

information-security-indicators:VOR="RCT.2"

Reaction plans unsuccessfully launched

This indicator measures failure in the performance of plans, leading to non-recovery of incidents and to subsequent possible launch of an escalation procedure.

information-security-indicators:VOR="PRT.1"

Launch of new IT projects without information classification

This indicator measures the launch of new IT projects without information classification. Availability of a classification model and scheme within the organization would make easier this task.

information-security-indicators:VOR="PRT.2"

Launch of new specific IT projects without risk analysis

This indicator measures the launch of new specific IT projects without performing a full risk analysis.

information-security-indicators:VOR="PRT.3"

```
Launch of new IT projects of a standard type without identification of vulnerabilities
and threats
```

This indicator measures the launch of new IT projects of a standard type without identification of vulnerabilities and threats and of related security measures. For these IT projects, potential implementation of a simplified risk analysis method or of pre-defined security profiles can be applied.

IMP

Indicators as regards impact measurement.

information-security-indicators:IMP="COS.1"

Average cost to tackle a critical security incident

The average cost taken into account includes the following kinds of overhead: disruption to

business operations (increased operating costs, etc.), fraud (money, etc.) and incident recovery costs (technical individual time, asset replacement, etc.). It does not include possible (generally very heavy) breach notification costs to customers and enforcement bodies (according to US and recently EU laws or regulations).

information-security-indicators:IMP="TIM.1"

Average time of Websites downtime due to whole security incidents

Applies to all 4 classes, but main security incidents concerned are malfunctions or breakdowns (software or hardware), DoS or DDoS attacks and Website defacements.

information-security-indicators:IMP="TIM.2"

Average time of Websites downtime due to successful malicious attacks

This indicator is a subset of the previous one (IMP_TIM.1) focusing on 3 possible classes (IEX, IUS, IMD).

information-security-indicators:IMP="TIM.3"

Average time of Websites downtime due to malfunctions or unintentional security incidents

This indicator is a subset of IMP_TIM.1 focusing on one class (IMF).

interactive-cyber-training-audience

interactive-cyber-training-audience namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Describes the target of cyber training and education.

sector

The sector from which the audience comes determines the nature of the training.

interactive-cyber-training-audience:sector="academic-school"

Academic - School

The focus is on the principles underlying cybersecurity, ranging from theoretical to applied, at school level.

interactive-cyber-training-audience:sector="academic-university"

Academic - University

The focus is on the principles underlying cybersecurity, ranging from theoretical to applied, at university level.

interactive-cyber-training-audience:sector="public-government"

Public - Government

In public sector such as government, Cybersecurity is seen as tool to protect the public interest. Hence, it emphasizes on developing policies and systems to implement laws and regulations.

interactive-cyber-training-audience:sector="public-authorities"

Public - Authorities

In public sector such as authorities, Cybersecurity is seen as tool to protect the public interest. Hence, it emphasizes on developing policies and systems to implement laws and regulations.

interactive-cyber-training-audience:sector="public-ngo"

Public - NGO

In public sector such as NGO, Cybersecurity is seen as tool to protect the public interest. Hence, it emphasizes on developing policies and systems to implement laws and regulations.

interactive-cyber-training-audience:sector="public-military"

Public - Military

In public sector such as military sector, Cybersecurity is seen as tool to protect the public interest. Hence, it emphasizes on developing policies and systems to implement laws and regulations.

interactive-cyber-training-audience:sector="private"

Private

The private sector and industry focuses more on protecting its investments. The effectiveness of security mechanisms and people are more important than principles they embody.

purpose

Purpose answered the question for which reason trainings should be used.

interactive-cyber-training-audience:purpose="awareness"

Awareness

This training should be used to raise the awareness in multiple and different security threats.

interactive-cyber-training-audience:purpose="skills"

Skills

This training should be used to recognize the different skill levels of the participants so that can they be improved in a targeted manner.

interactive-cyber-training-audience:purpose="collaboration"

Collaboration

This training should be used to improve the cooperation within a team or beyond.

interactive-cyber-training-audience:purpose="communication"

Communication

This training should be used to increase the efficiency of internal and external communication in case of an incident.

interactive-cyber-training-audience:purpose="leadership"

Leadership

This training should be used to improve the management and coordination of the responsible entities.

proficiency-level

Proficiency describes the knowledge of users and what they are able to do.

interactive-cyber-training-audience:proficiency-level="beginner"

Beginner

The lowest level. Beginner are limited in abilities and knowledge. They have the possibility to use foundational conceptual and procedural knowledge in a controlled and limited environment. Beginners cannot solve critical tasks and need significant supervision. They are able to perform daily processing tasks. The focus is on learning.

interactive-cyber-training-audience:proficiency-level="professional"

Professional

The mid level. Professionals have deeper knowledge and understanding in specific sectors. For these sectors they are able to complete tasks as requested. Sometimes supervision is needed but usually they perform independently. The focus is on enhancing and applying existing knowledge.

interactive-cyber-training-audience:proficiency-level="expert"

Expert

The highest level. Experts have deeper knowledge and understanding in different sectors. They complete tasks self-dependent and have the possibilities to achieve goals in the most effective and efficient way. Experts have comprehensive understanding and abilities to lead and train others. The focus is on strategic action.

target-audience

Target audience describes the audience, which is targeted by the training.

interactive-cyber-training-audience:target-audience="student-trainee"

Student/Trainee

Student and trainees have little to none practical knowledge. Training can be used for students and trainees, to enhance their knowledge and to practice theoretical courses.

interactive-cyber-training-audience:target-audience="it-user"

IT User

IT users use the IT but have little to none knowledge about IT security. Users can get trained to understand principles of IT security and to grow awareness.

interactive-cyber-training-audience:target-audience="it-professional"

IT Professional

Professionals have little to medium knowledge about IT security. Their professional focus is in specific sectors, therefore, they receive IT security knowledge for their sectors.

interactive-cyber-training-audience:target-audience="it-specialist"

IT Specialist

Specialists already have a comprehensive knowledge in IT security. Therefore, the training is focussed on specific aspects.

interactive-cyber-training-audience:target-audience="management"

Management

Management has little knowledge about IT security, but a broad overview. By the training, management can understand changed settings better.

interactive-cyber-training-technical-setup

interactive-cyber-training-technical-setup namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The technical setup consists of environment structure, deployment, and orchestration.

environment-structure

The environment structure refers to the basic characteristic of the event.

interactive-cyber-training-technical-setup:environment-structure="tabletop-style"

Tabletop Style

A session that involves the movement of counters or other objects round a board or on a flat surface

interactive-cyber-training-technical-setup:environment-structure="online-collaboration-platform"

Online Platform - Collaboration Platform

The environment allows organizations to incorporate real-time communication capabilities and providing remote access to other systems. This includes the exchange of files and messages in text, audio, and video formats between different computers or users.

interactive-cyber-training-technical-setup:environment-structure="online-e-learning-platform"

Online Platform - E-Learning Platform

A software application for the administration, documentation, tracking, reporting, and delivery of educational courses, training programs, or learning and development programs.

interactive-cyber-training-technical-setup:environment-structure="hosting"

Hosting

A cyber training based on single hosts uses primarily a personal computer to providing tasks and challenges for a user. It allows a direct interaction with the systems.

interactive-cyber-training-technical-setup:environment-structure="simulated-network-infrastructure"

Network Infrastruture - Simulated

Dependent of the realization type, a network-based environment consists of servers and clients, which are connected to each other in a local area network (LAN) or wide area network (WAN). A simulation copies the network components from the real world into a virtual environment. It provides an idea about how something works. It simulates the basic behavior but does not necessarily abide to all the rules of the real systems.

interactive-cyber-training-technical-setup:environment-structure="emulated-network-infrastructure"

Network Infrastruture - Emulated

Dependent of the realization type, a network-based environment consists of servers and clients, which are connected to each other in a local area network (LAN) or wide area network (WAN). An emulator duplicates things exactly as they exist in real life. The emulation is effectively a complete imitation of the real thing. It operates in a virtual environment instead of the real world.

interactive-cyber-training-technical-setup:environment-structure="real-network-infrastructure"

Network Infrastruture - Real

Dependent of the realization type, a network-based environment consists of servers and clients, which are connected to each other in a local area network (LAN) or wide area network (WAN). In a real network infrastructure, physical components are used to connect the systems and to setup a scenario.

deployment

The environment of cyber training can either be deployed on premise or on cloud infrastructures

interactive-cyber-training-technical-setup:deployment="physical-on-premise"

On Premise - Physical

The environment for the training run on physical machines. The data is stored locally and not on cloud; nor is a third party involved. The advantages of on premise solutions are the physical accessibility, which makes it possible to use the complete range of cyber challenges.

interactive-cyber-training-technical-setup:deployment="virtual-on-premise"

On Premise - Virtual

The environment for the training run virtual machines. The data is stored locally and not on cloud; nor is a third party involved. The benefit of virtual machines is the maximum of configurability. The advantages of on premise solutions are the physical accessibility, which makes it possible to use the complete range of cyber challenges.

interactive-cyber-training-technical-setup:deployment="cloud"

Cloud

Training setup deployed in the cloud has on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. In contrast to on premise setups, cloud solutions are rapid elastic on request. So the training can be adapted flexible on a large amount of users and is easily usable world wide.

orchestration

The composition of parts and components of a pool of tasks. The goal is to setup a holistic scenario and integrate cyber training session. Furthermore, it includes a declarative description of the overall process in the form of a composite and harmonic collaboration.

interactive-cyber-training-technical-setup:orchestration="none-automation"

None Automation

Specifies the automation of processes and the amount of human interaction with the system to maintain and administrate, especially for repetitive exercise; Here none automation is present.

interactive-cyber-training-technical-setup:orchestration="partially-automation"

Partially Automation

Specifies the automation of processes and the amount of human interaction with the system to maintain and administrate, especially for repetitive exercise; Here partially automated.

interactive-cyber-training-technical-setup:orchestration="complete-automation"

Complete Automation

Specifies the automation of processes and the amount of human interaction with the system to maintain and administrate, especially for repetitive exercise; Here full-automated.

interactive-cyber-training-technical-setup:orchestration="portability-miscellaneous"

Portability - Miscellaneous

Miscellaneous approaches are used to ensure the possibility to exchange data, challenges, or entire scenarios to other environments or locations.

interactive-cyber-training-technical-setup:orchestration="portability-exchangenable-format"

Portability - Exchangenable Format

Common data format (YALM, XML, JSON, ...) is used to ensure the possibility to exchange data, challenges, or entire scenarios to other environments or locations.

interactive-cyber-training-technical-setup:orchestration="maintainability-modifiability"

Maintability - Modifiability

Maintainability represents effectiveness and efficiency with which a session can be modified or adapted to changes.

interactive-cyber-training-technical-setup:orchestration="maintainability-modularity"

Maintability - Modularity

A modular concept has advantages in reusability and combinability.

interactive-cyber-training-technical-setup:orchestration="compatibility"

Compatibility

The Compatibility deals with the technical interaction possibilities via interfaces to other applications, data, and protocols.

interactive-cyber-training-training-environment

interactive-cyber-training-training-environment namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The training environment details the environment around the training, consisting of training type and scenario.

training-type

Education in cybersecurity follows different approaches. The level of interaction and hands-on experience distinguishes different types of training.

interactive-cyber-training-training-environment:training-type="tabletop-game-speech"

Tabletop Game - Speech

Table Top training -here based on speech-only- are a lightweight, but intellectually intense exercise. In this setting, the involved teams or participants focus on opposing missions. On a theoretical basis, the teams develop different strategies and countermeasures to explore the offensive cyber effects on operations.

interactive-cyber-training-training-environment:training-type="tabletop-game-text"

Tabletop Game - text

Table Top training -here based on text-only- are a lightweight, but intellectually intense exercise. In this setting, the involved teams or participants focus on opposing missions. On a theoretical basis, the teams develop different strategies and countermeasures to explore the offensive cyber effects on operations.

interactive-cyber-training-training-environment:training-type="tabletop-game-multimedia"

Tabletop Game - Multimedia

Table Top training -here based on multimedia- are a lightweight, but intellectually intense exercise. In this setting, the involved teams or participants focus on opposing missions. On a theoretical basis, the teams develop different strategies and countermeasures to explore the offensive cyber effects on operations.

interactive-cyber-training-training-environment:training-type="capture-the-flag-quiz"

Capture the Flag - Quiz

Capture the Flag (CTF) is a well-known cybersecurity contest in which participants compete in real-time, which can exists as a quiz.

interactive-cyber-training-training-environment:training-type="capture-the-flag-jeopardy"

Capture the Flag - Jeopardy

Capture the Flag (CTF) is a well-known cybersecurity contest in which participants compete in real-time, which can exists as jeopardy.

interactive-cyber-training-training-environment:training-type="capture-the-flag-attack"

Capture the Flag - Attack

Capture the Flag (CTF) is a well-known cybersecurity contest in which participants compete in real-time, which can exists as an attack-only scenario.

interactive-cyber-training-training-environment:training-type="capture-the-flag-defence"

Capture the Flag - Defence

Capture the Flag (CTF) is a well-known cybersecurity contest in which participants compete in real-time, which can exists as an defence-only scenario.

interactive-cyber-training-training-environment:training-type="capture-the-flag-attack-defence"

Capture the Flag - Attack-Defence

Capture the Flag (CTF) is a well-known cybersecurity contest in which participants compete in real-time, which can exists as an attack-defence scenario.

interactive-cyber-training-training-environment:training-type="cyber-training-range-classroom-practice"

Cyber Training Range - Classroom Practice

A cyber range provides an environment to practice network operation skills. It should represent real-world scenarios and offer isolation from other networks to contain malicious activity. In this training type, complex attacks take place in a simulated environment. The participants perform divers educational hands-on activities according to their role. In these trainings the roles that are not covered by participants are simulated or covered by the instructors. Trainings can be classroom practice.

interactive-cyber-training-training-environment:training-type="cyber-training-range-single-team-training"

Cyber Training Range - Single Team Training

A cyber range provides an environment to practice network operation skills. It should represent real-world scenarios and offer isolation from other networks to contain malicious activity. In this training type, complex attacks take place in a simulated environment. The participants perform divers educational hands-on activities according to their role. In these trainings the roles that are not covered by participants are simulated or covered by the instructors. Trainings can be single team trainings.

interactive-cyber-training-training-environment:training-type="cyber-training-range-multiple-team-training"

Cyber Training Range - Multiple Team Training

A cyber range provides an environment to practice network operation skills. It should represent real-world scenarios and offer isolation from other networks to contain malicious activity. In this training type, complex attacks take place in a simulated environment. The participants perform divers educational hands-on activities according to their role. In these trainings the roles that are not covered by participants are simulated or covered by the instructors. Trainings can be multiple team trainings.

interactive-cyber-training-training-environment:training-type="project-approach"

Project Approach

In this type of training, hands-on projects are to be completed during the training. Thereby, the participants learn and understand the basic concepts of security. During the projects, the teachers can intervene and control the learning process.

scenario

The scenario is a main component of cybersecurity training. Scenarios are needed to reach the goal of the training.

interactive-cyber-training-training-environment:scenario="supervised"

Supervision: Supervised

Describes if the training is supervised. For instance, cyber range trainings are typically supervised.

interactive-cyber-training-training-environment:scenario="unsupervised"

Supervision: Unsupervised

Describes if the training is unsupervised. For instance, jeopardy CTF are usually unsupervised.

interactive-cyber-training-training-environment:scenario="free-multiple-choice"

Style: Free-/Multiple Choice

Decribes the challenges within the training as Free-/Multi Choice. (can be the case with CTFs)

interactive-cyber-training-training-environment:scenario="problem-driven"

Style: Problem-Driven

Describes the challenge within the training as Problem-driven.

interactive-cyber-training-training-environment:scenario="storyline-driven"

Style: Storyline-Driven

Describes the challenge within the training as Storyline-driven.

interactive-cyber-training-training-environment:scenario="challenges-target-network"

Challenges: Network Target

The target in this challenge is network.

interactive-cyber-training-training-environment:scenario="challenges-target-host"

Challenges: Host Target

The target in this challenge is host.

interactive-cyber-training-training-environment:scenario="challenges-target-application"

Challenges: Application Target

The target in this challenge is application.

interactive-cyber-training-training-environment:scenario="challenges-target-protocol"

Challenges: Protocol Target

The target in this challenge is protocol.

interactive-cyber-training-training-environment:scenario="challenges-target-data"

Challenges: Data Target

The target in this challenge is data.

interactive-cyber-training-training-environment:scenario="challenges-target-person"

Challenges: Person Target

The target in this challenge is person.

interactive-cyber-training-training-environment:scenario="challenges-target-physical"

Challenges: Physical Target

The target in this challenge is physical.

interactive-cyber-training-training-environment:scenario="challenges-type-foot-printing"

Challenges: Foot-printing Type

Foot-printing is needed to solve this challenge.

interactive-cyber-training-training-environment:scenario="challenges-type-scanning"

Challenges: Scanning Type

Scanning is needed to solve this challenge.

interactive-cyber-training-training-environment:scenario="challenges-type-enumeration"

Challenges: Enumeration Type

Enumeration is needed to solve this challenge.

interactive-cyber-training-training-environment:scenario="challenges-type-pivoting"

Challenges: Pivoting Type

Pivoting is needed to solve this challenge.

interactive-cyber-training-training-environment:scenario="challenges-type-exploitation"

Challenges: Exploitation Type

Exploitation is needed to solve this challenge.

interactive-cyber-training-training-environment:scenario="challenges-type-privilege-escalation"

Challenges: Privilege escalation Type

Privilege escalation is needed to solve this challenge.

interactive-cyber-training-training-environment:scenario="challenges-type-covering-tracks"

Challenges: Covering tracks Type

Covering tracks is needed to solve this challenge.

interactive-cyber-training-training-environment:scenario="challenges-type-maintaining"

Challenges: maintaining Type

Maintaining access is needed to solve this challenge.

interactive-cyber-training-training-setup

interactive-cyber-training-training-setup namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The training setup further describes the training itself with the scoring, roles, the training mode as well as the customization level.

scoring

Scoring is not only used in competition-oriented training like CTF but also to motivate participants, give feedback, track the progress. The scoring can be based, but is not limited to monitoring systems, defined objectives, or over-the-shoulder evaluation mechanisms.

interactive-cyber-training-training-setup:scoring="no-scoring"

No Scoring

The training have no type of scoring.

interactive-cyber-training-training-setup:scoring="assessment-static"

Assessment: Static

The scoring in this variant relies on the static setting of different scores for tasks and objectives, possibly incluing a degree of difficulty as well.

interactive-cyber-training-training-setup:scoring="assessment-dynamic"

Assessment: Dynamic

The scoring in this variant is set dynamically using mathematical functions or dynamic methods such as teh Elo Rating System.

interactive-cyber-training-training-setup:scoring="awarding-manual"

Awarding: Manual

Awards are given manually.

interactive-cyber-training-training-setup:scoring="awarding-automatic"

Awarding: Automatic

Awards are given automatically.

interactive-cyber-training-training-setup:scoring="awarding-mixed"

Awarding: Mixed

Awards are given manually and/or automatically.

roles

Participants in a training are split in different teams, according to their skills, role and tasks.

interactive-cyber-training-training-setup:roles="no-specific-role"

No specific Role

Individuals who do not fit into the defined teams can be assigned to this role.

interactive-cyber-training-training-setup:roles="transparent-team-observer-watcher"

Transparent Team - Observer/Watcher

Members of this team observe the training. Usually, these people have a defined purpose, but have no influence on the training itself. Possible purposes are learning about the training topic and roles, studying strategies of participants, or supervising employees.

interactive-cyber-training-training-setup:roles="white-team-trainer-instructor"

White Team - Trainer/Instructor

This team consists of instructors, referees, organizers, and training managers. They design the training scenario including objectives, rules, background story, and tasks. During the training, this team controls the progress and assigns tasks to the teams. These so-called injects also include simulated media, operation coordination, or law enforcement agencies. Giving hints for the

training teams could also be part of this team.

interactive-cyber-training-training-setup:roles="green-team-organizer-admin"

Green Team - Organizer/Admin

The operators that are responsible for the exercise infrastructure build this team. Before a training, this team sets up and configures the environment and takes it down afterwards. During a training, it also monitors the environments health and handles problems that may arise.

interactive-cyber-training-training-setup:roles="red-team-attacker"

Red Team - Attacker

This team consists of people authorized and organized to model security adversaries. They are responsible to identify and exploit potential vulnerabilities present in the training environment. Depending on the training environment, the tasks can follow a predefined attack path.

interactive-cyber-training-training-setup:roles="blue-team-defender"

Blue Team - Defender

The group of individuals that is responsible for defending the training environment. They deal with the red team's attacks and secure the compromised networks. Guidelines for that team are the training rules and local cyber law.

interactive-cyber-training-training-setup:roles="gray-team-bystander"

Gray Team - Bystander

Bystanders of a training form this team. They do not necessarily have a specific intention or purpose, but an interest in the training event itself. It is also possible that this team interacts with participants and thereby unintentionally influences the training.

interactive-cyber-training-training-setup:roles="yellow-team-insider"

Yellow Team - Insider

Members of this team perform not only tasks like generating legitimate network traffic and user behavior but also perform erroneous actions that lead to vulnerabilities and attacks. This team can also include the regular system builders, like programmers, developers, and software engineers and architects.

interactive-cyber-training-training-setup:roles="purple-team-bridge"

Purple Team - Bridge

In a training, this team is a bridge between red and blue teams that helps to improve the performance of both. Through joint red-blue activities it improves the scope of the training

participants. Goals are to maximize the Blue Teams capability and the effectiveness of Red Teams activities.

training-mode

Defines whether the training opposes singles persons, teams or groups.

interactive-cyber-training-training-setup:training-mode="single"

Single

A single player plays against others. Others can be real persons, butalso scripted opponents.

interactive-cyber-training-training-setup:training-mode="team"

Team

A team plays against others. In this alignments, each player can bring its expertise into the training, focussing on different aspects. Examples are Blue and Red Teams.

interactive-cyber-training-training-setup:training-mode="cross-group"

Cross-Group

A group plays against others. In this setting, the group members might not know each other. Example are CTF competitions and training for the entire organization in a breach scenario.

customization-level

Defines the level of customization of the training.

interactive-cyber-training-training-setup:customization-level="general"

General

A general purpose training setup is not, or only little customized. This variant is suited for an entry level training or to learn about general processes without regard to the underlying setup.

interactive-cyber-training-training-setup:customization-level="specific"

Specific

The training setup can be customized for a specific training goal or target audience. Examples for this variant are specific trainings within the High School education or for the health sector.

interactive-cyber-training-training-setup:customization-level="individual"

Individual

The most tailored variant is an individual customization. Hereby, the training setup corresponds to a real environment in the best possible way. Exemplary uses of this variant are the training of teams in their environment or the training of new expert-level employees.

interception-method

interception-method namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The interception method used to intercept traffic.

man-in-the-middle

Interception where an attacker secretly relayed and possibly altered the communication between two parties.

interception-method:man-in-the-middle

Man-in-the-middle

Interception where an attacker secretly relayed and possibly altered the communication between two parties.

man-on-the-side

Interception where an attacker could read and send messages between two parties but not alter messages.

interception-method:man-on-the-side

Man-on-the-side

Interception where an attacker could read and send messages between two parties but not alter messages.

passive

Interception where an attacker could read messages between two parties.

interception-method:passive

Passive

Interception where an attacker could read messages between two parties.

search-result-poisoning

Interception where an attacker creates malicious websites intended to show up in search engine queries.

interception-method:search-result-poisoning

Search result poisoning

Interception where an attacker creates malicious websites intended to show up in search engine queries.

dns

Interception where domain name resolution is altered to re-direct traffic to a malicious IP address.

interception-method:dns

Dns

Interception where domain name resolution is altered to re-direct traffic to a malicious IP address.

host-file

Interception where the HOSTS file is modified to re-direct traffic to a malicious IP address.

interception-method:host-file

Host file

Interception where the HOSTS file is modified to re-direct traffic to a malicious IP address.

other

Other.

interception-method:other

Other

Other.

ioc

ioc namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

An IOC classification to facilitate automation of malicious and non malicious artifacts

artifact-state

ioc:artifact-state="malicious"

Malicious

ioc:artifact-state="not-malicious"

Not Malicious

iot

iot namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Internet of Things taxonomy, based on IOT UK report https://iotuk.org.uk/wp-content/uploads/2017/01/IOT-Taxonomy-Report.pdf

TCom

IoT projects vary tremendously in terms of their technical sophistication. Digital Catapult has developed a scale based on technology complexity (TCom) that enables us to understand the state of IoT in the UK, and to assess what is currently being researched, trialled or deployed in real-life implementations.

iot:TCom="0"

Unidentiable object

Dumb/passive objects . Not connected, identified or monitored. Example: Any unconnected, unidentified object

iot:TCom="1"

Identifiable object

Identifiable dumb/passive objects with a virtual existence that can meaningfully be counted/tracked by online systems. Examples: RFID Tags, barcoded or QR-coded objects

iot:TCom="2"

Connected object

Connected objects . Objects linked to an IP network, with some means of reading, programming or controlling them . These should be counted as elements within the IoT universe, but they are often

underused assets. Examples: Printers, doorbells, IP connected fire alarms or security systems

iot:TCom="3"

Connected homogeneous object

Connected broadly homogeneous objects in a simple integrated system, whether the benefit of that system accrues to the end user or the system provider. Examples: Networks of multiple temperature sensors within a single building or campus . Environmental monitoring networks, wearable devices (such as Fitbit or other wellness technologies)

iot:TCom="4"

Connected heterogeneous objects

Connected heterogeneous objects in a single, integrated system . This involves taking data from a variety of sensors of different types, all deployed for the same end user or organisation to help improve processes, make better decisions or change outcomes. Examples: The deployment of a range of sensors in a care home or hospital or the combination of parking, traffic volume and traffic control data in an urban road management system

iot:TCom="5"

Different objects in similar domain

Different objects deployed across multiple interconnected systems for multiple organisations, in multiple locations, all within a similar domain .System supports analysis of aggregated data derived from all deployment locations. Examples: Partnering university campuses' security cameras, fire alarms, temperature sensors, access control systems and energy monitoring systems integrated into a single unified control and monitoring solution

iot:TCom="6"

Different objects in multiple connected domains

As for TCom 5, but where multiple domains are connected . This involves gathering data from a variety of sensor types, across a variety of systems and ecosystems, and creating combined views of the data that offer new sources of value (economic or social) or where there is a high degree of automation across homogeneous systems. Examples: Smart cities where multiple organisations, or different city departments and their partners, have built applications that draw on diverse sets of data from multiple sources to develop or improve services. Such applications might include the adjustment of street lighting in response to incoming data on night-time police activity levels, or the adjustment of traffic lights in response to real-time data sources about local environment data, or current people movement data based on mobile phone location data. Or, in the second case, the automated adjustment of environmental controls across a service provider's care estate based on real-time data feeds from sensors deployed in those settings .

iot:TCom="7"

Involves multiple ecosystems and a high degree of automation

As for TCom 6, but involving both multiple ecosystems and a high degree of automation. Examples: A smart city solution drawing data from multiple providers and sources, which is then used for automated traffic control and routing of emergency services, or the automated adjustment of traffic lights based on real-time mobile phone location data

SSL

A second characteristic of an IoT system concerns the inherent level of safety, privacy and security of that system. At one end of the spectrum, an IoT system may not gather data that is sensitive either in terms of safety or privacy, while at the other it may collect data about identifiable individuals or groups of individuals, involve financial transactions, or access to system data or have the ability to control objects that could compromise health, safety or security.

iot:SSL="0"

No data involved

No data involved, no control of the system

iot:SSL="1"

No sensitive data involved

No sensitive data involved, no control of the objects in the system. Example: Wireless doorbell

iot:SSL="2"

Anonymous or aggregated data

System provides anonymous, aggregated statistics, no control of the system. Example: Remote temperature sensors

iot:SSL="3"

Sensitive data

System generates sensitive data or supports some degree of remote control of the system objects. Examples: Biometric data, door actuation mechanisms

iot:SSL="4"

Connects with external systems

System generates sensitive data, supports some degree of remote control of the system objects and connects with external systems. Examples: Integrated facilities management systems, tele-health monitoring, security and safety systems

DSL

A third characteristic of IoT systems concerns the degree of sharing of sensitive data between the object and the system, and subsequently between the system and the system operator(s) or participants, and third parties. Systems do not always need to share data, so IoT product, platform, service and system designers must be clear about when data is shared, what is shared and why.

Exclusive flag set which means the values or predicate below must be set exclusively.

iot:DSL="0"

No data shared

No data is shared. Examples: Simple point-to-point monitoring systems such as consumer weather stations and wireless doorbells

iot:DSL="1"

Sharing between two parties

Basic sharing between two parties: agreed sharing of sensitive data between the customer/buyer/user and the seller or provider (whether that seller or provider operates in the commercial or public sector). Examples: Cloud-based security systems, remote cameras, home monitoring systems

iot:DSL="2"

Third-party sharing

Third person sharing: sharing of sensitive data between the seller or provider and unrelated third parties in a commercial context. Examples: Person tracking information to support targeted marketing offers

iot:DSL="3"

Multi-domain sharing

Multi-domain and third-party sharing: sharing of sensitive data between the customer/buyer/user and multiple sellers or providers involved in delivering services, where those providers come from different ecosystems (including the commercial and public sectors). Examples: The aggregation of parking, traffic and environmental data in an urban traffic management application

iot:DSL="4"

Open access to sensitive data

Open access to sensitive data, including data generated through use of public finance or infrastructure. Examples: Integration of multiple security systems in a public safety context

kill-chain

kill-chain namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Cyber Kill Chain, a phase-based model developed by Lockheed Martin, aims to help categorise and identify the stage of an attack.

Reconnaissance

kill-chain:Reconnaissance

Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.

Weaponization

kill-chain:Weaponization

Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.

Delivery

kill-chain:Delivery

Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by APT actors, as observed by the Lockheed Martin Computer Incident Response Team (LM-CIRT) for the years 2004-2010, are email attachments, websites, and USB removable media.

Exploitation

kill-chain:Exploitation

After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

Installation

kill-chain:Installation

Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.

Command and Control

kill-chain:Command and Control

Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have 'hands on the keyboard' access inside the target environment.

Actions on Objectives

kill-chain:Actions on Objectives

Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.

maec-delivery-vectors

maec-delivery-vectors namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Vectors used to deliver malware based on MAEC 5.0

maec-delivery-vector

maec-delivery-vectors:maec-delivery-vector="active-attacker"

active Attacker

maec-delivery-vectors:maec-delivery-vector="auto-executing-media"

auto-executing-media

maec-delivery-vectors:maec-delivery-vector="downloader"

downloader

maec-delivery-vectors:maec-delivery-vector="dropper"

dropper

maec-delivery-vectors:maec-delivery-vector="email-attachment"

email-attachment

maec-delivery-vectors:maec-delivery-vector="exploit-kit-landing-page"

exploit-kit-landing-page

maec-delivery-vectors:maec-delivery-vector="fake-website"

fake-website

maec-delivery-vectors:maec-delivery-vector="janitor-attack"

janitor-attack

maec-delivery-vectors:maec-delivery-vector="malicious-iframes"

malicious-iframes

maec-delivery-vectors:maec-delivery-vector="malvertising"

malvertising

maec-delivery-vectors:maec-delivery-vector="media-baiting"

media-baiting

maec-delivery-vectors:maec-delivery-vector="pharming"

pharming

maec-delivery-vectors:maec-delivery-vector="phishing"

phishing

maec-delivery-vectors:maec-delivery-vector="trojanized-link"

trojanized-link

maec-delivery-vectors:maec-delivery-vector="trojanized-software"

trojanized-software

maec-delivery-vectors:maec-delivery-vector="usb-cable-syncing"

usb-cable-syncing

maec-delivery-vectors:maec-delivery-vector="watering-hole"

watering-hole

maec-malware-behavior

maec-malware-behavior namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Malware behaviours based on MAEC 5.0

maec-malware-behavior

maec-malware-behavior:maec-malware-behavior="access-premium-service"

access-premium-service

maec-malware-behavior:maec-malware-behavior="autonomous-remote-infection"

autonomous-remote-infection

maec-malware-behavior:maec-malware-behavior="block-security-websites"

block-security-websites

maec-malware-behavior:maec-malware-behavior="capture-camera-input"

capture-camera-input

maec-malware-behavior:maec-malware-behavior="capture-file-system-data"

capture-file-system-data

maec-malware-behavior:maec-malware-behavior="capture-gps-data"

capture-gps-data

maec-malware-behavior:maec-malware-behavior="capture-keyboard-input"

capture-keyboard-input

maec-malware-behavior:maec-malware-behavior="capture-microphone-input"

capture-microphone-input

maec-malware-behavior:maec-malware-behavior="capture-mouse-input"

capture-mouse-input

maec-malware-behavior:maec-malware-behavior="capture-printer-output"

capture-printer-output

maec-malware-behavior:maec-malware-behavior="capture-system-memory"

capture-system-memory

maec-malware-behavior:maec-malware-behavior="capture-system-network-traffic"

capture-system-network-traffic

maec-malware-behavior:maec-malware-behavior="capture-system-screenshot"

capture-system-screenshot

maec-malware-behavior:maec-malware-behavior="capture-touchscreen-input"

capture-touchscreen-input

maec-malware-behavior:maec-malware-behavior="check-for-payload"

check-for-payload

maec-malware-behavior:maec-malware-behavior="click-fraud"

click-fraud

maec-malware-behavior:maec-malware-behavior="compare-host-fingerprints"

compare-host-fingerprints

maec-malware-behavior:maec-malware-behavior="compromise-remote-machine"

compromise-remote-machinen

maec-malware-behavior:maec-malware-behavior="control-local-machine-via-remote-command"

control-local-machine-via-remote-command

maec-malware-behavior:maec-malware-behavior="control-malware-via-remote-command"

control-malware-via-remote-command

maec-malware-behavior:maec-malware-behavior="crack-passwords"

crack-passwords

maec-malware-behavior:maec-malware-behavior="defeat-call-graph-generation"

defeat-call-graph-generation

maec-malware-behavior:maec-malware-behavior="defeat-emulator"

defeat-emulator

maec-malware-behavior:maec-malware-behavior="defeat-flow-oriented-disassembler"

defeat-flow-oriented-disassembler

maec-malware-behavior:maec-malware-behavior="defeat-linear-disassembler"

defeat-linear-disassembler

maec-malware-behavior:maec-malware-behavior="degrade-security-program"

degrade-security-program

maec-malware-behavior:maec-malware-behavior="denial-of-service"

denial-of-service

maec-malware-behavior:maec-malware-behavior="destroy-hardware"

destroy-hardware

maec-malware-behavior:maec-malware-behavior="detect-debugging"

detect-debugging

maec-malware-behavior:maec-malware-behavior="detect-emulator"

detect-emulator

maec-malware-behavior:maec-malware-behavior="detect-installed-analysis-tools"

detect-installed-analysis-tools

maec-malware-behavior:maec-malware-behavior="detect-installed-av-tools"

detect-installed-av-tools

maec-malware-behavior:maec-malware-behavior="detect-sandbox-environment"

detect-sandbox-environment

maec-malware-behavior:maec-malware-behavior="detect-vm-environment"

detect-vm-environment

maec-malware-behavior:maec-malware-behavior="determine-host-ip-address"

determine-host-ip-address

maec-malware-behavior:maec-malware-behavior="disable-access-rights-checking"

disable-access-rights-checking

maec-malware-behavior:maec-malware-behavior="disable-firewall"

disable-firewall

maec-malware-behavior:maec-malware-behavior="disable-kernel-patch-protection"

disable-kernel-patch-protection

maec-malware-behavior:maec-malware-behavior="disable-os-security-alerts"

disable-os-security-alerts

maec-malware-behavior:maec-malware-behavior="disable-privilege-limiting"

disable-privilege-limiting

maec-malware-behavior:maec-malware-behavior="disable-service-pack-patch-installation"

disable-service-pack-patch-installation

maec-malware-behavior:maec-malware-behavior="disable-system-file-overwrite-protection"

disable-system-file-overwrite-protection

maec-malware-behavior:maec-malware-behavior="disable-update-services-daemons"

disable-update-services-daemons

maec-malware-behavior:maec-malware-behavior="disable-user-account-control"

disable-user-account-control

maec-malware-behavior:maec-malware-behavior="drop-retrieve-debug-log-file"

drop-retrieve-debug-log-file

maec-malware-behavior:maec-malware-behavior="elevate-privilege"

elevate-privilege

maec-malware-behavior:maec-malware-behavior="encrypt-data"

encrypt-data

maec-malware-behavior:maec-malware-behavior="encrypt-files"

encrypt-files

maec-malware-behavior:maec-malware-behavior="encrypt-self"

encrypt-self

maec-malware-behavior:maec-malware-behavior="erase-data"

erase-data

maec-malware-behavior:maec-malware-behavior="evade-static-heuristic"

evade-static-heuristic

maec-malware-behavior:maec-malware-behavior="execute-before-external-to-kernel-hypervisor"

execute-before-external-to-kernel-hypervisor

maec-malware-behavior:maec-malware-behavior="execute-non-main-cpu-code"

execute-non-main-cpu-code

maec-malware-behavior:maec-malware-behavior="execute-stealthy-code"

execute-stealthy-code

maec-malware-behavior:maec-malware-behavior="exfiltrate-data-via-covert channel"

exfiltrate-data-via-covert channel

maec-malware-behavior:maec-malware-behavior="exfiltrate-data-via—dumpster-dive"

exfiltrate-data-via-dumpster-dives

maec-malware-behavior:maec-malware-behavior="exfiltrate-data-via-fax"

exfiltrate-data-via-fax

maec-malware-behavior:maec-malware-behavior="exfiltrate-data-via-network"

exfiltrate-data-via-network

maec-malware-behavior:maec-malware-behavior="exfiltrate-data-via-physical-media"

exfiltrate-data-via-physical-media

maec-malware-behavior:maec-malware-behavior="exfiltrate-data-via-voip-phone"

exfiltrate-data-via-voip-phone

maec-malware-behavior:maec-malware-behavior="feed-misinformation-during-physical-memory-acquisition"

feed-misinformation-during-physical-memory-acquisition

maec-malware-behavior:maec-malware-behavior="file-system-instantiation"

file-system-instantiation

maec-malware-behavior:maec-malware-behavior="fingerprint-host"

fingerprint-host

maec-malware-behavior:maec-malware-behavior="generate-c2-domain-names"

generate-c2-domain-names

maec-malware-behavior:maec-malware-behavior="hide-arbitrary-virtual-memory"

hide-arbitrary-virtual-memory

maec-malware-behavior:maec-malware-behavior="hide-data-in-other-formats"

hide-data-in-other-formats

maec-malware-behavior:maec-malware-behavior="hide-file-system-artifacts"

hide-file-system-artifacts

maec-malware-behavior:maec-malware-behavior="hide-kernel-modules"

hide-kernel-modules

maec-malware-behavior:maec-malware-behavior="hide-network-traffic"

hide-network-traffic

maec-malware-behavior:maec-malware-behavior="hide-open-network-ports"

hide-open-network-ports

maec-malware-behavior:maec-malware-behavior="hide-processes"

hide-processes

maec-malware-behavior:maec-malware-behavior="hide-services"

hide-services

maec-malware-behavior:maec-malware-behavior="hide-threads"

hide-threads

maec-malware-behavior:maec-malware-behavior="hide-userspace-libraries"

hide-userspace-libraries

maec-malware-behavior:maec-malware-behavior="identify-file"

identify-file

maec-malware-behavior:maec-malware-behavior="identify-os"

identify-os

maec-malware-behavior:maec-malware-behavior="identify-target-machines"

identify-target-machines

maec-malware-behavior:maec-malware-behavior="impersonate-user"

impersonate-user

maec-malware-behavior:maec-malware-behavior="install-backdoor"

install-backdoor

maec-malware-behavior:maec-malware-behavior="install-legitimate-software"

install-legitimate-software

maec-malware-behavior:maec-malware-behavior="install-secondary-malware"

install-secondary-malware

maec-malware-behavior:maec-malware-behavior="install-secondary-module"

install-secondary-module

maec-malware-behavior:maec-malware-behavior="intercept-manipulate-network-traffic"

intercept-manipulate-network-traffic

maec-malware-behavior:maec-malware-behavior="inventory-security-products"

inventory-security-products

maec-malware-behavior:maec-malware-behavior="inventory-system-applications"

inventory-system-applications

maec-malware-behavior:maec-malware-behavior="inventory-victims"

inventory-victims

maec-malware-behavior:maec-malware-behavior="limit-application-type-version"

limit-application-type-version

maec-malware-behavior:maec-malware-behavior="log-activity"

log-activity

maec-malware-behavior:maec-malware-behavior="manipulate-file-system-data"

manipulate-file-system-data

maec-malware-behavior:maec-malware-behavior="map-local-network"

map-local-network

maec-malware-behavior:maec-malware-behavior="mine-for-cryptocurrency"

mine-for-cryptocurrency

maec-malware-behavior:maec-malware-behavior="modify-file"

modify-file

maec-malware-behavior:maec-malware-behavior="modify-security-software-configuration"

modify-security-software-configuration

maec-malware-behavior:maec-malware-behavior="move-data-to-staging-server"

move-data-to-staging-server

maec-malware-behavior:maec-malware-behavior="obfuscate-artifact-properties"

obfuscate-artifact-properties

maec-malware-behavior:maec-malware-behavior="overload-sandbox"

overload-sandbox

maec-malware-behavior:maec-malware-behavior="package-data"

package-data

maec-malware-behavior:maec-malware-behavior="persist-after-hardware-changes"

persist-after-hardware-changes

maec-malware-behavior:maec-malware-behavior="persist-after-os-changes"

persist-after-os-changes

maec-malware-behavior:maec-malware-behavior="persist-after-system-reboot"

persist-after-system-reboot

maec-malware-behavior:maec-malware-behavior="prevent-api-unhooking"

prevent-api-unhooking

maec-malware-behavior:maec-malware-behavior="prevent-concurrent-execution"

prevent-concurrent-execution

maec-malware-behavior:maec-malware-behavior="prevent-debugging"

prevent-debugging

maec-malware-behavior:maec-malware-behavior="prevent-file-access"

prevent-file-access

maec-malware-behavior:maec-malware-behavior="prevent-file-deletion"

prevent-file-deletion

maec-malware-behavior:maec-malware-behavior="prevent-memory-access"

prevent-memory-access

maec-malware-behavior:maec-malware-behavior="prevent-native-api-hooking"

prevent-native-api-hooking

maec-malware-behavior:maec-malware-behavior="prevent-physical-memory-acquisition"

prevent-physical-memory-acquisition

maec-malware-behavior:maec-malware-behavior="prevent-registry-access"

prevent-registry-access

maec-malware-behavior:maec-malware-behavior="prevent-registry-deletion"

prevent-registry-deletion

maec-malware-behavior:maec-malware-behavior="prevent-security-software-from-executing"

prevent-security-software-from-executing

maec-malware-behavior:maec-malware-behavior="re-instantiate-self"

re-instantiate-self

maec-malware-behavior:maec-malware-behavior="remove-self"

remove-self

maec-malware-behavior:maec-malware-behavior="remove-sms-warning-messages"

remove-sms-warning-messages

maec-malware-behavior:maec-malware-behavior="remove-system-artifacts"

remove-system-artifacts

maec-malware-behavior:maec-malware-behavior="request-email-address-list"

request-email-address-list

maec-malware-behavior:maec-malware-behavior="request-email-template"

request-email-template

maec-malware-behavior:maec-malware-behavior="search-for-remote-machines"

search-for-remote-machines

maec-malware-behavior:maec-malware-behavior="send-beacon"

send-beacon

maec-malware-behavior:maec-malware-behavior="send-email-message"

send-email-message

maec-malware-behavior:maec-malware-behavior="social-engineering-based-remote-infection"

social-engineering-based-remote-infection

maec-malware-behavior:maec-malware-behavior="steal-browser-cache"

steal-browser-cache

maec-malware-behavior:maec-malware-behavior="steal-browser-cookies"

steal-browser-cookies

maec-malware-behavior:maec-malware-behavior="steal-browser-history"

steal-browser-history

maec-malware-behavior:maec-malware-behavior="steal-contact-list-data"

steal-contact-list-data

maec-malware-behavior:maec-malware-behavior="steal-cryptocurrency-data"

steal-cryptocurrency-data

maec-malware-behavior:maec-malware-behavior="steal-database-content"

steal-database-content

maec-malware-behavior:maec-malware-behavior="steal-dialed-phone-numbers"

steal-dialed-phone-numbers

maec-malware-behavior:maec-malware-behavior="steal-digital-certificates"

steal-digital-certificates

maec-malware-behavior:maec-malware-behavior="steal-documents"

steal-documents

maec-malware-behavior:maec-malware-behavior="steal-email-data"

steal-email-data

maec-malware-behavior:maec-malware-behavior="steal-images"

steal-images

maec-malware-behavior:maec-malware-behavior="steal-password-hashes"

steal-password-hashes

maec-malware-behavior:maec-malware-behavior="steal-pki-key"

steal-pki-key

maec-malware-behavior:maec-malware-behavior="steal-referrer-urls"

steal-referrer-urls

maec-malware-behavior:maec-malware-behavior="steal-serial-numbers"

steal-serial-numbers

maec-malware-behavior:maec-malware-behavior="steal-sms-database"

steal-sms-database

maec-malware-behavior:maec-malware-behavior="steal-web-network-credential"

steal-web-network-credential

maec-malware-behavior:maec-malware-behavior="stop-execution-of-security-software"

stop-execution-of-security-software

maec-malware-behavior:maec-malware-behavior="suicide-exit"

suicide-exit

maec-malware-behavior:maec-malware-behavior="test-for-firewall"

test-for-firewall

maec-malware-behavior:maec-malware-behavior="test-for-internet-connectivity"

test-for-internet-connectivity

maec-malware-behavior:maec-malware-behavior="test-for-network-drives"

test-for-network-drives

maec-malware-behavior:maec-malware-behavior="test-for-proxy"

test-for-proxy

maec-malware-behavior:maec-malware-behavior="test-smtp-connection"

test-smtp-connection

maec-malware-behavior:maec-malware-behavior="update-configuration"

update-configuration

maec-malware-behavior:maec-malware-behavior="validate-data"

validate-data

maec-malware-behavior:maec-malware-behavior="write-code-into-file"

write-code-into-file

maec-malware-capabilities

maec-malware-capabilities namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Malware Capabilities based on MAEC 5.0

maec-malware-capability

maec-malware-capabilities:maec-malware-capability="anti-behavioral-analysis"

anti-behavioral-analysis

maec-malware-capabilities:maec-malware-capability="anti-code-analysis"

anti-code-analysis

maec-malware-capabilities:maec-malware-capability="anti-detection"

anti-detection

maec-malware-capabilities:maec-malware-capability="anti-removal"

anti-removal

maec-malware-capabilities:maec-malware-capability="availability-violation"

availability-violation

maec-malware-capabilities:maec-malware-capability="collection"

collection

maec-malware-capabilities:maec-malware-capability="command-and-control"

command-and-control

maec-malware-capabilities:maec-malware-capability="data-theft"

data-theft

maec-malware-capabilities:maec-malware-capability="destruction"

destruction

maec-malware-capabilities:maec-malware-capability="discovery"

discovery

maec-malware-capabilities:maec-malware-capability="exfiltration"

exfiltration

maec-malware-capabilities:maec-malware-capability="fraud"

fraud

maec-malware-capabilities:maec-malware-capability="infection-propagation"

infection-propagation

maec-malware-capabilities:maec-malware-capability="integrity-violation"

integrity-violation

maec-malware-capabilities:maec-malware-capability="machine-access-control"

machine-access-control

maec-malware-capabilities:maec-malware-capability="persistence"

persistence

maec-malware-capabilities:maec-malware-capability="privilege-escalation"

privilege-escalation

maec-malware-capabilities:maec-malware-capability="secondary-operation"

secondary-operation

maec-malware-capabilities:maec-malware-capability="security-degradation"

security-degradation

maec-malware-capabilities:maec-malware-capability="access-control-degradation"

access-control-degradation

maec-malware-capabilities:maec-malware-capability="anti-debugging"

anti-debugging

maec-malware-capabilities:maec-malware-capability="anti-disassembly"

anti-disassembly

maec-malware-capabilities:maec-malware-capability="anti-emulation"

anti-emulation

maec-malware-capabilities:maec-malware-capability="anti-memory-forensics"

anti-memory-forensics

maec-malware-capabilities:maec-malware-capability="anti-sandbox"

anti-sandbox

maec-malware-capabilities:maec-malware-capability="anti-virus-evasion"

anti-virus-evasion

maec-malware-capabilities:maec-malware-capability="anti-vm"

anti-vm

maec-malware-capabilities:maec-malware-capability="authentication-credentials-theft"

authentication-credentials-theft

maec-malware-capabilities:maec-malware-capability="clean-traces-of-infection"

clean-traces-of-infection

maec-malware-capabilities:maec-malware-capability="communicate-with-c2-server"

communicate-with-c2-server

maec-malware-capabilities:maec-malware-capability="compromise-data-availability"

compromise-data-availability

maec-malware-capabilities:maec-malware-capability="compromise-system-availability"

compromise-system-availability

maec-malware-capabilities:maec-malware-capability="consume-system-resources"

consume-system-resources

maec-malware-capabilities:maec-malware-capability="continuous-execution"

continuous-execution

maec-malware-capabilities:maec-malware-capability="data-integrity-violation"

data-integrity-violation

maec-malware-capabilities:maec-malware-capability="data-obfuscation"

data-obfuscation

maec-malware-capabilities:maec-malware-capability="data-staging"

data-staging

maec-malware-capabilities:maec-malware-capability="determine-c2-server"

determine-c2-server

maec-malware-capabilities:maec-malware-capability="email-spam"

email-spam

maec-malware-capabilities:maec-malware-capability="ensure-compatibility"

ensure-compatibility

maec-malware-capabilities:maec-malware-capability="environment-awareness"

environment-awareness

maec-malware-capabilities:maec-malware-capability="file-infection"

file-infection

maec-malware-capabilities:maec-malware-capability="hide-artifacts"

hide-artifacts

maec-malware-capabilities:maec-malware-capability="hide-executing-code"

hide-executing-code

maec-malware-capabilities:maec-malware-capability="hide-non-executing-code"

hide-non-executing-code

maec-malware-capabilities:maec-malware-capability="host-configuration-probing"

host-configuration-probing

maec-malware-capabilities:maec-malware-capability="information-gathering-for-improvement"

information-gathering-for-improvement

maec-malware-capabilities:maec-malware-capability="input-peripheral-capture"

input-peripheral-capture

maec-malware-capabilities:maec-malware-capability="install-other-components"

install-other-components

maec-malware-capabilities:maec-malware-capability="local-machine-control"

local-machine-control

maec-malware-capabilities:maec-malware-capability="network-environment-probing"

network-environment-probing

maec-malware-capabilities:maec-malware-capability="os-security-feature-degradation"

os-security-feature-degradation

maec-malware-capabilities:maec-malware-capability="output-peripheral-capture"

output-peripheral-capture

maec-malware-capabilities:maec-malware-capability="physical-entity-destruction"

physical-entity-destruction

maec-malware-capabilities:maec-malware-capability="prevent-artifact-access"

prevent-artifact-access

maec-malware-capabilities:maec-malware-capability="prevent-artifact-deletion"

prevent-artifact-deletion

maec-malware-capabilities:maec-malware-capability="remote-machine-access"

remote-machine-access

maec-malware-capabilities:maec-malware-capability="security-software-degradation"

security-software-degradation

maec-malware-capabilities:maec-malware-capability="security-software-evasion"

security-software-evasion

maec-malware-capabilities:maec-malware-capability="self-modification"

self-modification

maec-malware-capabilities:maec-malware-capability="service-provider-security-feature-degradation"

service-provider-security-feature-degradation

maec-malware-capabilities:maec-malware-capability="stored-information-theft"

stored-information-theft

maec-malware-capabilities:maec-malware-capability="system-interface-data-capture"

system-interface-data-capture

maec-malware-capabilities:maec-malware-capability="system-operational-integrity-violation"

system-operational-integrity-violation

maec-malware-capabilities:maec-malware-capability="system-re-infection"

system-re-infection

maec-malware-capabilities:maec-malware-capability="system-state-data-capture"

system-state-data-capture

maec-malware-capabilities:maec-malware-capability="system-update-degradation"

system-update-degradation

maec-malware-capabilities:maec-malware-capability="user-data-theft"

user-data-theft

maec-malware-capabilities:maec-malware-capability="virtual-entity-destruction"

virtual-entity-destruction

maec-malware-obfuscation-methods

maec-malware-obfuscation-methods namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Obfuscation methods used by malware based on MAEC 5.0

maec-obfuscation-methods

maec-malware-obfuscation-methods:maec-obfuscation-methods="packing"

packing

maec-malware-obfuscation-methods:maec-obfuscation-methods="code-encryption"

code-encryption

maec-malware-obfuscation-methods:maec-obfuscation-methods="dead-code-insertion"

dead-code-insertion

maec-malware-obfuscation-methods:maec-obfuscation-methods="entry-point-obfuscation"

entry-point-obfuscation

maec-malware-obfuscation-methods:maec-obfuscation-methods="import-address-table-obfuscation"

import-address-table-obfuscation

maec-malware-obfuscation-methods:maec-obfuscation-methods="interleaving-code"

interleaving-code

maec-malware-obfuscation-methods:maec-obfuscation-methods="symbolic-obfuscation"

symbolic-obfuscation

maec-malware-obfuscation-methods:maec-obfuscation-methods="string-obfuscation"

string-obfuscation

maec-malware-obfuscation-methods:maec-obfuscation-methods="subroutine-reordering"

subroutine-reordering

maec-malware-obfuscation-methods:maec-obfuscation-methods="code-transposition"

code-transposition

maec-malware-obfuscation-methods:maec-obfuscation-methods="instruction-substitution"

instruction-substitution

maec-malware-obfuscation-methods:maec-obfuscation-methods="register-reassignment"

register-reassignment

malware_classification

malware_classification namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Classification based on different categories. Based on https://www.sans.org/reading-room/whitepapers/incident/malware-101-viruses-32848

malware-category

malware_classification:malware-category="Virus"

Virus

malware_classification:malware-category="Worm"

Worm

malware_classification:malware-category="Trojan"

Trojan

malware_classification:malware-category="Ransomware"

Ransomware

malware_classification:malware-category="Rootkit"

Rootkit

malware_classification:malware-category="Downloader"

Downloader

malware_classification:malware-category="Adware"

Adware

malware_classification:malware-category="Spyware"

Spyware

malware_classification:malware-category="Botnet"

Botnet

obfuscation-technique

malware_classification:obfuscation-technique="no-obfuscation"

No obfuscation is used

malware_classification:obfuscation-technique="encryption"

encryption

malware_classification:obfuscation-technique="oligomorphism"

oligomorphism

malware_classification:obfuscation-technique="metamorphism"

metamorphism

malware_classification:obfuscation-technique="stealth"

stealth

malware_classification:obfuscation-technique="armouring"

armouring

malware_classification:obfuscation-technique="tunneling"

tunneling

malware_classification:obfuscation-technique="XOR"

XOR

malware_classification:obfuscation-technique="BASE64"

BASE64

malware_classification:obfuscation-technique="ROT13"

ROT13

payload-classification

malware_classification:payload-classification="no-payload"

No payload

malware_classification:payload-classification="non-destructive"

Non-Destructive

malware_classification:payload-classification="destructive"

Destructive

malware_classification:payload-classification="dropper"

Dropper

memory-classification

malware_classification:memory-classification="resident"

In memory

malware_classification:memory-classification="temporary-resident"

In memory temporarily

malware_classification:memory-classification="swapping-mode"

Only a part loaded in memory temporarily

malware_classification:memory-classification="non-resident"

Not in memory

malware_classification:memory-classification="user-process"

As a user level process

malware_classification:memory-classification="kernel-process"

As a process in the kernel

misinformation-website-label

misinformation-website-label namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

classification for the identification of type of misinformation among websites. Source:False, Misleading, Clickbait-y, and/or Satirical News Sources by Melissa Zimdars 2019

fake-news

Sources that fabricate information, disseminate deceptive content, or grossly distort actual news reports

satire

Sources that use humor, irony, exaggeration, ridicule, and false information to comment current events

misinformation-website-label:satire="humor"

Humor

misinformation-website-label:satire="irony"

Irony

misinformation-website-label:satire="exaggeration"

Exaggeration

misinformation-website-label:satire="false-information"

False information

extreme-bias

Sources that come from a particular point of view and may rely on propaganda, decontextualized information, opinions distorded as facts

misinformation-website-label:extreme-bias="propaganda"

Propaganda

misinformation-website-label:extreme-bias="decontextualized-information"

Decontextualized Information

misinformation-website-label:extreme-bias="opinions-distorded-as-facts"

Opinions distorded as facts

conspiracy

Sources that are well-known promoters of kooky conspiracy theories. Ex: 9/11 conspiracies, chem-trails, lizard people in the sewer systems, birther rumors, flat earth theory fluoride as mind control, vaccines as mind control etc

rumor

Sources that traffic in rumors, gossip, innuendo, unverified claims

misinformation-website-label:rumor="rumors"

Rumors

misinformation-website-label:rumor="gossip"

Gossip

misinformation-website-label:rumor="innuendo"

Innuendo

misinformation-website-label:rumor="unverified-claims"

Unverified Claims

state-news

Sources in repressive states operating under government sanction

junk-sciences

Sources that promotes pseudo-sciences, metaphysics, naturalistic fallacies, and other scientificallt dubious claims

hate-news

Sources that promote racism, misogyny, homophobia, and other forms of discrimination

misinformation-website-label:hate-news="racism"

Racism

misinformation-website-label:hate-news="misogyny"

Misogyny

misinformation-website-label:hate-news="homophobia"

Homophobia

misinformation-website-label:hate-news="discrimination-other"

Discrimination other

clickbait

Sources that provide generally credible content, but use exaggerated, misleading, OR questionable headlines, social media descriptions, and/or images. These sources may also use sensational language to generate interest, clickthroughs, and shares, but their content is typically verifiable

proceed-with-caution

Sources that may be reliable but whose contents require further verification or to be read in conjunction with other sources

political

Sources that provide generally verifiable information in support of certain points of view or political orientations

credible

Sources that circulate news and information in a manner consistent with traditional and ethical practices in journalism

unknown

Sources that have not yet been analyzed (many of these were suggested by readers/users or are found on other lists and resources).

misp

misp namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

MISP taxonomy to infer with MISP behavior or operation.

ui

misp:ui="hide"

tag to hide from the user-interface.

api

misp:api="hide"

tag to hide from the API.

expansion

Expansion tag incluencing the MISP behavior using expansion modules

misp:expansion="block"

block

contributor

misp:contributor="pgpfingerprint"

OpenPGP Fingerprint

confidence-level

Exclusive flag set which means the values or predicate below must be set exclusively.

misp:confidence-level="completely-confident"

Completely confident

Associated numerical value="100"

misp:confidence-level="usually-confident"

Usually confident

Associated numerical value="75"

misp:confidence-level="fairly-confident"

Fairly confident

Associated numerical value="50"

misp:confidence-level="rarely-confident"

Rarely confident

Associated numerical value="25"

misp:confidence-level="unconfident"

Unconfident

misp:confidence-level="confidence-cannot-be-evaluated"

Confidence cannot be evaluated

Associated numerical value="50"

threat-level

Exclusive flag set which means the values or predicate below must be set exclusively.

misp:threat-level="no-risk"

No risk

Harmless information. (CEUS threat level)

misp:threat-level="low-risk"

Low risk

Low risk which can include mass-malware. (CEUS threat level)

Associated numerical value="25"

misp:threat-level="medium-risk"

Medium risk

Medium risk which can include targeted attacks (e.g. APT). (CEUS threat level)

Associated numerical value="50"

misp:threat-level="high-risk"

High risk

High risk which can include highly sophisticated attacks or 0-day attack. (CEUS threat level)

Associated numerical value="100"

automation-level

Exclusive flag set which means the values or predicate below must be set exclusively.

misp:automation-level="unsupervised"

Generated automatically without human verification

misp:automation-level="reviewed"

Generated automatically but verified by a human

Associated numerical value="50"

misp:automation-level="manual"

Output of human analysis

Associated numerical value="100"

should-not-sync

Event with this tag should not be synced to other MISP instances

tool

Tool associated with the information taggged

misp:tool="misp2stix"

misp2stix

misp:tool="misp2yara"

misp2yara

misp2yara

Exclusive flag set which means the values or predicate below must be set exclusively.

misp:misp2yara="generated"

generated

misp:misp2yara="as-is"

as-is

misp:misp2yara="valid"

valid

misp:misp2yara="invalid"

invalid

event-type

misp:event-type="observation"

observation

misp:event-type="incident"

incident

misp:event-type="report"

report

misp:event-type="collection"

collection

misp:event-type="analysis"

analysis

misp:event-type="automatic-analysis"

automatic-analysis

ids

misp:ids="force"

force

Force the IDS flag to be the one from the tag.

misp:ids="true"

true

Overwrite the current IDS flag of the information tag by IDS true.

misp:ids="false"

false

Overwrite the current IDS flag of the information tag by IDS false.

monarc-threat

monarc-threat namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

MONARC Threats Taxonomy

compromise-of-functions

monarc-threat:compromise-of-functions="error-in-use"

Error in use

A person commits an operating error, input error or utilisation error on hardware or software.

monarc-threat:compromise-of-functions="forging-of-rights"

Forging of rights

A person assumes the identity of a different person in order to use his/her access rights to the information system, misinform the recipient, commit a fraud, etc.

monarc-threat:compromise-of-functions="eavesdropping"

Eavesdropping

Someone connected to communication equipment or media or located inside the transmission coverage boundaries of a communication.

monarc-threat:compromise-of-functions="denial-of-actions"

Denial of actions

A person or entity denies being involved in an exchange with a third party or carrying out an operation.

monarc-threat:compromise-of-functions="abuse-of-rights"

Abuse of rights

Someone with special rights (network administration, computer specialists, etc.) modifies the operating characteristics of the resources.

monarc-threat:compromise-of-functions="breach-of-personnel-availability"

Breach of personnel availability

Absence of qualified or authorised personnel to execute the usual operations.

unauthorised-actions

monarc-threat:unauthorised-actions="fraudulent-copying-or-use-of-counterfeit-software"

Fraudulent copying or use of counterfeit software

Someone inside the organisation makes fraudulent copies (also called pirated copies) of package software or in-house software.

monarc-threat:unauthorised-actions="corruption-of-data"

Corruption of data

Someone gains access to the communication equipment of the information system and corrupts transmission of information (by intercepting, inserting, destroying, etc.) or repeatedly attempts access until successful.

monarc-threat:unauthorised-actions="illegal-processing-of-data"

Illegal processing of data

A person carries out information processing that is forbidden by the law or a regulation.

compromise-of-information

monarc-threat:compromise-of-information="remote-spying"

Remote spying

Personnel actions observable from a distance. Visual observation with or without optical equipment, for example observation of a user entering a code or password on a keyboard.

monarc-threat:compromise-of-information="tampering-with-hardware"

Tampering with hardware

Someone with access to a communication medium or equipment installs an interception or destruction device in it.

monarc-threat:compromise-of-information="interception-of-compromising-interference-signals"

Interception of compromising interference signals

Interfering signals from an electromagnetic source emitted by the equipment (by conduction on the electrical power supply cables or earth wires or by radiation in free space). Capture of these signals depends on the distance to the targeted equipment or the possibility of connecting to cables or any other conductor passing close to the equipment (coupling phenomenon).

monarc-threat:compromise-of-information="theft-or-destruction-of-media-documents-or-equipment"

Theft or destruction of media, documents or equipment

Media, documents or equipment can be accessed by foreigners either internally or externally. It can be damaged or stolen.

monarc-threat:compromise-of-information="retrieval-of-recycled-or-discarded media"

Retrieval of recycled or discarded media

Retrieval of electronic media (hard discs, floppy discs, back-up cartridges, USB keys, ZIP discs, removable hard discs, etc.) or paper copies (lists, incomplete print-outs, messages, etc.) intended for recycling and containing retrievable information.

monarc-threat:compromise-of-information="malware-infection"

Malware infection

Unwanted software that is doing operations seeking to harm the company.

monarc-threat:compromise-of-information="data-from-untrustworthy-sources"

Data from untrustworthy sources

Receiving false data or unsuitable equipment from outside sources and using them in the organisation.

monarc-threat:compromise-of-information="disclosure"

Disclosure

Person who voluntarily or negligently disclosure information.

loss-of-essential-services

monarc-threat:loss-of-essential-services="failure-of-telecommunication-equipment"

Failure of telecommunication equipment

Disturbance, shutdown or incorrect sizing of telecommunications services (telephone, Internet access, Internet network).

monarc-threat:loss-of-essential-services="loss-of-power-supply"

Loss of power supply

Failure, shutdown or incorrect sizing of the power supply to the assets arising either from the supplier’s service or from the internal distribution system.

monarc-threat:loss-of-essential-services="failure-of-air-conditioning"

Failure of air-conditioning

Failure, shutdown or inadequacy of the air-conditioning service may cause assets requiring cooling or ventilation to shut down, malfunction or fail completely.

technical-failures

monarc-threat:technical-failures="software-malfunction"

Software malfunction

Design error, installation error or operating error committed during modification causing incorrect execution.

monarc-threat:technical-failures="equipment-malfunction-or-failure"

Equipment malfunction or failure

Logical or physical event causing hardware malfunctions or failures.

monarc-threat:technical-failures="saturation-of-the-information-system"

Saturation of the information system

A person or resource of a hardware, software or network type simulating an intense demand on resources by setting up continuous bombardment.

monarc-threat:technical-failures="breach-of-information-system-maintainability"

Breach of information system maintainability

Lack of expertise in the system making retrofitting and upgrading impossible

physical-damage

monarc-threat:physical-damage="destruction-of-equipment-or-supports"

Destruction of equipment or supports

Event causing destruction of equipment or media.

monarc-threat:physical-damage="fire"

Fire

Any situation that could facilitate the conflagration of premises or equipment.

monarc-threat:physical-damage="water-damage"

Water damage

Situation facilitating the water hazard on equipment (floods, water leak, cellars, etc.)

monarc-threat:physical-damage="major-accident"

Major accident

Any event that can physically destroy the premises

monarc-threat:physical-damage="pollution"

Pollution

Presence of dust, vapours, corrosive or toxic gases in the ambient air.

monarc-threat:physical-damage="environmental-disaster"

Environmental disaster (fire, flood, dust, dirt, etc.)

Any event that can physically ruin the premises

ms-caro-malware

ms-caro-malware namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Malware Type and Platform classification based on Microsoft's implementation of the Computer Antivirus Research Organization (CARO) Naming Scheme and Malware Terminology. Based on https://www.microsoft.com/en-us/security/portal/mmpc/shared/malwarenaming.aspx, https://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx, https://www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx, and http://www.caro.org/definitions/index.html. Malware families are extracted from Microsoft SIRs since 2008 based on https://www.microsoft.com/security/sir/archive/default.aspx and https://www.microsoft.com/en-us/security/portal/threat/threats.aspx. Note that SIRs do NOT include all Microsoft malware families.

malware-type

ms-caro-malware:malware-type="Adware"

Adware - Software that shows you extra promotions that you cannot control as you use your PC

ms-caro-malware:malware-type="Backdoor"

A type of trojan that gives a malicious hacker access to and control of your PC

ms-caro-malware:malware-type="Behavior"

A type of detection based on file actions that are often associated with malicious activity

ms-caro-malware:malware-type="BroswerModifier"

A program than makes changes to your Internet browser without your permission

ms-caro-malware:malware-type="Constructor"

A program that can be used to automatically create malware files

ms-caro-malware:malware-type="DDoS"

When a number of PCs are made to access a website, network or server repeatedly within a given time period. The aim of the attack is to overload the target so that it crashes and can’t respond

ms-caro-malware:malware-type="Dialer"

A program that makes unauthorized telephone calls. These calls may be charged at a premium rate and cost you a lot of money

ms-caro-malware:malware-type="DoS"

When a target PC or server is deliberately overloaded so that it doesn’t work for any visitors anymore

ms-caro-malware:malware-type="Exploit"

A piece of code that uses software vulnerabilities to access information on your PC or install malware

ms-caro-malware:malware-type="HackTool"

A type of tool that can be used to allow and maintain unauthorized access to your PC

ms-caro-malware:malware-type="Joke"

A program that pretends to do something malicious but actually doesn’t actually do anything harmful. For example, some joke programs pretend to delete files or format disks

ms-caro-malware:malware-type="Misleading"

The program that makes misleading or fraudulent claims about files, registry entries or other items on your PC

ms-caro-malware:malware-type="MonitoringTool"

A commercial program that monitors what you do on your PC. This can include monitoring what keys you press; your email or instant messages; your voice or video conversations; and your banking details and passwords. It can also take screenshots as you use your PC

ms-caro-malware:malware-type="Program"

Software that you may or may not want installed on your PC

ms-caro-malware:malware-type="PUA"

Potentially Unwanted Applications. Characteristics of unwanted software can include depriving users of adequate choice or control over what the software does to the computer, preventing users from removing the software, or displaying advertisements without clearly identifying their source.

ms-caro-malware:malware-type="PWS"

A type of malware that is used steal your personal information, such as user names and passwords. It often works along with a keylogger that collects and sends information about what keys you press and websites you visit to a malicious hacker

ms-caro-malware:malware-type="Ransom"

A detection for malicious programs that seize control of the computer on which they are installed. This trojan usually locks the screen and prevents the user from using the computer. It usually displays an alert message.

ms-caro-malware:malware-type="RemoteAccess"

A program that gives someone access to your PC from a remote location. This type of program is often installed by the computer owner

ms-caro-malware:malware-type="Rogue"

Software that pretends to be an antivirus program but doesn’t actually provide any security. This type of software usually gives you a lot of alerts about threats on your PC that don’t exist. It also tries to convince you to pay for its services

ms-caro-malware:malware-type="SettingsModifier"

A program that changes your PC settings

ms-caro-malware:malware-type="SoftwareBundler"

A program that installs unwanted software on your PC at the same time as the software you are trying to install, without adequate consent

ms-caro-malware:malware-type="Spammer"

A trojan that sends large numbers of spam emails. It may also describe the person or business responsible for sending spam

ms-caro-malware:malware-type="Spoofer"

A type of trojan that makes fake emails that look like they are from a legitimate source

ms-caro-malware:malware-type="Spyware"

A program that collects your personal information, such as your browsing history, and uses it without adequate consent

ms-caro-malware:malware-type="Tool"

A type of software that may have a legitimate purpose, but which may also be abused by malware

authors

ms-caro-malware:malware-type="Trojan"

A trojan is a program that tries to look innocent, but is actually a malicious application. Unlike a virus or a worm , a trojan doesn’t spread by itself. Instead they try to look innocent to convince you to download and install them. Once installed, a trojan can steal your personal information, download more malware, or give a malicious hacker access to your PC

ms-caro-malware:malware-type="TrojanClicker"

A type of trojan that can use your PC to click on websites or applications. They are usually used to make money for a malicious hacker by clicking on online advertisements and making it look like the website gets more traffic than it does. They can also be used to skew online polls, install programs on your PC, or make unwanted software appear more popular than it is

ms-caro-malware:malware-type="TrojanDownloader"

A type of trojan that installs other malicious files, including malware, onto your PC. It can download the files from a remote PC or install them directly from a copy that is included in its file.

ms-caro-malware:malware-type="TrojanDropper"

A type of trojan that installs other malicious files, including malware, onto your PC. It can download the files from a remote PC or install them directly from a copy that is included in its file.

ms-caro-malware:malware-type="TrojanNotifier"

A type of trojan that sends information about your PC to a malicious hacker. It is similar to a password stealer

ms-caro-malware:malware-type="TrojanProxy"

A type of trojan that installs a proxy server on your PC. The server can be configured so that when you use the Internet, any requests you make are sent through a server controlled by a malicious hacker.

ms-caro-malware:malware-type="TrojanSpy"

A program that collects your personal information, such as your browsing history, and uses it without adequate consent.

ms-caro-malware:malware-type="VirTool"

A detection that is used mostly for malware components, or tools used for malware-related actions, such as rootkits.

ms-caro-malware:malware-type="Virus"

A type of malware. Viruses spread on their own by attaching their code to other programs, or copying themselves across systems and networks.

ms-caro-malware:malware-type="Worm"

A type of malware that spreads to other PCs. Worms may spread using one or more of the following methods: Email programs, Instant messaging programs, File-sharing programs, Social networking sites, Network shares, Removable drives with Autorun enabled, Software vulnerabilities

malware-platform

ms-caro-malware:malware-platform="AndroidOS"

Android operating system

ms-caro-malware:malware-platform="DOS"

MS-DOS platform

ms-caro-malware:malware-platform="EPOC"

Psion devices

ms-caro-malware:malware-platform="FreeBSD"

FreeBSD platform

ms-caro-malware:malware-platform="iPhoneOS"

iPhone operating system

ms-caro-malware:malware-platform="Linux"

Linux platform

ms-caro-malware:malware-platform="MacOS"

MAC 9.x platform or earlier

ms-caro-malware:malware-platform="MacOS_X"

MacOS X or later

ms-caro-malware:malware-platform="OS2"

OS2 platform

ms-caro-malware:malware-platform="Palm"

Palm operating system

ms-caro-malware:malware-platform="Solaris"

System V-based Unix platforms

ms-caro-malware:malware-platform="SunOS"

Unix platforms 4.1.3 or earlier

ms-caro-malware:malware-platform="SymbOS"

Symbian operatings system

ms-caro-malware:malware-platform="Unix"

General Unix platforms

ms-caro-malware:malware-platform="Win16"

Win16 (3.1) platform

ms-caro-malware:malware-platform="Win2K"

Windows 2000 platform

ms-caro-malware:malware-platform="Win32"

Windows 32-bit platform

ms-caro-malware:malware-platform="Win64"

Windows 64-bit platform

ms-caro-malware:malware-platform="Win95"

Windows 95, 98 and ME platforms

ms-caro-malware:malware-platform="Win98"

Windows 98 platform only

ms-caro-malware:malware-platform="WinCE"

Windows CE platform

ms-caro-malware:malware-platform="WinNT"

WinNT

ms-caro-malware:malware-platform="ABAP"

Advanced Business Application Programming scripts

ms-caro-malware:malware-platform="ALisp"

ALisp scripts

ms-caro-malware:malware-platform="AmiPro"

AmiPro script

ms-caro-malware:malware-platform="ANSI"

American National Standards Institute scripts

ms-caro-malware:malware-platform="AppleScript"

compiled Apple scripts

ms-caro-malware:malware-platform="ASP"

Active Server Pages scripts

ms-caro-malware:malware-platform="AutoIt"

AutoIT scripts

ms-caro-malware:malware-platform="BAS"

Basic scripts

ms-caro-malware:malware-platform="BAT"

Basic scripts

ms-caro-malware:malware-platform="CorelScript"

Corelscript scripts

ms-caro-malware:malware-platform="HTA"

HTML Application scripts

ms-caro-malware:malware-platform="HTML"

HTML Application scripts

ms-caro-malware:malware-platform="INF"

Install scripts

ms-caro-malware:malware-platform="IRC"

mIRC/pIRC scripts

ms-caro-malware:malware-platform="Java"

Java binaries (classes)

ms-caro-malware:malware-platform="JS"

Javascript scripts

ms-caro-malware:malware-platform="LOGO"

LOGO scripts

ms-caro-malware:malware-platform="MPB"

MapBasic scripts

ms-caro-malware:malware-platform="MSH"

Monad shell scripts

ms-caro-malware:malware-platform="MSIL"

ms-caro-malware:malware-platform="Perl"

Net intermediate language scripts
Perl scripts

ms-caro-malware:malware-platform="PHP"

Hypertext Preprocessor scripts

ms-caro-malware:malware-platform="Python"

Python scripts

ms-caro-malware:malware-platform="SAP"

SAP platform scripts

ms-caro-malware:malware-platform="SH"

Shell scripts

ms-caro-malware:malware-platform="VBA"

Visual Basic for Applications scripts

ms-caro-malware:malware-platform="VBS"

Visual Basic scripts

ms-caro-malware:malware-platform="WinBAT"

Winbatch scripts

ms-caro-malware:malware-platform="WinHlp"

Windows Help scripts

ms-caro-malware:malware-platform="WinREG"

Windows registry scripts

ms-caro-malware:malware-platform="A97M"

Access 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware:malware-platform="HE"

macro scripting

ms-caro-malware:malware-platform="O97M"

Office 97, 2000, XP, 2003, 2007, and 2010 macros - those that affect Word, Excel, and Powerpoint

ms-caro-malware:malware-platform="PP97M"

PowerPoint 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware:malware-platform="V5M"

Visio5 macros

ms-caro-malware:malware-platform="W1M"

Word1Macro

ms-caro-malware:malware-platform="W2M"

Word2Macro

ms-caro-malware:malware-platform="W97M"

Word 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware:malware-platform="WM"

Word 95 macros

ms-caro-malware:malware-platform="X97M"

Excel 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware:malware-platform="XF"

Excel formulas

ms-caro-malware:malware-platform="XM"

Excel 95 macros

ms-caro-malware:malware-platform="ASX"

XML metafile of Windows Media .asf files

ms-caro-malware:malware-platform="HC"

HyperCard Apple scripts

ms-caro-malware:malware-platform="MIME"

MIME packets

ms-caro-malware:malware-platform="Netware"

Novell Netware files

ms-caro-malware:malware-platform="QT"

Quicktime files

ms-caro-malware:malware-platform="SB"

StarBasic (Staroffice XML) files

ms-caro-malware:malware-platform="SWF"

Shockwave Flash files

ms-caro-malware:malware-platform="TSQL"

MS SQL server files

ms-caro-malware:malware-platform="XML"

XML files

ms-caro-malware-full

ms-caro-malware-full namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Malware Type and Platform classification based on Microsoft's implementation of the Computer Antivirus Research Organization (CARO) Naming Scheme and Malware Terminology. Based on https://www.microsoft.com/en-us/security/portal/mmpc/shared/malwarenaming.aspx, https://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx, https://www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx, and http://www.caro.org/definitions/index.html. Malware families are extracted from Microsoft SIRs since 2008 based on https://www.microsoft.com/security/sir/archive/default.aspx and https://www.microsoft.com/en-us/security/portal/threat/threats.aspx. Note that SIRs do NOT include all Microsoft malware families.

malware-type

ms-caro-malware-full:malware-type="Adware"

Adware - Software that shows you extra promotions that you cannot control as you use your PC

ms-caro-malware-full:malware-type="Backdoor"

A type of trojan that gives a malicious hacker access to and control of your PC

ms-caro-malware-full:malware-type="Behavior"

A type of detection based on file actions that are often associated with malicious activity

ms-caro-malware-full:malware-type="BroswerModifier"

A program than makes changes to your Internet browser without your permission

ms-caro-malware-full:malware-type="Constructor"

A program that can be used to automatically create malware files

ms-caro-malware-full:malware-type="DDoS"

When a number of PCs are made to access a website, network or server repeatedly within a given time period. The aim of the attack is to overload the target so that it crashes and can’t respond

ms-caro-malware-full:malware-type="Dialer"

A program that makes unauthorized telephone calls. These calls may be charged at a premium rate and cost you a lot of money

ms-caro-malware-full:malware-type="DoS"

When a target PC or server is deliberately overloaded so that it doesn’t work for any visitors anymore

ms-caro-malware-full:malware-type="Exploit"

A piece of code that uses software vulnerabilities to access information on your PC or install malware

ms-caro-malware-full:malware-type="HackTool"

A type of tool that can be used to allow and maintain unauthorized access to your PC

ms-caro-malware-full:malware-type="Joke"

A program that pretends to do something malicious but actually doesn’t actually do anything harmful. For example, some joke programs pretend to delete files or format disks

ms-caro-malware-full:malware-type="Misleading"

The program that makes misleading or fraudulent claims about files, registry entries or other items on your PC

ms-caro-malware-full:malware-type="MonitoringTool"

A commercial program that monitors what you do on your PC. This can include monitoring what keys you press; your email or instant messages; your voice or video conversations; and your banking details and passwords. It can also take screenshots as you use your PC

ms-caro-malware-full:malware-type="Program"

Software that you may or may not want installed on your PC

ms-caro-malware-full:malware-type="PUA"

Potentially Unwanted Applications. Characteristics of unwanted software can include depriving users of adequate choice or control over what the software does to the computer, preventing users from removing the software, or displaying advertisements without clearly identifying their source.

ms-caro-malware-full:malware-type="PWS"

A type of malware that is used steal your personal information, such as user names and passwords. It often works along with a keylogger that collects and sends information about what keys you press and websites you visit to a malicious hacker

ms-caro-malware-full:malware-type="Ransom"

A detection for malicious programs that seize control of the computer on which they are installed. This trojan usually locks the screen and prevents the user from using the computer. It usually displays an alert message.

ms-caro-malware-full:malware-type="RemoteAccess"

A program that gives someone access to your PC from a remote location. This type of program is often installed by the computer owner

ms-caro-malware-full:malware-type="Rogue"

Software that pretends to be an antivirus program but doesn’t actually provide any security. This type of software usually gives you a lot of alerts about threats on your PC that don’t exist. It also tries to convince you to pay for its services

ms-caro-malware-full:malware-type="SettingsModifier"

A program that changes your PC settings

ms-caro-malware-full:malware-type="SoftwareBundler"

A program that installs unwanted software on your PC at the same time as the software you are trying to install, without adequate consent

ms-caro-malware-full:malware-type="Spammer"

A trojan that sends large numbers of spam emails. It may also describe the person or business responsible for sending spam

ms-caro-malware-full:malware-type="Spoofer"

A type of trojan that makes fake emails that look like they are from a legitimate source

ms-caro-malware-full:malware-type="Spyware"

A program that collects your personal information, such as your browsing history, and uses it without adequate consent

ms-caro-malware-full:malware-type="Tool"

A type of software that may have a legitimate purpose, but which may also be abused by malware authors

ms-caro-malware-full:malware-type="Trojan"

A trojan is a program that tries to look innocent, but is actually a malicious application. Unlike a virus or a worm , a trojan doesn’t spread by itself. Instead they try to look innocent to convince you to download and install them. Once installed, a trojan can steal your personal information, download more malware, or give a malicious hacker access to your PC

ms-caro-malware-full:malware-type="TrojanClicker"

A type of trojan that can use your PC to click on websites or applications. They are usually used to make money for a malicious hacker by clicking on online advertisements and making it look like the website gets more traffic than it does. They can also be used to skew online polls, install programs on your PC, or make unwanted software appear more popular than it is

ms-caro-malware-full:malware-type="TrojanDownloader"

A type of trojan that installs other malicious files, including malware, onto your PC. It can download the files from a remote PC or install them directly from a copy that is included in its file.

ms-caro-malware-full:malware-type="TrojanDropper"

A type of trojan that installs other malicious files, including malware, onto your PC. It can download the files from a remote PC or install them directly from a copy that is included in its file.

ms-caro-malware-full:malware-type="TrojanNotifier"

A type of trojan that sends information about your PC to a malicious hacker. It is similar to a password stealer

ms-caro-malware-full:malware-type="TrojanProxy"

A type of trojan that installs a proxy server on your PC. The server can be configured so that when you use the Internet, any requests you make are sent through a server controlled by a malicious hacker.

ms-caro-malware-full:malware-type="TrojanSpy"

A program that collects your personal information, such as your browsing history, and uses it without adequate consent.

ms-caro-malware-full:malware-type="VirTool"

A detection that is used mostly for malware components, or tools used for malware-related actions, such as rootkits.

ms-caro-malware-full:malware-type="Virus"

A type of malware. Viruses spread on their own by attaching their code to other programs, or copying themselves across systems and networks.

ms-caro-malware-full:malware-type="Worm"

A type of malware that spreads to other PCs. Worms may spread using one or more of the following methods: Email programs, Instant messaging programs, File-sharing programs, Social networking sites, Network shares, Removable drives with Autorun enabled, Software vulnerabilities

malware-platform

ms-caro-malware-full:malware-platform="AndroidOS"

Android operating system

ms-caro-malware-full:malware-platform="DOS"

MS-DOS platform

ms-caro-malware-full:malware-platform="EPOC"

Psion devices

ms-caro-malware-full:malware-platform="FreeBSD"

FreeBSD platform

ms-caro-malware-full:malware-platform="iPhoneOS"

iPhone operating system

ms-caro-malware-full:malware-platform="Linux"

Linux platform

ms-caro-malware-full:malware-platform="MacOS"

MAC 9.x platform or earlier

ms-caro-malware-full:malware-platform="MacOS_X"

MacOS X or later

ms-caro-malware-full:malware-platform="OS2"

OS2 platform

ms-caro-malware-full:malware-platform="Palm"

Palm operating system

ms-caro-malware-full:malware-platform="Solaris"

System V-based Unix platforms

ms-caro-malware-full:malware-platform="SunOS"

Unix platforms 4.1.3 or earlier

ms-caro-malware-full:malware-platform="SymbOS"

Symbian operatings system

ms-caro-malware-full:malware-platform="Unix"

General Unix platforms

ms-caro-malware-full:malware-platform="Win16"

Win16 (3.1) platform

ms-caro-malware-full:malware-platform="Win2K"

Windows 2000 platform

ms-caro-malware-full:malware-platform="Win32"

Windows 32-bit platform

ms-caro-malware-full:malware-platform="Win64"

Windows 64-bit platform

ms-caro-malware-full:malware-platform="Win95"

Windows 95, 98 and ME platforms

ms-caro-malware-full:malware-platform="Win98"

Windows 98 platform only

ms-caro-malware-full:malware-platform="WinCE"

Windows CE platform

ms-caro-malware-full:malware-platform="WinNT"

WinNT

ms-caro-malware-full:malware-platform="ABAP"

Advanced Business Application Programming scripts

ms-caro-malware-full:malware-platform="ALisp"

ALisp scripts

ms-caro-malware-full:malware-platform="AmiPro"

AmiPro script

ms-caro-malware-full:malware-platform="ANSI"

American National Standards Institute scripts

ms-caro-malware-full:malware-platform="AppleScript"

compiled Apple scripts

ms-caro-malware-full:malware-platform="ASP"

Active Server Pages scripts

ms-caro-malware-full:malware-platform="AutoIt"

AutoIT scripts

ms-caro-malware-full:malware-platform="BAS"

Basic scripts

ms-caro-malware-full:malware-platform="BAT"

Basic scripts

ms-caro-malware-full:malware-platform="CorelScript"

Corelscript scripts

ms-caro-malware-full:malware-platform="HTA"

HTML Application scripts

ms-caro-malware-full:malware-platform="HTML"

HTML Application scripts

ms-caro-malware-full:malware-platform="INF"

Install scripts

ms-caro-malware-full:malware-platform="IRC"

mIRC/pIRC scripts

ms-caro-malware-full:malware-platform="Java"

Java binaries (classes)

ms-caro-malware-full:malware-platform="JS"

Javascript scripts

ms-caro-malware-full:malware-platform="LOGO"

LOGO scripts

ms-caro-malware-full:malware-platform="MPB"

MapBasic scripts

ms-caro-malware-full:malware-platform="MSH"

Monad shell scripts

ms-caro-malware-full:malware-platform="MSIL"

ms-caro-malware-full:malware-platform="Perl"

Net intermediate language scripts

Perl scripts

ms-caro-malware-full:malware-platform="PHP"

Hypertext Preprocessor scripts

ms-caro-malware-full:malware-platform="Python"

Python scripts

ms-caro-malware-full:malware-platform="SAP"

SAP platform scripts

ms-caro-malware-full:malware-platform="SH"

Shell scripts

ms-caro-malware-full:malware-platform="VBA"

Visual Basic for Applications scripts

ms-caro-malware-full:malware-platform="VBS"

Visual Basic scripts

ms-caro-malware-full:malware-platform="WinBAT"

Winbatch scripts

ms-caro-malware-full:malware-platform="WinHlp"

Windows Help scripts

ms-caro-malware-full:malware-platform="WinREG"

Windows registry scripts

ms-caro-malware-full:malware-platform="A97M"

Access 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware-full:malware-platform="HE"

macro scripting

ms-caro-malware-full:malware-platform="O97M"

Office 97, 2000, XP, 2003, 2007, and 2010 macros - those that affect Word, Excel, and Powerpoint

ms-caro-malware-full:malware-platform="PP97M"

PowerPoint 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware-full:malware-platform="V5M"

Visio5 macros

ms-caro-malware-full:malware-platform="W1M"

Word1Macro

ms-caro-malware-full:malware-platform="W2M"

Word2Macro

ms-caro-malware-full:malware-platform="W97M"

Word 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware-full:malware-platform="WM"

Word 95 macros

ms-caro-malware-full:malware-platform="X97M"

Excel 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware-full:malware-platform="XF"

Excel formulas

ms-caro-malware-full:malware-platform="XM"

Excel 95 macros

ms-caro-malware-full:malware-platform="ASX"

XML metafile of Windows Media .asf files

ms-caro-malware-full:malware-platform="HC"

HyperCard Apple scripts

ms-caro-malware-full:malware-platform="MIME"

MIME packets

ms-caro-malware-full:malware-platform="Netware"

Novell Netware files

ms-caro-malware-full:malware-platform="QT"

Quicktime files

ms-caro-malware-full:malware-platform="SB"

StarBasic (Staroffice XML) files

ms-caro-malware-full:malware-platform="SWF"

Shockwave Flash files

ms-caro-malware-full:malware-platform="TSQL"

MS SQL server files

ms-caro-malware-full:malware-platform="XML"

XML files

malware-family

ms-caro-malware-full:malware-family="Zlob"

2008 - A family of trojans that often pose as downloadable media codecs. When installed, Win32/Zlob displays frequent pop-up advertisements for rogue security software

ms-caro-malware-full:malware-family="Vundo"

2008 - A multiplecomponent family of programs that deliver pop-up advertisements and may download and execute arbitrary files. Vundo is often installed as a browser helper object (BHO) without a user's consent

ms-caro-malware-full:malware-family="Virtumonde"

2008 - multi-component malware family that displays pop-up advertisements for rogue security software

ms-caro-malware-full:malware-family="Bancos"

```
2008 -  A data-stealing trojan that captures online banking credentials and relays
them to the attacker. Most variants target customers of Brazilian banks.
```

ms-caro-malware-full:malware-family="Cutwail"

2008 - A trojan that downloads and executes arbitrary files, usually to send spam. Win32/Cutwail has also been observed to transmit Win32/Newacc

ms-caro-malware-full:malware-family="Oderoor"

2008 - a backdoor trojan that allows an attacker access and control of the compromised computer. This trojan may connect with remote web sites and SMTP servers.

ms-caro-malware-full:malware-family="Newacc"

2008 - An attacker tool that automatically registers new e-mail accounts on Hotmail, AOL, Gmail, Lycos and other account service providers, using a Web service to decode CAPTCHA protection.

ms-caro-malware-full:malware-family="Captiya"

2008 - A trojan that transmits CAPTCHA images to a botnet, in what is believed to be an effort to improve the botnet's ability to detect characters and break CAPTCHAs more successfully

ms-caro-malware-full:malware-family="Taterf"

2008 - A family of worms that spread through mapped drives in order to steal login and account details for popular online games.

ms-caro-malware-full:malware-family="Frethog"

2008 - A large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games

ms-caro-malware-full:malware-family="Tilcun"

2008 - A family of trojans that steals online game passwords and sends this captured data to remote sites.

ms-caro-malware-full:malware-family="Ceekat"

2008 - A collection of trojans that steal information such as passwords for online games, usually by reading information directly from running processes in memory. Different variants target different processes.

ms-caro-malware-full:malware-family="Corripio"

2008 - a loosely-related family of trojans that attempt to steal passwords for popular online games. Detections containing the name Win32/Corripio are generic, and hence may be reported for a large number of different malicious password-stealing trojans that are otherwise behaviorally dissimilar.

ms-caro-malware-full:malware-family="Zuten"

2008 - A family of malware that steals information from online games.

ms-caro-malware-full:malware-family="Lolyda"

2008 - A family of trojans that sends account information from popular online games to a remote server. They may also download and execute arbitrary files.

ms-caro-malware-full:malware-family="Storark"

2008 - A family of trojans that steals online game passwords and sends this captured data to remote sites.

ms-caro-malware-full:malware-family="Renos"

2008 - A family of trojan downloaders that installs rogue security software.

ms-caro-malware-full:malware-family="ZangoSearchAssistant"

2008 - Adware that monitors the user’s Web-browsing activity and displays pop-up advertisements related to the Internet sites the user is viewing.

ms-caro-malware-full:malware-family="ZangoShoppingReports"

2008 - Adware that displays targeted advertising to affected users while they browse the Internet, based on search terms entered into search engines.

ms-caro-malware-full:malware-family="FakeXPA"

2008 - A rogue security software family that claims to scan for malware and then demands that the user pay to remove nonexistent threats. Some variants unlawfully use Microsoft logos and trademarks.

ms-caro-malware-full:malware-family="FakeSecSen"

2008 - A rogue security software family that claims to scan for malware and then demands that the user pay to remove non-existent threats. It appears to be based on Win32/SpySheriff

ms-caro-malware-full:malware-family="Hotbar"

2008 - Adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity.

ms-caro-malware-full:malware-family="Agent"

2008 - A generic detection for a number of trojans that may perform different malicious functions. The behaviors exhibited by this family are highly variable

ms-caro-malware-full:malware-family="Wimad"

2008 - A detection for malicious Windows Media files that can be used to encourage users to download and execute arbitrary files on an affected machine.

ms-caro-malware-full:malware-family="BaiduSobar"

2008 - A Chinese language Web browser toolbar that delivers pop-up and contextual advertisements, blocks certain other advertisements, and changes the Internet Explorer search page

ms-caro-malware-full:malware-family="VB"

2008 - A detection for various threats written in the Visual Basic programming language.

ms-caro-malware-full:malware-family="Antivirus2008"

2008 - A program that displays misleading security alerts in order to convince users to purchase rogue security software. It may be installed by Win32/Renos or manually by a computer user.

ms-caro-malware-full:malware-family="Playmp3z"

2008 - An adware family that may display advertisements in connection with the use of a 'free music player' from the site 'PlayMP3z.biz.'

ms-caro-malware-full:malware-family="Tibs"

2008 - a family of Trojans that may download and run other malicious software or may steal user data and send it to the attacker via HTTP POST or email. The Win32/Tibs family frequently downloads Trojans belonging to the Win32/Harnig and Win32/Passalert families, both of which are families of Trojan downloaders which may in turn download and run other malicious software

ms-caro-malware-full:malware-family="SeekmoSearchAssistant"

2008 - Adware that displays targeted search results and pop-up advertisements based on terms that the user enters for Web searches. The pop-up advertisements may include adult content.

ms-caro-malware-full:malware-family="RJump"

2008 - a worm that attempts to spread by copying itself to newly attached media (such as USB memory devices or network drives). It also contains backdoor functionality that allows an attacker unauthorized access to an affected computer

ms-caro-malware-full:malware-family="SpywareSecure"

2008 - A program that displays misleading warning messages in order to convince users to purchase a product that removes spyware

ms-caro-malware-full:malware-family="Winfixer"

2008 - A program that locates various registry entries, Windows prefetch content, and other types of data, identifies them as privacy violations, and urges the user to purchase the product to fix them.

ms-caro-malware-full:malware-family="C2Lop"

2008 - a trojan that modifies Web browser settings, adds Web browser bookmarks to advertisements, updates itself and delivers pop-up and contextual advertisements.

ms-caro-malware-full:malware-family="Matcash"

2008 - a multicomponent family of trojans that downloads and executes arbitrary files. Some variants of this family may install a toolbar. observed to use the Win32/Slenfbot worm as a means of distribution.

ms-caro-malware-full:malware-family="Horst"

2008 - CAPTCHA Breaker typically delivered through an executable application that masquerades as an illegal software crack or key generator

ms-caro-malware-full:malware-family="Slenfbot"

2008 - A family of worms that can spread via instant messaging programs, and may spread via removable drives. They also contain backdoor functionality that allows unauthorized access to an affected machine. This worm does not spread automatically upon installation but must be ordered to spread by a remote attacker.

ms-caro-malware-full:malware-family="Rustock"

2008 - A multicomponent family of rootkitenabled backdoor trojans, developed to aid in the distribution of spam. Recent variants appear to be associated with the incidence of rogue security programs.

ms-caro-malware-full:malware-family="Gimmiv"

2008 - a family of trojans that are sometimes installed by exploits of a vulnerability documented in Microsoft Security Bulletin MS08-067.

ms-caro-malware-full:malware-family="Yektel"

2008 - A family of trojans that display fake warnings of spyware or malware in an attempt to lure the user into installing or paying money to register rogue security products such as Win32/FakeXPA.

ms-caro-malware-full:malware-family="Roron"

2008 - This virus spreads by attaching its code to other files on your PC or network. Some of the

infected programs might no longer run correctly. Attempts to send personal information to a remote address. It may spread via e-mail, network shares, or peer-to-peer file sharing.

ms-caro-malware-full:malware-family="Swif"

2008 - A trojan that exploits a vulnerability in Adobe Flash Player to download malicious files. Adobe has published security bulletin APSB08-11 addressing the vulnerability.

ms-caro-malware-full:malware-family="Mult"

2008 - A group of threats, written in JavaScript, that attempt to exploit multiple vulnerabilities on affected computers in order to download, execute or otherwise run arbitrary code. The malicious JavaScript may be hosted on compromised or malicious websites, embedded in specially crafted PDF files, or could be called by other malicious scripts.

ms-caro-malware-full:malware-family="Wukill"

2008 - a family of mass-mailing e-mail and network worms. The Win32/Wukill worm spreads to root directories on certain local and mapped drives. The worm also spreads by sending a copy of itself as an attachment to e-mail addresses found on the infected computer.

ms-caro-malware-full:malware-family="Objsnapt"

2008 - A detection for a Javascript file that exploits a known vulnerability in the Microsoft Access Snapshot Viewer ActiveX Control.

ms-caro-malware-full:malware-family="Redirector"

2008 - The threat is a piece of JavaScript code that is inserted on bad or hacked websites. It can direct your browser to a website you don’t want to go to. You might see the detection for this threat if you visit a bad or hacked website, or if you open an email message.

ms-caro-malware-full:malware-family="Xilos"

2008 - a detection for a proof-of-concept JavaScript obfuscation technique, which was originally published in 2002 in the sixth issue of 29A, an early online magazine for virus creators

ms-caro-malware-full:malware-family="Decdec"

2008 - A detection for certain malicious JavaScript code injected in HTML pages. The virus will execute on user computers that visit compromised websites.

ms-caro-malware-full:malware-family="BearShare"

2008 - A P2P file-sharing client that uses the decentralized Gnutella network. Free versions of BearShare have come bundled with advertising supported and other potentially unwanted software.

ms-caro-malware-full:malware-family="BitAccelerator"

2008 - A program that redirects Web search results to other Web sites and may display various advertisements to users while browsing Web sites.

ms-caro-malware-full:malware-family="Blubtool"

2008 - An Internet browser search toolbar that may be installed by other third-party software, such as a peer-to-peer file sharing application. It may modify Internet explorer search settings and display unwanted advertisements.

ms-caro-malware-full:malware-family="RServer"

2008 - Commercial remote administration software that can be used to control a computer. These programs are typically installed by the computer owner or administrator and should only be removed if unexpected

ms-caro-malware-full:malware-family="UltraVNC"

2008 - A remote access program that can be used to control a computer. This program is typically installed by the computer owner or administrator, and should only be removed if unexpected.

ms-caro-malware-full:malware-family="GhostRadmin"

2008 - A remote administration tool that can be used to control a computer. These programs are typically installed by the computer owner or administrator and should only be removed if unexpected

ms-caro-malware-full:malware-family="TightVNC"

2008 - A remote control program that allows full control of the computer. These programs are typically installed by the computer owner or administrator and should only be removed if unexpected

ms-caro-malware-full:malware-family="DameWareMiniRemoteControl"

2008 - A detection for the DameWare Mini Remote Control tools. This program was detected by definitions prior to 1.147.1889.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.147.1889.0 which no longer detects this program.

ms-caro-malware-full:malware-family="SeekmoSearchAssistant_Repack"

2008 - A detection that is triggered by modified (that is, edited and re-packed) remote control programs based on DameWare Mini Remote Control, a commercial software product

ms-caro-malware-full:malware-family="Nbar"

2008 - A program that may display advertisements and redirect user searches to a certain website. It may also download malicious or unwanted content into the system without user consent.

ms-caro-malware-full:malware-family="Chir"

2008 - A family with a worm component and a virus component. The worm component spreads by email and by exploiting a vulnerability addressed by Microsoft Security Bulletin MS01-020. The virus component may infect .exe, .scr, and HTML files.

ms-caro-malware-full:malware-family="Sality"

2008 - A family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

ms-caro-malware-full:malware-family="Obfuscator"

2008 - A detection for programs that use a combination of obfuscation techniques to hinder analysis or detection by antivirus scanners

ms-caro-malware-full:malware-family="ByteVerify"

2008 - a detection of malicious code that attempts to exploit a vulnerability in the Microsoft Virtual Machine (VM). This flaw enables attackers to execute arbitrary code on a user's machine such as writing, downloading and executing additional malware. This vulnerability is addressed by update MS03-011, released in 2003.

ms-caro-malware-full:malware-family="Autorun"

2008 - A family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

ms-caro-malware-full:malware-family="Hamweq"

2008 - A worm that spreads through removable drives, such as USB memory sticks. It may contain an IRC-based backdoor enabling the computer to be controlled remotely by an attacker

ms-caro-malware-full:malware-family="Brontok"

2008 - a family of mass-mailing e-mail worms. The worm spreads by sending a copy of itself as an e-mail attachment to e-mail addresses that it gathers from files on the infected computer. It can also copy itself to USB and pen drives. Win32/Brontok can disable antivirus and security software, immediately terminate certain applications, and cause Windows to restart immediately when certain applications run. The worm may also conduct denial of service (DoS) attacks against certain Web sites

ms-caro-malware-full:malware-family="SpywareProtect"

2008 - A rogue security software family that may falsely claim that the user's computer is infected and encourages the user to buy a product for cleaning the alleged malware from the computer

ms-caro-malware-full:malware-family="Cbeplay"

2008 - A trojan that may upload computer operating system details to a remote Web site, download additional malware, and terminate debugging utilities

ms-caro-malware-full:malware-family="InternetAntivirus"

2008 - A program that displays false and misleading malware alerts to convince users to purchase rogue security software. This program also displays a fake Windows Security Center message

ms-caro-malware-full:malware-family="Nuwar"

2008 - A family of trojan droppers that install a distributed P2P downloader trojan. This downloader trojan in turn downloads an e-mail worm component.

ms-caro-malware-full:malware-family="Rbot"

2008 - A family of backdoor trojans that allows attackers to control the computer through an IRC channel

ms-caro-malware-full:malware-family="IRCbot"

2008 - A large family of backdoor trojans that drops malicious software and connects to IRC servers via a backdoor to receive commands from attackers.

ms-caro-malware-full:malware-family="SkeemoSearchAssistant"

2008 - A program that displays targeted search results and pop-up advertisements based on terms that the user enters for Web searches. The pop-up advertisements may include adult content

ms-caro-malware-full:malware-family="RealVNC"

2008 - A management tool that allows a computer to be controlled remotely. It can be installed for legitimate purposes, but can also be installed from a remote location by an attacker.

ms-caro-malware-full:malware-family="MoneyTree"

2008 - A family of software that provides the ability to search for adult content on local disk. It may also install other potentially unwanted software, such as programs that display pop-up ads.

ms-caro-malware-full:malware-family="Tracur"

2008 - A trojan that downloads and executes arbitrary files. It is sometimes distributed by ASX/Wimad.

ms-caro-malware-full:malware-family="Meredrop"

2008 - This is a generic detection for trojans that install and run malware on your PC. These trojans have been deliberately created in a complex way to hide their purpose and make them difficult to analyze.

ms-caro-malware-full:malware-family="Banker"

2008 - A family of data-stealing trojans that captures banking credentials such as account numbers and passwords from computer users and relays them to the attacker. Most variants target customers of Brazilian banks; some variants target customers of other banks.

ms-caro-malware-full:malware-family="Ldpinch"

2008 - a family of password-stealing trojans. This trojan gathers private user data such as passwords from the host computer and sends the data to the attacker at a preset e-mail address. The Win32/Ldpinch trojans use their own Simple Mail Transfer Protocol (SMTP) engine or a web-based proxy for sending the e-mail, thus copies of the sent e-mail will not appear in the affected user's e-mail client.

ms-caro-malware-full:malware-family="Advantage"

2008 - a family of adware that displays pop-up advertisements and contacts a remote server to download updates

ms-caro-malware-full:malware-family="Parite"

2008 - a family of polymorphic file infectors that targets computers running Microsoft Windows. The virus infects .exe and .scr executable files on the local file system and on writeable network shares. In turn, the infected executable files perform operations that cause other .exe and .scr files to become infected.

ms-caro-malware-full:malware-family="PossibleHostsFileHijack"

2008 - an indicator that the computer's HOSTS file may have been modified by malicious or potentially unwanted software

ms-caro-malware-full:malware-family="Alureon"

2008 - A data-stealing trojan that gathers confidential information such as user names, passwords, and credit card data from incoming and outgoing Internet traffic. It may also download malicious data and modify DNS settings.

ms-caro-malware-full:malware-family="PowerRegScheduler"

2008 - This program was detected by definitions prior to 1.159.567.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.159.567.0 which no longer detects this program.

ms-caro-malware-full:malware-family="APSB08-11"

2008 - A trojan that attempts to exploit a vulnerability in Adobe Flash Player. In the wild, this trojan has been used to download and execute arbitrary files, including other malware.

ms-caro-malware-full:malware-family="ConHook"

2008 - A family of Trojans that installs themselves as Browser Helper Objects (BHOs), and connects to the Internet without user consent. They also terminate specific security services, and download additional malware to the computer.

ms-caro-malware-full:malware-family="Starware"

2008 - This program was detected by definitions prior to 1.159.567.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.159.567.0 which no longer detects this program.

ms-caro-malware-full:malware-family="WinSpywareProtect"

2008 - A program that may falsely claim that the user's system is infected and encourages the user to buy a promoted product for cleaning the alleged malware from the computer.

ms-caro-malware-full:malware-family="MessengerSkinner"

2008 - A program, that may be distributed in the form of a freeware application, that displays advertisements, downloads additional files, and uses stealth to hide its presence

ms-caro-malware-full:malware-family="Skintrim"

2008 - A trojan that downloads and executes arbitrary files. It may be distributed by as a Microsoft Office Outlook addon used to display emoticons or other animated icons within e-mail messages.

ms-caro-malware-full:malware-family="AdRotator"

2008 - delivers advertisements, and as the name suggests, rotates advertisements among sponsors. AdRotator contacts remote Web sites in order to deliver updated content. This application also displays fake error messages that encourage users to download and install additional applications.

ms-caro-malware-full:malware-family="Wintrim"

2008 - A family of trojans that display pop-up advertisements depending on the user's keywords and browsing history. Its variants can monitor the user's activities, download applications, and send system information back to a remote server.

ms-caro-malware-full:malware-family="Busky"

2008 - A family of Trojans that monitor and redirect Internet traffic, gather system information and download unwanted software such as Win32/Renos and Win32/SpySheriff. Win32/Busky may be

installed by a Web browser exploit or other vulnerability when visiting a malicious Web site.

ms-caro-malware-full:malware-family="WhenU"

2008 - This program was detected by definitions prior to 1.173.303.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Mobis"

2008 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Sogou"

2008 - Detected by definitions prior to 1.155.995.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.155.995.0 which no longer detects this program.

ms-caro-malware-full:malware-family="Sdbot"

2008 - A family of backdoor trojans that allows attackers to control infected computers. After a computer is infected, the trojan connects to an internet relay chat (IRC) server and joins a channel to receive commands from attackers.

ms-caro-malware-full:malware-family="DelfInject"

2008 - This threat can download and run files on your PC.

ms-caro-malware-full:malware-family="Vapsup"

2008 - This threat can perform a number of actions of a malicious hacker’s choice on your PC.

ms-caro-malware-full:malware-family="BrowsingEnhancer"

2008 - This program was detected by definitions prior to 1.175.1834.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Jeefo"

2008 - virus infects executable files, such as files with a .exe extension. When an infected file runs, the virus tries to run the original content of the file while it infects other executable files on your PC. This threat might have got on your PC if you inserted a removable disk or accessed a network connection that was infected.

ms-caro-malware-full:malware-family="Sezon"

2008 - An adware that redirects web browsing to advertising or search sites.

ms-caro-malware-full:malware-family="RuPass"

2008 - a DLL component which may be utilized by adware or malicious programs in order to monitor an affected user’s Internet usage and to capture sensitive information. Win32/RuPass has been distributed as a 420,352 byte DLL file, with the file name 'ConnectionServices.dll'.

ms-caro-malware-full:malware-family="OneStepSearch"

2008 - Modifies the user’s browser to deliver targeted advertisements when the user enters search keywords. It may also replace or override web browser error pages that would otherwise be displayed when unresolvable web addresses are entered into the browser’s address bar.

ms-caro-malware-full:malware-family="GameVance"

2008 - Software that displays advertisements and tracks anonymous usage information in exchange for a free online gaming experience at the Web address 'gamevance.com.'

ms-caro-malware-full:malware-family="E404"

2008 - is a browser helper object (BHO) that takes advantage of invalid or mistyped URLs entered in the address bar by redirecting the browser to Web sites containing adware

ms-caro-malware-full:malware-family="Mirar"

2008 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Fotomoto"

2008 - A Trojan that lowers security settings, delivers advertisements, and sends system and network configuration details to a remote Web site.

ms-caro-malware-full:malware-family="Ardamax"

2008 - The tool can capture your activity on your PC (such as the keys you press when typing in passwords) and might send this information to a hacker.

ms-caro-malware-full:malware-family="Hupigon"

2008 - A family of trojans that uses a dropper to install one or more backdoor files and sometimes installs a password stealer or other malicious programs.

ms-caro-malware-full:malware-family="CNNIC"

2008 - enables Chinese keyword searching in Internet Explorer and adds support for other applications to use Chinese domain names that registered with CNNIC. Also contains a kernel driver that protects its files and registry settings from being modified or deleted

ms-caro-malware-full:malware-family="MotePro"

2008 - May display advertisement pop-ups, and download programs from predefined Web sites. When installed, Win32/MotePro runs as a Web Browser Helper Object (BHO).

ms-caro-malware-full:malware-family="CnsMin"

2008 - Installs a browser helper object (BHO) that redirects Internet Explorer searches to a Chinese search portal. CnsMin may be installed without adequate user consent. It may prevent its files from being removed or restore files that have been previously removed.

ms-caro-malware-full:malware-family="BaiduIebar"

2008 - A detection for an address line search tool. This program was detected by definitions prior to 1.153.956.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.153.956.0 which no longer detects this program.

ms-caro-malware-full:malware-family="Ejik"

2008 - This program was detected by definitions prior to 1.175.1915.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="AlibabaIEToolBar"

2008 - This program was detected by definitions prior to 1.175.1834.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="BDPlugin"

2008 - a DLL file which is usually introduced to an affected system as a component of BrowserModifier:Win32/BaiduSobar. It may display unwanted pop-ups and advertisements on the affected system.

ms-caro-malware-full:malware-family="Adialer"

2008 - A trojan dialer program that connects to a premium number, or attempts to connect to adult websites via particular phone numbers without your permission, connects to remote hosts without user consent.

ms-caro-malware-full:malware-family="EGroupSexDial"

2008 - A dialer program that may attempt to dial a premium number, thus possibly resulting in international phone charges for the user.

ms-caro-malware-full:malware-family="Zonebac"

2008 - A family of backdoor Trojans that allows a remote attacker to download and run arbitrary programs, and which may upload computer configuration information and other potentially sensitive data to remote Web sites.

ms-caro-malware-full:malware-family="Antinny"

2008 - A family of worms that targets certain versions of Microsoft Windows. The worm spreads using a Japanese peer-to-peer file-sharing application named Winny. The worm creates a copy of itself with a deceptive file name in the Winny upload folder so that it can be downloaded by other Winny users.

ms-caro-malware-full:malware-family="RewardNetwork"

2008 - A program that monitors an affected user’s Internet usage and reports this usage to a remote server. Win32/RewardNetwork may be visible as an Internet Explorer toolbar.

ms-caro-malware-full:malware-family="Virut"

2008 - A family of file infecting viruses that target and infect .exe and .scr files accessed on infected systems. Win32/Virut also opens a backdoor by connecting to an IRC server

ms-caro-malware-full:malware-family="Allaple"

2008 - A multi-threaded, polymorphic network worm capable of spreading to other computers connected to a local area network (LAN) and performing denial-of-service (DoS) attacks against targeted remote Web sites.

ms-caro-malware-full:malware-family="VKit_DA"

2008 - This virus spreads by attaching its code to other files on your PC or network. Some of the infected programs might no longer run correctly.

ms-caro-malware-full:malware-family="Small"

2008 - A generic detection for a variety of threats.

ms-caro-malware-full:malware-family="Netsky"

2008 - A mass-mailing worm that spreads by e-mailing itself to addresses found on an infected computer. Some variants contain a backdoor component and perform DoS attacks.

ms-caro-malware-full:malware-family="Luder"

2008 - A virus that spreads by infecting executable files, by inserting itself into .RAR archive files, and by sending a copy of itself as an attachment to e-mail addresses found on the infected computer. This virus has a date-activated, file damaging payload, and may connect to a remote server and accept commands from an attacker.

ms-caro-malware-full:malware-family="IframeRef"

2008 - A generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.

ms-caro-malware-full:malware-family="Lovelorn"

2008 - This threat is classified as a mass-mailing worm. A mass mailing email worm is self-contained malicious code that propagates by sending itself through e-mail. Typically, a mass mailing email worm uses its own SMTP engine to send itself, thus copies of the sent worm will not appear in the infected user's outgoing or sent email folders. Technical details are currently not available.

ms-caro-malware-full:malware-family="Cekar"

2008 - This threat downloads and installs other programs, including other malware, onto your PC without your consent.

ms-caro-malware-full:malware-family="Dialsnif"

2008 - This threat can perform a number of actions of a malicious hacker's choice on your PC.

ms-caro-malware-full:malware-family="Conficker"

2008 - A worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products and downloads arbitrary files.

ms-caro-malware-full:malware-family="LoveLetter"

2009 - A family of mass-mailing worms that targets computers running certain versions of Windows. It can spread as an e-mail attachment and through an Internet Relay Chat (IRC) channel. The worm can download, overwrite, delete, infect, and run files on the infected computer.

ms-caro-malware-full:malware-family="VBSWGbased"

2009 - A generic detection for VBScript code that is known to be automatically generated by a particular malware tool.

ms-caro-malware-full:malware-family="Slammer"

2009 - A memory resident worm that spreads through a vulnerability present in computers running

either MSDE 2000 or SQL Server that have not applied Microsoft Security Bulletin MS02-039.

ms-caro-malware-full:malware-family="Msblast"

2009 - A family of network worms that exploit a vulnerability addressed by security bulletin MS03-039. The worm may attempt Denial of Service (DoS) attacks on some server sites or create a backdoor on the infected system

ms-caro-malware-full:malware-family="Sasser"

2009 - A family of network worms that exploit a vulnerability fixed by security bulletin MS04-011. The worm spreads by randomly scanning IP addresses for vulnerable machines and infecting any that are found

ms-caro-malware-full:malware-family="Nimda"

2009 - A family of worms that spread by exploiting a vulnerability addressed by Microsoft Security Bulletin MS01-020. The worm compromises security by sharing the C drive and creating a Guest account with administrator permissions.

ms-caro-malware-full:malware-family="Mydoom"

2009 - A family of massmailing worms that spread through e-mail. Some variants also spread through P2P networks. It acts as a backdoor trojan and can sometimes be used to launch DoS attacks against specific Web sites

ms-caro-malware-full:malware-family="Bagle"

2009 - A worm that spreads by e-mailing itself to addresses found on an infected computer. Some variants also spread through peer-to-peer (P2P) networks. Bagle acts as a backdoor trojan and can be used to distribute other malicious software.

ms-caro-malware-full:malware-family="Winwebsec"

2009 - A family of rogue security software programs that have been distributed with several different names. The user interface varies to reflect each variant’s individual branding

ms-caro-malware-full:malware-family="Koobface"

2009 - A multicomponent family of malware used to compromise computers and use them to perform various malicious tasks. It spreads through the internal messaging systems of popular social networking sites

ms-caro-malware-full:malware-family="Pdfjsc"

2009 - a family of specially crafted PDF files that exploits vulnerabilities in Adobe Acrobat and Adobe Reader. The files contain malicious JavaScript that executes when opened with a vulnerable program.

ms-caro-malware-full:malware-family="Pointfree"

2009 - a browser modifier that redirects users when invalid Web site addresses or search terms are entered in the Windows Internet Explorer address bar

ms-caro-malware-full:malware-family="Chadem"

2009 - A trojan that steals password details from an infected computer by monitoring network traffic associated with FTP connections.

ms-caro-malware-full:malware-family="FakeIA"

2009 - A rogue security software family that impersonates the Windows Security Center. It may display product names or logos in an apparently unlawful attempt to impersonate Microsoft products

ms-caro-malware-full:malware-family="Waledac"

2009 - A trojan that is used to send spam. It also has the ability to download and execute arbitrary files, harvest e-mail addresses from the local machine, perform denial-of-service attacks, proxy network traffic, and sniff passwords

ms-caro-malware-full:malware-family="Provis"

2009 - This threat can perform a number of actions of a malicious hacker’s choice on your PC.

ms-caro-malware-full:malware-family="Prolaco"

2009 - A family of worms that spreads via email, removable drives, Peer-to-Peer (P2P) and network shares. This worm may also drop and execute other malware.

ms-caro-malware-full:malware-family="Mywife"

2009 - A mass-mailing network worm that targets certain versions of Microsoft Windows. The worm spreads through e-mail attachments and writeable network shares. It is designed to corrupt the content of specific files on the third day of every month.

ms-caro-malware-full:malware-family="Melissa"

2009 - A macro worm that spreads via e-mail and by infecting Word documents and templates. It is designed to work in Word 97 and Word 2000, and it uses Outlook to reach new targets through e-mail

ms-caro-malware-full:malware-family="Rochap"

2009 - A family of multicomponent trojans that download and execute additional malicious files. While downloading, some variants display a video from the Web site 'youtube.com' presumably to distract the user

ms-caro-malware-full:malware-family="Gamania"

2009 - A family of trojans that steals online game passwords and sends them to remote sites.

ms-caro-malware-full:malware-family="Mabezat"

2009 - a polymorphic virus that infects Windows executable files. Apart from spreading through file infection, it also attempts to spread through e-mail attachments, network shares, removable drives and by CD-burning. It also contains a date-based payload that encrypts files with particular extensions.

ms-caro-malware-full:malware-family="Helpud"

2009 - A family of trojans that steals login information for popular online games. The gathered information is then sent to remote websites.

ms-caro-malware-full:malware-family="PrivacyCenter"

2009 - a family of programs that claims to scan for malware and displays fake warnings of 'malicious programs and viruses'. They then inform the user that they need to pay money to register the software in order to remove these non-existent threats.

ms-caro-malware-full:malware-family="FakeRean"

2009 - This family of rogue security programs pretend to scan your PC for malware, and often report lots of infections. The program will say you have to pay for it before it can fully clean your PC. However, the program hasn’t really detected any malware at all and isn’t really an antivirus or antimalware scanner. It just looks like one so you’ll send money to the people who made the program. Some of these programs use product names or logos that unlawfully impersonate Microsoft products.

ms-caro-malware-full:malware-family="Bredolab"

2009 - A downloader that can access and execute arbitrary files from a remote host. Bredolab has been observed to download several other malware families to infected computers

ms-caro-malware-full:malware-family="Rugzip"

2009 - A trojan that downloads other malware from predefined Web sites. Rugzip may itself be installed by other malware. Once it has performed its malicious routines, it deletes itself to avoid detection.

ms-caro-malware-full:malware-family="Fakespypro"

2009 - A rogue security family that falsely claims that the affected computer is infected with malware and encourages the user to buy a promoted product it claims will clean the computer.

ms-caro-malware-full:malware-family="Buzuz"

2009 - A trojan that downloads malware known as 'SpywareIsolator' a rogue security software program.

ms-caro-malware-full:malware-family="PoisonIvy"

2009 - A family of backdoor trojans that allow unauthorized access to and control of an affected machine. Poisonivy attempts to hide by injecting itself into other processes

ms-caro-malware-full:malware-family="AgentBypass"

2009 - A detection for files that attempt to inject possibly malicious code into the explorer.exe process.

ms-caro-malware-full:malware-family="Enfal"

2009 - This threat can perform a number of actions of a malicious hacker’s choice on your PC.

ms-caro-malware-full:malware-family="SystemHijack"

2009 - A generic detection that uses advanced heuristics in the Microsoft Antivirus engine to detect malware that displays particular types of malicious behavior.

ms-caro-malware-full:malware-family="ProcInject"

2009 - This threat can perform a number of actions of a malicious hacker’s choice on your PC.

ms-caro-malware-full:malware-family="Malres"

2009 - A trojan that drops another malware, detected as Virtool:WinNT/Malres.A, into the system.

ms-caro-malware-full:malware-family="Kirpich"

2009 - a trojan that drops malicious code into the system. It also infects two system files; the infected files are detected as Virus:Win32/Kirpich.A, in the system. This does not constitute virus behavior for the trojan as it does not infect any other files and therefore does not have any conventional replication routines. TrojanDropper:Win32/Kirpich.A also disables Data Execution Protection and steals specific system information.

ms-caro-malware-full:malware-family="Malagent"

2009 - A generic detection for a variety of threats.

ms-caro-malware-full:malware-family="Bumat"

2009 - A generic detection for a variety of threats.

ms-caro-malware-full:malware-family="Bifrose"

2009 - A backdoor trojan that allows a remote attacker to access the compromised computer and injects its processes into the Windows shell and Internet Explorer.

ms-caro-malware-full:malware-family="Ripinip"

2009 - This threat can give a hacker unauthorized access and control of your PC.

ms-caro-malware-full:malware-family="Riler"

2009 - This threat can perform a number of actions of a malicious hacker’s choice on your PC.

ms-caro-malware-full:malware-family="Farfli"

2009 - A trojan that drops various files detected as malware into a system. It also has backdoor capabilities that allow it to contact a remote attacker and wait for instructions.

ms-caro-malware-full:malware-family="PcClient"

2009 - A backdoor trojan family with several components including a key logger, backdoor, and a rootkit.

ms-caro-malware-full:malware-family="Veden"

2009 - A name used for backdoor trojan detections that have been added to Microsoft signatures after advanced automated analysis.

ms-caro-malware-full:malware-family="Banload"

2009 - A family of trojans that download other malware. Banload usually downloads Win32/Banker, which steals banking credentials and other sensitive data and sends it back to a remote attacker.

ms-caro-malware-full:malware-family="Microjoin"

2009 - a tool that is used to deploy malware without being detected. It is used to bundle multiple files, consisting of a clean file and malware files, into a single executable.

ms-caro-malware-full:malware-family="Killav"

2009 - a trojan that terminates a large number of security-related processes, including those for antivirus, monitoring, or debugging tools, and may install certain exploits for the vulnerability addressed by Microsoft Security Bulletin MS08-067

ms-caro-malware-full:malware-family="Cinmus"

2009 - This threat can perform a number of actions of a malicious hacker’s choice on your PC.

ms-caro-malware-full:malware-family="MessengerPlus"

2009 - A non-Microsoft add-on for Microsoft's Windows Live Messenger, called Messenger Plus!. It comes with an optional sponsor program installation, detected as Spyware:Win32/C2Lop.

ms-caro-malware-full:malware-family="Haxdoor"

2009 - a backdoor trojan that allows remote control of the machine over the Internet. The trojan is rootkit-enabled, allowing it to hide processes and files related to the threat. Haxdoor lowers security settings on the computer and gathers user and system information to send to a third party

ms-caro-malware-full:malware-family="Nieguide"

2009 - a detection for a DLL file that connects to a Web site and may display advertisements or download other programs

ms-caro-malware-full:malware-family="Ithink"

2009 - displays pop-up advertisements; it is usually bundled with other applications

ms-caro-malware-full:malware-family="Pointad"

2009 - This program was detected by definitions prior to 1.175.2145.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Webdir"

2009 - A Web Browser Helper Object (BHO) used to collect user information and display targeted advertisings using Internet Explorer browser. Webdir attempts to modify certain visited urls to include affiliate IDs.

ms-caro-malware-full:malware-family="Microbillsys"

2009 - a program that processes payments made to a billing Web site. It is considered potentially unwanted software because it cannot be removed from the Add/Remove Programs list in Control Panel; rather, a user requires an 'uninstall code' before the program can be removed.

ms-caro-malware-full:malware-family="Kerlofost"

2009 - a browser helper object (BHO) that may modify browsing behavior; redirect searches; report user statistics, behavior, and searches back to a remote server; and display pop-up advertisements.

ms-caro-malware-full:malware-family="Zwangi"

2009 - A program that runs as a service in the background and modifies Web browser settings to visit a particular Web site

ms-caro-malware-full:malware-family="DoubleD"

2009 - an adware program that displays pop-up advertising, runs at each system start and is installed as an Internet Explorer toolbar.

ms-caro-malware-full:malware-family="ShopAtHome"

2009 - A browser redirector that monitors Web-browsing behavior and online purchases. It claims to track points for ShopAtHome rebates when the user buys products directly from affiliated merchant Web sites.

ms-caro-malware-full:malware-family="FakeVimes"

2009 - a downloading component of Win32/FakeVimes - a family of programs that claims to scan for malware and displays fake warnings of 'malicious programs and viruses'. They then inform the user that they need to pay money to register the software in order to remove these non-existent threats.

ms-caro-malware-full:malware-family="FakeCog"

2009 - This threat claims to scan your PC for malware and then shows you fake warnings. They try to convince you to pay to register the software to remove the non-existent threats.

ms-caro-malware-full:malware-family="FakeAdPro"

2009 - a program that may display false and misleading alerts regarding errors and malware to entice users to purchase it.

ms-caro-malware-full:malware-family="FakeSmoke"

2009 - a family of trojans consisting of a fake Security Center interface and a fake antivirus program.

ms-caro-malware-full:malware-family="FakeBye"

2009 - A rogue security software family that uses a Korean-language user interface.

ms-caro-malware-full:malware-family="Hiloti"

2009 - a generic detection for a trojan that interferes with an affected user’s browsing habits and downloads and executes arbitrary files.

ms-caro-malware-full:malware-family="Tikayb"

2009 - A trojan that attempts to establish a secure network connection to various Web sites without the user’s consent.

ms-caro-malware-full:malware-family="Ursnif"

2009 - A family of trojans that steals sensitive information from an affected computer

ms-caro-malware-full:malware-family="Rimecud"

2009 - A family of worms with multiple components that spreads via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system

ms-caro-malware-full:malware-family="Lethic"

2009 - A trojan that connects to remote servers, which may lead to unauthorized access to an affected system.

ms-caro-malware-full:malware-family="CeeInject"

2009 - This threat has been 'obfuscated', which means it has tried to hide its purpose so your security software doesn’t detect it. The malware that lies underneath this obfuscation can have almost any purpose.

ms-caro-malware-full:malware-family="Cmdow"

2009 - a detection for a command-line tool and violated the guidelines by which Microsoft identified unwanted software.

ms-caro-malware-full:malware-family="Yabector"

2009 - This trojan can use your PC to click on online advertisements without your permission or knowledge. This can earn money for a malicious hacker by making a website or application appear more popular than it is.

ms-caro-malware-full:malware-family="Renocide"

2009 - a family of worms that spread via local, removable, and network drives and also using file sharing applications. They have IRC-based backdoor functionality, which may allow a remote attacker to execute commands on the affected computer.

ms-caro-malware-full:malware-family="Liften"

2009 - a trojan that is used to stop affected users from downloading security updates. It is downloaded by Trojan:Win32/FakeXPA.

ms-caro-malware-full:malware-family="ShellCode"

2009 - A generic detection for JavaScript-enabled objects that contain exploit code and may exhibit suspicious behavior. Malicious websites and malformed PDF documents may contain JavaScript that attempts to execute code without the affected user’s consent.

ms-caro-malware-full:malware-family="FlyAgent"

2009 - A backdoor trojan program that is capable of performing several actions depending on the commands of a remote attacker.

ms-caro-malware-full:malware-family="Psyme"

2009 - This threat downloads and installs other programs, including other malware, onto your PC without your consent.

ms-caro-malware-full:malware-family="Orsam"

2009 - A generic detection for a variety of threats. A name used for trojans that have been added to MS signatures after advanced automated analysis.

ms-caro-malware-full:malware-family="AgentOff"

2009 - This threat can perform a number of actions of a malicious hacker’s choice on your PC.

ms-caro-malware-full:malware-family="Nuj"

2009 - a worm that copies itself to fixed, removable or network drives. Some variants of this worm may also terminate antivirus-related processes.

ms-caro-malware-full:malware-family="Sohanad"

2009 - Worms automatically spread to other PCs. They can do this in a number of ways, including by copying themselves to removable drives, network folders, or spreading through email.

ms-caro-malware-full:malware-family="I2ISolutions"

2009 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Dpoint"

2009 - This program was detected by definitions prior to 1.175.1915.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Silly_P2P"

2009 - Worms automatically spread to other PCs. They can do this in a number of ways, including by copying themselves to removable drives, network folders, or spreading through email.

ms-caro-malware-full:malware-family="Vobfus"

2009 - This family of worms can download other malware onto your PC, including: Win32/Beebone,

Win32/Fareit, Win32/Zbot. Vobfus worms can be downloaded by other malware or spread via removable drives, such as USB flash drives.

ms-caro-malware-full:malware-family="Daurso"

2009 - a family of trojans that attempts to steal sensitive information, including passwords and FTP authentication details from affected computers. This family targets particular FTP applications and also attempts to steal data from Protected Storage.

ms-caro-malware-full:malware-family="MyDealAssistant"

2009 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Adsubscribe"

2009 - This program was detected by definitions prior to 1.175.1834.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="MyCentria"

2009 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Fierads"

2009 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="VBInject"

2009 - This is a generic detection for malicious files that are obfuscated using particular techniques to prevent their detection or analysis.

ms-caro-malware-full:malware-family="PerfectKeylogger"

2009 - a commercial monitoring program that monitors user activity, such as keystrokes typed. MonitoringTool:Win32/PerfectKeylogger is available for purchase at the company's website. It may also have been installed without user consent by a Trojan or other malware.

ms-caro-malware-full:malware-family="AgoBot"

2010 VOL09 - A backdoor that communicates with a central server using IRC.

ms-caro-malware-full:malware-family="Bubnix"

2010 VOL09 - A generic detection for a kernel-mode driver installed by other malware that hides its presence on an affected computer by blocking registry and file access to itself. The trojan may report its installation to a remote server and download and distribute spam email messages and could download and execute arbitrary files.

ms-caro-malware-full:malware-family="Citeary"

2010 VOL09 - A kernel mode driver installed by Win32/Citeary, a worm that spreads to all available drives including the local drive, installs device drivers and attempts to download other malware from a predefined website.

ms-caro-malware-full:malware-family="Fakeinit"

2010 VOL09 - A rogue security software family distributed under the names Internet Security 2010, Security Essentials 2010, and others.

ms-caro-malware-full:malware-family="Oficla"

2010 VOL09 - A family of trojans that attempt to inject code into running processes in order to download and execute arbitrary files. It may download rogue security programs.

ms-caro-malware-full:malware-family="Pasur"

2010 VOL09 - a name used for backdoor trojan detections that have been added to Microsoft signatures after advanced automated analysis.

ms-caro-malware-full:malware-family="PrettyPark"

2010 VOL09 - A worm that spreads via email attachments. It allows backdoor access and control of an infected computer.

ms-caro-malware-full:malware-family="Prorat"

2010 VOL09 - A trojan that opens random ports that allow remote access from an attacker to the affected computer. This backdoor may download and execute other malware from predefined websites and may terminate several security applications or services.

ms-caro-malware-full:malware-family="Pushbot"

2010 VOL09 - A detection for a family of malware that spreads via MSN Messenger, Yahoo! Messenger, and AIM when commanded by a remote attacker. It contains backdoor functionality that allows unauthorized access and control of an affected machine.

ms-caro-malware-full:malware-family="Randex"

2010 VOL09 - A worm that scans randomly generated IP addresses to attempt to spread to network shares with weak passwords. After the worm infects a computer, it connects to an IRC server to

receive commands from the attacker.

ms-caro-malware-full:malware-family="SDBot"

2010 VOL09 - A family of backdoor trojans that allows attackers to control infected computers over an IRC channel.

ms-caro-malware-full:malware-family="Trenk"

2010 VOL09 - a name used for backdoor trojan detections that have been added to Microsoft signatures after advanced automated analysis.

ms-caro-malware-full:malware-family="Tofsee"

2010 VOL09 - A multi-component family of backdoor trojans that act as a spam and traffic relay.

ms-caro-malware-full:malware-family="Ursap"

2010 VOL09 - a name used for backdoor trojan detections that have been added to Microsoft signatures after advanced automated analysis.

ms-caro-malware-full:malware-family="Zbot"

2010 VOL09 - A family of password stealing trojans that also contains backdoor functionality allowing unauthorized access and control of an affected machine.

ms-caro-malware-full:malware-family="Ciucio"

2010 VOL10 - A family of trojans that connect to certain websites in order to download arbitrary files.

ms-caro-malware-full:malware-family="ClickPotato"

2010 VOL10 - A program that displays popup and notification-style advertisements based on the user’s browsing habits.

ms-caro-malware-full:malware-family="CVE-2010-0806"

2010 VOL10 - A detection for malicious JavaScript that attempts to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-018.

ms-caro-malware-full:malware-family="Delf"

2010 VOL10 - A detection for various threats written in the Delphi programming language. The behaviors displayed by this malware family are highly variable.

ms-caro-malware-full:malware-family="FakePAV"

2010 VOL10 - A rogue security software family that masquerades as Microsoft Security Essentials.

ms-caro-malware-full:malware-family="Keygen"

2010 VOL10 - A generic detection for tools that generate product keys for illegally obtained versions of various software products.

ms-caro-malware-full:malware-family="Onescan"

2010 VOL10 - A Korean-language rogue security software family distributed under the names One Scan, Siren114, EnPrivacy, PC Trouble, My Vaccine, and others.

ms-caro-malware-full:malware-family="Pornpop"

2010 VOL10 - A generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

ms-caro-malware-full:malware-family="Startpage"

2010 VOL10 - A detection for various threats that change the configured start page of the affected user's web browser, and may also perform other malicious actions.

ms-caro-malware-full:malware-family="Begseabug"

2011 VOL11 - A trojan that downloads and executes arbitrary files on an affected computer.

ms-caro-malware-full:malware-family="CVE-2010-0840"

2011 VOL11 - A detection for a malicious and obfuscated Java class that exploits a vulnerability described in CVE-2010-0840. Oracle Corporation addressed the vulnerability with a security update in March 2010.

ms-caro-malware-full:malware-family="Cycbot"

2011 VOL11 - A backdoor trojan that allows attackers unauthorized access and control of an affected computer. After a computer is infected, the trojan connects to a specific remote server to receive commands from attackers.

ms-caro-malware-full:malware-family="DroidDream"

2011 VOL11 - A malicious program that affects mobile devices running the Android operating system. It may be bundled with clean applications, and is capable of allowing a remote attacker to gain access to the mobile device.

ms-caro-malware-full:malware-family="FakeMacdef"

2011 VOL11 - A rogue security software family that affects Apple Mac OS X. It has been distributed under the names MacDefender, MacSecurity, MacProtector, and possibly others.

ms-caro-malware-full:malware-family="GameHack"

2011 VOL11 - Malware that is often bundled with game applications. It commonly displays unwanted pop-up advertisements and may be installed as a web browser helper object.

ms-caro-malware-full:malware-family="Loic"

2011 VOL11 - An open-source network attack tool designed to perform denial-ofservice (DoS) attacks.

ms-caro-malware-full:malware-family="Lotoor"

2011 VOL11 - A detection for specially crafted Android programs that attempt to exploit vulnerabilities in the Android operating system to gain root privilege.

ms-caro-malware-full:malware-family="Nuqel"

2011 VOL11 - A worm that spreads via mapped drives and certain instant messaging applications. It may modify system settings, connect to certain websites, download arbitrary files, or take other malicious actions.

ms-caro-malware-full:malware-family="OfferBox"

2011 VOL11 - A program that displays offers based on the user's web browsing habits. Some versions may display advertisements in a pop-under window. Win32/OfferBox may be installed without adequate user consent by malware.

ms-caro-malware-full:malware-family="OpenCandy"

2011 VOL11 - An adware program that may be bundled with certain thirdparty software installation programs. Some versions may send user-specific information, including a unique machine code, operating system information, locale, and certain other information to a remote server without obtaining adequate user consent.

ms-caro-malware-full:malware-family="Pameseg"

2011 VOL11 - A fake program installer that requires the user to send SMS messages to a premium number to successfully install certain programs.

ms-caro-malware-full:malware-family="Pramro"

2011 VOL11 - A trojan that creates a proxy on the infected computer for email and HTTP traffic, and is used to send spam email.

ms-caro-malware-full:malware-family="Ramnit"

2011 VOL11 - A family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await

instructions from a remote attacker.

ms-caro-malware-full:malware-family="Rlsloup"

2011 VOL11 - A family of trojans that are used to send spam email. Rlsloup consists of several components, including an installation trojan component and a spamming payload component.

ms-caro-malware-full:malware-family="ShopperReports"

2011 VOL11 - Adware that displays targeted advertising to affected users while browsing the Internet, based on search terms entered into search engines.

ms-caro-malware-full:malware-family="Sinowal"

2011 VOL11 - A family of password-stealing and backdoor trojans. It may try to install a fraudulent SSL certificate on the computer. Sinowal may also capture user data such as banking credentials from various user accounts and send the data to Web sites specified by the attacker.

ms-caro-malware-full:malware-family="Stuxnet"

2011 VOL11 - A multi-component family that spreads via removable volumes by exploiting the vulnerability addressed by Microsoft Security Bulletin MS10-046.

ms-caro-malware-full:malware-family="Swimnag"

2011 VOL11 - A worm that spreads via removable drives and drops a randomly-named DLL in the Windows system folder.

ms-caro-malware-full:malware-family="Tedroo"

2011 VOL11 - A trojan that sends spam email messages. Some variants may disable certain Windows services or allow backdoor access by a remote attacker.

ms-caro-malware-full:malware-family="Yimfoca"

2011 VOL11 - A worm family that spreads via common instant messaging applications and social networking sites. It is capable of connecting to a remote HTTP or IRC server to receive updated configuration data. It also modifies certain system and security settings.

ms-caro-malware-full:malware-family="Bamital"

2011 VOL12 - A family of malware that intercepts web browser traffic and prevents access to specific security-related websites by modifying the Hosts file. Bamital variants may also modify specific legitimate Windows files in order to execute their payload.

ms-caro-malware-full:malware-family="Blacole"

2011 VOL12 - An exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a

vulnerable computer browses a compromised website containing the exploit pack, various malware may be downloaded and run.

ms-caro-malware-full:malware-family="Bulilit"

2011 VOL12 - A trojan that silently downloads and installs other programs without consent. Infection could involve the installation of additional malware or malware components to an affected computer.

ms-caro-malware-full:malware-family="Dorkbot"

2011 VOL12 - A worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. Win32/Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits.

ms-caro-malware-full:malware-family="EyeStye"

2011 VOL12 - A trojan that attempts to steal sensitive data using a method known as form grabbing, and sends it to a remote attacker. It may also download and execute arbitary files and use a rootkit component to hide its activities.

ms-caro-malware-full:malware-family="FakeSysdef"

2011 VOL12 - A rogue security software family that claims to discover nonexistent hardware defects related to system memory, hard drives, and overall system performance, and charges a fee to fix the supposed problems.

ms-caro-malware-full:malware-family="Helompy"

2011 VOL12 - A worm that spreads via removable drives and attempts to capture and steal authentication details for a number of different websites or online services, including Facebook and Gmail.

ms-caro-malware-full:malware-family="Malf"

2011 VOL12 - A generic detection for malware that drops additional malicious files.

ms-caro-malware-full:malware-family="Rugo"

2011 VOL12 - A program that installs silently on the user’s computer and displays advertisements.

ms-caro-malware-full:malware-family="Sirefef"

2011 VOL12 - A rogue security software family distributed under the name Antivirus 2010 and others.

ms-caro-malware-full:malware-family="Sisproc"

2011 VOL12 - A generic detection for a group of trojans that have been observed to perform a number of various and common malware behaviors.

ms-caro-malware-full:malware-family="Swisyn"

2011 VOL12 - A trojan that drops and executes arbitrary files on an infected computer. The dropped files may be potentially unwanted or malicious programs.

ms-caro-malware-full:malware-family="BlacoleRef"

2012 VOL13 - An obfuscated script, often found inserted into compromised websites, that uses a hidden inline frame to redirect the browser to a Blacole exploit server.

ms-caro-malware-full:malware-family="CVE-2012-0507"

2012 VOL13 - A detection for a malicious Java applet that exploits the Java Runtime Environment (JRE) vulnerability described in CVE-2012-0507, addressed by an Oracle security update in February 2012.

ms-caro-malware-full:malware-family="Flashback"

2012 VOL13 - A trojan that targets Java JRE vulnerability CVE-2012-0507 on Mac OS X to enroll the infected computer in a botnet.

ms-caro-malware-full:malware-family="Gendows"

2012 VOL13 - A tool that attempts to activate Windows 7 and Windows Vista operating system installations.

ms-caro-malware-full:malware-family="GingerBreak"

2012 VOL13 - A program that affects mobile devices running the Android operating system. It drops and executes an exploit that, if run successfully, gains administrator privileges on the device.

ms-caro-malware-full:malware-family="GingerMaster"

2012 VOL13 - A malicious program that affects mobile devices running the Android operating system. It may be bundled with clean applications, and is capable of allowing a remote attacker to gain access to the mobile device.

ms-caro-malware-full:malware-family="Mult_JS"

2012 VOL13 - A generic detection for various exploits written in the JavaScript language.

ms-caro-malware-full:malware-family="Patch"

2012 VOL13 - A family of tools intended to modify, or 'patch' programs that may be evaluation

copies, or unregistered versions with limited features for the purpose of removing the limitations.

ms-caro-malware-full:malware-family="Phoex"

2012 VOL13 - A malicious script that exploits the Java Runtime Environment (JRE) vulnerability discussed in CVE-2010-4452. If run in a computer running a vulnerable version of Java, it downloads and executes arbitrary files.

ms-caro-malware-full:malware-family="Pluzoks"

2012 VOL13 - A trojan that silently downloads and installs other programs without consent. This could include the installation of additional malware or malware components.

ms-caro-malware-full:malware-family="Popupper"

2012 VOL13 - A detection for a particular JavaScript script that attempts to display pop-under advertisements.

ms-caro-malware-full:malware-family="Wizpop"

2012 VOL13 - Adware that may track user search habits and download executable programs without user consent.

ms-caro-malware-full:malware-family="Wpakill"

2012 VOL13 - A family of tools that attempt to disable or bypass WPA (Windows Product Activation), WGA (Windows Genuine Advantage) checks, or WAT (Windows Activation Technologies), by altering Windows operating system files, terminating processes, or stopping services.

ms-caro-malware-full:malware-family="Yeltminky"

2012 VOL13 - A family of worms that spreads by making copies of itself on all available drives and creating an autorun.inf file to execute that copy.

ms-caro-malware-full:malware-family="Aimesu"

2013 VOL15 - A threat that exploits vulnerabilities in unpatched versions of Java, Adobe Reader, or Flash Player. It then installs other malare on the computer, including components of the Blackhole and Cool exploit kits.

ms-caro-malware-full:malware-family="Bdaejec"

2013 VOL15 - A trojan that allows unauthorized access and control of an affected computer, and that may download and install other programs without consent.

ms-caro-malware-full:malware-family="Bursted"

2013 VOL15 - A virus written in the AutoLISP scripting language used by the AutoCAD computer-aided design program. It infects other AutoLISP files with the extension .lsp.

ms-caro-malware-full:malware-family="Colkit"

2013 VOL15 - A detection for obfuscated, malicious JavaScript code that redirects to or loads files that may exploit a vulnerable version of Java, Adobe Reader, or Adobe Flash, possibly in an attempt to load malware onto the computer.

ms-caro-malware-full:malware-family="Coolex"

2013 VOL15 - A detection for scripts from an exploit pack known as the Cool Exploit Kit. These scripts are often used in ransomware schemes in which an attacker locks a victim’s computer or encrypts the user’s data and demands money to make it available again.

ms-caro-malware-full:malware-family="CplLnk"

2013 VOL15 - A generic detection for specially crafted malicious shortcut files that attempt to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-046, CVE-2010-2568.

ms-caro-malware-full:malware-family="CVE-2011-1823"

2013 VOL15 - A detection for specially crafted Android programs that attempt to exploit a vulnerability in the Android operating system to gain root privilege.

ms-caro-malware-full:malware-family="CVE-2012-1723"

2013 VOL15 - A family of malicious Java applets that attempt to exploit vulnerability CVE-2012-1723 in the Java Runtime Environment (JRE) to download and install files of an attacker’s choice onto the computer.

ms-caro-malware-full:malware-family="DealPly"

2013 VOL15 - Adware that displays offers related to the user’s web browsing habits. It may be bundled with certain third-party software installation programs.

ms-caro-malware-full:malware-family="Fareit"

2013 VOL15 - A malware family that has multiple components: a password stealing component that steals sensitive information and sends it to an attacker, and a DDoS component that could be used against other computers.

ms-caro-malware-full:malware-family="FastSaveApp"

2013 VOL15 - An adware program that displays offers related to the user’s web browsing habits. It may use the name 'SaveAs' or 'SaveByClick'.

ms-caro-malware-full:malware-family="FindLyrics"

2013 VOL15 - An adware program that displays ads related to the user’s web browsing habits.

ms-caro-malware-full:malware-family="Gamarue"

2013 VOL15 - A worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

ms-caro-malware-full:malware-family="Gisav"

2013 VOL15 - An adware program that displays offers related to the user's web browsing habits. It can be downloaded from the program's website, and can be bundled with some third-party software installation programs.

ms-caro-malware-full:malware-family="InfoAtoms"

2013 VOL15 - An adware program that displays advertisements related to the user's web browsing habits and inserts advertisements into websites.

ms-caro-malware-full:malware-family="Perl/IRCbot.E"

2013 VOL15 - A backdoor trojan that drops other malicious software and connects to IRC servers to receive commands from attackers.

ms-caro-malware-full:malware-family="Javrobat"

2013 VOL15 - An exploit that tries to check whether certain versions of Adobe Acrobat or Adobe Reader are installed on the computer. If so, it tries to install malware.

ms-caro-malware-full:malware-family="Kraddare"

2013 VOL15 - Adware that displays Korean-language advertisements.

ms-caro-malware-full:malware-family="PriceGong"

2013 VOL15 - An adware program that shows certain deals related to the search terms entered on any web page.

ms-caro-malware-full:malware-family="Protlerdob"

2013 VOL15 - A software installer with a Portuguese language user interface. It presents itself as a free movie download but bundles with it a number of programs that may charge for services.

ms-caro-malware-full:malware-family="Qhost"

2013 VOL15 - A generic detection for trojans that modify the HOSTS file on the computer to redirect or limit Internet traffic to certain sites.

ms-caro-malware-full:malware-family="Reveton"

2013 VOL15 - A ransomware family that targets users from certain countries or regions. It locks the

computer and displays a location-specific webpage that covers the desktop and demands that the user pay a fine for the supposed possession of illicit material.

ms-caro-malware-full:malware-family="Rongvhin"

2013 VOL15 - A family of malware that perpetrates click fraud. It might be delivered to the computer via hack tools for the game CrossFire.

ms-caro-malware-full:malware-family="Seedabutor"

2013 VOL15 - A JavaScript trojan that attempts to redirect the browser to another website.

ms-caro-malware-full:malware-family="SMSer"

2013 VOL15 - A ransomware trojan that locks an affected user's computer and requests that the user send a text message to a premium-charge number to unlock it.

ms-caro-malware-full:malware-family="Tobfy"

2013 VOL15 - A family of ransomware trojans that targets users from certain countries. It locks the computer and displays a localized message demanding the payment of a fine for the supposed possession of illicit material. Some variants may also take webcam screenshots, play audio messages, or affect certain processes or drivers.

ms-caro-malware-full:malware-family="Truado"

2013 VOL15 - A trojan that poses as an update for certain Adobe software.

ms-caro-malware-full:malware-family="Urausy"

2013 VOL15 - A family of ransomware trojans that locks the computer and displays a localized message, supposedly from police authorities, demanding the payment of a fine for alleged criminal activity.

ms-caro-malware-full:malware-family="Wecykler"

2013 VOL15 - A family of worms that spread via removable drives, such as USB drives, that may stop security processes and other processes on the computer, and log keystrokes that are later sent to a remote attacker.

ms-caro-malware-full:malware-family="Weelsof"

2013 VOL15 - A family of ransomware trojans that targets users from certain countries. It locks the computer and displays a localized message demanding the payment of a fine for the alleged possession of illicit material. Some variants may take steps that make it difficult to run or update virus protection.

ms-caro-malware-full:malware-family="Yakdowpe"

2013 VOL15 - A family of trojans that connect to certain websites to silently download and install other programs without consent.

ms-caro-malware-full:malware-family="Anogre"

2013 VOL16 - A threat that exploits a vulnerability addressed by Microsoft Security Bulletin MS11-087. This vulnerability can allow a hacker to install programs, view, change, or delete data or create new accounts with full administrative privileges.

ms-caro-malware-full:malware-family="Brantall"

2013 VOL16 - A family of trojans that download and install other programs, including Win32/Sefnit and Win32/Rotbrow. Brantall often pretends to be an installer for other, legitimate programs.

ms-caro-malware-full:malware-family="Comame"

2013 VOL16 - A generic detection for a variety of threats.

ms-caro-malware-full:malware-family="Crilock"

2013 VOL16 - A ransomware family that encrypts the computer’s files and displays a webpage that demands a fee to unlock them.

ms-caro-malware-full:malware-family="CVE-2011-3874"

2013 VOL16 - A threat that attempts to exploit a vulnerability in the Android operating system to gain access to and control of the device Java/CVE-2012-1723. A family of malicious Java applets that attempt to exploit vulnerability CVE-2012-1723 in the Java Runtime Environment (JRE) in order to download and install files of an attacker’s choice onto the computer.

ms-caro-malware-full:malware-family="Deminnix"

2013 VOL16 - A trojan that uses the computer for Bitcoin mining and changes the home page of the web browser. It can accidentally be downloaded along with other files from torrent sites.

ms-caro-malware-full:malware-family="Detplock"

2013 VOL16 - A generic detection for a variety of threats.

ms-caro-malware-full:malware-family="Dircrypt"

2013 VOL16 - Ransomware that encrypts the user’s files and demands payment to release them. It is distributed through spam email messages and can be downloaded by other malware.

ms-caro-malware-full:malware-family="DonxRef"

2013 VOL16 - A generic detection for malicious JavaScript objects that construct shellcode. The

scripts may try to exploit vulnerabilities in Java, Adobe Flash Player, and Windows.

ms-caro-malware-full:malware-family="Faceliker"

2013 VOL16 - A malicious script that likes content on Facebook without the user's knowledge or consent.

ms-caro-malware-full:malware-family="FakeAlert"

2013 VOL16 - A malicious script that falsely claims that the computer is infected with viruses and that additional software is needed to disinfect it.

ms-caro-malware-full:malware-family="Jenxcus"

2013 VOL16 - A worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

ms-caro-malware-full:malware-family="Loktrom"

2013 VOL16 - Ransomware that locks the computer and displays a full-screen message pretending to be from a national police force, demanding payment to unlock the computer.

ms-caro-malware-full:malware-family="Miposa"

2013 VOL16 - A trojan that downloads and runs malicious Windows Scripting Host (.wsh) files.

ms-caro-malware-full:malware-family="Nitol"

2013 VOL16 - A family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access and control, download and run files, and perform a number of other malicious activities on the computer.

ms-caro-malware-full:malware-family="Oceanmug"

2013 VOL16 - A trojan that silently downloads and installs other programs without consent.

ms-caro-malware-full:malware-family="Proslikefan"

2013 VOL16 - A worm that spreads through removable drives, network shares, and P2P programs. It can lower the computer's security settings and disable antivirus products.

ms-caro-malware-full:malware-family="Rotbrow"

2013 VOL16 - A trojan that installs browser add-ons that claim to offer protection from other add-ons. Rotbrow can change the browser's home page, and can install the trojan Win32/Sefnit. It is commonly installed by Win32/Brantall.

ms-caro-malware-full:malware-family="Sefnit"

2013 VOL16 - A family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.

ms-caro-malware-full:malware-family="Urntone"

2013 VOL16 - A webpage component of the Neutrino exploit kit. It checks the version numbers of popular applications installed on the computer, and attempts to install malware that targets vulnerabilities in the software.

ms-caro-malware-full:malware-family="Wysotot"

2013 VOL16 - A threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.

ms-caro-malware-full:malware-family="AddLyrics"

2014 VOL17 - A browser add-on that displays lyrics for songs on YouTube, and displays advertisements in the browser window.

ms-caro-malware-full:malware-family="Adpeak"

2014 VOL17 - Adware that displays extra ads as the user browses the Internet, without revealing where the ads are coming from. It may be bundled with some third-party software installation programs.

ms-caro-malware-full:malware-family="Axpergle"

2014 VOL17 - A detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.

ms-caro-malware-full:malware-family="Bepush"

2014 VOL17 - A family of trojans that download and install add-ons for the Firefox and Chrome browsers that post malicious links to social networking sites, track browser usage, and redirect the browser to specific websites.

ms-caro-malware-full:malware-family="BetterSurf"

2014 VOL17 - Adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

ms-caro-malware-full:malware-family="Bladabindi"

2014 VOL17 - A family of backdoors created by a malicious hacker tool called NJ Rat. They can steal sensitive information, download other malware, and allow backdoor access to an infected

computer.

ms-caro-malware-full:malware-family="Caphaw"

2014 VOL17 - A family of backdoors that spread via Facebook, YouTube, Skype, removable drives, and drive-by download. They can make Facebook posts via the user's account, and may steal online banking details.

ms-caro-malware-full:malware-family="Clikug"

2014 VOL17 - A threat that uses a computer for click fraud. It has been observed using as much as a gigabyte of bandwidth per hour.

ms-caro-malware-full:malware-family="CVE-2014-0322"

This threat uses a vulnerability MS14-012, CVE-2014-0322 in Internet Explorer 9 and 10 to download and run files on your PC, including other malware.

ms-caro-malware-full:malware-family="CVE-2013-0422"

2014 VOL17 - A detection for a malicious Java applet that exploits the Java Runtime Environment (JRE) vulnerability described in CVE-2013-0422, addressed by an Oracle security update in January 2013.

ms-caro-malware-full:malware-family="Dowque"

2014 VOL17 - A generic detection for malicious files that are capable of installing other malware.

ms-caro-malware-full:malware-family="Fashack"

2014 VOL17 - A detection for the Safehack exploit kit, also known as Flashpack. It uses vulnerabilities in Adobe Flash Player, Java, and Silverlight to install malware on a computer.

ms-caro-malware-full:malware-family="Feven"

2014 VOL17 - A browser add-on for Internet Explorer, Firefox, or Chrome that displays ads on search engine results pages and other websites, and redirects the browser to specific websites.

ms-caro-malware-full:malware-family="Fiexp"

2014 VOL17 - A detection for the Fiesta exploit kit, which attempts to exploit Java, Adobe Flash Player, Adobe Reader, Silverlight, and Internet Explorer to install malware.

ms-caro-malware-full:malware-family="Filcout"

2014 VOL17 - An application that offers to locate and download programs to run unknown files. It has been observed installing variants in the Win32/Sefnit family.

ms-caro-malware-full:malware-family="Genasom"

2014 VOL17 - A ransomware family that locks a computer and demands money to unlock it. It usually targets Russian-language users, and may open pornographic websites.

ms-caro-malware-full:malware-family="Kegotip"

2014 VOL17 - A password-stealing trojan that can steal email addresses, personal information, or user account information for certain programs.

ms-caro-malware-full:malware-family="Krypterade"

2014 VOL17 - Ransomware that fraudulently claims a computer has been used for unlawful activity, locks it, and demands that the user pay to unlock it.

ms-caro-malware-full:malware-family="Lecpetex"

2014 VOL17 - A family of trojans that steal sensitive information, such as user names and passwords. It can also use a computer for Litecoin mining, install other malware, and post malicious content via the user's Facebook account.

ms-caro-malware-full:malware-family="Lollipop"

2014 VOL17 - Adware that may be installed by third-party software bundlers. It displays ads based on search engine searches, which can differ by geographic location and may be pornographic.

ms-caro-malware-full:malware-family="Meadgive"

2014 VOL17 - A detection for the Redkit exploit kit, also known as Infinity and Goon. It attempts to exploit vulnerabilities in programs such as Java and Silverlight to install other malware.

ms-caro-malware-full:malware-family="Neclu"

2014 VOL17 - A detection for the Nuclear exploit kit, which attempts to exploit vulnerabilities in programs such as Java and Adobe Reader to install other malware.

ms-caro-malware-full:malware-family="Ogimant"

2014 VOL17 - A threat that claims to help download items from the Internet, but actually downloads and runs files that are specified by a remote attacker.

ms-caro-malware-full:malware-family="OptimizerElite"

2014 VOL17 - A misleading program that uses legitimate files in the Prefetch folder to claim that the computer is damaged, and offers to fix the damage for a price.

ms-caro-malware-full:malware-family="Pangimop"

2014 VOL17 - A detection for the Magnitude exploit kit, also known as Popads. It attempts to exploit

vulnerabilities in programs such as Java and Adobe Flash Player to install other malware.

ms-caro-malware-full:malware-family="Phish"

2014 VOL17 - A password-stealing malicious webpage, known as a phishing page, that disguises itself as a page from a legitimate website.

ms-caro-malware-full:malware-family="Prast"

2014 VOL17 - A generic detection for various password stealing trojans.

ms-caro-malware-full:malware-family="Slugin"

2014 VOL17 - A file infector that infects .exe and .dll files. It may also perform backdoor actions.

ms-caro-malware-full:malware-family="Spacekito"

2014 VOL17 - A threat that steals information about the computer and installs browser add-ons that display ads.

ms-caro-malware-full:malware-family="Tranikpik"

This threat is a backdoor that can give a hacker unauthorized access and control of your PC

ms-caro-malware-full:malware-family="Wordinvop"

2014 VOL17 - A detection for a specially-crafted Microsoft Word file that attempts to exploit the vulnerability CVE-2006-6456, addressed by Microsoft Security Bulletin MS07-014.

ms-caro-malware-full:malware-family="Zegost"

2014 VOL17 - A backdoor that allows an attacker to remotely access and control a computer.

ms-caro-malware-full:malware-family="Archost"

2014 VOL18 - A downloader that installs other programs on the computer without the user’s consent, including other malware.

ms-caro-malware-full:malware-family="Balamid"

2014 VOL18 - A trojan that can use the computer to click on online advertisements without the user’s permission or knowledge. This can earn money for a malicious hacker by making a website or application appear more popular than it is.

ms-caro-malware-full:malware-family="BeeVry"

2014 VOL18 - A trojan that modifies a number of settings to prevent the computer from accessing security-related websites, and lower the computer’s security.

ms-caro-malware-full:malware-family="Bondat"

2014 VOL18 - A family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.

ms-caro-malware-full:malware-family="Bregent"

2014 VOL18 - A downloader that injects malicious code into legitimate processes such as explorer.exe and svchost.exe, and downloads other malware onto the computer.

ms-caro-malware-full:malware-family="Brolo"

2014 VOL18 - A ransomware family that locks the web browser and displays a message, often pretending to be from a law enforcement agency, demanding money to unlock the browser.

ms-caro-malware-full:malware-family="CostMin"

2014 VOL18 - An adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

ms-caro-malware-full:malware-family="CouponRuc"

2014 VOL18 - A browser modifier that changes browser settings and may also modify some computer and Internet settings.

ms-caro-malware-full:malware-family="Crastic"

2014 VOL18 - A trojan that sends sensitive information to a remote attacker, such as user names, passwords and information about the computer. It can also delete System Restore points, making it harder to recover the computer to a pre-infected state.

ms-caro-malware-full:malware-family="Crowti"

2014 VOL18 - A ransomware family that encrypts files on the computer and demands that the user pay a fee to decrypt them, using Bitcoins.

ms-caro-malware-full:malware-family="CVE-2013-1488"

2014 VOL18 - A detection for threats that use a Java vulnerability to download and run files on your PC, including other malware. Oracle addressed the vulnerability with a security update in April 2013.

ms-caro-malware-full:malware-family="DefaultTab"

2014 VOL18 - A browser modifier that redirects web browser searches and prevents the user from changing browser settings.

ms-caro-malware-full:malware-family="Ippedo"

2014 VOL18 - A worm that can send sensitive information to a malicious hacker. It spreads through infected removable drives, such as USB flash drives.

ms-caro-malware-full:malware-family="Kilim"

2014 VOL18 - A trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

ms-caro-malware-full:malware-family="Mofin"

2014 VOL18 - A worm that can steal files from your PC and send them to a malicious hacker. It spreads via infected removable drives, such as USB flash drives.

ms-caro-malware-full:malware-family="MpTamperSrp"

2014 VOL18 - A generic detection for an attempt to add software restriction policies to restrict Microsoft antimalware products, such as Microsoft Security Essentials and Windows Defender, from functioning properly.

ms-caro-malware-full:malware-family="Mujormel"

2014 VOL18 - A password stealer that can steal personal information, such as user names and passwords, and send the stolen information to a malicious hacker.

ms-caro-malware-full:malware-family="PennyBee"

2014 VOL18 - Adware that shows ads as the user browses the web. It can be installed from the program's website or bundled with some third-party software installation programs.

ms-caro-malware-full:malware-family="Phdet"

2014 VOL18 - A family of backdoor trojans that is used to perform distributed denial-of service (DDoS) attacks against specified targets.

ms-caro-malware-full:malware-family="Rimod"

2014 VOL18 - A generic detection for files that change various security settings in the computer Win32/Rotbrow. A trojan that installs browser add-ons that claim to offer protection from other add-ons. Rotbrow can change the browser's home page, and can install the trojan Win32/Sefnit. It is commonly installed by Win32/Brantall.

ms-caro-malware-full:malware-family="Sigru"

2014 VOL18 - A virus that can stop some files from working correctly in Windows XP and earlier operating systems. It spreads by infecting the master boot record (MBR) on connected hard disks and floppy disks.

ms-caro-malware-full:malware-family="SimpleShell"

2014 VOL18 - A backdoor that can give a malicious hacker unauthorized access to and control of the computer.

ms-caro-malware-full:malware-family="Softpulse"

2014 VOL18 - A software bundler that no longer meets Microsoft detection criteria for unwanted software following a program update in September of 2014.

ms-caro-malware-full:malware-family="SquareNet"

2014 VOL18 - A software bundler that installs other unwanted software, including adware and click-fraud malware.

ms-caro-malware-full:malware-family="Tugspay"

2014 VOL18 - A downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.

ms-caro-malware-full:malware-family="Tupym"

2014 VOL18 - A worm that copies itself to the system folder of the affected computer, and attempts to contact remote hosts.

ms-caro-malware-full:malware-family="Vercuser"

2014 VOL18 - A worm that typically spreads via drive-by download. It also receives commands from a remote server, and has been observed dropping other malware on the infected computer.

ms-caro-malware-full:malware-family="Adnel"

2015 VOL19 - A family of macro malware that can download other threats to the computer, including TrojanDownloader:Win32/Drixed.

ms-caro-malware-full:malware-family="Adodb"

2015 VOL19 - A generic detection for script trojans that exploit a vulnerability in Microsoft Data Access Components (MDAC) that allows remote code execution. Microsoft released Security Bulletin MS06-014 in April 2006 to address the vulnerability.

ms-caro-malware-full:malware-family="AlterbookSP"

2015 VOL19 - A browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.

ms-caro-malware-full:malware-family="BrobanDel"

2015 VOL19 - A family of trojans that can modify boletos bancários, a common payment method in Brazil. They can be installed on the computer when a user opens a malicious spam email attachment.

ms-caro-malware-full:malware-family="CompromisedCert"

2015 VOL19 - A detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.

ms-caro-malware-full:malware-family="CouponRuc_new"

2015 VOL19 - A browser modifier that changes browser settings and may also modify some computer and Internet settings.

ms-caro-malware-full:malware-family="CVE-2014-6332"

2015 VOL19 - This threat uses a Microsoft vulnerability MS14-064 to download and run files on your PC, including other malware.

ms-caro-malware-full:malware-family="Dyzap"

2015 VOL19 - A threat that steals login credentials for a long list of banking websites using man-in-the-browser (MITB) attacks. It is usually installed on the infected computer by TrojanDownloader:Win32/Upatre.

ms-caro-malware-full:malware-family="EoRezo"

2015 VOL19 - Adware that displays targeted advertising to affected users while browsing the Internet, based on downloaded pre-configured information.

ms-caro-malware-full:malware-family="FakeCall"

2015 VOL19 - This threat is a webpage that claims your PC is infected with malware. It asks you to phone a number to receive technical support to help remove the malware.

ms-caro-malware-full:malware-family="Foosace"

2015 VOL19 - A threat that creates files on the compromised computer and contacts a remote host. Observed in the STRONTIUM APT.

ms-caro-malware-full:malware-family="IeEnablerCby"

2015 VOL19 - A browser modifier that installs additional browser addons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

ms-caro-malware-full:malware-family="InstalleRex"

2015 VOL19 - A software bundler that installs unwanted software, including Win32/CouponRuc and Win32/SaverExtension. It alters its own 'Installed On' date in Programs and Features to make it more difficult for a user to locate it and remove it.

ms-caro-malware-full:malware-family="JackTheRipper"

2015 VOL19 - A virus that can stop some files from working correctly in Windows XP and earlier operating systems. It spreads by infecting the master boot record (MBR) on connected hard disks and floppy disks.

ms-caro-malware-full:malware-family="Kenilfe"

2015 VOL19 - A worm written in AutoCAD Lisp that only runs if AutoCAD is installed on the computer or network. It renames and deletes certain AutoCAD files, and may download and execute arbitrary files from a remote host.

ms-caro-malware-full:malware-family="KipodToolsCby"

2015 VOL19 - A browser modifier that installs additional browser addons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

ms-caro-malware-full:malware-family="Macoute"

2015 VOL19 - A worm that can spread itself to removable USB drives, and may communicate with a remote host.

ms-caro-malware-full:malware-family="NeutrinoEK"

2015 VOL19 - This threat is a webpage that spreads the exploit kit known as Neutrino.

ms-caro-malware-full:malware-family="Peaac"

2015 VOL19 - A generic detection for various threats that display trojan characteristics.

ms-caro-malware-full:malware-family="Peals"

2015 VOL19 - A generic detection for various threats that display trojan characteristics.

ms-caro-malware-full:malware-family="Radonskra"

2015 VOL19 - A family of threats that perform a variety of malicious acts, including stealing information about the computer, showing extra advertisements as the user browses the web, performing click fraud, and downloading other programs without consent.

ms-caro-malware-full:malware-family="SaverExtension"

2015 VOL19 - A browser add-on that shows ads in the browser without revealing their source, and

prevents itself from being removed normally.

ms-caro-malware-full:malware-family="Sdbby"

2015 VOL19 - A threat that exploits a bypass to gain administrative privileges on a machine without going through a User Access Control prompt.

ms-caro-malware-full:malware-family="Simda"

2015 VOL19 - A threat that can give an attacker backdoor access and control of an infected computer. It can then steal passwords and gather information about the computer to send to the attacker.

ms-caro-malware-full:malware-family="Skeeyah"

2015 VOL19 - A generic detection for various threats that display trojan characteristics.

ms-caro-malware-full:malware-family="Wordjmp"

2015 VOL19 - An exploit that targets a vulnerability in Word 2002 and 2003 that could allow an attacker to remotely execute arbitrary code. Microsoft released Security Bulletin MS06-027 in June 2006 to address the vulnerability.

ms-caro-malware-full:malware-family="Bayads"

2015 VOL20 - A program that displays ads as the user browses the web. It can be bundled with other software. It may call itself bdraw, delta, dlclient, Pay-ByAds, or pricehorse in Programs and Features.

ms-caro-malware-full:malware-family="CandyOpen"

2015 VOL20 - This application can also affect the quality of your computing experience. We have seen this leading to the following potentially unwanted behaviors on PCs: Adds files that run at startup, Modifies boot configuration data, Modifies file associations, Injects into other processes on your system, Changes browser settings, Adds a local proxy, Modifies your system DNS settings, Stops Windows Update, Disables User Access Control (UAC), These applications are most commonly software bundlers or installers for applications such as toolbars, adware, or system optimizers. We have observed this application installing software that you might not have intended on your PC.

ms-caro-malware-full:malware-family="Colisi"

2015 VOL20 - Behavioral detection of certain files acting in a malicious way.

ms-caro-malware-full:malware-family="Creprote"

2015 VOL20 - These programs are most commonly software bundlers or installers for software such as toolbars, adware, or system optimizers. The software might modify your homepage, your search provider, or perform other actions that you might not have intended.

ms-caro-malware-full:malware-family="Diplugem"

2015 VOL20 - A browser modifier that installs browser add-ons without obtaining the user's consent. The add-ons show extra advertisements as the user browses the web, and can inject additional ads into web search results pages.

ms-caro-malware-full:malware-family="Dipsind"

2015 VOL20 - A threat that is often used in targeted attacks. It can give an attacker access to the computer to download and run files, steal domain credentials, and perform other malicious actions.

ms-caro-malware-full:malware-family="Donoff"

2015 VOL20 - A threat that uses an infected Microsoft Office file to download other malware onto the computer. It can arrive as a spam email attachment, usually as a Word file (.doc).

ms-caro-malware-full:malware-family="Dorv"

2015 VOL20 - A trojan is a type of malware that can't spread on its own. It relies on you to run them on your PC by mistake, or visit a hacked or malicious webpage. They can steal your personal information, download more malware, or give a malicious hacker access to your PC.

ms-caro-malware-full:malware-family="Dowadmin"

2015 VOL20 - A software bundler that does not provide the user with the option to decline installation of unwanted software.

ms-caro-malware-full:malware-family="Fourthrem"

2015 VOL20 - A program that installs unwanted software without adequate consent on the computer at the same time as the software the user is trying to install.

ms-caro-malware-full:malware-family="Hao123"

2015 VOL20 - This threat is a modified Internet Explorer shortcut that changes your Internet Explorer homepage. It might arrive on your PC through bundlers that offer free software. The threat will run a separate threat-related file that changes the Internet Explorer.

ms-caro-malware-full:malware-family="Mizenota"

2015 VOL20 - This program is a software bundler that installs unwanted software on your PC at the same time as the software you are trying to install. It may install one of the following: BrowserModifier:Win32/SupTab, BrowserModifier:Win32/Sasquor, BrowserModifier:Win32/Smudplu, SoftwareBundler:Win32/Pokavampo, BrowserModifier:Win32/Shopperz, Adware:Win32/EoRezo

ms-caro-malware-full:malware-family="Mytonel"

2015 VOL20 - A program that downloads and installs other programs onto the computer without the user's consent, including other malware.

ms-caro-malware-full:malware-family="OutBrowse"

2015 VOL20 - A software bundler that installs additional unwanted programs alongside software that the user wishes to install. It can remove or hide the installer's close button, leaving no way to decline the additional applications.

ms-caro-malware-full:malware-family="Peapoon"

2015 VOL20 - An adware program that shows users ads that they cannot control as they browse the web. It may identify itself as Coupon in Programs and Features.

ms-caro-malware-full:malware-family="Pokki"

2015 VOL20 - A browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.

ms-caro-malware-full:malware-family="Putalol"

2015 VOL20 - An adware program that shows users ads that they cannot control as they browse the web. It may identify itself as Lolliscan in Programs and Features.

ms-caro-malware-full:malware-family="SpigotSearch"

2015 VOL20 - This application can affect the quality of your computing experience. For example, some potentially unwanted applications can: Install additional bundled software, Modify your homepage, Modify your search provider. These applications are most commonly software bundlers or installers for applications such as toolbars, adware, or system optimizers. We have observed this application installing software that you might not have intended on your PC.

ms-caro-malware-full:malware-family="Spursint"

2015 VOL20 - This threat has been detected as one of the executable malware that are distributed through URLs.

ms-caro-malware-full:malware-family="Sulunch"

2015 VOL20 - A generic detection for a group of trojans that perform a number of common malware behaviors.

ms-caro-malware-full:malware-family="SupTab"

2015 VOL20 - A browser modifier that installs itself and changes the browser's default search provider, without obtaining the user's consent for either action.

ms-caro-malware-full:malware-family="Sventore"

2015 VOL20 - This trojan can install other malware or unwanted software onto your PC.

ms-caro-malware-full:malware-family="Tillail"

2015 VOL20 - A software bundler that installs unwanted software alongside the software the user is trying to install. It has been observed to install the browser modifier Win32/SupTab.

ms-caro-malware-full:malware-family="VOPackage"

2015 VOL20 - This application can also affect the quality of your computing experience. We have seen this leading to the following potentially unwanted behaviors on PCs: Adds files that run at startup, Installs a driver, Injects into other processes on your system, Injects into browsers, Changes browser settings, Changes browser shortcuts, Installs browser extensions, Adds a local proxy, Tampers with root certificate trust, Modifies the system hosts file, Modifies your system DNS settings, Disables anti-virus products, Tampers with system Group Policy settings, These applications are most commonly software bundlers or installers for applications such as toolbars, adware, or system optimizers. We have observed this application installing software that you might not have intended on your PC.

ms-caro-malware-full:malware-family="Xiazai"

2015 VOL20 - A program that installs unwanted software on the computer at the same time as the software the user is trying to install, without adequate consent.

mwdb

mwdb namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Malware Database (mwdb) Taxonomy - Tags used across the platform

location_type

Type of malicious URL.

mwdb:location_type="cnc"

CNC

C&C server, usually administrated by criminals. Malware connects to it (usually with a custom protocol) to get new commands and updates.

mwdb:location_type="download_url"

Download URL

Download url. Used to download more malware samples. Sometimes just a hacked legitimate website.

mwdb:location_type="panel"

Panel

Malware panel. HTTP service used by criminals to manage the botnet.

mwdb:location_type="peer"

Peer

Peer. IP/port of infected machine of a legitimate computer user.

mwdb:location_type="other"

Other

Other kind of URL found in the malware.

family

mwdb:family="agenttesla"

agenttesla

mwdb:family="andromeda"

andromeda

mwdb:family="anubis"

anubis

mwdb:family="avemaria"

avemaria

mwdb:family="azorult"

azorult

mwdb:family="brushaloader"

brushaloader

mwdb:family="bublik"

bublik

mwdb:family="bunitu"

bunitu

mwdb:family="cerber"

cerber

mwdb:family="chthonic"

chthonic

mwdb:family="citadel"

citadel

mwdb:family="corebot"

corebot

mwdb:family="cryptomix"

cryptomix

mwdb:family="cryptoshield"

cryptoshield

mwdb:family="cryptowall"

cryptowall

mwdb:family="danabot"

danabot

mwdb:family="danaloader"

danaloader

mwdb:family="dridex"

dridex

mwdb:family="dridex-worker"

dridex-worker

mwdb:family="dyre"

dyre

mwdb:family="emotet"

emotet

mwdb:family="emotet5_upnp"

emotet5_upnp

mwdb:family="emotet_doc"

emotet_doc

mwdb:family="emotet_spam"

emotet_spam

mwdb:family="emotet_upnp"

emotet_upnp

mwdb:family="evil-pony"

evil-pony

mwdb:family="flokibot"

flokibot

mwdb:family="formbook"

formbook

mwdb:family="gandcrab"

gandcrab

mwdb:family="get2"

get2

mwdb:family="globeimposter"

globeimposter

mwdb:family="gluedropper"

gluedropper

mwdb:family="gootkit"

gootkit

mwdb:family="h1n1"

h1n1

mwdb:family="hancitor"

hancitor

mwdb:family="hawkeye"

hawkeye

mwdb:family="icedid"

icedid

mwdb:family="iceid"

iceid

mwdb:family="iceix"

iceix

mwdb:family="isfb"

isfb

mwdb:family="jaff"

jaff

mwdb:family="kbot"

kbot

mwdb:family="kegotip"

kegotip

mwdb:family="kins"

kins

mwdb:family="kovter"

kovter

mwdb:family="kpot"

kpot

mwdb:family="kronos"

kronos

mwdb:family="locky"

locky

mwdb:family="lokibot"

lokibot

mwdb:family="madlocker"

madlocker

mwdb:family="madness_pro"

madness_pro

mwdb:family="maoloa"

maoloa

mwdb:family="mirai"

mirai

mwdb:family="mmbb"

mmbb

mwdb:family="nanocore"

nanocore

mwdb:family="necurs"

necurs

mwdb:family="netwire"

netwire

mwdb:family="neutrino"

neutrino

mwdb:family="njrat"

njrat

mwdb:family="nymaim"

nymaim

mwdb:family="odinaff"

odinaff

mwdb:family="onliner"

onliner

mwdb:family="ostap"

ostap

mwdb:family="panda"

panda

mwdb:family="phorpiex"

phorpiex

mwdb:family="pony"

pony

mwdb:family="pushdo"

pushdo

mwdb:family="qadars"

qadars

mwdb:family="qakbot"

qakbot

mwdb:family="quantloader"

quantloader

mwdb:family="quasarrat"

quasarrat

mwdb:family="ramnit"

ramnit

mwdb:family="remcos"

remcos

mwdb:family="retefe"

retefe

mwdb:family="ruckguv"

ruckguv

mwdb:family="sage"

sage

mwdb:family="sendsafe"

sendsafe

mwdb:family="shifu"

shifu

mwdb:family="slave"

slave

mwdb:family="smokeloader"

smokeloader

mwdb:family="systembc"

systembc

mwdb:family="teslacrypt"

teslacrypt

mwdb:family="test"

test

mwdb:family="testmod"

testmod

mwdb:family="tinba"

tinba

mwdb:family="tinba_dga"

tinba_dga

mwdb:family="tinynuke"

tinynuke

mwdb:family="tofsee"

tofsee

mwdb:family="torment"

torment

mwdb:family="torrentlocker"

torrentlocker

mwdb:family="trickbot"

trickbot

mwdb:family="troldesh"

troldesh

mwdb:family="unknown"

unknown

mwdb:family="vawtrak"

vawtrak

mwdb:family="vjworm"

vjworm

mwdb:family="vmzeus"

vmzeus

mwdb:family="vmzeus2"

vmzeus2

mwdb:family="wannacry"

wannacry

mwdb:family="xagent"

xagent

mwdb:family="zeus"

zeus

mwdb:family="zloader"

zloader

nato

nato namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

NATO classification markings.

Exclusive flag set which means the values or predicate below must be set exclusively.

classification

nato:classification="CTS"

COSMIC TOP SECRET

nato:classification="CTS-B"

COSMIC TOP SECRET BOHEMIA

nato:classification="NS"

NATO SECRET

nato:classification="NC"

NATO CONFIDENTIAL

nato:classification="NR"

NATO RESTRICTED

nato:classification="NU"

NATO UNCLASSIFIED

nato:classification="CTS-A"

COSMIC TOP SECRET ATOMAL

nato:classification="NS-A"

SECRET ATOMAL

nato:classification="NC-A"

CONFIDENTIAL ATOMAL

nis

nis namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The taxonomy is meant for large scale cybersecurity incidents, as mentioned in the Commission Recommendation of 13 September 2017, also known as the blueprint. It has two core parts: The nature of the incident, i.e. the underlying cause, that triggered the incident, and the impact of the incident, i.e. the impact on services, in which sector(s) of economy and society.

impact-sectors-impacted

The impact on services, in the real world, indicating the sectors of the society and economy, where there is an impact on the services.

nis:impact-sectors-impacted="energy"

Energy

The impact is in the Energy sector and its subsectors such as electricity, oil, or gas, for example, impacting electricity suppliers, power plants, distribution system operators, transmission system operators, oil transmission, natural gas distribution, etc.

nis:impact-sectors-impacted="transport"

Transport

The impact is in the transport sector and subsectors such as air, rail, water, road, for example, impacting air traffic control systems, railway companies, maritime port authorities, road traffic management systems, etc.

nis:impact-sectors-impacted="banking"

Banking

The impact is in the Banking sector, for example impacting banks, online banking, credit services, payment services, etc.

nis:impact-sectors-impacted="financial"

Financial

The impact is in the Financial market infrastructure sector, for example, impacting traders, trading platforms, clearing services, etc.

nis:impact-sectors-impacted="health"

Health

The impact is in the Health sector, for example, impacting hospitals, medical devices, medicine supply, pharmacies, etc.

nis:impact-sectors-impacted="drinking-water"

Drinking water

The impact is in the Drinking water supply and distribution sector, for example impacting drinking water supply, drinking water distribution systems, etc.

nis:impact-sectors-impacted="digital-infrastructure"

Digital infrastructure

The impact is in the Digital infrastructure sector, for example impacting internet exchange points, domain name systems, top level domain registries, etc.

nis:impact-sectors-impacted="communications"

Communications

The impact is in the Electronic communications sector, for example,impacting mobile network services, fixed telephone lines, satellite communications, etc.

nis:impact-sectors-impacted="digital-services"

Digital services

The impact is in the digital services sector, for example, impacting cloud services, online market places, online search engines, etc.

nis:impact-sectors-impacted="trust-and-identification-services"

Trust and identification services

The impact is in the electronic trust and identification services, for example, impacting certificate authorities, electronic identity systems, smartcards, etc.

nis:impact-sectors-impacted="government"

Government

The impact is in the government sector, for example, impacting the functioning of public administrations, elections, or emergency services

impact-severity

The severity of the impact, nationally, in the real world, for society and/or the economy, i.e. the level of disruption for the country or a large region of the country, the level of risks for health and/or safety, the level of physical damages and/or financial costs.

Exclusive flag set which means the values or predicate below must be set exclusively.

nis:impact-severity="red"

Red

Very large impact

nis:impact-severity="yellow"

Yellow

Large impact.

nis:impact-severity="green"

Green

Minor impact.

nis:impact-severity="white"

White

No impact.

impact-outlook

The outlook for the incident, the prognosis, for the coming hours, considering the impact in the real world, the impact on services, for the society and/or the economy

Exclusive flag set which means the values or predicate below must be set exclusively.

nis:impact-outlook="improving"

Improving

Severity of impact is expected to decrease in the next 6 hours.

nis:impact-outlook="stable"

Stable

Severity of impact is expected to remain the same in the 6 hours.

nis:impact-outlook="worsening"

Worsening

Severity of impact is expected to increase in the next 6 hours.

nature-root-cause

The Root cause category is used to indicate what type event or threat triggered the incident.

Exclusive flag set which means the values or predicate below must be set exclusively.

nis:nature-root-cause="system-failures"

System failures

The incident is due to a failure of a system, i.e. without external causes. For example a hardware failure, software bug, a flaw in a procedure, etc. triggered the incident.

nis:nature-root-cause="natural-phenomena"

Natural phenomena

The incident is due to a natural phenomenon. For example a storm, lightning, solar flare, flood, earthquake, wildfire, etc. triggered the incident.

nis:nature-root-cause="human-errors"

Human errors

The incident is due to a human error, i.e. system worked correctly, but was used wrong. For example, a mistake, or carelessness triggered the incident.

nis:nature-root-cause="malicious-actions"

Malicious actions

The incident is due to a malicious action. For example, a cyber-attack or physical attack, vandalism, sabotage, insider attack, theft, etc., triggered the incident.

nis:nature-root-cause="third-party-failures"

Third party failures

The incident is due to a disruption of a third party service, like a utility. For example a power cut, or an internet outage, etc. triggered the incident.

nature-severity

The severity of the threat is used to indicate, from a technical perspective, the potential impact, the risk associated with the threat. For example, the severity is high if an upcoming storm is exceptionally strong, if an observed DDoS attack is exceptionally powerful, or if a software vulnerability is easily exploited and present in many different systems. For example, in certain situations a critical software vulnerability would require concerted and urgent work by different organizations.

Exclusive flag set which means the values or predicate below must be set exclusively.

nis:nature-severity="high"

High

High severity, potential impact is high.

nis:nature-severity="medium"

Medium

Medium severity, potential impact is medium.

nis:nature-severity="low"

Low

Low severity, potential impact is low.

test

A test predicate meant to test interoperability between tools. Tags contained within this predicate are to be ignored.

nis:test="test"

Test

Test value meant for testing interoperability. Tags with this value are to be ignored.

open_threat

open_threat namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Open Threat Taxonomy v1.1 base on James Tarala of SANS http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf, https://files.sans.org/summit/Threat_Hunting_Incident_Response_Summit_2016/PDFs/Using-Open-Tools-to-Convert-Threat-Intelligence-into-Practical-Defenses-James-Tarala-SANS-Institute.pdf, https://www.youtube.com/watch?v=5rdGOOFC_yE, and https://www.rsaconference.com/writable/presentations/file_upload/str-r04_using-an-open-source-threat-model-for-prioritized-defense-final.pdf

threat-category

open_threat:threat-category="Physical"

Threats to the confidentiality, integrity, or availability of information systems that are physical in nature. These threats generally describe actions that could lead to the theft, harm, or destruction of information systems.

open_threat:threat-category="Resource"

Threats to the confidentiality, integrity, or availability of information systems that are the result of a lack of resources required by the information system. These threats often cause failures of information systems through a disruption of resources required for operations.

open_threat:threat-category="Personal"

Threats to the confidentiality, integrity, or availability of information systems that are the result of failures or actions performed by an organization's personnel. These threats can be the result of deliberate or accidental actions that cause harm to information systems.

open_threat:threat-category="Technical"

Threats to the confidentiality, integrity, or availability of information systems that are technical in nature. These threats are most often considered when identifying threats and constitute the technical actions performed by a threat actor that can cause harm to an information system.

threat-name

open_threat:threat-name="PHY-001"

Loss of Property - Rating: 5.0

open_threat:threat-name="PHY-002"

Theft of Property - Rating: 5.0

open_threat:threat-name="PHY-003"

Accidental Destruction of Property - Rating: 3.0

open_threat:threat-name="PHY-004"

Natural Destruction of Property - Rating: 3.0

open_threat:threat-name="PHY-005"

Intentional Destruction of Property - Rating: 2.0

open_threat:threat-name="PHY-006"

Intentional Sabotage of Property - Rating: 2.0

open_threat:threat-name="PHY-007"

Intentional Vandalism of Property - Rating: 2.0

open_threat:threat-name="PHY-008"

Electrical System Failure - Rating: 4.0

open_threat:threat-name="PHY-009"

Heating, Ventilation, Air Conditioning (HVAC) Failure - Rating: 3.0

open_threat:threat-name="PHY-010"

Structural Facility Failure - Rating: 2.0

open_threat:threat-name="PHY-011"

Water Distribution System Failure - Rating: 2.0

open_threat:threat-name="PHY-012"

Sanitation System Failure - Rating: 1.0

open_threat:threat-name="PHY-013"

Natural Gas Distribution Failure - Rating: 1.0

open_threat:threat-name="PHY-014"

Electronic Media Failure - Rating: 3.0

open_threat:threat-name="RES-001"

Disruption of Water Resources - Rating: 2.0

open_threat:threat-name="RES-002"

Disruption of Fuel Resources - Rating: 2.0

open_threat:threat-name="RES-003"

Disruption of Materials Resources - Rating: 2.0

open_threat:threat-name="RES-004"

Disruption of Electrical Resources - Rating: 4.0

open_threat:threat-name="RES-005"

Disruption of Transportation Services - Rating: 1.0

open_threat:threat-name="RES-006"

Disruption of Communications Services - Rating: 4.0

open_threat:threat-name="RES-007"

Disruption of Emergency Services - Rating: 1.0

open_threat:threat-name="RES-008"

Disruption of Governmental Services - Rating: 1.0

open_threat:threat-name="RES-009"

Supplier Viability - Rating: 2.0

open_threat:threat-name="RES-010"

Supplier Supply Chain Failure - Rating: 2.0

open_threat:threat-name="RES-011"

Logistics Provider Failures - Rating: 1.0

open_threat:threat-name="RES-012"

Logistics Route Disruptions - Rating: 1.0

open_threat:threat-name="RES-013"

Technology Services Manipulation - Rating: 3.0

open_threat:threat-name="PER-001"

Personnel Labor / Skills Shortage - Rating: 5.0

open_threat:threat-name="PER-002"

Loss of Personnel Resources - Rating: 3.0

open_threat:threat-name="PER-003"

Disruption of Personnel Resources - Rating: 3.0

open_threat:threat-name="PER-004"

Social Engineering of Personnel Resources - Rating: 4.0

open_threat:threat-name="PER-005"

Negligent Personnel Resources - Rating: 4.0

open_threat:threat-name="PER-006"

Personnel Mistakes / Errors - Rating: 4.0

open_threat:threat-name="PER-007"

Personnel Inaction - Rating: 3.0

open_threat:threat-name="TEC-001"

Organizational Fingerprinting via Open Sources - Rating:

open_threat:threat-name="TEC-002"

System Fingerprinting via Open Sources - Rating: 2.0

open_threat:threat-name="TEC-003"

System Fingerprinting via Scanning - Rating: 2.0

open_threat:threat-name="TEC-004"

System Fingerprinting via Sniffing - Rating: 2.0

open_threat:threat-name="TEC-005"

Credential Discovery via Open Sources - Rating: 4.0

open_threat:threat-name="TEC-006"

Credential Discovery via Scanning - Rating: 3.0

open_threat:threat-name="TEC-007"

Credential Discovery via Sniffing - Rating: 4.0

open_threat:threat-name="TEC-008"

Credential Discovery via Brute Force - Rating: 4.0

open_threat:threat-name="TEC-009"

Credential Discovery via Cracking - Rating: 4.0

open_threat:threat-name="TEC-010"

Credential Discovery via Guessing - Rating: 2.0

open_threat:threat-name="TEC-011"

Credential Discovery via Pre-Computational Attacks - Rating: 3.0

open_threat:threat-name="TEC-012"

Misuse of System Credentials - Rating: 3.0

open_threat:threat-name="TEC-013"

Escalation of Privilege - Rating: 5.0

open_threat:threat-name="TEC-014"

Abuse of System Privileges - Rating: 4.0

open_threat:threat-name="TEC-015"

Memory Manipulation - Rating: 4.0

open_threat:threat-name="TEC-016"

Cache Poisoning - Rating: 3.0

open_threat:threat-name="TEC-017"

Physical Manipulation of Technical Device - Rating: 2.0

open_threat:threat-name="TEC-018"

Manipulation of Trusted System - Rating: 4.0

open_threat:threat-name="TEC-019"

Cryptanalysis - Rating: 1.0

open_threat:threat-name="TEC-020"

Data Leakage / Theft - Rating: 3.0

open_threat:threat-name="TEC-021"

Denial of Service - Rating: 2.0

open_threat:threat-name="TEC-022"

Maintaining System Persistence - Rating: 5.0

open_threat:threat-name="TEC-023"

Manipulation of Data in Transit / Use - Rating: 2.0

open_threat:threat-name="TEC-024"

Capture of Data in Transit / Use via Sniffing - Rating: 3.0

open_threat:threat-name="TEC-025"

Capture of Data in Transit / Use via Debugging - Rating: 2.0

open_threat:threat-name="TEC-026"

Capture of Data in Transit / Use via Keystroke Logging - Rating: 3.0

open_threat:threat-name="TEC-027"

Replay of Data in Transit / Use - Rating: 2.0

open_threat:threat-name="TEC-028"

Misdelivery of Data - Rating: 2.0

open_threat:threat-name="TEC-029"

Capture of Stored Data - Rating: 3.0

open_threat:threat-name="TEC-030"

Manipulation of Stored Data - Rating: 3.0

open_threat:threat-name="TEC-031"

Application Exploitation via Input Manipulation - Rating: 5.0

open_threat:threat-name="TEC-032"

Application Exploitation via Parameter Injection - Rating: 4.0

open_threat:threat-name="TEC-033"

Application Exploitation via Code Injection - Rating: 4.0

open_threat:threat-name="TEC-034"

Application Exploitation via Command Injection - Rating: 4.0

open_threat:threat-name="TEC-035"

Application Exploitation via Path Traversal - Rating: 3.0

open_threat:threat-name="TEC-036"

Application Exploitation via API Abuse - Rating: 3.0

open_threat:threat-name="TEC-037"

Application Exploitation via Fuzzing - Rating: 3.0

open_threat:threat-name="TEC-038"

Application Exploitation via Reverse Engineering - Rating: 3.0

open_threat:threat-name="TEC-039"

Application Exploitation via Resource Location Guessing - Rating: 2.0

open_threat:threat-name="TEC-040"

Application Exploitation via Source Code Manipulation - Rating: 3.0

open_threat:threat-name="TEC-041"

Application Exploitation via Authentication Bypass - Rating: 2.0

osint

osint namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Open Source Intelligence - Classification (MISP taxonomies)

source-type

osint:source-type="blog-post"

Blog post

osint:source-type="microblog-post"

Microblog post like Twitter

osint:source-type="technical-report"

Technical or analysis report

osint:source-type="presentation"

Presentation or slidedeck

osint:source-type="news-report"

News report

osint:source-type="pastie-website"

Pastie-like website

osint:source-type="electronic-forum"

Electronic forum

osint:source-type="mailing-list"

Mailing-list

osint:source-type="block-or-filter-list"

Block or Filter List

osint:source-type="source-code-repository"

Source code repository

osint:source-type="accessible-evidence"

Infrastructure allowing the gathering of the evidences such as open directories, public web services or left over on public services

osint:source-type="expansion"

Expansion

osint:source-type="automatic-analysis"

Automatic analysis including dynamic analysis or sandboxes output

osint:source-type="automatic-collection"

Automatic collection including honeypots, spamtraps or equivalent technologies

osint:source-type="manual-analysis"

Manual analysis or investigation

osint:source-type="manual-collection"

Manual collection from crawlers, honeypots, spamtraps, gathering tools or equivalent technologies

osint:source-type="unknown"

Unknown

osint:source-type="other"

Other source not specified in this list

lifetime

osint:lifetime="perpetual"

Perpetual

Information available publicly on long-term

osint:lifetime="ephemeral"

Ephemeral

Information available publicly on short-term

certainty

osint:certainty="100"

Certainty (probability equals 1 - 100%)

Certainty

Associated numerical value="100"

osint:certainty="93"

Almost certain (probability equals 0.93 - 93%)

Almost certain

Associated numerical value="93"

osint:certainty="75"

Probable (probability equals 0.75 - 75%)

Probable

Associated numerical value="75"

osint:certainty="50"

Chances about even (probability equals 0.50 - 50%)

Chances about even

Associated numerical value="50"

osint:certainty="30"

Probably not (probability equals 0.30 - 30%)

Probably not

Associated numerical value="30"

osint:certainty="7"

Almost certainly not (probability equals 0.07 - 7%)

Almost certainly not

Associated numerical value="7"

osint:certainty="0"

Impossibility (probability equals 0 - 0%)

Impossibility

pandemic

pandemic namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Pandemic

covid-19

pandemic:covid-19="health"

Health

Information tagged about COVID-19 and related to health

pandemic:covid-19="cyber"

Cyber

Information tagged about COVID-19 and related to cybersecurity

pandemic:covid-19="disinformation"

Disinformation

Information tagged about COVID-19 and related to disinformation

pandemic:covid-19="geostrategy"

Geostrategy

Information tagged about COVID-19 and related to geostrategy or geopolitics

passivetotal

passivetotal namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Tags from RiskIQ's PassiveTotal service

sinkholed

passivetotal:sinkholed="yes"

Yes

passivetotal:sinkholed="no"

No

ever-compromised

passivetotal:ever-compromised="yes"

Yes

passivetotal:ever-compromised="no"

No

dynamic-dns

passivetotal:dynamic-dns="yes"

Yes

passivetotal:dynamic-dns="no"

No

class

passivetotal:class="malicious"

Malicious

passivetotal:class="suspicious"

Suspicious

passivetotal:class="non-malicious"

Non Malicious

passivetotal:class="unknown"

Unknown

pentest

pentest namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Penetration test (pentest) classification.

approach

This is group is dealing with differents types of pentest

pentest:approach="blackbox"

Blackbox penetration test requires no prior information about the target network or application and is actually performed keeping it as a real world hacker attack scenario. (https://www.evolution-sec.com/en/products/blackbox-penetration-testing)

pentest:approach="greybox"

Gray box testing lies between black and white. Testers will have knowledge of some areas but not others. These areas are defined at the start of an engagement.(https://www.intelisecure.com/security-assessments-pen-testing/approaches/)

pentest:approach="whitebox"

White box, or authenticated tests, target the security of your underlying technology with full knowledge of your IT department. Information typically shared with the tester includes: network diagrams, IP addresses, system configurations and access credentials.(https://www.intelisecure.com/security-assessments-pen-testing/approaches/)

pentest:approach="vulnerability_scanning"

Vulnerability scanning is a security technique used to identify security weaknesses in a computer system. (https://www.techopedia.com/definition/4160/vulnerability-scanning)

pentest:approach="redteam"

A red team is an group that challenges an organization to improve its effectiveness by assuming an adversarial role or point of view without any predefined scope. (https://en.wikipedia.org/wiki/Red_team)

scan

Automated tool that perform network checks

pentest:scan="vertical"

A scan against multiple ports of a single IP.

pentest:scan="horizontal"

A scan against a group of IPs for a single port.

pentest:scan="network_scan"

It is the discovery of networks and machines with services.

pentest:scan="vulnerability"

Vulnerability scanning is a security technique used to identify security weaknesses in a computer system. (https://www.techopedia.com/definition/4160/vulnerability-scanning)

exploit

Exploitation of a vulnerability

pentest:exploit="type confusion"

When a piece of code doesn't verify the type of object that is passed to it, and uses it blindly without type-checking, it leads to type confusion. (https://cloudblogs.microsoft.com/microsoftsecure/2015/06/17/understanding-type-confusion-vulnerabilities-cve-2015-0336/)

pentest:exploit="format_strings"

The format string exploit occurs when the submitted data of an input string leads to arbitrary read or write in the memory. In this way, the attacker could execute code, read the stack, or cause a segmentation fault in the running application, causing new behaviors that could compromise the security or the stability of the system. (https://www.owasp.org/index.php/Format_string_attack)

pentest:exploit="stack_overflow"

In software, a stack overflow is type of buffer overflow that occurs if the call stack pointer exceeds the stack bound. (https://en.wikipedia.org/wiki/Stack_overflow)

pentest:exploit="heap_overflow"

A heap overflow is a type of buffer overflow that occurs in the heap data area. (https://en.wikipedia.org/wiki/Heap_overflow)

pentest:exploit="heap_spraying"

Heap spraying is a technique used in exploits to facilitate arbitrary code execution. In general, code that sprays the heap attempts to put a certain sequence of bytes at a predetermined location in the memory of a target process by having it allocate (large) blocks on the process's heap and fill the

bytes in these blocks with the right values. (https://en.wikipedia.org/wiki/Heap_spraying)

pentest:exploit="fuzzing"

Fuzzing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. (https://en.wikipedia.org/wiki/Fuzzing)

pentest:exploit="ROP"

The Return-Oriented Programming (ROP) is a computer security exploit technique in which the attacker uses control of the call stack to indirectly execute cherry-picked machine instructions or groups of machine instructions immediately prior to the return instruction in subroutines within the existing program code, in a way similar to the execution of a threaded code interpreter. (https://en.wikipedia.org/wiki/Return-oriented_programming)

pentest:exploit="null_pointer_dereference"

A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit. (https://cwe.mitre.org/data/definitions/476.html)

post_exploitation

Utilizing post exploitation techniques will ensure that a penetration tester maintains some level of access and can potentially lead to deeper footholds into the targets trusted infrastructure. (https://www.offensive-security.com/metasploit-unleashed/msf-post-exploitation/)

pentest:post_exploitation="privilege_escalation"

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. (https://en.wikipedia.org/wiki/Privilege_escalation)

pentest:post_exploitation="pivoting"

Pivoting refers to a method used by penetration testers that uses the compromised system to attack other systems on the same network to avoid restrictions such as firewall configurations, which may prohibit direct access to all machines. (https://en.wikipedia.org/wiki/Exploit_(computer_security)#Pivoting)

pentest:post_exploitation="password_cracking"

Password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system. (https://en.wikipedia.org/wiki/Password_cracking)

pentest:post_exploitation="persistence"

The persistence is when a penetration tester let him a way to keep its exploitation on a machine or

a domain even if the system is rebooted.

pentest:post_exploitation="data_exfiltration"

After an exploitation of a machine, a penetration tester will try to exfiltrate sensitive data.

web

This is group is dealing with web vulnerabilities

pentest:web="injection"

Code injection is the exploitation of a computer bug that is caused by processing invalid data. Injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution. (https://en.wikipedia.org/wiki/Code_injection)

pentest:web="SQLi"

An SQL injection is a computer attack in which malicious code is embedded in a poorly-designed application and then passed to the SQL backend database. The malicious data then produces database query results or actions that should never have been executed.(https://www.techopedia.com/definition/4126/sql-injection)

pentest:web="NoSQLi"

An NoSQL injection is a computer attack in which malicious code is embedded in a poorly-designed application and then passed to the NoSQL backend database. The malicious data then produces database query results or actions that should never have been executed.

pentest:web="XML injection"

XML Injection is an attack technique used to manipulate or compromise the logic of an XML application or service. The injection of unintended XML content and/or structures into an XML message can alter the intend logic of the application. Further, XML injection can cause the insertion of malicious content into the resulting message/document.(http://projects.webappsec.org/w/page/13247004/XML%20Injection)

pentest:web="CSRF"

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request.(https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF))

pentest:web="SSRF"

Server Side Request Forgery (SSRF) refers to an attack where in an attacker is able to send a crafted request from a vulnerable web application. SSRF is usually used to target internal systems behind

firewalls that are normally inaccessible to an attacker from the external network. (https://www.acunetix.com/blog/articles/server-side-request-forgery-vulnerability/)

pentest:web="XSS"

Cross-site scripting (XSS) is a security breach that takes advantage of dynamically generated Web pages. In an XSS attack, a Web application is sent with a script that activates when it is read by an unsuspecting user's browser or by an application that has not protected itself against cross-site scripting. (https://www.webopedia.com/TERM/X/XSS.html)

pentest:web="file_inclusion"

The File Inclusion vulnerability allows an attacker to include a file, usually exploiting a "dynamic file inclusion" mechanisms implemented in the target application. The vulnerability occurs due to the use of user-supplied input without proper validation. (https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion)

pentest:web="web_tree_discovery"

A web tree discovery is a brute force directories and files names on web/application server

pentest:web="bruteforce"

A brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly. (https://en.wikipedia.org/wiki/Brute-force_attack)

pentest:web="fuzzing"

Fuzzing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. (https://en.wikipedia.org/wiki/Fuzzing)

network

This is group is dealing with network vulnerabilities

pentest:network="sniffing"

Sniffing involves capturing, decoding, inspecting and interpreting the information inside a network packet on a TCP/IP network. (http://www.valencynetworks.com/articles/cyber-security-attacks-network-sniffing.html)

pentest:network="spoofing"

Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security. (https://www.techopedia.com/definition/5398/spoofing)

pentest:network="man_in_the_middle"

man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. (https://en.wikipedia.org/wiki/Man-in-the-middle_attack)

pentest:network="network_discovery"

It is the discovery of networks and machines with services.

social_engineering

Social engineering is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. (https://krashconsulting.com/index.php/services/sea/)

pentest:social_engineering="phishing"

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. (https://en.wikipedia.org/wiki/Phishing)

pentest:social_engineering="malware"

Malware, short for malicious software, is an umbrella term used to refer to a variety of forms of harmful or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. (https://en.wikipedia.org/wiki/Malware)

vulnerability

This is group is dealing with the classification of weaknesses and vulnerabilities

pentest:vulnerability="CWE"

Targeted to developers and security practitioners, the Common Weakness Enumeration (CWE) is a formal list of software weakness types. (https://cwe.mitre.org/about/)

pentest:vulnerability="CVE"

Common Vulnerabilities and Exposures (CVE) is a dictionary-type list of standardized names for vulnerabilities and other information related to security exposures. (https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures)

phishing

phishing namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Taxonomy to classify phishing attacks including techniques, collection mechanisms and analysis status.

techniques

Phishing techniques used.

phishing:techniques="fake-website"

Social engineering fake website

Adversary controls a fake website to phish for credentials or information.

phishing:techniques="email-spoofing"

Social engineering email spoofing

Adversary sends email with domains related to target. Adversary controls the domains used.

phishing:techniques="clone-phishing"

Clone phishing

Adversary clones an email to target potential victims with duplicated content.

phishing:techniques="voice-phishing"

Voice phishing

Adversary uses voice-based techniques to trick a potential victim to give credentials or sensitive information. This is also known as vishing.

phishing:techniques="search-engines-abuse"

Social engineering search engines abuse

Adversary controls the search engine result to get an advantage

phishing:techniques="sms-phishing"

SMS phishing

Adversary sends an SMS to a potential victims to gather sensitive information or use another phishing technique at a later stage.

phishing:techniques="business email compromise"

Business Email Compromise

Adversary sends an email containing a malicious artefact from a legitimate business email address which has connections to you as an individual or your organisation.

distribution

How the phishing is distributed.

phishing:distribution="spear-phishing"

Spear phishing

Adversary attempts targeted phishing to a user or a specific group of users based on knowledge known by the adversary.

phishing:distribution="bulk-phishing"

Bulk phishing

Adversary attempts to target a large group of potential targets without specific knowledge of the victims.

phishing:distribution="whaling"

Whaling phishing

Adversary attempts to target executives and high-level employees (like public spokespersons).

report-type

How the phishing information was reported.

phishing:report-type="manual-reporting"

Manual reporting

Phishing reported by a human (e.g. tickets, manual reporting).

phishing:report-type="automatic-reporting"

Automatic reporting

Phishing collected by automatic reporting (e.g. phishing report tool, API).

report-origin

Origin or source of the phishing information such as tools or services.

phishing:report-origin="url-abuse"

url-abuse

CIRCL url-abuse service.

phishing:report-origin="lookyloo"

lookyloo

CIRCL lookyloo service.

phishing:report-origin="phishtank"

Phishtank

Phishtank service.

phishing:report-origin="spambee"

Spambee

C-3 Spambee service.

action

Action(s) taken related to the phishing tagged with this taxonomy.

phishing:action="take-down"

Take down

Take down notification sent to the operator where the phishing infrastructure is hosted.

phishing:action="pending-law-enforcement-request"

Pending law enforcement request

Law enforcement requests are ongoing on the phishing infrastructure.

phishing:action="pending-dispute-resolution"

Pending dispute resolution

Dispute resolution sent to competent authorities (e.g. domain authority, trademark dispute).

state

State of the phishing.

Exclusive flag set which means the values or predicate below must be set exclusively.

phishing:state="unknown"

Phishing state is unknown or cannot be evaluated

Associated numerical value="50"

phishing:state="active"

Phishing state is active and actively used by the adversary

Associated numerical value="100"

phishing:state="down"

Phishing state is known to be down

psychological-acceptability

Quality of the phishing by its level of acceptance by the target.

Exclusive flag set which means the values or predicate below must be set exclusively.

phishing:psychological-acceptability="unknown"

Phishing acceptance rate is unknown.

phishing:psychological-acceptability="low"

Phishing acceptance rate is low.

Associated numerical value="25"

phishing:psychological-acceptability="medium"

Phishing acceptance rate is medium.

Associated numerical value="50"

phishing:psychological-acceptability="high"

Phishing acceptance rate is high.

Associated numerical value="75"

principle-of-persuasion

The principle of persuasion used during the attack to higher psychological acceptability.

phishing:principle-of-persuasion="authority"

Society trains people not to question authority so they are conditioned to respond to it. People usually follow an expert or pretense of authority and do a great deal for someone they think is an authority.

phishing:principle-of-persuasion="social-proof"

People tend to mimic what the majority of people do or seem to be doing. People let their guard and suspicion down when everyone else appears to share the same behaviours and risks. In this way, they will not be held solely responsible for their actions.

phishing:principle-of-persuasion="liking-similarity-deception"

People prefer to abide to whom (they think) they know or like, or to whom they are similar to or familiar with, as well as attracted to.

phishing:principle-of-persuasion="commitment-reciprocation-consistency"

People feel more confident in their decision once they commit (publically) to a specific action and need to follow it through until the end. This is true whether in the workplace, or in a situation when their action is illegal. People have tendency to believe what others say and need, and they want to appear consistent in what they do, for instance, when they owe a favour. There is an automatic response of repaying a favour.

phishing:principle-of-persuasion="distraction"

People focus on one thing and ignore other things that may happen without them noticing; they focus attention on what they can gain, what they need, what they can lose or miss out on, or if that thing will soon be unavailable, has been censored, restricted or will be more expensive later. These distractions can heighten people’s emotional state and make them forget other logical facts to consider when making decisions.

political-spectrum

political-spectrum namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A political spectrum is a system to characterize and classify different political positions in relation to one another.

ideology

Political ideologies are one of the major organizing features of political parties, and parties often officially align themselves with specific ideologies.

political-spectrum:ideology="agrarianism"

Agrarianism

political and social philosophy that has promoted subsistence agriculture, smallholdings, egalitarianism, with agrarian political parties normally supporting the rights and sustainability of small farmers and poor peasants against the wealthy in society.

political-spectrum:ideology="anarchism"

Anarchism

Anarchism is a political philosophy and movement that is sceptical of authority and rejects all involuntary, coercive forms of hierarchy.

political-spectrum:ideology="centrism"

Centrism

Centrism is a political outlook or position that involves acceptance and/or support of a balance of social equality and a degree of social hierarchy, while opposing political changes which would result in a significant shift of society strongly to either the left or the right.

political-spectrum:ideology="christian-democracy"

Christian Democracy

combination of modern democratic ideas and traditional Christian values, incorporating social justice as well as the social teachings espoused by the Catholic, Lutheran, Reformed, Pentecostal and other denominational traditions of Christianity in various parts of the world. After World War II, Catholic and Protestant movements of neo-scholasticism and the Social Gospel, respectively, played a role in shaping Christian democracy.

political-spectrum:ideology="communism"

Communism

Communism is a philosophical, social, political, and economic ideology and movement whose goal is the establishment of a communist society, namely a socioeconomic order structured upon the ideas of common ownership of the means of production and the absence of social classes, money, and the state.

political-spectrum:ideology="conservatism"

Conservatism

Conservatism is an aesthetic, cultural, social, and political philosophy, which seeks to promote and to preserve traditional social institutions. The central tenets of conservatism may vary in relation to the traditional values or practices of the culture and civilization in which it appears. In Western culture, conservatives seek to preserve a range of institutions such as organized religion, parliamentary government, and property rights. Adherents of conservatism often oppose modernism and seek a return to traditional values.

political-spectrum:ideology="democratic-socialism"

Democratic socialism

Democratic socialism is a political philosophy that supports political democracy within a socially owned economy, with a particular emphasis on economic democracy, workplace democracy, and workers' self-management within a market socialist economy, or an alternative form of decentralised planned socialist economy.

political-spectrum:ideology="fascism"

Fascism

Fascism is a form of far-right, authoritarian ultranationalism characterized by dictatorial power, forcible suppression of opposition, and strong regimentation of society and of the economy, which came to prominence in early 20th-century Europe.Fascists believe that liberal democracy is obsolete. They regard the complete mobilization of society under a totalitarian one-party state as necessary to prepare a nation for armed conflict and to respond effectively to economic difficulties.

political-spectrum:ideology="feminism"

Feminism

Feminism is a range of social movements and ideologies that aim to define and establish the political, economic, personal, and social equality of the sexes. Feminism incorporates the position that societies prioritize the male point of view, and that women are treated unjustly within those societies. Efforts to change that include fighting against gender stereotypes and establishing educational, professional, and interpersonal opportunities and outcomes for women that are equal to those for men.

political-spectrum:ideology="green-politics"

Green politics

Green politics, or ecopolitics, is a political ideology that aims to foster an ecologically sustainable society often, but not always, rooted in environmentalism, nonviolence, social justice and grassroots democracy.

political-spectrum:ideology="islamism"

Islamism

Islamism (also often called political Islam or Islamic fundamentalism) is a political ideology which posits that modern states and regions should be reconstituted in constitutional, economic and judicial terms, in accordance with what is conceived as a revival or a return to authentic Islamic practice in its totality.

political-spectrum:ideology="liberalism"

Liberalism

Liberalism is a political and moral philosophy based on liberty, consent of the governed and equality before the law. Liberals espouse a wide array of views depending on their understanding of these principles, but they generally support individual rights (including civil rights and human rights), democracy, secularism, freedom of speech, freedom of the press, freedom of religion and a market economy.

political-spectrum:ideology="libertarianism"

Libertarianism

Libertarianism is a political philosophy that upholds liberty as a core principle. Libertarians seek to maximize autonomy and political freedom, emphasizing free association, freedom of choice, individualism and voluntary association. Libertarians share a skepticism of authority and state power, but some libertarians diverge on the scope of their opposition to existing economic and political systems.

political-spectrum:ideology="monarchism"

Monarchism

Monarchism is the advocacy of the system of monarchy or monarchical rule.

political-spectrum:ideology="pacifism"

Pacifism

Pacifism covers a spectrum of views, including the belief that international disputes can and should be peacefully resolved, calls for the abolition of the institutions of the military and war, opposition to any organization of society through governmental force (anarchist or libertarian pacifism), rejection of the use of physical violence to obtain political, economic or social goals, the obliteration of force, and opposition to violence under any circumstance, even defence of self and others.

political-spectrum:ideology="social-democracy"

Social democracy

Social democracy is a political, social, and economic philosophy within socialism that supports political and economic democracy. As a policy regime, it is described by academics as advocating economic and social interventions to promote social justice within the framework of a liberal-democratic polity and a capitalist-oriented mixed economy.

political-spectrum:ideology="socialism"

Socialism

Socialism is a political, social, and economic philosophy encompassing a range of economic and social systems characterised by social ownership of the means of production. It includes the political theories and movements associated with such systems. Social ownership can be public, collective, cooperative, or of equity. While no single definition encapsulates the many types of socialism, social ownership is the one common element.

left-right-spectrum

The left–right political spectrum is a system of classifying political positions characteristic of left-right politics, ideologies and parties with emphasis placed on issues of social equality and social hierarchy.

political-spectrum:left-right-spectrum="far-left"

Far-left

There are different definitions of the far-left. It could represent the left of social democraty, or also limited to the left of communist parties. Sometimes it is also associated with some forms of anarchism and communims, or groupsthat advocate for revolutionary anti-capitalism and anti-globalization.

political-spectrum:left-right-spectrum="centre-left"

Centre-left

Also refered as moderate-left politics. Believes in working within the established systems to improve social justice. Promotes a degree of social equality that it believes is achievable through promoting equal opportunity. Emphasizes that the achievement of equality requires personal responsibility in areas in control by the individual person through their abilities and talents as well as social responsibility in areas outside control by the person in their abilities or talents.

political-spectrum:left-right-spectrum="radical-centre"

Radical centre

The radical in the term refers to a willingness on the part of most radical centrists to call for

fundamental reform of institutions.[The centrism refers to a belief that genuine solutions require realism and pragmatism, not just idealism and emotion. Radical centrists borrow ideas from the left and the right, often melding them together.

political-spectrum:left-right-spectrum="centre-right"

Centre-right

Also referred to as moderate-right politics. Ideologies characterised as centre-right include liberal conservatism and some variants of liberalism and Christian democracy, among others.

political-spectrum:left-right-spectrum="far-right"

Far-right

Referred to as the extreme right or right-wing extremism. Are usually described as anti-communist, authoritarian, ultranationalist, and having nativist ideologies and tendencies. Today far-right politics include neo-fascism, neo-Nazism, the Third Position, the alt-right, racial supremacism, and other ideologies or organizations that feature aspects of ultranationalist, chauvinist, xenophobic, theocratic, racist, homophobic, transphobic, or reactionary views.

priority-level

priority-level namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

After an incident is scored, it is assigned a priority level. The six levels listed below are aligned with NCCIC, DHS, and the CISS to help provide a common lexicon when discussing incidents. This priority assignment drives NCCIC urgency, pre-approved incident response offerings, reporting requirements, and recommendations for leadership escalation. Generally, incident priority distribution should follow a similar pattern to the graph below. Based on https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System.

Exclusive flag set which means the values or predicate below must be set exclusively.

emergency

An Emergency priority incident poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons.

priority-level:emergency

Emergency

An Emergency priority incident poses an imminent threat to the provision of wide-scale critical

infrastructure services, national government stability, or the lives of U.S. persons.

100

severe

A Severe priority incident is likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.

priority-level:severe

Severe

A Severe priority incident is likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.

90

high

A High priority incident is likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

priority-level:high

High

A High priority incident is likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

85

medium

A Medium priority incident may affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

priority-level:medium

Medium

A Medium priority incident may affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

75

low

A Low priority incident is unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

priority-level:low

Low

A Low priority incident is unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

50

baseline-minor

A Baseline–Minor priority incident is an incident that is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. The potential for impact, however, exists and warrants additional scrutiny.

priority-level:baseline-minor

Baseline - Minor

A Baseline–Minor priority incident is an incident that is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. The potential for impact, however, exists and warrants additional scrutiny.

25

baseline-negligible

A Baseline–Negligible priority incident is an incident that is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

priority-level:baseline-negligible

Baseline - Negligible

A Baseline–Negligible priority incident is an incident that is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

ransomware

ransomware namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Ransomware is used to define ransomware types and the elements that compose them.

type

Type is used to describe the type of a ransomware and how it works.

ransomware:type="scareware"

Scareware is a form of malware which uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying unwanted software.

ransomware:type="locker-ransomware"

Locker ransomware, also called screen locker, denies access to the browser, computer or device.

ransomware:type="crypto-ransomware"

Crypto ransomware, also called data locker or cryptoware, prevents access to files or data. Crypto ransomware doesn't necessarily have to use encryption to stop users from accessing their data, but the vast majority of it does.

element

Elements that composed or are linked to a ransomware and its execution.

ransomware:element="ransomnote"

A ransomnote is the message left by the attacker to threaten their victim and ask for a ransom. It is usually seen as a text or HTML file, or a picture set as background.

ransomware:element="ransomware-appended-extension"

This is the extension added by the ransomware to the files.

ransomware:element="ransomware-encrypted-extensions"

This is the list of extensions that will be encrypted by the ransomware. Beware to keep the order.

ransomware:element="ransomware-excluded-extensions"

This is the list of extensions that will not be encrypted by the ransomware. Beware to keep the order.

ransomware:element="dropper"

A dropper is a means of getting malware into a machine while bypassing the security checks, often by containing the malware inside of itself.

ransomware:element="downloader"

A downloader is a means of getting malware into a machine while bypassing the security checks, by downloading it instead of containing it.

complexity-level

Level of complexity of the ransomware.

ransomware:complexity-level="no-actual-encryption-scareware"

No actual encryption (scareware). Infection merely poses as a ransomware by displaying a ransom note or message while not actually encrypting user files.

ransomware:complexity-level="display-ransomnote-before-encrypting"

Displaying the ransom note before the encryption process commences. As seen in the case of Nemucod, some ransomware will display a ransom note before file encryption. This is a serious operational flaw in the ransomware. The victim or their antivirus solution could effectively take prompt evasive action to prevent ransomware from commencing encryption.

ransomware:complexity-level="decryption-essentials-extracted-from-binary"

Decryption essentials can be reverse engineered from ransomware code or the user's system. For example, if the ransomware uses a hard-coded key, then it becomes straight-forward for malware analysts to extract the key by reverse engineering the ransomware binary.

ransomware:complexity-level="derived-encryption-key-predicted "

Another possibility of reverse engineering the key is demonstrated in the case of Linux.Encoder, a type of ransomware where a timestamp on the system was used to create keys for encryption resulting in easy decryption provided that the timestamp is still accessible.

ransomware:complexity-level="same-key used-for-each-infection"

Ransomware uses the same key for every victim. If the same key is used to encrypt all victims during a campaign, then one victim can share the secret key with others.

ransomware:complexity-level="encryption-circumvented"

Decryption possible without key - files can be decrypted without the need for a key due to poor choice or implementation of the encryption algorithm. Consider the case of desuCrypt that used an RC4 stream cipher for encryption. Using a stream cipher with key reuse is vulnerable to known plaintext attacks and known ciphertext attacks due to key reuse and hence this is a poor implementation of an encryption algorithm.

ransomware:complexity-level="file-restoration-possible-using-shadow-volume-copies"

Files can be restored using Shadow Volume Copies (“Previous Versions”) on the New Technology File System (NTFS), that were neglected to be deleted by the ransomware.

ransomware:complexity-level="file-restoration-possible-using-backups"

Files can be restored using a System State backup, System Image backup or other means of backup mechanisms (such as third-party backup software) that will render the ransomware’s extortion attempt unsuccessful.

ransomware:complexity-level="key-recovered-from-file-system-or-memory"

Decryption key can be retrieved from the host machine’s file structure or memory by an average user without the need for an expert. In the case of CryptoDefense, the ransomware did not securely delete keys from the host machine. The user can examine the right file or folder to discover the decryption key.

ransomware:complexity-level="due-diligence-prevented-ransomware-from-acquiring-key"

User can prevent ransomware from acquiring the encryption key. Ransomware belongs in this category if its encryption procedure can be interrupted or blocked by due diligence on part of the user. For example, CryptoLocker discussed above cannot commence operation until it receives a key from the C&C server. A host or border firewall can block a list of known C&C servers hence rendering ransomware ineffective.

ransomware:complexity-level="click-and-run-decryptor-exists"

Easy “Click-and-run” solutions such as a decryptor has been created by the security community such that a user can simply run the program to decrypt all files.

ransomware:complexity-level="kill-switch-exists-outside-of-attacker-s-control"

There exists a kill switch outside of an attacker’s control that renders the cryptoviral infection ineffective. For example, in the case of WannaCry, a global kill switch existed in the form of a domain name. The ransomware reached out to this domain before commencing encryption and if the domain existed, the ransomware aborted execution. This kill switch was outside the attacker’s control as anyone could register it and neutralize the ransomware outbreak.

ransomware:complexity-level="decryption-key-recovered-from-a-C&C-server-or-network-communications"

Key can be retrieved from a central location such as a C&C server on a compromised host or gleaned with some difficulty from communication between ransomware on the host and the C&C

server. For instance, in the case of CryptoLocker, authorities were able to seize a network of compromised hosts used to spread CryptoLocker and gain access to decryption essentials of around 500,000 victims.

ransomware:complexity-level="custom-encryption-algorithm-used"

Ransomware uses custom encryption techniques and violates the fundamental rule of cryptography: “do not roll your own crypto.” It is tempting to design a custom cipher that one cannot break themselves, however it will likely not withstand the scrutiny of professional cryptanalysts. Amateur custom cryptography in the ransomware implies there will likely soon be a solution to decrypt files without paying the ransom. An example of this is an early variant of the GPCode ransomware that emerged in 2005 with weak custom encryption.

ransomware:complexity-level="decryption-key-recovered-under-specialized-lab-setting"

Key can only be retrieved under rare, specialized laboratory settings. For example, in the case of WannaCry, a vulnerability in a cryptographic API on an unpatched Windows XP system allowed users to acquire from RAM the prime numbers used to compute private keys and hence retrieve the decryption key. However, the victim had to have been running a specific version of Windows XP and be fortunate enough that the related address space in memory has not been reallocated to another process. In another example, it is theoretically possible to reverse WannaCry encryption by exploiting a flaw in the pseudo-random-number-generator (PRNG) in an unpatched Windows XP system that reveals keys generated in the past. Naturally, these specialized conditions are not true for most victims.

ransomware:complexity-level="small-subset-of-files-left-unencrypted"

A small subset of files left unencrypted by the ransomware for any number of reasons. Certain ransomware are known to only encrypt a file if its size exceeds a predetermined value. In addition, ransomware might decrypt a few files for free to prove decryption is possible. In such cases, a small number of victims may be lucky enough to only need these unencrypted files and can tolerate loss of the rest.

ransomware:complexity-level="encryption-model-is-seemingly-flawless"

Encryption model is resistant to cryptographic attacks and has been implemented seemingly flawlessly such that there are no known vulnerabilities in its execution. Simply put, there is no proven way yet to decrypt the files without paying the ransom.

purpose

Purpose of the ransomware.

ransomware:purpose="deployed-as-ransomware-extortion"

This has been the traditional approach - ransomware is installed on the victim’s machine, and its only purpose is to create income for the cybercriminal(s). In fact, ransomware is simple extortion,

but via digital means.

ransomware:purpose="deployed-to-showcase-skills-for-fun-or-for-testing-purposes"

Some cybercriminals like to show off, and as such create the side-business of ransomware, or, more particularly to showcase their coding skills. Another example may be to send ransomware 'as a joke' or for fun to your friends, and giving them a bad time. Some cybercriminals may be testing the waters by deploying ransomware in an organisation, to stress-test the defenses, or to test their own programming skills, or the lack thereof.

ransomware:purpose="deployed-as-smokescreen"

A very interesting occurrence indeed: ransomware is installed to hide the real purpose of whatever the cybercriminal or attacker is doing. This may be data exfiltration, lateral movement, or anything else, in theory, everything is a possible scenario… except for the ransomware itself.

ransomware:purpose="deployed-to-cause-frustration"

Another possible angle that goes hand in hand with the classic extortion scheme - deploying ransomware with intent of frustrating the victim. Basically, cyber bullying. While there may be a request for a monetary amount, it is not the purpose.

ransomware:purpose="deployed-out-of-frustration"

Sometimes, an attacker may gain initial access to a server or other machine, but consequent attempts to, for example, exfiltrate data or attack other machine, is unsuccessful. This may be due to a number of things, but often due to the access being discovered, and quickly patched. On the other hand, it may have not been discovered yet, but the attacker is sitting with the same problem: the purpose is not fulfilled. Then, out of frustration, or to gain at least something out of the victim, the machine gets trashed with ransomware. Another possibility is a disgruntled employee, leaving ransomware as a 'present' before leaving the company.

ransomware:purpose="deployed-as-a-cover-up"

This may sound ambiguous at first, but imagine a scenario where a company may face sanctions, is already compromised, or has a running investigation. The company or organisation deploying ransomware itself, is a viable way of destroying data forever, and any evidence may be lost. Another possibility is, in order to cover up a much larger compromise, ransomware is installed, and everything is formatted to hide what actually happened. Again, there is also the possibility of a disgruntled employee, or even an intruder: which brings us back to 'deployed as a smokescreen'.

ransomware:purpose="deployed-as-a-penetration-test-or-user-awareness-training"

Ransomware is very effective in the sense that most people know what its purpose is, and the dangers it may cause. As such, it is an excellent tool that can be used for demonstration purposes, such as a user awareness training. Another possibility is an external pentest, with same purpose.

ransomware:purpose="deployed-as-a-means-of-disruption-destruction"

Last but not least - while ransomware can have several purposes, it can also serve a particularly nasty goal: destroy a company or organisation, or at least take them offline for several days, or even weeks. Again, there are some possibilities, but this may be a rivalry company in a similar business, again a disgruntled employee, or to disrupt large organisations on a worldwide scale.

target

Target of the ransomware.

ransomware:target="pc-workstation"

Ransomware that targets PCs or workstations.

ransomware:target="mobile-device"

Ransomware that targets mobile devices.

ransomware:target="iot-cps-device"

Ransomware that targets IoT or CPS devoces.

ransomware:target="end-user"

Ransomware that targets end users.

ransomware:target="organisation"

Ransomware that targets organisation.

infection

Infection vector used by the ransomware.

ransomware:infection="phishing-e=mails"

Malicious e-mails are the most commonly used infection vectors for ransomware. Attackers send spam e-mails to victims that have attachments containing ransomware. Such spam campaigns can be distributed using botnets. Ransomware may come with an attached malicious file, or the e-mail may contain a malicious link that will trigger the installation of ransomware once visited (drive-by download).

ransomware:infection="sms-instant-message"

SMS Messages or IMs are used frequently for mobile ransomware. In such kind of infections, attackers send SMS messages or IMs to the victims that will cause them to browse a malicious website to download ransomware to their platforms.

ransomware:infection="malicious-apps"

Malicious Applications are used by ransomware attackers who develop and deploy mobile applications that contain ransomware camouflaged as a benign application.

ransomware:infection="drive-by-download"

Drive-by download happens when a user unknowingly visits an infected website or clicks a malicious advertisement (i.e., malvertisement) and then the malware is downloaded and installed without the user's knowledge.

ransomware:infection="vulnerabilities"

Vulnerabilities in the victim platform such as vulnerabilities in operating systems, browsers, or software can be used by ransomware authors as infection vectors. Attackers can use helper applications, exploit kits, to exploit the known or zero-day vulnerabilities in target systems. Attackers can redirect victims to those kits via malvertisement and malicious links.

communication

Communication method used by the ransomware;

ransomware:communication="hard-coded-ip"

Ransomware connecting to C&C via hard-coded IP addresses or domains

ransomware:communication="dga-based"

Ransomware connecting to C&C via dynamically fast-fluxed/generated/shifted domain names using Domain Generation Algorithms (DGA)

malicious-action

Malicious action performed by the ransomware.

ransomware:malicious-action="symmetric-key-encryption"

Ransomware that encrypts data using symmetric-key encryption.

ransomware:malicious-action="asymmetric-key-encryption"

Ransomware that encrypts data using asymmetric-key encryption.

ransomware:malicious-action="hybrid-key-encryption"

Ransomware that encrypts data using hybrid-key encryption.

ransomware:malicious-action="screen-locking"

Ransomware that locks the system's graphical user interface and prevent access.

ransomware:malicious-action="browser-locking"

Ransomware that locks slock web browser of the victim.

ransomware:malicious-action="mbr-locking"

Ransomware that locks Master Boot Records.

ransomware:malicious-action="data-exfiltration"

Ransomware that exfiltrates data.

retention

retention namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Add a retenion time to events to automatically remove the IDS-flag on ip-dst or ip-src attributes. We calculate the time elapsed based on the date of the event. Supported time units are: d(ays), w(eeks), m(onths), y(ears). The numerical_value is just for sorting in the web-interface and is not used for calculations.

Exclusive flag set which means the values or predicate below must be set exclusively.

expired

retention:expired

Set when the retention period has expired

1d

retention:1d

1 day

1

2d

retention:2d

2 days

2

7d

retention:7d

7 days

7

2w

retention:2w

2 weeks

14

1m

retention:1m

1 month

30

2m

retention:2m

2 months

60

3m

retention:3m

3 months

90

6m

retention:6m

6 months

180

1y

retention:1y

1 year

365

10y

retention:10y

10 year

3650

rsit

rsit namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Reference Security Incident Classification Taxonomy

abusive-content

Abusive Content.

rsit:abusive-content="spam"

Spam

Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content. This IOC refers to resources which make up spam infrastructure, for example, harvesters like address verification, URLs in spam emails, etc.

rsit:abusive-content="harmful-speech"

Harmful Speech

Bullying, harassment or discrimination of somebody, e.g., cyber stalking, racism or threats against one or more individuals.

rsit:abusive-content="violence"

(Child) Sexual Exploitation/Sexual/Violent Content

Child Sexual Exploitation (CSE), sexual content, glorification of violence, etc.

malicious-code

Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.

rsit:malicious-code="infected-system"

Infected System

System infected with malware, e.g., a PC, smartphone or server infected with a rootkit. Most often this refers to a connection to a sinkholed command and control server.

rsit:malicious-code="c2-server"

C2 Server

Command and control server contacted by malware on infected systems.

rsit:malicious-code="malware-distribution"

Malware Distribution

URI used for malware distribution, e.g., a download URL included in fake invoice malware spam or exploit kits (on websites).

rsit:malicious-code="malware-configuration"

Malware Configuration

URI hosting a malware configuration file, e.g., web injects for a banking trojan.

information-gathering

Information Gathering.

rsit:information-gathering="scanner"

Scanning

Attacks that send requests to a system to discover weaknesses. This also includes testing processes to gather information on hosts, services and accounts. This includes fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, etc) port scanning.

rsit:information-gathering="sniffing"

Sniffing

Observing and recording of network traffic (i.e. wiretapping).

rsit:information-gathering="social-engineering"

Social Engineering

Gathering information from a human being in a non-technical way (e.g., using lies, tricks, bribes, or threats).

intrusion-attempts

Intrusion Attempts.

rsit:intrusion-attempts="ids-alert"

Exploitation of Known Vulnerabilities

An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g., using a buffer overflow, backdoor, cross site scripting)

rsit:intrusion-attempts="brute-force"

Login Attempts

Multiple brute-force login attempts (including guessing or cracking of passwords). This IOC refers to a resource, which has been observed to perform brute-force attacks over a given application protocol.

rsit:intrusion-attempts="exploit"

New Attack Signature

An attack using an unknown exploit.

intrusions

A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorised local access. Also includes being part of a botnet.

rsit:intrusions="privileged-account-compromise"

Privileged Account Compromise

Compromise of a system where the attacker has gained administrative privileges.

rsit:intrusions="unprivileged-account-compromise"

Unprivileged Account Compromise

Compromise of a system using an unprivileged (user/service) account.

rsit:intrusions="application-compromise"

Application Compromise

Compromise of an application by exploiting (un)known software vulnerabilities, e.g., SQL injection.

rsit:intrusions="system-compromise"

System Compromise

Compromise of a system, e.g., unauthorised logins or commands. This includes attempts to compromise honeypot systems.

rsit:intrusions="burglary"

Burglary

Physical intrusion, e.g., into a corporate building or data centre.

availability

By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) – or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.

rsit:availability="dos"

Denial of Service

Denial of Service attack, e.g., sending specially crafted requests to a web application which causes the application to crash or slow down.

rsit:availability="ddos"

Distributed Denial of Service

Distributed Denial of Service attack, e.g., SYN flood or UDP-based reflection/amplification attacks.

rsit:availability="misconfiguration"

Misconfiguration

Software misconfiguration resulting in service availability issues, e.g., DNS server with outdated DNSSEC Root Zone KSK.

rsit:availability="sabotage"

Sabotage

Physical sabotage, e.g., cutting wires or malicious arson.

rsit:availability="outage"

Outage

An outage caused, for example, by air conditioning failure or natural disaster.

information-content-security

Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/software error can also be the cause.

rsit:information-content-security="unauthorised-information-access"

Unauthorised Access to Information

Unauthorised access to information, e.g., by abusing stolen login credentials for a system or application, intercepting traffic or gaining access to physical documents.

rsit:information-content-security="unauthorised-information-modification"

Unauthorised Modification of Information

Unauthorised modification of information, e.g., by an attacker abusing stolen login credentials for a system or application, or ransomware encrypting data. Also includes defacements.

rsit:information-content-security="data-loss"

Data Loss

Loss of data caused by, for example, hard disk failure or physical theft.

rsit:information-content-security="data-leak"

Leak of Confidential Information

Leaked confidential information, e.g., credentials or personal data.

fraud

Fraud.

rsit:fraud="unauthorised-use-of-resources"

Unauthorised Use of Resources

Using resources for unauthorised purposes including profit-making ventures, e.g., the use of email to participate in illegal profit chain letters or pyramid schemes.

rsit:fraud="copyright"

Copyright

Offering or installing copies of unlicensed commercial software or other copyright protected materials (also known as Warez).

rsit:fraud="masquerade"

Masquerade

Type of attack in which one entity illegitimately impersonates the identity of another in order to benefit from it.

rsit:fraud="phishing"

Phishing

Masquerading as another entity in order to persuade the user to reveal private credentials. This IOC most often refers to a URL, which is used to phish user credentials.

vulnerable

Open resolvers, world-readable printers, vulnerabilities apparent from scans, anti-virus signatures not up-to-date, etc.

rsit:vulnerable="weak-crypto"

Weak Cryptography

Publicly accessible services offering weak cryptography, e.g., web servers susceptible to POODLE/FREAK attacks.

rsit:vulnerable="ddos-amplifier"

DDoS Amplifier

Publicly accessible services that can be abused for conducting DDoS reflection/amplification attacks, e.g., DNS open-resolvers or NTP servers with monlist enabled.

rsit:vulnerable="potentially-unwanted-accessible"

Potentially Unwanted Accessible Services

Potentially unwanted publicly accessible services, e.g., Telnet, RDP or VNC.

rsit:vulnerable="information-disclosure"

Information disclosure

Publicly accessible services potentially disclosing sensitive information, e.g., SNMP or Redis.

rsit:vulnerable="vulnerable-system"

Vulnerable System

A system which is vulnerable to certain attacks, e.g., misconfigured client proxy settings (such as WPAD), outdated operating system version, or cross-site scripting vulnerabilities.

other

All incidents which don’t fit in one of the given categories should be put into this class. If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.

rsit:other="other"

Uncategorised

All incidents which don’t fit in one of the given categories should be put into this class or the incident is not categorised.

rsit:other="undetermined"

Undetermined

The categorisation of the incident is unknown/undetermined.

test

Meant for testing.

rsit:test="test"

Test

Meant for testing.

rt_event_status

rt_event_status namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Status of events used in Request Tracker.

Exclusive flag set which means the values or predicate below must be set exclusively.

event-status

rt_event_status:event-status="new"

New

rt_event_status:event-status="open"

Open

rt_event_status:event-status="stalled"

Stalled

rt_event_status:event-status="rejected"

rejected

rt_event_status:event-status="resolved"

Resolved

rt_event_status:event-status="deleted"

Deleted

runtime-packer

runtime-packer namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Runtime or software packer used to combine compressed data with the decompression code. The decompression code can add additional obfuscations mechanisms including polymorphic-packer or other obfuscation techniques. This taxonomy lists all the known or official packer used for legitimate use or for packing malicious binaries.

portable-executable

runtime-packer:portable-executable=".netshrink"

runtime-packer:portable-executable="armadillo"

netshrink

Armadillo

runtime-packer:portable-executable="aspack"

ASPack

runtime-packer:portable-executable="aspr-asprotect"

ASPR (ASProtect)

runtime-packer:portable-executable="boxedapp-packer"

BoxedApp Packer

runtime-packer:portable-executable="cexe"

CExe

runtime-packer:portable-executable="dotbundle"

dotBundle

runtime-packer:portable-executable="enigma-protector"

Enigma Protector

runtime-packer:portable-executable="exe-bundle"

EXE Bundle

runtime-packer:portable-executable="exe-stealth"

EXE Stealth

runtime-packer:portable-executable="expressor"

eXPressor

runtime-packer:portable-executable="fsg"

FSG

runtime-packer:portable-executable="kkrunchy-src"

kkrunchy src

runtime-packer:portable-executable="mew"

MEW

runtime-packer:portable-executable="mpress"

MPRESS

runtime-packer:portable-executable="obsidium"

Obsidium

runtime-packer:portable-executable="pelock"

PELock

runtime-packer:portable-executable="pespin"

PESpin

runtime-packer:portable-executable="petite"

Petite

runtime-packer:portable-executable="rlpack-basic"

RLPack Basic

runtime-packer:portable-executable="smart-packer-pro"

Smart Packer Pro

runtime-packer:portable-executable="themida"

Themida

runtime-packer:portable-executable="upx"

UPX

runtime-packer:portable-executable="vmprotect"

VMProtect

runtime-packer:portable-executable="xcomp-xpack"

XComp/XPack

elf

cli-assembly

scrippsco2-fgc

scrippsco2-fgc namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Flags describing the sample

-3

Potentially Suspect Data Accepted

scrippsco2-fgc:-3

accepted-suspect

Potentially Suspect Data Accepted

-2

Accepted value from continuous analyzer replacing flask data

scrippsco2-fgc:-2

accepted-continuous-analyzer

Accepted value from continuous analyzer replacing flask data

-1

Acepted Value retained although individual measurements deviated by more than selected tolerance

scrippsco2-fgc:-1

accepted-deviated-tolerance

Acepted Value retained although individual measurements deviated by more than selected tolerance

0

Accepted Value

scrippsco2-fgc:0

accepted

Accepted Value

1

Rejected during analysis

scrippsco2-fgc:1

rejected-during-analysis

Rejected during analysis

2

Rejected unacceptably large flask-analyzer differences associated with night sampling (used only at MLO between Dec 1962 and Sep 1968)

scrippsco2-fgc:2

rejected-legacy-difference-night-mlo

Rejected unacceptably large flask-analyzer differences associated with night sampling (used only at

MLO between Dec 1962 and Sep 1968)

3

Rejected flask measurement; used continuous data instead

scrippsco2-fgc:3

rejected-continuous-data

Rejected flask measurement; used continuous data instead

4

Rejected Replicates do not agree to selected tolerance or single flask

scrippsco2-fgc:4

rejected-tolerance-single-flask

Rejected Replicates do not agree to selected tolerance or single flask

5

Rejected Daily average deviates from fit by more than 3 standard deviations

scrippsco2-fgc:5

rejected-derivation

Rejected Daily average deviates from fit by more than 3 standard deviations

6

Rejected to improve local distribution of data such as too many data of generally poor quality (used only at two stations: KUM Aug 1979 - Jun 1980 and LJO Apr 1979 - Sep 1985)

scrippsco2-fgc:6

rejected-legacy-poor-quality-kum-ljo

Rejected to improve local distribution of data such as too many data of generally poor quality (used only at two stations: KUM Aug 1979 - Jun 1980 and LJO Apr 1979 - Sep 1985)

7

Rejected Unsteady air at site (La Jolla only)

scrippsco2-fgc:7

rejected-unsteady-ljo

Rejected Unsteady air at site (La Jolla only)

8

Rejected manually (see input/flag_flasks.csv)

scrippsco2-fgc:8

rejected-manual

Rejected manually (see input/flag_flasks.csv)

scrippsco2-fgi

scrippsco2-fgi namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Flags describing the sample for isotopic data (C14, O18)

-3

Suspect but accepted isotopic measurement

scrippsco2-fgi:-3

accepted-suspect

Suspect but accepted isotopic measurement

0

Accepted isotopic measurement

scrippsco2-fgi:0

accepted

Accepted isotopic measurement

3

Rejected

scrippsco2-fgi:3

rejected

Rejected

5

Outlier from fit

scrippsco2-fgi:5

outlier

Outlier from fit

6

Other rejected, older data

scrippsco2-fgi:6

rejected-old-data

Other rejected, older data

8

Flask extracted but not analyzed yet

scrippsco2-fgi:8

extracted-not-analyzed

Flask extracted but not analyzed yet

9

Flask not extracted

scrippsco2-fgi:9

not-extracted

Flask not extracted

scrippsco2-sampling-stations

scrippsco2-sampling-stations namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Sampling stations of the Scripps CO2 Program

ALT

scrippsco2-sampling-stations:ALT

Alert, NWT, Canada

PTB

scrippsco2-sampling-stations:PTB

Point Barrow, Alaska

STP

scrippsco2-sampling-stations:STP

Station P

LJO

scrippsco2-sampling-stations:LJO

La Jolla Pier, California

BCS

scrippsco2-sampling-stations:BCS

Baja California Sur, Mexico

MLO

scrippsco2-sampling-stations:MLO

Mauna Loa Observatory, Hawaii

KUM

scrippsco2-sampling-stations:KUM

Cape Kumukahi, Hawaii

CHR

scrippsco2-sampling-stations:CHR

Christmas Island, Fanning Island

SAM

scrippsco2-sampling-stations:SAM

American Samoa

KER

scrippsco2-sampling-stations:KER

Kermadec Islands, Raoul Island

NZD

scrippsco2-sampling-stations:NZD

Baring Head, New Zealand

PSA

scrippsco2-sampling-stations:PSA

Palmer Station, Antarctica

SPO

scrippsco2-sampling-stations:SPO

South Pole

smart-airports-threats

smart-airports-threats namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Threat taxonomy in the scope of securing smart airports by ENISA. https://www.enisa.europa.eu/publications/securing-smart-airports

human-errors

smart-airports-threats:human-errors="configuration-errors"

Configuration errors

smart-airports-threats:human-errors="operator-or-user-error"

Operator/user error

smart-airports-threats:human-errors="loss-of-hardware"

Loss of hardware

smart-airports-threats:human-errors="non-compliance-with-policies-or-procedure"

Non compliance with policies or procedure

system-failures

smart-airports-threats:system-failures="failures-of-devices-or-systems"

Failures of devices or systems

smart-airports-threats:system-failures="failures-or-disruptions-of-communication-links"

Failures or disruptions of communication links (communication networks

smart-airports-threats:system-failures="failures-of-parts-of-devices"

Failures of parts of devices

smart-airports-threats:system-failures="failures-or-disruptions-of-main-supply"

Failures or disruptions of main supply

smart-airports-threats:system-failures="failures-or-disruptions-of-the-power-supply"

Failures or disruptions of the power supply

smart-airports-threats:system-failures="malfunctions-of-parts-of-devices"

Malfunctions of parts of devices

smart-airports-threats:system-failures="malfunctions-of-devices-or-systems"

Malfunctions of devices or systems

smart-airports-threats:system-failures="failures-of-hardware"

Failures of hardware

smart-airports-threats:system-failures="software-bugs"

Software bugs

natural-and-social-phenomena

smart-airports-threats:natural-and-social-phenomena="earthquakes"

Earthquakes

smart-airports-threats:natural-and-social-phenomena="fires"

Fires

smart-airports-threats:natural-and-social-phenomena="extreme-weather"

Extreme weather (e.g. flood, heavy snow, blizzard, high temperatures, fog, sandtorm)

smart-airports-threats:natural-and-social-phenomena="solar-flare"

Solar flare

smart-airports-threats:natural-and-social-phenomena="volcano-explosion"

Volcano explosion

smart-airports-threats:natural-and-social-phenomena="nuclear-incident"

Nuclear incident

smart-airports-threats:natural-and-social-phenomena="dangerous-chemical-incidents"

Dangerous chemical incidents

smart-airports-threats:natural-and-social-phenomena="pandemic"

Pandemic (e.g. Ebola)

smart-airports-threats:natural-and-social-phenomena="social-disruptions"

Social disruptions (e.g. industrial actions, civil unrest, strikes, military actions, terrorist attacks, political instability)

smart-airports-threats:natural-and-social-phenomena="shortage-of-fuel"

Shortage of fuel

smart-airports-threats:natural-and-social-phenomena="space-debris-and-meteorites"

Space debirs and meteorites

third-party-failures

smart-airports-threats:third-party-failures="internet-service-provider"

Internet service provider

smart-airports-threats:third-party-failures="cloud-service-provider"

Cloud service provider (SaaS / PaaS / IaaS / SecaaS)

smart-airports-threats:third-party-failures="utilities-power-or-gas-or-water"

Utilities (power / gas /water)

smart-airports-threats:third-party-failures="remote-maintenance-provider"

Remote maintenance provider

smart-airports-threats:third-party-failures="security-testing-companies"

Security testing companies (i.e. penetration testing/vulnerability assessment)

malicious-actions

smart-airports-threats:malicious-actions="denial-of-service-attacks-via-amplification-reflection"

Denial of Service attacks via amplifcation/reflection

smart-airports-threats:malicious-actions="denial-of-service-attacks-via-flooding"

Denial of Service via flooding

smart-airports-threats:malicious-actions="denial-of-service-attacks-via-jamming"

Denial of Service via jamming

smart-airports-threats:malicious-actions="malicious-software-on-it-assets-malware"

Malicious software on IT assets (including passenger and staff devices) which can be Worm, Trojan, Virus, Rootkit, Exploitkit…

smart-airports-threats:malicious-actions="malicious-software-on-it-assets-remote-arbitrary-code-execution"

Malicious software on IT assets such as remote arbitrary code execution (device under attacker control)

smart-airports-threats:malicious-actions="exploitation-of-software-vulnerabilities-implementation-flaws"

exploitation of known or unknown software vulnerabilities such as implementation flaws (flaw in code)

smart-airports-threats:malicious-actions="exploitation-of-software-vulnerabilities-design-flaws"

exploitation of known or unknown software vulnerabilities such as design flaws in IT assets (flaw in logic)

smart-airports-threats:malicious-actions="exploitation-of-software-vulnerabilities-apt"

exploitation of known or unknown software vulnerabilities such as Advanced Persistent Threats (APT)

smart-airports-threats:malicious-actions="misuse-of-authority-or-authorisation-unauthorized-use-of-software"

misuse of authority or authorisation - unauthorized use of software

smart-airports-threats:malicious-actions="misuse-of-authority-or-authorisation-unauthorized-installation-of-software"

misuse of authority or authorisation - unauthorized installation of software

smart-airports-threats:malicious-actions="misuse-of-authority-or-authorisation-repudiation-of-actions"

misuse of authority or authorisation - repudiation of actions

smart-airports-threats:malicious-actions="misuse-of-authority-or-authorisation-abuse-of-personal-data"

misuse of authority or authorisation - abuse of personal data or identity fraud

smart-airports-threats:malicious-actions="misuse-of-authority-or-authorisation-using-information-from-an-unreliable-source"

misuse of authority or authorisation - using information from an unreliable source

smart-airports-threats:malicious-actions="misuse-of-authority-or-authorisation-unintentional-change-of-data-in-an-information-system"

misuse of authority or authorisation - unintional change of data in an information system

smart-airports-threats:malicious-actions="misuse-of-authority-or-authorisation-inadequate-design-and-planning-or-lack-of-adoption"

misuse of authority or authorisation inadequate design and planning or lack of adoption

smart-airports-threats:malicious-actions="misuse-of-authority-or-authorisation-data-leakage-or-sharing"

misuse of authority data leakage or sharing (exfiltration, discarded, stolen media

smart-airports-threats:malicious-actions="network-or-interception-attacks-manipulation-of-routing-information"

network or interception attacks - manipulation of routing information (including redirection to malicious sites)

smart-airports-threats:malicious-actions="network-or-interception-attacks-spoofing"

network or interception attacks - spoofing

smart-airports-threats:malicious-actions="network-or-interception-attacks-unauthorized-access"

network or interception attacks - unauthorized access to network/services

smart-airports-threats:malicious-actions="network-or-interception-attacks-authentication-attacks"

network or interception attacks - authentication attacks (against insecure protocols or PKI)

smart-airports-threats:malicious-actions="network-or-interception-attacks-replay-attacks"

network or interception attacks - replay attacks

smart-airports-threats:malicious-actions="network-or-interception-attacks-repudiation-of-actions"

network or interception attacks - repudiation of actions

smart-airports-threats:malicious-actions="network-or-interception-attacks-wiretaps"

network or interception attacks - wiretaps (wired)

smart-airports-threats:malicious-actions="network-or-interception-attacks-wireless-comms"

network or interception attacks - wireless comms (eavesdropping, interception, jamming, electromagnetic interference)

smart-airports-threats:malicious-actions="network-or-interception-attacks-network-reconnaissance-information-gathering"

network or interception attacks - network reconnaissance/information gathering

smart-airports-threats:malicious-actions="social-attacks-phishing-spearphishing"

social attacks phishing or spearphishing

smart-airports-threats:malicious-actions="social-attacks-pretexting"

social attacks pretexting

smart-airports-threats:malicious-actions="social-attacks-untrusted-links"

social attacks untrusted links (fake websites/CSRF/XSS)

smart-airports-threats:malicious-actions="social-attacks-baiting"

social attacks baiting

smart-airports-threats:malicious-actions="social-attacks-reverse-social-engineering"

social attacks reverse social engineering

smart-airports-threats:malicious-actions="social-attacks-impersonation"

social attacks impersonation

smart-airports-threats:malicious-actions="tampering-with-devices-unauthorised-modification-of-data"

tampering with devices unauthorised modification of data (including compromising smart sensor data or threat image projection

smart-airports-threats:malicious-actions="tampering-with-devices-unauthorised-modification-of-hardware-or-software"

tampering with devices unauthorised modification of hardware or software (including tampering with kiosk devices, inserting keyloggers, or malware)

smart-airports-threats:malicious-actions="breach-of-physical-access-controls-bypass-authentication"

breach of physical access controls / administrative controls - bypass authentication

smart-airports-threats:malicious-actions="breach-of-physical-access-controls-privilege-escalation"

breach of physical access controls / administrative controls - privilege escalation

smart-airports-threats:malicious-actions="physical-attacks-on-airport-assets-vandalism"

Physical attacks on airport assets - vandalism

smart-airports-threats:malicious-actions="physical-attacks-on-airport-assets-sabotage"

Physical attacks on airport assets - sabotage

smart-airports-threats:malicious-actions="physical-attacks-on-airport-assets-explosive-or-bomb-threats"

Physical attacks on airport assets - explosive or bomb threats

smart-airports-threats:malicious-actions="physical-attacks-on-airport-assets-malicious-tampering"

Physical attacks on airport assets - malicious tampering or control of assets resulting in damage

state-responsibility

state-responsibility namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A spectrum of state responsibility to more directly tie the goals of attribution to the needs of policymakers.

state-prohibited.

The national government will help stop the third-party attack, which may originate from its territory or merely be transiting through its networks. This responsibility is the most passive on the scale: though the government is cooperating, it still has some small share of responsibility for the insecure systems involved in the attack. In reality, nations cannot ensure the proper behavior of the tens or hundreds of millions of computers in their borders at all times.

state-responsibility:state-prohibited.

State-prohibited.

The national government will help stop the third-party attack, which may originate from its territory or merely be transiting through its networks. This responsibility is the most passive on the scale: though the government is cooperating, it still has some small share of responsibility for the insecure systems involved in the attack. In reality, nations cannot ensure the proper behavior of the tens or hundreds of millions of computers in their borders at all times.

state-prohibited-but-inadequate.

The national government is cooperative and would stop the third-party attack but is unable to do so. The country might lack the proper laws, procedures, technical tools, or political will to use them. Though the nation could itself be a victim, it bears some passive responsibility for the attack, both for being unable to stop it and for having insecure systems in the first place.

state-responsibility:state-prohibited-but-inadequate.

State-prohibited-but-inadequate

The national government is cooperative and would stop the third-party attack but is unable to do so. The country might lack the proper laws, procedures, technical tools, or political will to use them. Though the nation could itself be a victim, it bears some passive responsibility for the attack, both for being unable to stop it and for having insecure systems in the first place.

state-ignored

The national government knows about the third-party attacks but, as a matter of policy, is unwilling to take any official action. A government may even agree with the goals and results of the attackers and tip them off to avoid being detected.

state-responsibility:state-ignored

State-ignored

The national government knows about the third-party attacks but, as a matter of policy, is unwilling to take any official action. A government may even agree with the goals and results of the attackers and tip them off to avoid being detected.

state-encouraged

Third parties control and conduct the attack, but the national government encourages them to continue as a matter of policy. This encouragement could include editorials in state-run press or leadership publicly agreeing with the goals of the attacks; members of government cyber offensive or intelligence organizations may be encouraged to undertake supportive recreational hacking while off duty. The nation is unlikely to be cooperative in any investigation and is likely to tip off the attackers

state-responsibility:state-encouraged

State-encouraged

Third parties control and conduct the attack, but the national government encourages them to continue as a matter of policy. This encouragement could include editorials in state-run press or leadership publicly agreeing with the goals of the attacks; members of government cyber offensive or intelligence organizations may be encouraged to undertake supportive recreational hacking while off duty. The nation is unlikely to be cooperative in any investigation and is likely to tip off

the attackers

state-shaped

Third parties control and conduct the attack, but the state provides some support, such as informal coordination between like-minded individuals in the government and the attacking group. To further their policy while retaining plausible deniability, the government may encourage members of their cyber forces to undertake 'recreational hacking' while off duty.

state-responsibility:state-shaped

State-shaped

Third parties control and conduct the attack, but the state provides some support, such as informal coordination between like-minded individuals in the government and the attacking group. To further their policy while retaining plausible deniability, the government may encourage members of their cyber forces to undertake 'recreational hacking' while off duty.

state-coordinated

The national government coordinates the third-party attackers—usually out of public view—by 'suggesting' targets, timing, or other operational details. The government may also provide technical or tactical assistance. Similar to state-shaped attacks, the government may encourage its cyber forces to engage in recreational hacking during off hours

state-responsibility:state-coordinated

State-coordinated

The national government coordinates the third-party attackers—usually out of public view—by 'suggesting' targets, timing, or other operational details. The government may also provide technical or tactical assistance. Similar to state-shaped attacks, the government may encourage its cyber forces to engage in recreational hacking during off hours

state-ordered

The national government, as a matter of policy, directs third-party proxies to conduct the attack on its behalf. This is as “state-sponsored” as an attack can be, without direct attack from government cyber forces. Any attackers that are under state control could be considered to be de facto agents of the state under international law.

state-responsibility:state-ordered

State-ordered

The national government, as a matter of policy, directs third-party proxies to conduct the attack on its behalf. This is as “state-sponsored” as an attack can be, without direct attack from government cyber forces. Any attackers that are under state control could be considered to be de facto agents of

the state under international law.

state-rogue-conducted

Elements of cyber forces of the national government conduct the attack. In this case, however, they carry out attacks without the knowledge, or approval, of the national leadership, which may act to stop the attacks should they learn of them. For example, local units or junior officers could be taking the initiative to counterattack out of the senior officers sight. More worrisome, this category could include sophisticated and persistent attacks from large bureaucracies conducting attacks that are at odds with the national leadership. Based on current precedence, a state could likely be held responsible by international courts for such rogue attacks.

state-responsibility:state-rogue-conducted

State-rogue-conducted.

Elements of cyber forces of the national government conduct the attack. In this case, however, they carry out attacks without the knowledge, or approval, of the national leadership, which may act to stop the attacks should they learn of them. For example, local units or junior officers could be taking the initiative to counterattack out of the senior officers sight. More worrisome, this category could include sophisticated and persistent attacks from large bureaucracies conducting attacks that are at odds with the national leadership. Based on current precedence, a state could likely be held responsible by international courts for such rogue attacks.

state-executed

The national government, as a matter of policy, directly controls and conducts the attack using its own cyber forces

state-responsibility:state-executed

State-executed

The national government, as a matter of policy, directly controls and conducts the attack using its own cyber forces

state-integrated

The national government integrates third-party attackers and government cyber forces, with common command and control. Orders and coordination may be formal or informal, but the government is in control of selecting targets, timing, and tempo. The attackers are de facto agents of the state

state-responsibility:state-integrated

State-integrated

The national government integrates third-party attackers and government cyber forces, with

common command and control. Orders and coordination may be formal or informal, but the government is in control of selecting targets, timing, and tempo. The attackers are de facto agents of the state

stealth_malware

stealth_malware namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Classification based on malware stealth techniques. Described in https://vxheaven.org/lib/pdf/Introducing%20Stealth%20Malware%20Taxonomy.pdf

type

stealth_malware:type="0"

No OS or system compromise. The malware runs as a normal user process using only official API calls.

stealth_malware:type="I"

The malware modifies constant sections of the kernel and/or processes such as code sections.

stealth_malware:type="II"

The malware does not modify constant sections but only the dynamic sections of the kernel and/or processes such as data sections.

stealth_malware:type="III"

The malware does not modify any sections of the kernel and/or processes but influences the system without modifying the OS. For example using hardware virtualization techniques.

stix-ttp

stix-ttp namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

TTPs are representations of the behavior or modus operandi of cyber adversaries.

victim-targeting

stix-ttp:victim-targeting="business-professional-sector"

Business & Professional Services Sector

stix-ttp:victim-targeting="retail-sector"

Retail Sector

stix-ttp:victim-targeting="financial-sector"

Financial Services Sector

stix-ttp:victim-targeting="media-entertainment-sector"

Media & Entertainment Sector

stix-ttp:victim-targeting="construction-engineering-sector"

Construction & Engineering Sector

stix-ttp:victim-targeting="government-international-organizations-sector"

Goverment & International Organizations

stix-ttp:victim-targeting="legal-sector"

Legal Services

stix-ttp:victim-targeting="hightech-it-sector"

High-Tech & IT Sector

stix-ttp:victim-targeting="healthcare-sector"

Healthcare Sector

stix-ttp:victim-targeting="transportation-sector"

Transportation Sector

stix-ttp:victim-targeting="aerospace-defence-sector"

Aerospace & Defense Sector

stix-ttp:victim-targeting="energy-sector"

Energy Sector

stix-ttp:victim-targeting="food-sector"

Food Sector

stix-ttp:victim-targeting="natural-resources-sector"

Natural Resources Sector

stix-ttp:victim-targeting="other-sector"

Other Sector

stix-ttp:victim-targeting="corporate-employee-information"

Corporate Employee Information

stix-ttp:victim-targeting="customer-pii"

Customer PII

stix-ttp:victim-targeting="email-lists-archives"

Email Lists/Archives

stix-ttp:victim-targeting="financial-data"

Financial Data

stix-ttp:victim-targeting="intellectual-property"

Intellectual Property

stix-ttp:victim-targeting="mobile-phone-contacts"

Mobile Phone Contacts

stix-ttp:victim-targeting="user-credentials"

User Credentials

stix-ttp:victim-targeting="authentification-cookies"

Authentication Cookies

targeted-threat-index

targeted-threat-index namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Targeted Threat Index is a metric for assigning an overall threat ranking score to email messages that deliver malware to a victim's computer. The TTI metric was first introduced at SecTor 2013 by Seth Hardy as part of the talk "RATastrophe: Monitoring a Malware Menagerie" along with Katie Kleemola and Greg Wiseman.

targeting-sophistication-base-value

The base value of the score ranges from 0 to 5, based on the sophistication of the email's social engineering techniques used to get the victim to open the attachment. This score considers the content and presentation of the message as well as the claimed sender identity. This determination also includes the content of any associated files; many times malware is injected into legitimate relevant documents.

targeted-threat-index:targeting-sophistication-base-value="not-targeted"

Not targeted, e.g. spam or financially motivated malware.

Associated numerical value="1"

targeted-threat-index:targeting-sophistication-base-value="targeted-but-not-customized"

Targeted but not customized. Sent with a message that is obviously false with little to no validation required.

Associated numerical value="25"

targeted-threat-index:targeting-sophistication-base-value="targeted-and-poorly-customized"

Targeted and poorly customized. Content is generally relevant to the target. May look questionable.

Associated numerical value="50"

targeted-threat-index:targeting-sophistication-base-value="targeted-and-customized"

Targeted and customized. May use a real person/organization or content to convince the target the message is legitimate. Content is specifically relevant to the target and looks legitimate.

Associated numerical value="65"

targeted-threat-index:targeting-sophistication-base-value="targeted-and-well-customized"

Targeted and well-customized. Uses a real person/organization and content to convince the target the message is legitimate. Probably directly addressing the recipient. Content is specifically relevant to the target, looks legitimate, and can be externally referenced (e.g. by a website). May be sent from a hacked account.

Associated numerical value="85"

targeted-threat-index:targeting-sophistication-base-value="targeted-and-highly-customized-using-sensitive-data"

Targeted and highly customized using sensitive data. Individually targeted and customized, likely using inside/sensitive information that is directly relevant to the target.

Associated numerical value="100"

technical-sophistication-multiplier

The technical sophistication score is a multiplier ranging from 1 to 2 based on how advanced the associated malware is, including malicious file attachments as well as links to malware hosted on another system. We use a multiplier because advanced malware requires significantly more effort and time (or money, in the case of commercial solutions) to custom-tune for a particular target.

targeted-threat-index:technical-sophistication-multiplier="the-sample-contains-no code-protection"

The sample contains no code protection such as packing, obfuscation (e.g. simple rotation of C2 names or other interesting strings), or anti-reversing tricks.

Associated numerical value="1"

targeted-threat-index:technical-sophistication-multiplier="the-sample-contains-a-simple-method-of-protection"

The sample contains a simple method of protection, such as one of the following: code protection using publicly available tools where the reverse method is available, such as UPX packing; simple anti-reversing techniques such as not using import tables, or a call to IsDebuggerPresent(); self-disabling in the presence of AV software.

Associated numerical value="25"

targeted-threat-index:technical-sophistication-multiplier="the-sample-contains-multiple-minor-code-protection-techniques"

The sample contains multiple minor code protection techniques (anti-reversing tricks, packing, VM / reversing tools detection) that require some low-level knowledge. This level includes malware

where code that contains the core functionality of the program is decrypted only in memory.

Associated numerical value="50"

targeted-threat-index:technical-sophistication-multiplier="the-sample-contains-minor-code-protection-techniques-plus-one-advanced"

The sample contains minor code protection techniques along with at least one advanced protection method such as rootkit functionality or a custom virtualized packer.

Associated numerical value="75"

targeted-threat-index:technical-sophistication-multiplier="the-sample-contains-multiple-advanced-protection-techniques"

The sample contains multiple advanced protection techniques, e.g. rootkit capability, virtualized packer, multiple anti-reversing techniques, and is clearly designed by a professional software engineering team.

Associated numerical value="100"

thales_group

thales_group namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Thales Group Taxonomy - was designed with the aim of enabling desired sharing and preventing unwanted sharing between Thales Group security communities.

distribution

Exclusive flag set which means the values or predicate below must be set exclusively.

thales_group:distribution="team_eyes_only"

Use it when you want to keep the Event on your Organization ONLY. Distribution: Your organisation only

This TAG will insure you that this Event will be kept on your side. This Event will NOT be shared to the Thales Group community. Distribution: Your organisation only

thales_group:distribution="limited_distribution"

Use it when you want to share to the Thales Group Community ONLY. Distribution: All communities

This TAG will insure you to share ONLY to the Thales Group Community. Distribution: All communities

Associated numerical value="1"

thales_group:distribution="external_alliances"

Use it when you want to share to the Thales Group External Alliances (MinArm, ACN, InterCERT-FR). Distribution: All communities

This TAG will insure you to share to the Thales Group External Alliances. Distribution: All communities

Associated numerical value="2"

thales_group:distribution="customers"

Use it when you want to share to the Thales Group Customers. Distribution: All communities

This TAG will insure you to share to the Thales Group Customers. Distribution: All communities

Associated numerical value="3"

to_block

This TAG will insure you that these Event Attributes will be blocked on the Thales DIS Proxy (More to come). Distribution: All communities

minarm

This TAG will insure you to share ONLY to the Thales Group MinArm alliance. Distribution: All communities

acn

This TAG will insure you to share ONLY to the Thales Group ACN alliance. Distribution: All communities

sigpart

This TAG will insure you to share ONLY to the Thales Group Sigpart alliance. Distribution: All communities

ioc_confidence

Distribution: All communities

Exclusive flag set which means the values or predicate below must be set exclusively.

thales_group:ioc_confidence="high"

High

Associated numerical value="8"

thales_group:ioc_confidence="medium"

Medium

Associated numerical value="9"

thales_group:ioc_confidence="low"

Low

Associated numerical value="10"

tlp:black

Distribution: Restricted Sharing Group

Watcher

Distribution: All communities

threatmatch

threatmatch namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The ThreatMatch Sectors, Incident types, Malware types and Alert types are applicable for any ThreatMatch instances and should be used for all CIISI and TIBER Projects.

sector

threatmatch:sector="Banking & Capital Markets"

Banking & capital markets

threatmatch:sector="Financial Services"

Financial Services

threatmatch:sector="Insurance"

Insurance

threatmatch:sector="Pension"

Pension

threatmatch:sector="Government & Public Service"

Government & Public Service

threatmatch:sector="Diplomatic Services"

Diplomatic Services

threatmatch:sector="Energy, Utilities & Mining"

Energy, Utilities & Mining

threatmatch:sector="Telecommunications"

Telecommunications

threatmatch:sector="Technology"

Technology

threatmatch:sector="Academic/Research Institutes"

Academic/Research Institutes

threatmatch:sector="Aerospace, Defence & Security"

Aerospace, Defence & Security

threatmatch:sector="Agriculture"

Agriculture

threatmatch:sector="Asset & Wealth Management"

Asset & Wealth Management

threatmatch:sector="Automotive"

Automotive

threatmatch:sector="Business and Professional Services"

Business and Professional Services

threatmatch:sector="Capital Projects & Infrastructure"

Capital Projects & Infrastructure

threatmatch:sector="Charity/Not-for-Profit"

Charity/Not-for-Profit

threatmatch:sector="Chemicals"

Chemicals

threatmatch:sector="Commercial Aviation"

Commercial Aviation

threatmatch:sector="Commodities"

Commodities

threatmatch:sector="Education"

Education

threatmatch:sector="Engineering & Construction"

Engineering & Construction

threatmatch:sector="Entertainment & Media"

Entertainment & Media

threatmatch:sector="Forest, Paper & Packaging"

Forest, Paper & Packaging

threatmatch:sector="Healthcare"

Healthcare

threatmatch:sector="Hospitality & Leisure"

Hospitality & Leisure

threatmatch:sector="Industrial Manufacturing"

Industrial Manufacturing

threatmatch:sector="IT Industry"

IT Industry

threatmatch:sector="Legal"

Legal

threatmatch:sector="Metals"

Metals

threatmatch:sector="Pharmaceuticals & Life Sciences"

Pharmaceuticals & Life Sciences

threatmatch:sector="Private Equity"

Private Equity

threatmatch:sector="Retail & Consumer"

Retail & Consumer

threatmatch:sector="Semiconductors"

Semiconductors

threatmatch:sector="Sovereign Investment Funds"

Sovereign Investment Funds

threatmatch:sector="Transport & Logistics"

Transport & Logistics

incident-type

threatmatch:incident-type="ATM Attacks"

ATM Attacks

threatmatch:incident-type="ATM Breach"

ATM Breach

threatmatch:incident-type="Attempted Exploitation"

Attempted Exploitation

threatmatch:incident-type="Botnet Activity"

Botnet Activity

threatmatch:incident-type="Business Email Compromise"

Business Email Compromise

threatmatch:incident-type="Crypto Mining"

Crypto Mining

threatmatch:incident-type="Data Breach/Compromise"

Data Breach/Compromise

threatmatch:incident-type="Data Dump"

Data Dump

threatmatch:incident-type="Data Leakage"

Data Leakage

threatmatch:incident-type="DDoS"

DDoS

threatmatch:incident-type="Defacement Activity"

Defacement Activity

threatmatch:incident-type="Denial of Service (DoS)"

Denial of Service (DoS)

threatmatch:incident-type="Disruption Activity"

Disruption Activity

threatmatch:incident-type="Espionage"

Espionage

threatmatch:incident-type="Espionage Activity"

Espionage Activity

threatmatch:incident-type="Exec Targeting "

Exec Targeting

threatmatch:incident-type="Exposure of Data"

Exposure of Data

threatmatch:incident-type="Extortion Activity"

Extortion Activity

threatmatch:incident-type="Fraud Activity"

Fraud Activity

threatmatch:incident-type="General Notification"

General Notification

threatmatch:incident-type="Hacktivism Activity"

Hacktivism Activity

threatmatch:incident-type="Malicious Insider"

Malicious Insider

threatmatch:incident-type="Malware Infection"

Malware Infection

threatmatch:incident-type="Man in the Middle Attacks"

Man in the Middle Attacks

threatmatch:incident-type="MFA Attack"

MFA Attack

threatmatch:incident-type="Mobile Malware"

Mobile Malware

threatmatch:incident-type="Phishing Activity"

Phishing Activity

threatmatch:incident-type="Ransomware Activity"

Ransomware Activity

threatmatch:incident-type="Social Engineering Activity"

Social Engineering Activity

threatmatch:incident-type="Social Media Compromise"

Social Media Compromise

threatmatch:incident-type="Spear-phishing Activity"

Spear-phishing Activity

threatmatch:incident-type="Spyware"

Spyware

threatmatch:incident-type="SQL Injection Activity"

SQL Injection Activity

threatmatch:incident-type="Supply Chain Compromise"

Supply Chain Compromise

threatmatch:incident-type="Trojanised Software"

Trojanised Software

threatmatch:incident-type="Vishing"

Vishing

threatmatch:incident-type="Website Attack (Other)"

Website Attack (Other)

threatmatch:incident-type="Unknown"

Unknown

malware-type

threatmatch:malware-type="Adware"

Adware

threatmatch:malware-type="Backdoor"

Backdoor

threatmatch:malware-type="Banking Trojan"

Banking Trojan

threatmatch:malware-type="Botnet"

Botnet

threatmatch:malware-type="Destructive"

Destructive

threatmatch:malware-type="Downloader"

Downloader

threatmatch:malware-type="Exploit Kit"

Exploit Kit

threatmatch:malware-type="Fileless Malware"

Fileless Malware

threatmatch:malware-type="Keylogger"

Keylogger

threatmatch:malware-type="Legitimate Tool"

Legitimate Tool

threatmatch:malware-type="Mobile Application"

Mobile Application

threatmatch:malware-type="Mobile Malware"

Mobile Malware

threatmatch:malware-type="Point-of-Sale (PoS)"

Point-of-Sale (PoS)

threatmatch:malware-type="Remote Access Trojan"

Remote Access Trojan

threatmatch:malware-type="Rootkit"

Rootkit

threatmatch:malware-type="Skimmer"

Skimmer

threatmatch:malware-type="Spyware"

Spyware

threatmatch:malware-type="Surveillance Tool"

Surveillance Tool

threatmatch:malware-type="Trojan"

Trojan

threatmatch:malware-type="Virus"

Virus

threatmatch:malware-type="Worm"

Worm

threatmatch:malware-type="Zero-day"

Zero-day

threatmatch:malware-type="Unknown"

Unknown

alert-type

threatmatch:alert-type="Actor Campaigns"

Actor Campaigns

threatmatch:alert-type="Credential Breaches"

Credential Breaches

threatmatch:alert-type="DDoS"

DDoS

threatmatch:alert-type="Exploit Alert"

Exploit Alert

threatmatch:alert-type="General Notification"

General Notification

threatmatch:alert-type="High Impact Vulnerabilities"

High Impact Vulnerabilities

threatmatch:alert-type="Information Leakages"

Information Leakages

threatmatch:alert-type="Malware Analysis"

Malware Analysis

threatmatch:alert-type="Nefarious Domains"

Nefarious Domains

threatmatch:alert-type="Nefarious Forum Mention"

Nefarious Forum Mention

threatmatch:alert-type="Pastebin Dumps"

Pastebin Dumps

threatmatch:alert-type="Phishing Attempts"

Phishing Attempts

threatmatch:alert-type="PII Exposure"

PII Exposure

threatmatch:alert-type="Sensitive Information Disclosures"

Sensitive Information Disclosures

threatmatch:alert-type="Social Media Alerts"

Social Media Alerts

threatmatch:alert-type="Supply Chain Event"

Supply Chain Event

threatmatch:alert-type="Technical Exposure"

Technical Exposure

threatmatch:alert-type="Threat Actor Updates"

Threat Actor Updates

threatmatch:alert-type="Trigger Events"

Trigger Events

threats-to-dns

threats-to-dns namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

An overview of some of the known attacks related to DNS as described by Torabi, S., Boukhtouta, A., Assi, C., & Debbabi, M. (2018) in Detecting Internet Abuse by Analyzing Passive DNS Traffic: A

Survey of Implemented Systems. IEEE Communications Surveys & Tutorials, 1–1. doi:10.1109/comst.2018.2849614

dns-protocol-attacks

DNS protocol attacks

threats-to-dns:dns-protocol-attacks="man-in-the-middle-attack"

Man-in-the-middle attack

Man-in-the-middle attack

threats-to-dns:dns-protocol-attacks="dns-spoofing"

DNS spoofing

DNS spoofing

threats-to-dns:dns-protocol-attacks="dns-rebinding"

DNS rebinding

DNS rebinding

dns-server-attacks

DNS server attacks

threats-to-dns:dns-server-attacks="server-dos-and-ddos"

Server DoS & DDoS

Server DoS & DDoS

threats-to-dns:dns-server-attacks="server-hijacking"

Server hijacking

Server hijacking

threats-to-dns:dns-server-attacks="cache-poisoning"

Cache poisoning

Cache poisoning

dns-abuse-or-misuse

DNS abuse/misuse

threats-to-dns:dns-abuse-or-misuse="domain-name-registration-abuse-cybersquatting"

Domain name registration abuse such as cybersquatting

Domain name registration abuse such as cybersquatting

threats-to-dns:dns-abuse-or-misuse="domain-name-registration-abuse-typosquatting"

Domain name registration abuse such as typosquatting

Domain name registration abuse such as typosquatting

threats-to-dns:dns-abuse-or-misuse="domain-name-registration-abuse-domain-reputation-and-re-registration"

Domain name registration abuse as domain reputation and re-registration

Domain name registration abuse as domain reputation and re-gistration

threats-to-dns:dns-abuse-or-misuse="dns-reflection-dns-amplification"

DNS reflection - DNS amplification

DNS reflection - DNS amplification

threats-to-dns:dns-abuse-or-misuse="malicious-or-compromised-domains-ips-malicious-botnets-c2"

Malicious or compromised domains/IPs - Malicious botnets (C&C servers)

Malicious or compromised domains/IPs - Malicious botnets (C&C servers)

threats-to-dns:dns-abuse-or-misuse="malicious-or-compromised-domains-ips-fast-flux-domains"

Malicious or compromised domains/IPs - Malicious fast-flux domain & networks

Malicious or compromised domains/IPs - Malicious fast-flux domain & networks

threats-to-dns:dns-abuse-or-misuse="malicious-or-compromised-domains-ips-malicious-dgas"

Malicious or compromised domains/IPs - Malicious DGAs

Malicious or compromised domains/IPs - Malicious DGAs

threats-to-dns:dns-abuse-or-misuse="covert-channels-malicious-dns-tunneling"

Covert channels - Malicious DNS tunneling

Covert channels - Malicious DNS tunneling

threats-to-dns:dns-abuse-or-misuse="covert-channels-malicious-payload-distribution"

Covert channels - Malicious DNS tunneling

Covert channels - Malicious DNS tunneling

threats-to-dns:dns-abuse-or-misuse="benign-services-applications-malicious-dns-resolvers"

Benign services and applications - Malicious DNS resolvers

Benign services and applications - Malicious DNS resolvers

threats-to-dns:dns-abuse-or-misuse="benign-services-applications-malicious-scanners"

Benign services and applications - Malicious scanners

Benign services and applications - Malicious scanners

threats-to-dns:dns-abuse-or-misuse="benign-services-applications-url-shorteners"

Benign services and applications - URL shorteners

Benign services and applications - URL shorteners

tlp

tlp namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.

Exclusive flag set which means the values or predicate below must be set exclusively.

red

Not for disclosure, restricted to participants only. Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

tlp:red

(TLP:RED) Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not legitimate.

Not for disclosure, restricted to participants only. Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

amber

Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

tlp:amber

(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.

Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

green

Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner

organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

tlp:green

(TLP:GREEN) Information given to a community or a group of organizations at large. The information cannot be publicly released.

Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

white

Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

tlp:white

(TLP:WHITE) Information can be shared publicly in accordance with the law.

Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

ex:chr

tlp:ex:chr

(TLP:EX:CHR) Information extended with a specific tag called Chatham House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. This additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag.

tor

tor namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Taxonomy to describe Tor network infrastructure

tor-relay-type

tor:tor-relay-type="entry-guard-relay"

Entry node to the Tor network

tor:tor-relay-type="middle-relay"

Tor node relaying traffic between an entry-guard-relay to an exit-relay

tor:tor-relay-type="exit-relay"

Tor node relaying traffic outside of the Tor network to the original destination

tor:tor-relay-type="bridge-relay"

Entry node to the Tor network - partially unpublished

trust

trust namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Indicator of Trust provides insight about data on what can be trusted and known as a good actor. Similar to a whitelist but on steroids, reusing features one would use with Indicators of Compromise, but to filter out what is known to be good.

Exclusive flag set which means the values or predicate below must be set exclusively.

trust

trust:trust="unknown"

Unknown Confidence State

trust:trust="none"

Cannot Trust, no confidence

trust:trust="partial"

Low confidence

trust:trust="relationship"

Inherited Full Trust by a third party that we trust

trust:trust="full"

We fully trust it

frequency

trust:frequency="hourly"

This attribute is likely to happen at an hourly interval

trust:frequency="daily"

This attribute is likely to happen at a daily interval

trust:frequency="weekly"

This attribute is likely to happen at a weekly interval

trust:frequency="monthly"

This attribute is likely to happen at a monthly interval

trust:frequency="yearly"

Thie attribute is likely to happen at a yearly interval

valid

trust:valid="true"

This Trust is valid

trust:valid="false"

This trust is invalid. Such as a MD5 Hash etc.

type

type namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Taxonomy to describe different types of intelligence gathering discipline which can be described the origin of intelligence.

OSINT

gathered from open sources

type:OSINT

Open Source Intelligence

gathered from open sources

SIGINT

gathered from interception of signals

type:SIGINT

Signal Intelligence

gathered from interception of signals

TECHINT

gathered from analysis of weapons and equipment used by the armed forces of foreign nations, or environmental conditions

type:TECHINT

Technical Intelligence

gathered from analysis of weapons and equipment used by the armed forces of foreign nations, or environmental conditions

CYBINT

gathered from active or passive exploitation (CNE) in the cyberspace

type:CYBINT

Cyberspace Intelligence

gathered from active or passive exploitation (CNE) in the cyberspace

DNINT

gathered from active or passive expoilation (CNE) in the digital network.

type:DNINT

Digital Network Intelligence

gathered from active or passive expoilation (CNE) in the digital network.

HUMINT

gathered from a person in the location in question

type:HUMINT

Human Intelligence

gathered from a person in the location in question

MEDINT

gathered from analysis of medical records and/or actual physiological examinations to determine health and/or particular ailments/allergetic conditions for consideration

type:MEDINT

Medical Intelligence

gathered from analysis of medical records and/or actual physiological examinations to determine health and/or particular ailments/allergetic conditions for consideration

GEOINT

gathered from satellite, aerial photography, mapping/terrain data

type:GEOINT

Geospatial Intelligence

gathered from satellite, aerial photography, mapping/terrain data

IMINT

gathered from satellite and aerial photography

type:IMINT

Imagery Intelligence

gathered from satellite and aerial photography

MASINT

gathered from electro-optical, nuclear survey, geophysical measurements, radar, materials analysis

type:MASINT

Measurement and signature intelligence

gathered from electro-optical, nuclear survey, geophysical measurements, radar, materials analysis

FININT

gathered from analysis of monetary or financial transactions

type:FININT

Financial Intelligence

gathered from analysis of monetary or financial transactions

unified-kill-chain

unified-kill-chain namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Unified Kill Chain is a refinement to the Kill Chain.

Initial Foothold

unified-kill-chain:Initial Foothold="reconnaissance"

Reconnaissance

unified-kill-chain:Initial Foothold="weaponization"

Weaponization

unified-kill-chain:Initial Foothold="delivery"

Delivery

unified-kill-chain:Initial Foothold="social-engineering"

Social Engineering

unified-kill-chain:Initial Foothold="exploitation"

Exploitation

unified-kill-chain:Initial Foothold="persistence"

Persistence

unified-kill-chain:Initial Foothold="defense-evasion"

Defense Evasion

unified-kill-chain:Initial Foothold="command-control"

Command & Control

Network Propagation

unified-kill-chain:Network Propagation="pivoting"

Pivoting

unified-kill-chain:Network Propagation="discovery"

Discovery

unified-kill-chain:Network Propagation="privilege-escalation"

Privilege Escalation

unified-kill-chain:Network Propagation="execution"

Execution

unified-kill-chain:Network Propagation="credential-access"

Credential Access

unified-kill-chain:Network Propagation="lateral-movement"

Lateral Movement

Action on Objectives

unified-kill-chain:Action on Objectives="access"

Access

unified-kill-chain:Action on Objectives="collection"

Collection

unified-kill-chain:Action on Objectives="exfiltration"

Exfiltration

unified-kill-chain:Action on Objectives="impact"

Impact

unified-kill-chain:Action on Objectives="objectives"

Objectives

use-case-applicability

use-case-applicability namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Use Case Applicability categories reflect standard resolution categories, to clearly display alerting rule configuration problems.

announced-administrative/user-action

The process to communicate administrative activities or special user actions was in place and working correctly. Internal sensors are working and detecting privileged or irregular administrative behaviour.

use-case-applicability:announced-administrative/user-action

Announced administrative/user action

The process to communicate administrative activities or special user actions was in place and working correctly. Internal sensors are working and detecting privileged or irregular administrative behaviour.

unannounced-administrative/user-action

Internal sensors have detected privileged or user activity, which was not previously communicated. This category also includes improper usage.

use-case-applicability:unannounced-administrative/user-action

Unannounced administrative/user action

Internal sensors have detected privileged or user activity, which was not previously communicated. This category also includes improper usage.

log-management-rule-configuration-error

This category reflects false alerts that were raised due to configuration errors in the central log management system, often a SIEM, rule.

use-case-applicability:log-management-rule-configuration-error

Log management rule configuration error

This category reflects false alerts that were raised due to configuration errors in the central log management system, often a SIEM, rule.

detection-device/rule-configuration-error

This category reflects rules on detection devices, which are usually passive or active components of network security.

use-case-applicability:detection-device/rule-configuration-error

Detection device/rule configuration error

This category reflects rules on detection devices, which are usually passive or active components of network security.

bad-IOC/rule-pattern-value

Products often require external indicator information or security feeds to be applied on active or passive infrastructure components to create alerts.

use-case-applicability:bad-IOC/rule-pattern-value

Bad IOC/rule pattern value

Products often require external indicator information or security feeds to be applied on active or passive infrastructure components to create alerts.

test-alert

This alert reflects alerts created for testing purposes.

use-case-applicability:test-alert

Test alert

This alert reflects alerts created for testing purposes.

confirmed-attack-with-IR-actions

This alert represents the classic true positives, where all security controls in place were circumvented, a security control was lacking or a misconfiguration of a security element occurred.

use-case-applicability:confirmed-attack-with-IR-actions

Confirmed Attack with IR actions

This alert represents the classic true positives, where all security controls in place were circumvented, a security control was lacking or a misconfiguration of a security element occurred.

confirmed-attack-attempt-without-IR-actions

This category reflects an attempt by a threat actor, which in the end could be prevented by in place security measures but passed security controls associated with the delivery phase of the Cyber Kill Chain.

use-case-applicability:confirmed-attack-attempt-without-IR-actions

Confirmed Attack attempt without IR actions

This category reflects an attempt by a threat actor, which in the end could be prevented by in place security measures but passed security controls associated with the delivery phase of the Cyber Kill Chain.

veris

veris namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Vocabulary for Event Recording and Incident Sharing (VERIS)

confidence

veris:confidence="High"

High confidence

veris:confidence="Low"

Low confidence

veris:confidence="Medium"

Medium confidence

veris:confidence="None"

No confidence

cost_corrective_action

veris:cost_corrective_action="Difficult and expensive"

Difficult and expensive

veris:cost_corrective_action="Simple and cheap"

Simple and cheap

veris:cost_corrective_action="Something in-between"

Something in-between

veris:cost_corrective_action="Unknown"

Unknown

discovery_method

veris:discovery_method="Ext - actor disclosure"

External - disclosed by threat agent (e.g., public brag, private blackmail)

veris:discovery_method="Ext - audit"

External - security audit or scan

veris:discovery_method="Ext - customer"

External - reported by customer or partner affected by the incident

veris:discovery_method="Ext - emergency response team"

External - Emergency response team

veris:discovery_method="Ext - found documents"

External - Found documents

veris:discovery_method="Ext - fraud detection"

External - fraud detection (e.g., CPP)

veris:discovery_method="Ext - incident response"

External - Notified while investigating another incident

veris:discovery_method="Ext - law enforcement"

Internal - notified by law enforcement or government agency

veris:discovery_method="Ext - monitoring service"

External - managed security event monitoring service

veris:discovery_method="Ext - other"

Discovery method was external and known but not listed

veris:discovery_method="Ext - suspicious traffic"

External - Report of suspicious traffic

veris:discovery_method="Ext - unknown"

External - unknown

veris:discovery_method="Ext - unrelated 3rd party"

Discovered by person unaffiliated with victim or threat actor

veris:discovery_method="Int - HIDS"

Internal - host IDS or file integrity monitoring

veris:discovery_method="Int - IT review"

Any routine maintenance, testing or review of it assets. (Includes inspect of assets, vulnerability scans, etc.)

veris:discovery_method="Int - NIDS"

Internal - All network-based security tool detection (including IPS, IDS, firewalls and other network-based security tools)

veris:discovery_method="Int - antivirus"

Internal - antivirus alert

veris:discovery_method="Int - break in discovered"

Internal - employee discovered evidence of a break in

veris:discovery_method="Int - data loss prevention"

Internal - Data loss prevention software

veris:discovery_method="Int - financial audit"

Internal - financial audit and reconciliation process

veris:discovery_method="Int - fraud detection"

Internal - fraud detection mechanism

veris:discovery_method="Int - incident response"

Internal - discovered while responding to another (separate) incident

veris:discovery_method="Int - infrastructure monitoring"

Internal - Health and welfare monitoring of assets such as utilization, uptime, and SNMP alerts

veris:discovery_method="Int - log review"

Internal - log review process or SIEM

veris:discovery_method="Int - other"

Discovery method was internal and known but not listed

veris:discovery_method="Int - reported by employee"

Internal - reported by employee who saw something odd

veris:discovery_method="Int - security alarm"

Internal - physical security system alarm

veris:discovery_method="Int - unknown"

Internal - unknown

veris:discovery_method="Other"

Other

veris:discovery_method="Prt - antivirus"

Partner - Notified by antivirus company but not through AV product

veris:discovery_method="Prt - audit"

Partner - Audit performed by a partner organization

veris:discovery_method="Prt - incident response"

Partner - notified while investigating another incident

veris:discovery_method="Prt - monitoring service"

Partner - Reported by a monitoring service

veris:discovery_method="Prt - other"

Discovery method was partner and known but not listed

veris:discovery_method="Prt - unknown"

Partner - Unknown

veris:discovery_method="Unknown"

Unknown

security_incident

veris:security_incident="Confirmed"

Yes - Confirmed

veris:security_incident="False positive"

False positive (response triggered, but no incident)

veris:security_incident="Near miss"

Near miss (actions did not compromise asset)

veris:security_incident="Suspected"

Suspected

targeted

veris:targeted="NA"

Not applicable

veris:targeted="Opportunistic"

Opportunistic: victim attacked because they exhibited a weakness the actor knew how to exploit

veris:targeted="Targeted"

Targeted: victim chosen as target then actor determined what weaknesses could be exploited

veris:targeted="Unknown"

Unknown

asset:accessibility

veris:asset:accessibility="External"

Publicly accessible

veris:asset:accessibility="Internal"

Internally accessible

veris:asset:accessibility="Isolated"

Internally isolated or restricted environment

veris:asset:accessibility="NA"

Not applicable

veris:asset:accessibility="Other"

Accessibility known but not listed

veris:asset:accessibility="Unknown"

Unknown

asset:cloud

veris:asset:cloud="Customer attack"

Penetration of another web site on shared device

veris:asset:cloud="Hosting error"

Misconfiguration or error by hosting provider

veris:asset:cloud="Hosting governance"

Lack of security process or procedure by hosting provider

veris:asset:cloud="Hypervisor"

Hypervisor break-out attack

veris:asset:cloud="NA"

It is known no cloud assets were involved

veris:asset:cloud="No"

It is known that a cloud asset was involved and it being a cloud asset did not affect the outcome

veris:asset:cloud="Other"

Cloud hosting known but not listed

veris:asset:cloud="Partner application"

Application vulnerability in partner-developed application

veris:asset:cloud="Unknown"

The involvement of cloud assets was not measured

veris:asset:cloud="User breakout"

Elevation of privilege by another customer in shared environment

asset:country

veris:asset:country="AD"

Andorra

veris:asset:country="AE"

United Arab Emirates

veris:asset:country="AF"

Afghanistan

veris:asset:country="AG"

Antigua and Barbuda

veris:asset:country="AI"

Anguilla

veris:asset:country="AL"

Albania

veris:asset:country="AM"

Armenia

veris:asset:country="AO"

Angola

veris:asset:country="AQ"

Antarctica

veris:asset:country="AR"

Argentina

veris:asset:country="AS"

American Samoa

veris:asset:country="AT"

Austria

veris:asset:country="AU"

Australia

veris:asset:country="AW"

Aruba

veris:asset:country="AX"

Aland Islands

veris:asset:country="AZ"

Azerbaijan

veris:asset:country="BA"

Bosnia and Herzegovina

veris:asset:country="BB"

Barbados

veris:asset:country="BD"

Bangladesh

veris:asset:country="BE"

Belgium

veris:asset:country="BF"

Burkina Faso

veris:asset:country="BG"

Bulgaria

veris:asset:country="BH"

Bahrain

veris:asset:country="BI"

Burundi

veris:asset:country="BJ"

Benin

veris:asset:country="BL"

Saint-Barthelemy

veris:asset:country="BM"

Bermuda

veris:asset:country="BN"

Brunei Darussalam

veris:asset:country="BO"

Bolivia

veris:asset:country="BQ"

Bonaire, Saint Eustatius and Saba

veris:asset:country="BR"

Brazil

veris:asset:country="BS"

Bahamas

veris:asset:country="BT"

Bhutan

veris:asset:country="BV"

Bouvet Island

veris:asset:country="BW"

Botswana

veris:asset:country="BY"

Belarus

veris:asset:country="BZ"

Belize

veris:asset:country="CA"

Canada

veris:asset:country="CC"

Cocos (Keeling) Islands

veris:asset:country="CD"

Congo, Democratic Republic of the

veris:asset:country="CF"

Central African Republic

veris:asset:country="CG"

Congo

veris:asset:country="CH"

Switzerland

veris:asset:country="CI"

Cote d’Ivoire

veris:asset:country="CK"

Cook Islands

veris:asset:country="CL"

Chile

veris:asset:country="CM"

Cameroon

veris:asset:country="CN"

China

veris:asset:country="CO"

Colombia

veris:asset:country="CR"

Costa Rica

veris:asset:country="CU"

Cuba

veris:asset:country="CV"

Cape Verde

veris:asset:country="CW"

Curacao

veris:asset:country="CX"

Christmas Island

veris:asset:country="CY"

Cyprus

veris:asset:country="CZ"

Czech Republic

veris:asset:country="DE"

Germany

veris:asset:country="DJ"

Djibouti

veris:asset:country="DK"

Denmark

veris:asset:country="DM"

Dominica

veris:asset:country="DO"

Dominican Republic

veris:asset:country="DZ"

Algeria

veris:asset:country="EC"

Ecuador

veris:asset:country="EE"

Estonia

veris:asset:country="EG"

Egypt

veris:asset:country="EH"

Western Sahara

veris:asset:country="ER"

Eritrea

veris:asset:country="ES"

Spain

veris:asset:country="ET"

Ethiopia

veris:asset:country="FI"

Finland

veris:asset:country="FJ"

Fiji

veris:asset:country="FK"

Faeroe Islands

veris:asset:country="FM"

Micronesia (Federated States of)

veris:asset:country="FO"

Falkland Islands (Malvinas)

veris:asset:country="FR"

France

veris:asset:country="GA"

Gabon

veris:asset:country="GB"

United Kingdom

veris:asset:country="GD"

Grenada

veris:asset:country="GE"

Georgia

veris:asset:country="GF"

French Guiana

veris:asset:country="GG"

Guernsey

veris:asset:country="GH"

Ghana

veris:asset:country="GI"

Gibraltar

veris:asset:country="GL"

Greenland

veris:asset:country="GM"

Gambia

veris:asset:country="GN"

Guinea

veris:asset:country="GP"

Guadeloupe

veris:asset:country="GQ"

Equatorial Guinea

veris:asset:country="GR"

Greece

veris:asset:country="GS"

South Georgia and the South Sandwich Islands

veris:asset:country="GT"

Guatemala

veris:asset:country="GU"

Guam

veris:asset:country="GW"

Guinea-Bissau

veris:asset:country="GY"

Guyana

veris:asset:country="HK"

Hong Kong

veris:asset:country="HM"

Heard Island and McDonal Islands

veris:asset:country="HN"

Honduras

veris:asset:country="HR"

Croatia

veris:asset:country="HT"

Haiti

veris:asset:country="HU"

Hungary

veris:asset:country="ID"

Indonesia

veris:asset:country="IE"

Ireland

veris:asset:country="IL"

Israel

veris:asset:country="IM"

Isle of Man

veris:asset:country="IN"

India

veris:asset:country="IO"

British Virgin Islands

veris:asset:country="IQ"

Iraq

veris:asset:country="IR"

Iran (Islamic Republic of)

veris:asset:country="IS"

Iceland

veris:asset:country="IT"

Italy

veris:asset:country="JE"

Jersey

veris:asset:country="JM"

Jamaica

veris:asset:country="JO"

Jordan

veris:asset:country="JP"

Japan

veris:asset:country="KE"

Kenya

veris:asset:country="KG"

Kyrgyzstan

veris:asset:country="KH"

Cambodia

veris:asset:country="KI"

Kiribati

veris:asset:country="KM"

Comoros

veris:asset:country="KN"

Saint Kitts and Nevis

veris:asset:country="KP"

Korea, Democratic People’s Republic of

veris:asset:country="KR"

Korea, Republic of

veris:asset:country="KW"

Kuwait

veris:asset:country="KY"

Cayman Islands

veris:asset:country="KZ"

Kazakhstan

veris:asset:country="LA"

Lao People’s Democratic Republic

veris:asset:country="LB"

Lebanon

veris:asset:country="LC"

Saint Lucia

veris:asset:country="LI"

Liechtenstein

veris:asset:country="LK"

Sri Lanka

veris:asset:country="LR"

Liberia

veris:asset:country="LS"

Lesotho

veris:asset:country="LT"

Lithuania

veris:asset:country="LU"

Luxembourg

veris:asset:country="LV"

Latvia

veris:asset:country="LY"

Libya

veris:asset:country="MA"

Morocco

veris:asset:country="MC"

Monaco

veris:asset:country="MD"

Moldova, Republic of

veris:asset:country="ME"

Montenegro

veris:asset:country="MF"

Saint Martin (French part)

veris:asset:country="MG"

Madagascar

veris:asset:country="MH"

Marshall Islands

veris:asset:country="MK"

Macedonia, The former Yugoslav Republic of

veris:asset:country="ML"

Mali

veris:asset:country="MM"

Myanmar

veris:asset:country="MN"

Mongolia

veris:asset:country="MO"

Macao

veris:asset:country="MP"

Northern Mariana Islands

veris:asset:country="MQ"

Martinique

veris:asset:country="MR"

Mauritania

veris:asset:country="MS"

Montserrat

veris:asset:country="MT"

Malta

veris:asset:country="MU"

Mauritius

veris:asset:country="MV"

Maldives

veris:asset:country="MW"

Malawi

veris:asset:country="MX"

Mexico

veris:asset:country="MY"

Malaysia

veris:asset:country="MZ"

Mozambique

veris:asset:country="NA"

Namibia

veris:asset:country="NC"

New Caledonia

veris:asset:country="NE"

Niger

veris:asset:country="NF"

Norfolk Island

veris:asset:country="NG"

Nigeria

veris:asset:country="NI"

Nicaragua

veris:asset:country="NL"

Netherlands

veris:asset:country="NO"

Norway

veris:asset:country="NP"

Nepal

veris:asset:country="NR"

Nauru

veris:asset:country="NU"

Niue

veris:asset:country="NZ"

New Zealand

veris:asset:country="OM"

Oman

veris:asset:country="Other"

Other

veris:asset:country="PA"

Panama

veris:asset:country="PE"

Peru

veris:asset:country="PF"

French Polynesia

veris:asset:country="PG"

Papua New Guinea

veris:asset:country="PH"

Philippines

veris:asset:country="PK"

Pakistan

veris:asset:country="PL"

Poland

veris:asset:country="PM"

Saint Pierre and Miquelon

veris:asset:country="PN"

Pitcairn

veris:asset:country="PR"

Puerto Rico

veris:asset:country="PS"

Palestinian Territory, Occupied

veris:asset:country="PT"

Portugal

veris:asset:country="PW"

Palau

veris:asset:country="PY"

Paraguay

veris:asset:country="QA"

Qatar

veris:asset:country="RE"

Reunion

veris:asset:country="RO"

Romania

veris:asset:country="RS"

Serbia

veris:asset:country="RU"

Russian Federation

veris:asset:country="RW"

Rwanda

veris:asset:country="SA"

Saudi Arabia

veris:asset:country="SB"

Solomon Islands

veris:asset:country="SC"

Seychelles

veris:asset:country="SD"

Sudan

veris:asset:country="SE"

Sweden

veris:asset:country="SG"

Singapore

veris:asset:country="SH"

Saint Helena

veris:asset:country="SI"

Slovenia

veris:asset:country="SJ"

Svalbard and Jan Mayen Islands

veris:asset:country="SK"

Slovakia

veris:asset:country="SL"

Sierra Leone

veris:asset:country="SM"

San Marino

veris:asset:country="SN"

Senegal

veris:asset:country="SO"

Somalia

veris:asset:country="SR"

Suriname

veris:asset:country="SS"

South Sudan

veris:asset:country="ST"

Sao Tome and Principe

veris:asset:country="SV"

El Salvador

veris:asset:country="SX"

Sint Maarten (Dutch part)

veris:asset:country="SY"

Syrian Arab Republic

veris:asset:country="SZ"

Swaziland

veris:asset:country="TC"

Turks and Caicos Islands

veris:asset:country="TD"

Chad

veris:asset:country="TF"

French Southern Territories

veris:asset:country="TG"

Togo

veris:asset:country="TH"

Thailand

veris:asset:country="TJ"

Tajikistan

veris:asset:country="TK"

Tokelau

veris:asset:country="TL"

Timor-Leste

veris:asset:country="TM"

Turkmenistan

veris:asset:country="TN"

Tunisia

veris:asset:country="TO"

Tonga

veris:asset:country="TR"

Turkey

veris:asset:country="TT"

Trinidad and Tobago

veris:asset:country="TV"

Tuvalu

veris:asset:country="TW"

Taiwan, Province of China

veris:asset:country="TZ"

Tanzania, United Republic of

veris:asset:country="UA"

Ukraine

veris:asset:country="UG"

Uganda

veris:asset:country="UM"

United States Minor Outlying Islands

veris:asset:country="US"

United States of America

veris:asset:country="UY"

Uruguay

veris:asset:country="UZ"

Uzbekistan

veris:asset:country="Unknown"

Unknown

veris:asset:country="VA"

Holy See

veris:asset:country="VC"

Saint Vincent and the Grenadines

veris:asset:country="VE"

Venezuela (Bolivarian Republic of)

veris:asset:country="VG"

British Virgin Islands

veris:asset:country="VI"

United States Virgin Islands

veris:asset:country="VN"

Viet Nam

veris:asset:country="VU"

Vanuatu

veris:asset:country="WF"

Wallis and Futuna Islands

veris:asset:country="WS"

Samoa

veris:asset:country="YE"

Yemen

veris:asset:country="YT"

Mayotte

veris:asset:country="ZA"

South Africa

veris:asset:country="ZM"

Zambia

veris:asset:country="ZW"

Zimbabwe

asset:governance

veris:asset:governance="3rd party hosted"

Hosted by 3rd party

veris:asset:governance="3rd party managed"

Managed by 3rd party

veris:asset:governance="3rd party owned"

Owned by 3rd party

veris:asset:governance="Internally isolated"

Isolated internal asset

veris:asset:governance="Other"

Governance known but not listed

veris:asset:governance="Personally owned"

Personally owned asset

veris:asset:governance="Unknown"

Unknown

veris:asset:governance="Victim governed"

The victim owns and controls the asset

asset:hosting

veris:asset:hosting="External"

Externally hosted (unsure if dedicated or shared)

veris:asset:hosting="External dedicated"

Externally hosted in a dedicated environment

veris:asset:hosting="External shared"

Externally hosted in a shared environment

veris:asset:hosting="Internal"

Internally hosted

veris:asset:hosting="NA"

Not applicable

veris:asset:hosting="Other"

Hosting known but not listed

veris:asset:hosting="Unknown"

Unknown

asset:management

veris:asset:management="External"

Externally managed

veris:asset:management="Internal"

Internally managed

veris:asset:management="NA"

Not applicable

veris:asset:management="Other"

Ownership known but not listed

veris:asset:management="Unknown"

Unknown

asset:ownership

veris:asset:ownership="Customer"

Customer owned

veris:asset:ownership="Employee"

Employee owned

veris:asset:ownership="NA"

Not applicable

veris:asset:ownership="Other"

Owner known but not listed

veris:asset:ownership="Partner"

Partner owned

veris:asset:ownership="Unknown"

Unknown

veris:asset:ownership="Victim"

Victim owned

impact:iso_currency_code

veris:impact:iso_currency_code="AED"

AED - UAE Dirham

veris:impact:iso_currency_code="AFN"

AFN - Afghani

veris:impact:iso_currency_code="ALL"

ALL - Lek

veris:impact:iso_currency_code="AMD"

AMD - Armenian Dram

veris:impact:iso_currency_code="ANG"

ANG - Netherlands Antillean Guilder

veris:impact:iso_currency_code="AOA"

AOA - Kwanza

veris:impact:iso_currency_code="ARS"

ARS - Argentine Peso

veris:impact:iso_currency_code="AUD"

AUD - Australian Dollar

veris:impact:iso_currency_code="AWG"

AWG - Aruban Florin

veris:impact:iso_currency_code="AZN"

AZN - Azerbaijanian Manat

veris:impact:iso_currency_code="BAM"

BAM - Convertible Mark

veris:impact:iso_currency_code="BBD"

BBD - Barbados Dollar

veris:impact:iso_currency_code="BDT"

BDT - Taka

veris:impact:iso_currency_code="BGN"

BGN - Bulgarian Lev

veris:impact:iso_currency_code="BHD"

BHD - Bahraini Dinar

veris:impact:iso_currency_code="BIF"

BIF - Burundi Franc

veris:impact:iso_currency_code="BMD"

BMD - Bermudian Dollar

veris:impact:iso_currency_code="BND"

BND - Brunei Dollar

veris:impact:iso_currency_code="BOB"

BOB - Boliviano

veris:impact:iso_currency_code="BRL"

BRL - Brazilian Real

veris:impact:iso_currency_code="BSD"

BSD - Bahamian Dollar

veris:impact:iso_currency_code="BTN"

BTN - Ngultrum

veris:impact:iso_currency_code="BWP"

BWP - Pula

veris:impact:iso_currency_code="BYR"

BYR - Belarussian Ruble

veris:impact:iso_currency_code="BZD"

BZD - Belize Dollar

veris:impact:iso_currency_code="CAD"

CAD - Canadian Dollar

veris:impact:iso_currency_code="CDF"

CDF - Congolese Franc

veris:impact:iso_currency_code="CHF"

CHF - Swiss Franc

veris:impact:iso_currency_code="CLP"

CLP - Chilean Peso

veris:impact:iso_currency_code="CNY"

CNY - Yuan Renminbi

veris:impact:iso_currency_code="COP"

COP - Colombian Peso

veris:impact:iso_currency_code="CRC"

CRC - Costa Rican Colon

veris:impact:iso_currency_code="CUC"

CUC - Peso Convertible

veris:impact:iso_currency_code="CUP"

CUP - Cuban Peso

veris:impact:iso_currency_code="CVE"

CVE - Cape Verde Escudo

veris:impact:iso_currency_code="CZK"

CZK - Czech Koruna

veris:impact:iso_currency_code="DJF"

DJF - Djibouti Franc

veris:impact:iso_currency_code="DKK"

DKK - Danish Krone

veris:impact:iso_currency_code="DOP"

DOP - Dominican Peso

veris:impact:iso_currency_code="DZD"

DZD - Algerian Dinar

veris:impact:iso_currency_code="EGP"

EGP - Egyptian Pound

veris:impact:iso_currency_code="ERN"

ERN - Nakfa

veris:impact:iso_currency_code="ETB"

ETB - Ethiopian Birr

veris:impact:iso_currency_code="EUR"

EUR - Euro

veris:impact:iso_currency_code="FJD"

FJD - Fiji Dollar

veris:impact:iso_currency_code="FKP"

FKP - Falkland Islands Pound

veris:impact:iso_currency_code="GBP"

GBP - Pound Sterling

veris:impact:iso_currency_code="GEL"

GEL - Lari

veris:impact:iso_currency_code="GGP"

GGP - Guernsey pound

veris:impact:iso_currency_code="GHS"

GHS - Ghana Cedi

veris:impact:iso_currency_code="GIP"

GIP - Gibraltar Pound

veris:impact:iso_currency_code="GMD"

GMD - Dalasi

veris:impact:iso_currency_code="GNF"

GNF - Guinea Franc

veris:impact:iso_currency_code="GTQ"

GTQ - Quetzal

veris:impact:iso_currency_code="GYD"

GYD - Guyana Dollar

veris:impact:iso_currency_code="HKD"

HKD - Hong Kong Dollar

veris:impact:iso_currency_code="HNL"

HNL - Lempira

veris:impact:iso_currency_code="HRK"

HRK - Croatian Kuna

veris:impact:iso_currency_code="HTG"

HTG - Gourde

veris:impact:iso_currency_code="HUF"

HUF - Forint

veris:impact:iso_currency_code="IDR"

IDR - Rupiah

veris:impact:iso_currency_code="ILS"

ILS - New Israeli Sheqel

veris:impact:iso_currency_code="IMP"

IMP - Isle of Man Pound

veris:impact:iso_currency_code="INR"

INR - Indian Rupee

veris:impact:iso_currency_code="IQD"

IQD - Iraqi Dinar

veris:impact:iso_currency_code="IRR"

IRR - Iranian Rial

veris:impact:iso_currency_code="ISK"

ISK - Iceland Krona

veris:impact:iso_currency_code="JEP"

JEP - Jersey pound

veris:impact:iso_currency_code="JMD"

JMD - Jamaican Dollar

veris:impact:iso_currency_code="JOD"

JOD - Jordanian Dinar

veris:impact:iso_currency_code="JPY"

JPY - Yen

veris:impact:iso_currency_code="KES"

KES - Kenyan Shilling

veris:impact:iso_currency_code="KGS"

KGS - Som

veris:impact:iso_currency_code="KHR"

KHR - Riel

veris:impact:iso_currency_code="KMF"

KMF - Comoro Franc

veris:impact:iso_currency_code="KPW"

KPW - North Korean Won

veris:impact:iso_currency_code="KRW"

KRW - South Korean Won

veris:impact:iso_currency_code="KWD"

KWD - Kuwaiti Dinar

veris:impact:iso_currency_code="KYD"

KYD - Cayman Islands Dollar

veris:impact:iso_currency_code="KZT"

KZT - Tenge

veris:impact:iso_currency_code="LAK"

LAK - Kip

veris:impact:iso_currency_code="LBP"

LBP - Lebanese Pound

veris:impact:iso_currency_code="LKR"

LKR - Sri Lanka Rupee

veris:impact:iso_currency_code="LRD"

LRD - Liberian Dollar

veris:impact:iso_currency_code="LSL"

LSL - Loti

veris:impact:iso_currency_code="LTL"

LTL - Lithuanian Litas

veris:impact:iso_currency_code="LVL"

LVL - Latvian Lats

veris:impact:iso_currency_code="LYD"

LYD - Libyan Dinar

veris:impact:iso_currency_code="MAD"

MAD - Moroccan Dirham

veris:impact:iso_currency_code="MDL"

MDL - Moldovan Leu

veris:impact:iso_currency_code="MGA"

MGA - Malagasy Ariary

veris:impact:iso_currency_code="MKD"

MKD - Denar

veris:impact:iso_currency_code="MMK"

MMK - Kyat

veris:impact:iso_currency_code="MNT"

MNT - Tugrik

veris:impact:iso_currency_code="MOP"

MOP - Pataca

veris:impact:iso_currency_code="MRO"

MRO - Ouguiya

veris:impact:iso_currency_code="MUR"

MUR - Mauritius Rupee

veris:impact:iso_currency_code="MVR"

MVR - Rufiyaa

veris:impact:iso_currency_code="MWK"

MWK - Kwacha

veris:impact:iso_currency_code="MXN"

MXN - Mexican Peso

veris:impact:iso_currency_code="MYR"

MYR - Malaysian Ringgit

veris:impact:iso_currency_code="MZN"

MZN - Mozambique Metical

veris:impact:iso_currency_code="NAD"

NAD - Namibia Dollar

veris:impact:iso_currency_code="NGN"

NGN - Naira

veris:impact:iso_currency_code="NIO"

NIO - Cordoba Oro

veris:impact:iso_currency_code="NOK"

NOK - Norwegian Krone

veris:impact:iso_currency_code="NPR"

NPR - Nepalese Rupee

veris:impact:iso_currency_code="NZD"

NZD - New Zealand Dollar

veris:impact:iso_currency_code="OMR"

OMR - Rial Omani

veris:impact:iso_currency_code="PAB"

PAB - Balboa

veris:impact:iso_currency_code="PEN"

PEN - Nuevo Sol

veris:impact:iso_currency_code="PGK"

PGK - Kina

veris:impact:iso_currency_code="PHP"

PHP - Philippine Peso

veris:impact:iso_currency_code="PKR"

PKR - Pakistan Rupee

veris:impact:iso_currency_code="PLN"

PLN - Zloty

veris:impact:iso_currency_code="PYG"

PYG - Guarani

veris:impact:iso_currency_code="QAR"

QAR - Qatari Rial

veris:impact:iso_currency_code="RON"

RON - New Romanian Leu

veris:impact:iso_currency_code="RSD"

RSD - Serbian Dinar

veris:impact:iso_currency_code="RUB"

RUB - Russian Ruble

veris:impact:iso_currency_code="RWF"

RWF - Rwanda Franc

veris:impact:iso_currency_code="SAR"

SAR - Saudi Riyal

veris:impact:iso_currency_code="SBD"

SBD - Solomon Islands Dollar

veris:impact:iso_currency_code="SCR"

SCR - Seychelles Rupee

veris:impact:iso_currency_code="SDG"

SDG - Sudanese Pound

veris:impact:iso_currency_code="SEK"

SEK - Swedish Krona

veris:impact:iso_currency_code="SGD"

SGD - Singapore Dollar

veris:impact:iso_currency_code="SHP"

SHP - Saint Helena Pound

veris:impact:iso_currency_code="SLL"

SLL - Leone

veris:impact:iso_currency_code="SOS"

SOS - Somali Shilling

veris:impact:iso_currency_code="SPL"

SPL - Seborga Luigino

veris:impact:iso_currency_code="SRD"

SRD - Surinam Dollar

veris:impact:iso_currency_code="STD"

STD - Dobra

veris:impact:iso_currency_code="SVC"

SVC - El Salvador Colon

veris:impact:iso_currency_code="SYP"

SYP - Syrian Pound

veris:impact:iso_currency_code="SZL"

SZL - Lilangeni

veris:impact:iso_currency_code="THB"

THB - Baht

veris:impact:iso_currency_code="TJS"

TJS - Somoni

veris:impact:iso_currency_code="TMT"

TMT - Turkmenistan New Manat

veris:impact:iso_currency_code="TND"

TND - Tunisian Dinar

veris:impact:iso_currency_code="TOP"

TOP - Pa’anga

veris:impact:iso_currency_code="TRY"

TRY - Turkish Lira

veris:impact:iso_currency_code="TTD"

TTD - Trinidad and Tobago Dollar

veris:impact:iso_currency_code="TVD"

TVD - Tuvalu Dollar

veris:impact:iso_currency_code="TWD"

TWD - New Taiwan Dollar

veris:impact:iso_currency_code="TZS"

TZS - Tanzanian Shilling

veris:impact:iso_currency_code="UAH"

UAH - Hryvnia

veris:impact:iso_currency_code="UGX"

UGX - Uganda Shilling

veris:impact:iso_currency_code="USD"

USD - US Dollar

veris:impact:iso_currency_code="UYU"

UYU - Peso Uruguayo

veris:impact:iso_currency_code="UZS"

UZS - Uzbekistan Sum

veris:impact:iso_currency_code="VEF"

VEF - Bolivar

veris:impact:iso_currency_code="VND"

VND - Dong

veris:impact:iso_currency_code="VUV"

VUV - Vatu

veris:impact:iso_currency_code="WST"

WST - Tala

veris:impact:iso_currency_code="XAF"

XAF - CFA Franc BEAC

veris:impact:iso_currency_code="XCD"

XCD - East Caribbean Dollar

veris:impact:iso_currency_code="XDR"

XDR - SDR (Special Drawing Right)

veris:impact:iso_currency_code="XOF"

XOF - CFA Franc BCEAO

veris:impact:iso_currency_code="XPF"

XPF - CFP Franc

veris:impact:iso_currency_code="YER"

YER - Yemeni Rial

veris:impact:iso_currency_code="ZAR"

ZAR - South African Rand

veris:impact:iso_currency_code="ZMK"

ZMK - Zambian Kwacha

veris:impact:iso_currency_code="ZWD"

ZWD - Zimbabwean Dollar A/06

impact:overall_rating

veris:impact:overall_rating="Catastrophic"

Catastrophic: A business-ending event (don’t choose this if the victim will continue operations)

veris:impact:overall_rating="Damaging"

Damaging: Real and serious effect on the "bottom line" and/or long-term ability to generate revenue

veris:impact:overall_rating="Distracting"

Distracting: Limited "hard costs", but impact felt through having to deal with the incident rather than conducting normal duties

veris:impact:overall_rating="Insignificant"

Insignificant: Impact absorbed by normal activities

veris:impact:overall_rating="Painful"

Painful: Moderate "hard costs", and impact felt through having to deal with the incident rather than conducting normal duties has quantifiable indirect costs

veris:impact:overall_rating="Unknown"

Unknown

victim:country

veris:victim:country="AD"

Andorra

veris:victim:country="AE"

United Arab Emirates

veris:victim:country="AF"

Afghanistan

veris:victim:country="AG"

Antigua and Barbuda

veris:victim:country="AI"

Anguilla

veris:victim:country="AL"

Albania

veris:victim:country="AM"

Armenia

veris:victim:country="AO"

Angola

veris:victim:country="AQ"

Antarctica

veris:victim:country="AR"

Argentina

veris:victim:country="AS"

American Samoa

veris:victim:country="AT"

Austria

veris:victim:country="AU"

Australia

veris:victim:country="AW"

Aruba

veris:victim:country="AX"

Aland Islands

veris:victim:country="AZ"

Azerbaijan

veris:victim:country="BA"

Bosnia and Herzegovina

veris:victim:country="BB"

Barbados

veris:victim:country="BD"

Bangladesh

veris:victim:country="BE"

Belgium

veris:victim:country="BF"

Burkina Faso

veris:victim:country="BG"

Bulgaria

veris:victim:country="BH"

Bahrain

veris:victim:country="BI"

Burundi

veris:victim:country="BJ"

Benin

veris:victim:country="BL"

Saint-Barthelemy

veris:victim:country="BM"

Bermuda

veris:victim:country="BN"

Brunei Darussalam

veris:victim:country="BO"

Bolivia

veris:victim:country="BQ"

Bonaire, Saint Eustatius and Saba

veris:victim:country="BR"

Brazil

veris:victim:country="BS"

Bahamas

veris:victim:country="BT"

Bhutan

veris:victim:country="BV"

Bouvet Island

veris:victim:country="BW"

Botswana

veris:victim:country="BY"

Belarus

veris:victim:country="BZ"

Belize

veris:victim:country="CA"

Canada

veris:victim:country="CC"

Cocos (Keeling) Islands

veris:victim:country="CD"

Congo, Democratic Republic of the

veris:victim:country="CF"

Central African Republic

veris:victim:country="CG"

Congo

veris:victim:country="CH"

Switzerland

veris:victim:country="CI"

Cote d’Ivoire

veris:victim:country="CK"

Cook Islands

veris:victim:country="CL"

Chile

veris:victim:country="CM"

Cameroon

veris:victim:country="CN"

China

veris:victim:country="CO"

Colombia

veris:victim:country="CR"

Costa Rica

veris:victim:country="CU"

Cuba

veris:victim:country="CV"

Cape Verde

veris:victim:country="CW"

Curacao

veris:victim:country="CX"

Christmas Island

veris:victim:country="CY"

Cyprus

veris:victim:country="CZ"

Czech Republic

veris:victim:country="DE"

Germany

veris:victim:country="DJ"

Djibouti

veris:victim:country="DK"

Denmark

veris:victim:country="DM"

Dominica

veris:victim:country="DO"

Dominican Republic

veris:victim:country="DZ"

Algeria

veris:victim:country="EC"

Ecuador

veris:victim:country="EE"

Estonia

veris:victim:country="EG"

Egypt

veris:victim:country="EH"

Western Sahara

veris:victim:country="ER"

Eritrea

veris:victim:country="ES"

Spain

veris:victim:country="ET"

Ethiopia

veris:victim:country="FI"

Finland

veris:victim:country="FJ"

Fiji

veris:victim:country="FK"

Faeroe Islands

veris:victim:country="FM"

Micronesia (Federated States of)

veris:victim:country="FO"

Falkland Islands (Malvinas)

veris:victim:country="FR"

France

veris:victim:country="GA"

Gabon

veris:victim:country="GB"

United Kingdom

veris:victim:country="GD"

Grenada

veris:victim:country="GE"

Georgia

veris:victim:country="GF"

French Guiana

veris:victim:country="GG"

Guernsey

veris:victim:country="GH"

Ghana

veris:victim:country="GI"

Gibraltar

veris:victim:country="GL"

Greenland

veris:victim:country="GM"

Gambia

veris:victim:country="GN"

Guinea

veris:victim:country="GP"

Guadeloupe

veris:victim:country="GQ"

Equatorial Guinea

veris:victim:country="GR"

Greece

veris:victim:country="GS"

South Georgia and the South Sandwich Islands

veris:victim:country="GT"

Guatemala

veris:victim:country="GU"

Guam

veris:victim:country="GW"

Guinea-Bissau

veris:victim:country="GY"

Guyana

veris:victim:country="HK"

Hong Kong

veris:victim:country="HM"

Heard Island and McDonal Islands

veris:victim:country="HN"

Honduras

veris:victim:country="HR"

Croatia

veris:victim:country="HT"

Haiti

veris:victim:country="HU"

Hungary

veris:victim:country="ID"

Indonesia

veris:victim:country="IE"

Ireland

veris:victim:country="IL"

Israel

veris:victim:country="IM"

Isle of Man

veris:victim:country="IN"

India

veris:victim:country="IO"

British Virgin Islands

veris:victim:country="IQ"

Iraq

veris:victim:country="IR"

Iran (Islamic Republic of)

veris:victim:country="IS"

Iceland

veris:victim:country="IT"

Italy

veris:victim:country="JE"

Jersey

veris:victim:country="JM"

Jamaica

veris:victim:country="JO"

Jordan

veris:victim:country="JP"

Japan

veris:victim:country="KE"

Kenya

veris:victim:country="KG"

Kyrgyzstan

veris:victim:country="KH"

Cambodia

veris:victim:country="KI"

Kiribati

veris:victim:country="KM"

Comoros

veris:victim:country="KN"

Saint Kitts and Nevis

veris:victim:country="KP"

Korea, Democratic People’s Republic of

veris:victim:country="KR"

Korea, Republic of

veris:victim:country="KW"

Kuwait

veris:victim:country="KY"

Cayman Islands

veris:victim:country="KZ"

Kazakhstan

veris:victim:country="LA"

Lao People’s Democratic Republic

veris:victim:country="LB"

Lebanon

veris:victim:country="LC"

Saint Lucia

veris:victim:country="LI"

Liechtenstein

veris:victim:country="LK"

Sri Lanka

veris:victim:country="LR"

Liberia

veris:victim:country="LS"

Lesotho

veris:victim:country="LT"

Lithuania

veris:victim:country="LU"

Luxembourg

veris:victim:country="LV"

Latvia

veris:victim:country="LY"

Libya

veris:victim:country="MA"

Morocco

veris:victim:country="MC"

Monaco

veris:victim:country="MD"

Moldova, Republic of

veris:victim:country="ME"

Montenegro

veris:victim:country="MF"

Saint Martin (French part)

veris:victim:country="MG"

Madagascar

veris:victim:country="MH"

Marshall Islands

veris:victim:country="MK"

Macedonia, The former Yugoslav Republic of

veris:victim:country="ML"

Mali

veris:victim:country="MM"

Myanmar

veris:victim:country="MN"

Mongolia

veris:victim:country="MO"

Macao

veris:victim:country="MP"

Northern Mariana Islands

veris:victim:country="MQ"

Martinique

veris:victim:country="MR"

Mauritania

veris:victim:country="MS"

Montserrat

veris:victim:country="MT"

Malta

veris:victim:country="MU"

Mauritius

veris:victim:country="MV"

Maldives

veris:victim:country="MW"

Malawi

veris:victim:country="MX"

Mexico

veris:victim:country="MY"

Malaysia

veris:victim:country="MZ"

Mozambique

veris:victim:country="NA"

Namibia

veris:victim:country="NC"

New Caledonia

veris:victim:country="NE"

Niger

veris:victim:country="NF"

Norfolk Island

veris:victim:country="NG"

Nigeria

veris:victim:country="NI"

Nicaragua

veris:victim:country="NL"

Netherlands

veris:victim:country="NO"

Norway

veris:victim:country="NP"

Nepal

veris:victim:country="NR"

Nauru

veris:victim:country="NU"

Niue

veris:victim:country="NZ"

New Zealand

veris:victim:country="OM"

Oman

veris:victim:country="Other"

Other

veris:victim:country="PA"

Panama

veris:victim:country="PE"

Peru

veris:victim:country="PF"

French Polynesia

veris:victim:country="PG"

Papua New Guinea

veris:victim:country="PH"

Philippines

veris:victim:country="PK"

Pakistan

veris:victim:country="PL"

Poland

veris:victim:country="PM"

Saint Pierre and Miquelon

veris:victim:country="PN"

Pitcairn

veris:victim:country="PR"

Puerto Rico

veris:victim:country="PS"

Palestinian Territory, Occupied

veris:victim:country="PT"

Portugal

veris:victim:country="PW"

Palau

veris:victim:country="PY"

Paraguay

veris:victim:country="QA"

Qatar

veris:victim:country="RE"

Reunion

veris:victim:country="RO"

Romania

veris:victim:country="RS"

Serbia

veris:victim:country="RU"

Russian Federation

veris:victim:country="RW"

Rwanda

veris:victim:country="SA"

Saudi Arabia

veris:victim:country="SB"

Solomon Islands

veris:victim:country="SC"

Seychelles

veris:victim:country="SD"

Sudan

veris:victim:country="SE"

Sweden

veris:victim:country="SG"

Singapore

veris:victim:country="SH"

Saint Helena

veris:victim:country="SI"

Slovenia

veris:victim:country="SJ"

Svalbard and Jan Mayen Islands

veris:victim:country="SK"

Slovakia

veris:victim:country="SL"

Sierra Leone

veris:victim:country="SM"

San Marino

veris:victim:country="SN"

Senegal

veris:victim:country="SO"

Somalia

veris:victim:country="SR"

Suriname

veris:victim:country="SS"

South Sudan

veris:victim:country="ST"

Sao Tome and Principe

veris:victim:country="SV"

El Salvador

veris:victim:country="SX"

Sint Maarten (Dutch part)

veris:victim:country="SY"

Syrian Arab Republic

veris:victim:country="SZ"

Swaziland

veris:victim:country="TC"

Turks and Caicos Islands

veris:victim:country="TD"

Chad

veris:victim:country="TF"

French Southern Territories

veris:victim:country="TG"

Togo

veris:victim:country="TH"

Thailand

veris:victim:country="TJ"

Tajikistan

veris:victim:country="TK"

Tokelau

veris:victim:country="TL"

Timor-Leste

veris:victim:country="TM"

Turkmenistan

veris:victim:country="TN"

Tunisia

veris:victim:country="TO"

Tonga

veris:victim:country="TR"

Turkey

veris:victim:country="TT"

Trinidad and Tobago

veris:victim:country="TV"

Tuvalu

veris:victim:country="TW"

Taiwan, Province of China

veris:victim:country="TZ"

Tanzania, United Republic of

veris:victim:country="UA"

Ukraine

veris:victim:country="UG"

Uganda

veris:victim:country="UM"

United States Minor Outlying Islands

veris:victim:country="US"

United States of America

veris:victim:country="UY"

Uruguay

veris:victim:country="UZ"

Uzbekistan

veris:victim:country="Unknown"

Unknown

veris:victim:country="VA"

Holy See

veris:victim:country="VC"

Saint Vincent and the Grenadines

veris:victim:country="VE"

Venezuela (Bolivarian Republic of)

veris:victim:country="VG"

British Virgin Islands

veris:victim:country="VI"

United States Virgin Islands

veris:victim:country="VN"

Viet Nam

veris:victim:country="VU"

Vanuatu

veris:victim:country="WF"

Wallis and Futuna Islands

veris:victim:country="WS"

Samoa

veris:victim:country="YE"

Yemen

veris:victim:country="YT"

Mayotte

veris:victim:country="ZA"

South Africa

veris:victim:country="ZM"

Zambia

veris:victim:country="ZW"

Zimbabwe

victim:employee_count

veris:victim:employee_count="1 to 10"

1 to 10 employees

veris:victim:employee_count="10001 to 25000"

10,001 to 25,000 employees

veris:victim:employee_count="1001 to 10000"

1,001 to 10,000 employees

veris:victim:employee_count="101 to 1000"

101 to 1,000 employees

veris:victim:employee_count="11 to 100"

11 to 100 employees

veris:victim:employee_count="25001 to 50000"

25,001 to 50,000 employees

veris:victim:employee_count="50001 to 100000"

50,001 to 100,000 employees

veris:victim:employee_count="Large"

Large organizations (over 1,000 employees)

veris:victim:employee_count="Over 100000"

Over 100,0001 employees

veris:victim:employee_count="Small"

Small organizations (1,000 employees or less)

veris:victim:employee_count="Unknown"

Unknown number of employees

action:environmental:variety

veris:action:environmental:variety="Deterioration"

Deterioration and degradation

veris:action:environmental:variety="EMI"

Electromagnetic interference (EMI)

veris:action:environmental:variety="ESD"

Electrostatic discharge (ESD)

veris:action:environmental:variety="Earthquake"

Earthquake

veris:action:environmental:variety="Fire"

Fire

veris:action:environmental:variety="Flood"

Flood

veris:action:environmental:variety="Hazmat"

Hazardous material

veris:action:environmental:variety="Humidity"

Humidity

veris:action:environmental:variety="Hurricane"

Hurricane

veris:action:environmental:variety="Ice"

Ice and snow

veris:action:environmental:variety="Landslide"

Landslide

veris:action:environmental:variety="Leak"

Water leak

veris:action:environmental:variety="Lightning"

Lightning

veris:action:environmental:variety="Meteorite"

Meteorite

veris:action:environmental:variety="Other"

Other

veris:action:environmental:variety="Particulates"

Particulate matter (e.g., dust, smoke)

veris:action:environmental:variety="Pathogen"

Pathogen

veris:action:environmental:variety="Power failure"

Power failure or fluctuation

veris:action:environmental:variety="Temperature"

Extreme temperature

veris:action:environmental:variety="Tornado"

Tornado

veris:action:environmental:variety="Tsunami"

Tsunami

veris:action:environmental:variety="Unknown"

Unknown

veris:action:environmental:variety="Vermin"

Vermin

veris:action:environmental:variety="Volcano"

Volcanic eruption

veris:action:environmental:variety="Wind"

Wind

action:error:variety

veris:action:error:variety="Capacity shortage"

Poor capacity planning

veris:action:error:variety="Classification error"

Classification or labeling error

veris:action:error:variety="Data entry error"

Data entry error

veris:action:error:variety="Disposal error"

Disposal error

veris:action:error:variety="Gaffe"

Gaffe (social or verbal slip)

veris:action:error:variety="Loss"

Loss or misplacement

veris:action:error:variety="Maintenance error"

Maintenance error

veris:action:error:variety="Malfunction"

Technical malfunction or glitch

veris:action:error:variety="Misconfiguration"

Misconfiguration

veris:action:error:variety="Misdelivery"

Misdelivery (send wrong info or to wrong recipient)

veris:action:error:variety="Misinformation"

Misinformation (unintentionally giving false info)

veris:action:error:variety="Omission"

Omission (something intended, but not done)

veris:action:error:variety="Other"

Other

veris:action:error:variety="Physical accidents"

Physical accidents (e.g., drops, bumps, spills)

veris:action:error:variety="Programming error"

Programming error (flaws or bugs in custom code)

veris:action:error:variety="Publishing error"

Publishing error (private info to public doc or site)

veris:action:error:variety="Unknown"

Unknown

action:error:vector

veris:action:error:vector="Carelessness"

Carelessness

veris:action:error:vector="Inadequate personnel"

Inadequate or insufficient personnel

veris:action:error:vector="Inadequate processes"

Inadequate or insufficient processes

veris:action:error:vector="Inadequate technology"

Inadequate or insufficient technology resources

veris:action:error:vector="Other"

Other

veris:action:error:vector="Random error"

Random error (no reason, no fault)

veris:action:error:vector="Unknown"

Unknown

action:hacking:result

veris:action:hacking:result="Elevate"

The hacking action resulted in additional permissions

veris:action:hacking:result="Exfiltrate"

The hacking action exfiltrated data from the victim

veris:action:hacking:result="Infiltrate"

The hacking action infiltrated the victim

action:hacking:variety

veris:action:hacking:variety="Abuse of functionality"

Abuse of functionality

veris:action:hacking:variety="Brute force"

Brute force or password guessing attacks

veris:action:hacking:variety="Buffer overflow"

Buffer overflow

veris:action:hacking:variety="CSRF"

Cross-site request forgery

veris:action:hacking:variety="Cache poisoning"

Cache poisoning

veris:action:hacking:variety="Cryptanalysis"

Cryptanalysis

veris:action:hacking:variety="DoS"

Denial of service

veris:action:hacking:variety="Footprinting"

Footprinting and fingerprinting

veris:action:hacking:variety="Forced browsing"

Forced browsing or predictable resource location

veris:action:hacking:variety="Format string attack"

Format string attack

veris:action:hacking:variety="Fuzz testing"

Fuzz testing

veris:action:hacking:variety="HTTP Response Splitting"

HTTP Response Splitting

veris:action:hacking:variety="HTTP request smuggling"

HTTP request smuggling

veris:action:hacking:variety="HTTP request splitting"

HTTP request splitting

veris:action:hacking:variety="HTTP response smuggling"

HTTP response smuggling

veris:action:hacking:variety="Integer overflows"

Integer overflows

veris:action:hacking:variety="LDAP injection"

LDAP injection

veris:action:hacking:variety="Mail command injection"

Mail command injection

veris:action:hacking:variety="MitM"

Man-in-the-middle attack

veris:action:hacking:variety="Null byte injection"

Null byte injection

veris:action:hacking:variety="OS commanding"

OS commanding

veris:action:hacking:variety="Offline cracking"

Offline password or key cracking (e.g., rainbow tables, Hashcat, JtR)

veris:action:hacking:variety="Other"

Other

veris:action:hacking:variety="Pass-the-hash"

Pass-the-hash

veris:action:hacking:variety="Path traversal"

Path traversal

veris:action:hacking:variety="RFI"

Remote file inclusion

veris:action:hacking:variety="Reverse engineering"

Reverse engineering

veris:action:hacking:variety="Routing detour"

Routing detour

veris:action:hacking:variety="SQLi"

SQL injection

veris:action:hacking:variety="SSI injection"

SSI injection

veris:action:hacking:variety="Session fixation"

Session fixation

veris:action:hacking:variety="Session prediction"

Credential or session prediction

veris:action:hacking:variety="Session replay"

Session replay

veris:action:hacking:variety="Soap array abuse"

Soap array abuse

veris:action:hacking:variety="Special element injection"

Special element injection

veris:action:hacking:variety="URL redirector abuse"

URL redirector abuse

veris:action:hacking:variety="Unknown"

Unknown

veris:action:hacking:variety="Use of backdoor or C2"

Use of Backdoor or C2 channel

veris:action:hacking:variety="Use of stolen creds"

Use of stolen authentication credentials

veris:action:hacking:variety="Virtual machine escape"

Virtual machine escape

veris:action:hacking:variety="XML attribute blowup"

XML attribute blowup

veris:action:hacking:variety="XML entity expansion"

XML entity expansion

veris:action:hacking:variety="XML external entities"

XML external entities

veris:action:hacking:variety="XML injection"

XML injection

veris:action:hacking:variety="XPath injection"

XPath injection

veris:action:hacking:variety="XQuery injection"

XQuery injection

veris:action:hacking:variety="XSS"

Cross-site scripting

action:hacking:vector

veris:action:hacking:vector="3rd party desktop"

3rd party online desktop sharing (LogMeIn, Go2Assist)

veris:action:hacking:vector="Backdoor or C2"

Backdoor or command and control channel

veris:action:hacking:vector="Command shell"

Remote shell

veris:action:hacking:vector="Desktop sharing"

Graphical desktop sharing (RDP, VNC, PCAnywhere, Citrix)

veris:action:hacking:vector="Desktop sharing software"

Superset of 'Desktop sharing' and '3rd party desktop'. Please use in place of the other two

veris:action:hacking:vector="Other"

Other

veris:action:hacking:vector="Partner"

Partner connection or credential

veris:action:hacking:vector="Physical access"

Physical access or connection (i.e., at keyboard or via cable)

veris:action:hacking:vector="Unknown"

Unknown

veris:action:hacking:vector="VPN"

VPN

veris:action:hacking:vector="Web application"

Web application

action:malware:result

veris:action:malware:result="Elevate"

The malware action resulted in additional permissions

veris:action:malware:result="Exfiltrate"

The malware action exfiltrated data from the victim

veris:action:malware:result="Infiltrate"

The malware action infiltrated the victim

action:malware:variety

veris:action:malware:variety="Adminware"

System or network utilities (e.g., PsTools, Netcat)

veris:action:malware:variety="Adware"

Adware

veris:action:malware:variety="Backdoor"

Backdoor (enable remote access)

veris:action:malware:variety="Brute force"

Brute force attack

veris:action:malware:variety="C2"

Command and control (C2)

veris:action:malware:variety="Capture app data"

Capture data from application or system process

veris:action:malware:variety="Capture stored data"

Capture data stored on system disk

veris:action:malware:variety="Click fraud"

Click fraud or Bitcoin mining

veris:action:malware:variety="Client-side attack"

Client-side or browser attack (e.g., redirection, XSS, MitB)

veris:action:malware:variety="Destroy data"

Destroy or corrupt stored data

veris:action:malware:variety="Disable controls"

Disable or interfere with security controls

veris:action:malware:variety="DoS"

DoS attack

veris:action:malware:variety="Downloader"

Downloader (pull updates or other malware)

veris:action:malware:variety="Exploit vuln"

Exploit vulnerability in code (vs misconfig or weakness)

veris:action:malware:variety="Export data"

Export data to another site or system

veris:action:malware:variety="Modify data"

Malware which compromises a legitimate file rather than creating new filess

veris:action:malware:variety="Other"

Other

veris:action:malware:variety="Packet sniffer"

Packet sniffer (capture data from network)

veris:action:malware:variety="Password dumper"

Password dumper (extract credential hashes)

veris:action:malware:variety="Ram scraper"

Ram scraper or memory parser (capture data from volatile memory)

veris:action:malware:variety="Ransomware"

Ransomware (encrypt or seize stored data)

veris:action:malware:variety="Rootkit"

Rootkit (maintain local privileges and stealth)

veris:action:malware:variety="SQL injection"

SQL injection attack

veris:action:malware:variety="Scan network"

Scan or footprint network

veris:action:malware:variety="Spam"

Send spam

veris:action:malware:variety="Spyware/Keylogger"

Spyware, keylogger or form-grabber (capture user input or activity)

veris:action:malware:variety="Unknown"

Unknown

veris:action:malware:variety="Worm"

Worm (propagate to other systems or devices)

action:malware:vector

veris:action:malware:vector="Direct install"

Directly installed or inserted by threat agent (after system access)

veris:action:malware:vector="Download by malware"

Downloaded and installed by local malware

veris:action:malware:vector="Email attachment"

Email via user-executed attachment

veris:action:malware:vector="Email autoexecute"

Email via automatic execution

veris:action:malware:vector="Email link"

Email via embedded link

veris:action:malware:vector="Email unknown"

Email but sub-variety (attachment, autoexecute, link, etc) not known

veris:action:malware:vector="Instant messaging"

Instant Messaging

veris:action:malware:vector="Network propagation"

Network propagation

veris:action:malware:vector="Other"

Other

veris:action:malware:vector="Remote injection"

Remotely injected by agent (i.e. via SQLi)

veris:action:malware:vector="Removable media"

Removable storage media or devices

veris:action:malware:vector="Software update"

Included in automated software update

veris:action:malware:vector="Unknown"

Unknown

veris:action:malware:vector="Web download"

Web via user-executed or downloaded content

veris:action:malware:vector="Web drive-by"

Web via auto-executed or "drive-by" infection

action:misuse:result

veris:action:misuse:result="Elevate"

The misuse action resulted in additional permissions

veris:action:misuse:result="Exfiltrate"

The misuse action exfiltrated data from the victim

veris:action:misuse:result="Infiltrate"

The misuse action infiltrated the victim

action:misuse:variety

veris:action:misuse:variety="Data mishandling"

Handling of data in an unapproved manner

veris:action:misuse:variety="Email misuse"

Inappropriate use of email or IM

veris:action:misuse:variety="Illicit content"

Storage or distribution of illicit content

veris:action:misuse:variety="Knowledge abuse"

Abuse of private or entrusted knowledge

veris:action:misuse:variety="Net misuse"

Inappropriate use of network or Web access

veris:action:misuse:variety="Other"

```
Other
```

veris:action:misuse:variety="Possession abuse"

Abuse of physical access to asset

veris:action:misuse:variety="Privilege abuse"

Abuse of system access privileges

veris:action:misuse:variety="Unapproved hardware"

Use of unapproved hardware or devices

veris:action:misuse:variety="Unapproved software"

Use of unapproved software or services

veris:action:misuse:variety="Unapproved workaround"

Unapproved workaround or shortcut

veris:action:misuse:variety="Unknown"

Unknown

action:misuse:vector

veris:action:misuse:vector="LAN access"

Local network access within corporate facility

veris:action:misuse:vector="Non-corporate"

Non-corporate facilities or networks

veris:action:misuse:vector="Other"

Other

veris:action:misuse:vector="Physical access"

Physical access within corporate facility

veris:action:misuse:vector="Remote access"

Remote access connection to corporate network (i.e. VPN)

veris:action:misuse:vector="Unknown"

Unknown

action:physical:result

veris:action:physical:result="Elevate"

The physical action resulted in additional permissions

veris:action:physical:result="Exfiltrate"

The physical action exfiltrated data from the victim

veris:action:physical:result="Infiltrate"

The physical action infiltrated the victim

action:physical:variety

veris:action:physical:variety="Assault"

Assault (threats or acts of physical violence)

veris:action:physical:variety="Bypassed controls"

Bypassed physical barriers or controls

veris:action:physical:variety="Connection"

Connection

veris:action:physical:variety="Destruction"

Destruction (deliberate damaging or disabling)

veris:action:physical:variety="Disabled controls"

Disabled physical barriers or controls

veris:action:physical:variety="Other"

Other

veris:action:physical:variety="Skimmer"

Installing card skimming device

veris:action:physical:variety="Snooping"

Snooping (sneak about to gain info or access)

veris:action:physical:variety="Surveillance"

Surveillance (monitoring and observation)

veris:action:physical:variety="Tampering"

Tampering (alter physical form or function)

veris:action:physical:variety="Theft"

Theft (taking assets without permission)

veris:action:physical:variety="Unknown"

Unknown

veris:action:physical:variety="Wiretapping"

Wiretapping (Physical tap to comms line)

action:physical:vector

veris:action:physical:vector="Other"

Other

veris:action:physical:vector="Partner facility"

Partner facility or area

veris:action:physical:vector="Partner vehicle"

Partner vehicle (e.g., delivery truck)

veris:action:physical:vector="Personal residence"

Personal residence

veris:action:physical:vector="Personal vehicle"

Personal vehicle

veris:action:physical:vector="Privileged access"

Held privileged access to location

veris:action:physical:vector="Public facility"

Public facility or area

veris:action:physical:vector="Public vehicle"

Public vehicle (e.g., plane, taxi)

veris:action:physical:vector="Uncontrolled location"

The location was uncontrolled (public)

veris:action:physical:vector="Unknown"

Unknown

veris:action:physical:vector="Victim grounds"

Victim outdoor grounds

veris:action:physical:vector="Victim public area"

Victim public or customer area (e.g., lobby, storefront)

veris:action:physical:vector="Victim secure area"

Victim high security area (e.g., server room, R&D labs)

veris:action:physical:vector="Victim work area"

Victim private or work area (e.g., office space)

veris:action:physical:vector="Visitor privileges"

Given temporary visitor access

action:social:result

veris:action:social:result="Elevate"

The social action resulted in additional permissions

veris:action:social:result="Exfiltrate"

The social action exfiltrated data from the victim

veris:action:social:result="Infiltrate"

The social action infiltrated the victim

action:social:target

veris:action:social:target="Auditor"

Auditor

veris:action:social:target="Call center"

Call center staff

veris:action:social:target="Cashier"

Cashier, teller or waiter

veris:action:social:target="Customer"

Customer (B2C)

veris:action:social:target="Developer"

Software developer

veris:action:social:target="End-user"

End-user or regular employee

veris:action:social:target="Executive"

Executive or upper management

veris:action:social:target="Finance"

Finance or accounting staff

veris:action:social:target="Former employee"

Former employee

veris:action:social:target="Guard"

Security guard

veris:action:social:target="Helpdesk"

Helpdesk staff

veris:action:social:target="Human resources"

Human resources staff

veris:action:social:target="Maintenance"

Maintenance or janitorial staff

veris:action:social:target="Manager"

Manager or supervisor

veris:action:social:target="Other"

Other

veris:action:social:target="Partner"

Partner (B2B)

veris:action:social:target="System admin"

System or network administrator

veris:action:social:target="Unknown"

Unknown

action:social:variety

veris:action:social:variety="Baiting"

Baiting (planting infected media)

veris:action:social:variety="Bribery"

Bribery or solicitation

veris:action:social:variety="Elicitation"

Elicitation (subtle extraction of info through conversation)

veris:action:social:variety="Extortion"

Extortion or blackmail

veris:action:social:variety="Forgery"

Forgery or counterfeiting (fake hardware, software, documents, etc)

veris:action:social:variety="Influence"

Influence tactics (Leveraging authority or obligation, framing, etc)

veris:action:social:variety="Other"

Other

veris:action:social:variety="Phishing"

Phishing (or any type of *ishing)

veris:action:social:variety="Pretexting"

Pretexting (dialogue leveraging invented scenario)

veris:action:social:variety="Propaganda"

Propaganda or disinformation

veris:action:social:variety="Scam"

Online scam or hoax (e.g., scareware, 419 scam, auction fraud)

veris:action:social:variety="Spam"

Spam (unsolicited or undesired email and advertisements)

veris:action:social:variety="Unknown"

Unknown

action:social:vector

veris:action:social:vector="Documents"

Documents

veris:action:social:vector="Email"

Email

veris:action:social:vector="IM"

Instant messaging

veris:action:social:vector="In-person"

In-person

veris:action:social:vector="Other"

Other

veris:action:social:vector="Phone"

Phone

veris:action:social:vector="Removable media"

Removable storage media

veris:action:social:vector="SMS"

SMS or texting

veris:action:social:vector="Social media"

Social media or networking

veris:action:social:vector="Software"

Software

veris:action:social:vector="Unknown"

Unknown

veris:action:social:vector="Website"

Website

action:unknown:result

veris:action:unknown:result="Elevate"

The hacking action resulted in additional permissions

veris:action:unknown:result="Exfiltrate"

The hacking action exfiltrated data from the victim

veris:action:unknown:result="Infiltrate"

The hacking action infiltrated the victim

actor:external:country

veris:actor:external:country="AD"

Andorra

veris:actor:external:country="AE"

United Arab Emirates

veris:actor:external:country="AF"

Afghanistan

veris:actor:external:country="AG"

Antigua and Barbuda

veris:actor:external:country="AI"

Anguilla

veris:actor:external:country="AL"

Albania

veris:actor:external:country="AM"

Armenia

veris:actor:external:country="AO"

Angola

veris:actor:external:country="AQ"

Antarctica

veris:actor:external:country="AR"

Argentina

veris:actor:external:country="AS"

American Samoa

veris:actor:external:country="AT"

Austria

veris:actor:external:country="AU"

Australia

veris:actor:external:country="AW"

Aruba

veris:actor:external:country="AX"

Aland Islands

veris:actor:external:country="AZ"

Azerbaijan

veris:actor:external:country="BA"

Bosnia and Herzegovina

veris:actor:external:country="BB"

Barbados

veris:actor:external:country="BD"

Bangladesh

veris:actor:external:country="BE"

Belgium

veris:actor:external:country="BF"

Burkina Faso

veris:actor:external:country="BG"

Bulgaria

veris:actor:external:country="BH"

Bahrain

veris:actor:external:country="BI"

Burundi

veris:actor:external:country="BJ"

Benin

veris:actor:external:country="BL"

Saint-Barthelemy

veris:actor:external:country="BM"

Bermuda

veris:actor:external:country="BN"

Brunei Darussalam

veris:actor:external:country="BO"

Bolivia

veris:actor:external:country="BQ"

Bonaire, Saint Eustatius and Saba

veris:actor:external:country="BR"

Brazil

veris:actor:external:country="BS"

Bahamas

veris:actor:external:country="BT"

Bhutan

veris:actor:external:country="BV"

Bouvet Island

veris:actor:external:country="BW"

Botswana

veris:actor:external:country="BY"

Belarus

veris:actor:external:country="BZ"

Belize

veris:actor:external:country="CA"

Canada

veris:actor:external:country="CC"

Cocos (Keeling) Islands

veris:actor:external:country="CD"

Congo, Democratic Republic of the

veris:actor:external:country="CF"

Central African Republic

veris:actor:external:country="CG"

Congo

veris:actor:external:country="CH"

Switzerland

veris:actor:external:country="CI"

Cote d’Ivoire

veris:actor:external:country="CK"

Cook Islands

veris:actor:external:country="CL"

Chile

veris:actor:external:country="CM"

Cameroon

veris:actor:external:country="CN"

China

veris:actor:external:country="CO"

Colombia

veris:actor:external:country="CR"

Costa Rica

veris:actor:external:country="CU"

Cuba

veris:actor:external:country="CV"

Cape Verde

veris:actor:external:country="CW"

Curacao

veris:actor:external:country="CX"

Christmas Island

veris:actor:external:country="CY"

Cyprus

veris:actor:external:country="CZ"

Czech Republic

veris:actor:external:country="DE"

Germany

veris:actor:external:country="DJ"

Djibouti

veris:actor:external:country="DK"

Denmark

veris:actor:external:country="DM"

Dominica

veris:actor:external:country="DO"

Dominican Republic

veris:actor:external:country="DZ"

Algeria

veris:actor:external:country="EC"

Ecuador

veris:actor:external:country="EE"

Estonia

veris:actor:external:country="EG"

Egypt

veris:actor:external:country="EH"

Western Sahara

veris:actor:external:country="ER"

Eritrea

veris:actor:external:country="ES"

Spain

veris:actor:external:country="ET"

Ethiopia

veris:actor:external:country="FI"

Finland

veris:actor:external:country="FJ"

Fiji

veris:actor:external:country="FK"

Faeroe Islands

veris:actor:external:country="FM"

Micronesia (Federated States of)

veris:actor:external:country="FO"

Falkland Islands (Malvinas)

veris:actor:external:country="FR"

France

veris:actor:external:country="GA"

Gabon

veris:actor:external:country="GB"

United Kingdom

veris:actor:external:country="GD"

Grenada

veris:actor:external:country="GE"

Georgia

veris:actor:external:country="GF"

French Guiana

veris:actor:external:country="GG"

Guernsey

veris:actor:external:country="GH"

Ghana

veris:actor:external:country="GI"

Gibraltar

veris:actor:external:country="GL"

Greenland

veris:actor:external:country="GM"

Gambia

veris:actor:external:country="GN"

Guinea

veris:actor:external:country="GP"

Guadeloupe

veris:actor:external:country="GQ"

Equatorial Guinea

veris:actor:external:country="GR"

Greece

veris:actor:external:country="GS"

South Georgia and the South Sandwich Islands

veris:actor:external:country="GT"

Guatemala

veris:actor:external:country="GU"

Guam

veris:actor:external:country="GW"

Guinea-Bissau

veris:actor:external:country="GY"

Guyana

veris:actor:external:country="HK"

Hong Kong

veris:actor:external:country="HM"

Heard Island and McDonal Islands

veris:actor:external:country="HN"

Honduras

veris:actor:external:country="HR"

Croatia

veris:actor:external:country="HT"

Haiti

veris:actor:external:country="HU"

Hungary

veris:actor:external:country="ID"

Indonesia

veris:actor:external:country="IE"

Ireland

veris:actor:external:country="IL"

Israel

veris:actor:external:country="IM"

Isle of Man

veris:actor:external:country="IN"

India

veris:actor:external:country="IO"

British Virgin Islands

veris:actor:external:country="IQ"

Iraq

veris:actor:external:country="IR"

Iran (Islamic Republic of)

veris:actor:external:country="IS"

Iceland

veris:actor:external:country="IT"

Italy

veris:actor:external:country="JE"

Jersey

veris:actor:external:country="JM"

Jamaica

veris:actor:external:country="JO"

Jordan

veris:actor:external:country="JP"

Japan

veris:actor:external:country="KE"

Kenya

veris:actor:external:country="KG"

Kyrgyzstan

veris:actor:external:country="KH"

Cambodia

veris:actor:external:country="KI"

Kiribati

veris:actor:external:country="KM"

Comoros

veris:actor:external:country="KN"

Saint Kitts and Nevis

veris:actor:external:country="KP"

Korea, Democratic People’s Republic of

veris:actor:external:country="KR"

Korea, Republic of

veris:actor:external:country="KW"

Kuwait

veris:actor:external:country="KY"

Cayman Islands

veris:actor:external:country="KZ"

Kazakhstan

veris:actor:external:country="LA"

Lao People’s Democratic Republic

veris:actor:external:country="LB"

Lebanon

veris:actor:external:country="LC"

Saint Lucia

veris:actor:external:country="LI"

Liechtenstein

veris:actor:external:country="LK"

Sri Lanka

veris:actor:external:country="LR"

Liberia

veris:actor:external:country="LS"

Lesotho

veris:actor:external:country="LT"

Lithuania

veris:actor:external:country="LU"

Luxembourg

veris:actor:external:country="LV"

Latvia

veris:actor:external:country="LY"

Libya

veris:actor:external:country="MA"

Morocco

veris:actor:external:country="MC"

Monaco

veris:actor:external:country="MD"

Moldova, Republic of

veris:actor:external:country="ME"

Montenegro

veris:actor:external:country="MF"

Saint Martin (French part)

veris:actor:external:country="MG"

Madagascar

veris:actor:external:country="MH"

Marshall Islands

veris:actor:external:country="MK"

Macedonia, The former Yugoslav Republic of

veris:actor:external:country="ML"

Mali

veris:actor:external:country="MM"

Myanmar

veris:actor:external:country="MN"

Mongolia

veris:actor:external:country="MO"

Macao

veris:actor:external:country="MP"

Northern Mariana Islands

veris:actor:external:country="MQ"

Martinique

veris:actor:external:country="MR"

Mauritania

veris:actor:external:country="MS"

Montserrat

veris:actor:external:country="MT"

Malta

veris:actor:external:country="MU"

Mauritius

veris:actor:external:country="MV"

Maldives

veris:actor:external:country="MW"

Malawi

veris:actor:external:country="MX"

Mexico

veris:actor:external:country="MY"

Malaysia

veris:actor:external:country="MZ"

Mozambique

veris:actor:external:country="NA"

Namibia

veris:actor:external:country="NC"

New Caledonia

veris:actor:external:country="NE"

Niger

veris:actor:external:country="NF"

Norfolk Island

veris:actor:external:country="NG"

Nigeria

veris:actor:external:country="NI"

Nicaragua

veris:actor:external:country="NL"

Netherlands

veris:actor:external:country="NO"

Norway

veris:actor:external:country="NP"

Nepal

veris:actor:external:country="NR"

Nauru

veris:actor:external:country="NU"

Niue

veris:actor:external:country="NZ"

New Zealand

veris:actor:external:country="OM"

Oman

veris:actor:external:country="Other"

Other

veris:actor:external:country="PA"

Panama

veris:actor:external:country="PE"

Peru

veris:actor:external:country="PF"

French Polynesia

veris:actor:external:country="PG"

Papua New Guinea

veris:actor:external:country="PH"

Philippines

veris:actor:external:country="PK"

Pakistan

veris:actor:external:country="PL"

Poland

veris:actor:external:country="PM"

Saint Pierre and Miquelon

veris:actor:external:country="PN"

Pitcairn

veris:actor:external:country="PR"

Puerto Rico

veris:actor:external:country="PS"

Palestinian Territory, Occupied

veris:actor:external:country="PT"

Portugal

veris:actor:external:country="PW"

Palau

veris:actor:external:country="PY"

Paraguay

veris:actor:external:country="QA"

Qatar

veris:actor:external:country="RE"

Reunion

veris:actor:external:country="RO"

Romania

veris:actor:external:country="RS"

Serbia

veris:actor:external:country="RU"

Russian Federation

veris:actor:external:country="RW"

Rwanda

veris:actor:external:country="SA"

Saudi Arabia

veris:actor:external:country="SB"

Solomon Islands

veris:actor:external:country="SC"

Seychelles

veris:actor:external:country="SD"

Sudan

veris:actor:external:country="SE"

Sweden

veris:actor:external:country="SG"

Singapore

veris:actor:external:country="SH"

Saint Helena

veris:actor:external:country="SI"

Slovenia

veris:actor:external:country="SJ"

Svalbard and Jan Mayen Islands

veris:actor:external:country="SK"

Slovakia

veris:actor:external:country="SL"

Sierra Leone

veris:actor:external:country="SM"

San Marino

veris:actor:external:country="SN"

Senegal

veris:actor:external:country="SO"

Somalia

veris:actor:external:country="SR"

Suriname

veris:actor:external:country="SS"

South Sudan

veris:actor:external:country="ST"

Sao Tome and Principe

veris:actor:external:country="SV"

El Salvador

veris:actor:external:country="SX"

Sint Maarten (Dutch part)

veris:actor:external:country="SY"

Syrian Arab Republic

veris:actor:external:country="SZ"

Swaziland

veris:actor:external:country="TC"

Turks and Caicos Islands

veris:actor:external:country="TD"

Chad

veris:actor:external:country="TF"

French Southern Territories

veris:actor:external:country="TG"

Togo

veris:actor:external:country="TH"

Thailand

veris:actor:external:country="TJ"

Tajikistan

veris:actor:external:country="TK"

Tokelau

veris:actor:external:country="TL"

Timor-Leste

veris:actor:external:country="TM"

Turkmenistan

veris:actor:external:country="TN"

Tunisia

veris:actor:external:country="TO"

Tonga

veris:actor:external:country="TR"

Turkey

veris:actor:external:country="TT"

Trinidad and Tobago

veris:actor:external:country="TV"

Tuvalu

veris:actor:external:country="TW"

Taiwan, Province of China

veris:actor:external:country="TZ"

Tanzania, United Republic of

veris:actor:external:country="UA"

Ukraine

veris:actor:external:country="UG"

Uganda

veris:actor:external:country="UM"

United States Minor Outlying Islands

veris:actor:external:country="US"

United States of America

veris:actor:external:country="UY"

Uruguay

veris:actor:external:country="UZ"

Uzbekistan

veris:actor:external:country="Unknown"

Unknown

veris:actor:external:country="VA"

Holy See

veris:actor:external:country="VC"

Saint Vincent and the Grenadines

veris:actor:external:country="VE"

Venezuela (Bolivarian Republic of)

veris:actor:external:country="VG"

British Virgin Islands

veris:actor:external:country="VI"

United States Virgin Islands

veris:actor:external:country="VN"

Viet Nam

veris:actor:external:country="VU"

Vanuatu

veris:actor:external:country="WF"

Wallis and Futuna Islands

veris:actor:external:country="WS"

Samoa

veris:actor:external:country="YE"

Yemen

veris:actor:external:country="YT"

Mayotte

veris:actor:external:country="ZA"

South Africa

veris:actor:external:country="ZM"

Zambia

veris:actor:external:country="ZW"

Zimbabwe

actor:external:motive

veris:actor:external:motive="Convenience"

Convenience of expediency

veris:actor:external:motive="Espionage"

Espionage or competitive advantage

veris:actor:external:motive="Fear"

Fear or duress

veris:actor:external:motive="Financial"

Financial or personal gain

veris:actor:external:motive="Fun"

Fun, curiosity, or pride

veris:actor:external:motive="Grudge"

Grudge or personal offense

veris:actor:external:motive="Ideology"

Ideology or protest

veris:actor:external:motive="NA"

Not Applicable (unintentional action)

veris:actor:external:motive="Other"

Other

veris:actor:external:motive="Secondary"

Aid in a different attack

veris:actor:external:motive="Unknown"

Unknown

actor:external:variety

veris:actor:external:variety="Acquaintance"

Relative or acquaintance of employee

veris:actor:external:variety="Activist"

Activist group

veris:actor:external:variety="Auditor"

Auditor

veris:actor:external:variety="Competitor"

Competitor

veris:actor:external:variety="Customer"

Customer (B2C)

veris:actor:external:variety="Force majeure"

Force majeure (nature and chance)

veris:actor:external:variety="Former employee"

Former employee (no longer had access)

veris:actor:external:variety="Nation-state"

Nation-state

veris:actor:external:variety="Organized crime"

Organized or professional criminal group

veris:actor:external:variety="Other"

Other

veris:actor:external:variety="State-affiliated"

State-sponsored or affiliated group

veris:actor:external:variety="Terrorist"

Terrorist group

veris:actor:external:variety="Unaffiliated"

Unaffiliated person(s)

veris:actor:external:variety="Unknown"

Unknown

actor:internal:job_change

veris:actor:internal:job_change="Demoted"

Recently demoted or hours reduced

veris:actor:internal:job_change="Hired"

Recently hired

veris:actor:internal:job_change="Job eval"

Recent poor job evaluation

veris:actor:internal:job_change="Lateral move"

Lateral move

veris:actor:internal:job_change="Let go"

Fired, laid off, or let go

veris:actor:internal:job_change="Other"

Other

veris:actor:internal:job_change="Passed over"

Recently passed over for promotion

veris:actor:internal:job_change="Personal issues"

Personal issues

veris:actor:internal:job_change="Promoted"

Recently promoted

veris:actor:internal:job_change="Reprimanded"

Recently reprimanded

veris:actor:internal:job_change="Resigned"

Preparing to resign or recently resigned

veris:actor:internal:job_change="Unknown"

Unknown

actor:internal:motive

veris:actor:internal:motive="Convenience"

Convenience of expediency

veris:actor:internal:motive="Espionage"

Espionage or competitive advantage

veris:actor:internal:motive="Fear"

Fear or duress

veris:actor:internal:motive="Financial"

Financial or personal gain

veris:actor:internal:motive="Fun"

Fun, curiosity, or pride

veris:actor:internal:motive="Grudge"

Grudge or personal offense

veris:actor:internal:motive="Ideology"

Ideology or protest

veris:actor:internal:motive="NA"

Not Applicable (unintentional action)

veris:actor:internal:motive="Other"

Other

veris:actor:internal:motive="Secondary"

Aid in a different attack

veris:actor:internal:motive="Unknown"

Unknown

actor:internal:variety

veris:actor:internal:variety="Auditor"

Auditor

veris:actor:internal:variety="Call center"

Call center staff

veris:actor:internal:variety="Cashier"

Cashier, teller, or waiter

veris:actor:internal:variety="Developer"

Software developer

veris:actor:internal:variety="Doctor or nurse"

A doctor or a nurse

veris:actor:internal:variety="End-user"

End-user or regular employee

veris:actor:internal:variety="Executive"

Executive or upper management

veris:actor:internal:variety="Finance"

Finance or accounting staff

veris:actor:internal:variety="Guard"

Security guard

veris:actor:internal:variety="Helpdesk"

Helpdesk staff

veris:actor:internal:variety="Human resources"

Human resources staff

veris:actor:internal:variety="Maintenance"

Maintenance or janitorial staff

veris:actor:internal:variety="Manager"

Manager or supervisor

veris:actor:internal:variety="Other"

Other

veris:actor:internal:variety="System admin"

System or network administrator

veris:actor:internal:variety="Unknown"

Unknown

actor:partner:country

veris:actor:partner:country="AD"

Andorra

veris:actor:partner:country="AE"

United Arab Emirates

veris:actor:partner:country="AF"

Afghanistan

veris:actor:partner:country="AG"

Antigua and Barbuda

veris:actor:partner:country="AI"

Anguilla

veris:actor:partner:country="AL"

Albania

veris:actor:partner:country="AM"

Armenia

veris:actor:partner:country="AO"

Angola

veris:actor:partner:country="AQ"

Antarctica

veris:actor:partner:country="AR"

Argentina

veris:actor:partner:country="AS"

American Samoa

veris:actor:partner:country="AT"

Austria

veris:actor:partner:country="AU"

Australia

veris:actor:partner:country="AW"

Aruba

veris:actor:partner:country="AX"

Aland Islands

veris:actor:partner:country="AZ"

Azerbaijan

veris:actor:partner:country="BA"

Bosnia and Herzegovina

veris:actor:partner:country="BB"

Barbados

veris:actor:partner:country="BD"

Bangladesh

veris:actor:partner:country="BE"

Belgium

veris:actor:partner:country="BF"

Burkina Faso

veris:actor:partner:country="BG"

Bulgaria

veris:actor:partner:country="BH"

Bahrain

veris:actor:partner:country="BI"

Burundi

veris:actor:partner:country="BJ"

Benin

veris:actor:partner:country="BL"

Saint-Barthelemy

veris:actor:partner:country="BM"

Bermuda

veris:actor:partner:country="BN"

Brunei Darussalam

veris:actor:partner:country="BO"

Bolivia

veris:actor:partner:country="BQ"

Bonaire, Saint Eustatius and Saba

veris:actor:partner:country="BR"

Brazil

veris:actor:partner:country="BS"

Bahamas

veris:actor:partner:country="BT"

Bhutan

veris:actor:partner:country="BV"

Bouvet Island

veris:actor:partner:country="BW"

Botswana

veris:actor:partner:country="BY"

Belarus

veris:actor:partner:country="BZ"

Belize

veris:actor:partner:country="CA"

Canada

veris:actor:partner:country="CC"

Cocos (Keeling) Islands

veris:actor:partner:country="CD"

Congo, Democratic Republic of the

veris:actor:partner:country="CF"

Central African Republic

veris:actor:partner:country="CG"

Congo

veris:actor:partner:country="CH"

Switzerland

veris:actor:partner:country="CI"

Cote d’Ivoire

veris:actor:partner:country="CK"

Cook Islands

veris:actor:partner:country="CL"

Chile

veris:actor:partner:country="CM"

Cameroon

veris:actor:partner:country="CN"

China

veris:actor:partner:country="CO"

Colombia

veris:actor:partner:country="CR"

Costa Rica

veris:actor:partner:country="CU"

Cuba

veris:actor:partner:country="CV"

Cape Verde

veris:actor:partner:country="CW"

Curacao

veris:actor:partner:country="CX"

Christmas Island

veris:actor:partner:country="CY"

Cyprus

veris:actor:partner:country="CZ"

Czech Republic

veris:actor:partner:country="DE"

Germany

veris:actor:partner:country="DJ"

Djibouti

veris:actor:partner:country="DK"

Denmark

veris:actor:partner:country="DM"

Dominica

veris:actor:partner:country="DO"

Dominican Republic

veris:actor:partner:country="DZ"

Algeria

veris:actor:partner:country="EC"

Ecuador

veris:actor:partner:country="EE"

Estonia

veris:actor:partner:country="EG"

Egypt

veris:actor:partner:country="EH"

Western Sahara

veris:actor:partner:country="ER"

Eritrea

veris:actor:partner:country="ES"

Spain

veris:actor:partner:country="ET"

Ethiopia

veris:actor:partner:country="FI"

Finland

veris:actor:partner:country="FJ"

Fiji

veris:actor:partner:country="FK"

Faeroe Islands

veris:actor:partner:country="FM"

Micronesia (Federated States of)

veris:actor:partner:country="FO"

Falkland Islands (Malvinas)

veris:actor:partner:country="FR"

France

veris:actor:partner:country="GA"

Gabon

veris:actor:partner:country="GB"

United Kingdom

veris:actor:partner:country="GD"

Grenada

veris:actor:partner:country="GE"

Georgia

veris:actor:partner:country="GF"

French Guiana

veris:actor:partner:country="GG"

Guernsey

veris:actor:partner:country="GH"

Ghana

veris:actor:partner:country="GI"

Gibraltar

veris:actor:partner:country="GL"

Greenland

veris:actor:partner:country="GM"

Gambia

veris:actor:partner:country="GN"

Guinea

veris:actor:partner:country="GP"

Guadeloupe

veris:actor:partner:country="GQ"

Equatorial Guinea

veris:actor:partner:country="GR"

Greece

veris:actor:partner:country="GS"

South Georgia and the South Sandwich Islands

veris:actor:partner:country="GT"

Guatemala

veris:actor:partner:country="GU"

Guam

veris:actor:partner:country="GW"

Guinea-Bissau

veris:actor:partner:country="GY"

Guyana

veris:actor:partner:country="HK"

Hong Kong

veris:actor:partner:country="HM"

Heard Island and McDonal Islands

veris:actor:partner:country="HN"

Honduras

veris:actor:partner:country="HR"

Croatia

veris:actor:partner:country="HT"

Haiti

veris:actor:partner:country="HU"

Hungary

veris:actor:partner:country="ID"

Indonesia

veris:actor:partner:country="IE"

Ireland

veris:actor:partner:country="IL"

Israel

veris:actor:partner:country="IM"

Isle of Man

veris:actor:partner:country="IN"

India

veris:actor:partner:country="IO"

British Virgin Islands

veris:actor:partner:country="IQ"

Iraq

veris:actor:partner:country="IR"

Iran (Islamic Republic of)

veris:actor:partner:country="IS"

Iceland

veris:actor:partner:country="IT"

Italy

veris:actor:partner:country="JE"

Jersey

veris:actor:partner:country="JM"

Jamaica

veris:actor:partner:country="JO"

Jordan

veris:actor:partner:country="JP"

Japan

veris:actor:partner:country="KE"

Kenya

veris:actor:partner:country="KG"

Kyrgyzstan

veris:actor:partner:country="KH"

Cambodia

veris:actor:partner:country="KI"

Kiribati

veris:actor:partner:country="KM"

Comoros

veris:actor:partner:country="KN"

Saint Kitts and Nevis

veris:actor:partner:country="KP"

Korea, Democratic People’s Republic of

veris:actor:partner:country="KR"

Korea, Republic of

veris:actor:partner:country="KW"

Kuwait

veris:actor:partner:country="KY"

Cayman Islands

veris:actor:partner:country="KZ"

Kazakhstan

veris:actor:partner:country="LA"

Lao People’s Democratic Republic

veris:actor:partner:country="LB"

Lebanon

veris:actor:partner:country="LC"

Saint Lucia

veris:actor:partner:country="LI"

Liechtenstein

veris:actor:partner:country="LK"

Sri Lanka

veris:actor:partner:country="LR"

Liberia

veris:actor:partner:country="LS"

Lesotho

veris:actor:partner:country="LT"

Lithuania

veris:actor:partner:country="LU"

Luxembourg

veris:actor:partner:country="LV"

Latvia

veris:actor:partner:country="LY"

Libya

veris:actor:partner:country="MA"

Morocco

veris:actor:partner:country="MC"

Monaco

veris:actor:partner:country="MD"

Moldova, Republic of

veris:actor:partner:country="ME"

Montenegro

veris:actor:partner:country="MF"

Saint Martin (French part)

veris:actor:partner:country="MG"

Madagascar

veris:actor:partner:country="MH"

Marshall Islands

veris:actor:partner:country="MK"

Macedonia, The former Yugoslav Republic of

veris:actor:partner:country="ML"

Mali

veris:actor:partner:country="MM"

Myanmar

veris:actor:partner:country="MN"

Mongolia

veris:actor:partner:country="MO"

Macao

veris:actor:partner:country="MP"

Northern Mariana Islands

veris:actor:partner:country="MQ"

Martinique

veris:actor:partner:country="MR"

Mauritania

veris:actor:partner:country="MS"

Montserrat

veris:actor:partner:country="MT"

Malta

veris:actor:partner:country="MU"

Mauritius

veris:actor:partner:country="MV"

Maldives

veris:actor:partner:country="MW"

Malawi

veris:actor:partner:country="MX"

Mexico

veris:actor:partner:country="MY"

Malaysia

veris:actor:partner:country="MZ"

Mozambique

veris:actor:partner:country="NA"

Namibia

veris:actor:partner:country="NC"

New Caledonia

veris:actor:partner:country="NE"

Niger

veris:actor:partner:country="NF"

Norfolk Island

veris:actor:partner:country="NG"

Nigeria

veris:actor:partner:country="NI"

Nicaragua

veris:actor:partner:country="NL"

Netherlands

veris:actor:partner:country="NO"

Norway

veris:actor:partner:country="NP"

Nepal

veris:actor:partner:country="NR"

Nauru

veris:actor:partner:country="NU"

Niue

veris:actor:partner:country="NZ"

New Zealand

veris:actor:partner:country="OM"

Oman

veris:actor:partner:country="Other"

Other

veris:actor:partner:country="PA"

Panama

veris:actor:partner:country="PE"

Peru

veris:actor:partner:country="PF"

French Polynesia

veris:actor:partner:country="PG"

Papua New Guinea

veris:actor:partner:country="PH"

Philippines

veris:actor:partner:country="PK"

Pakistan

veris:actor:partner:country="PL"

Poland

veris:actor:partner:country="PM"

Saint Pierre and Miquelon

veris:actor:partner:country="PN"

Pitcairn

veris:actor:partner:country="PR"

Puerto Rico

veris:actor:partner:country="PS"

Palestinian Territory, Occupied

veris:actor:partner:country="PT"

Portugal

veris:actor:partner:country="PW"

Palau

veris:actor:partner:country="PY"

Paraguay

veris:actor:partner:country="QA"

Qatar

veris:actor:partner:country="RE"

Reunion

veris:actor:partner:country="RO"

Romania

veris:actor:partner:country="RS"

Serbia

veris:actor:partner:country="RU"

Russian Federation

veris:actor:partner:country="RW"

Rwanda

veris:actor:partner:country="SA"

Saudi Arabia

veris:actor:partner:country="SB"

Solomon Islands

veris:actor:partner:country="SC"

Seychelles

veris:actor:partner:country="SD"

Sudan

veris:actor:partner:country="SE"

Sweden

veris:actor:partner:country="SG"

Singapore

veris:actor:partner:country="SH"

Saint Helena

veris:actor:partner:country="SI"

Slovenia

veris:actor:partner:country="SJ"

Svalbard and Jan Mayen Islands

veris:actor:partner:country="SK"

Slovakia

veris:actor:partner:country="SL"

Sierra Leone

veris:actor:partner:country="SM"

San Marino

veris:actor:partner:country="SN"

Senegal

veris:actor:partner:country="SO"

Somalia

veris:actor:partner:country="SR"

Suriname

veris:actor:partner:country="SS"

South Sudan

veris:actor:partner:country="ST"

Sao Tome and Principe

veris:actor:partner:country="SV"

El Salvador

veris:actor:partner:country="SX"

Sint Maarten (Dutch part)

veris:actor:partner:country="SY"

Syrian Arab Republic

veris:actor:partner:country="SZ"

Swaziland

veris:actor:partner:country="TC"

Turks and Caicos Islands

veris:actor:partner:country="TD"

Chad

veris:actor:partner:country="TF"

French Southern Territories

veris:actor:partner:country="TG"

Togo

veris:actor:partner:country="TH"

Thailand

veris:actor:partner:country="TJ"

Tajikistan

veris:actor:partner:country="TK"

Tokelau

veris:actor:partner:country="TL"

Timor-Leste

veris:actor:partner:country="TM"

Turkmenistan

veris:actor:partner:country="TN"

Tunisia

veris:actor:partner:country="TO"

Tonga

veris:actor:partner:country="TR"

Turkey

veris:actor:partner:country="TT"

Trinidad and Tobago

veris:actor:partner:country="TV"

Tuvalu

veris:actor:partner:country="TW"

Taiwan, Province of China

veris:actor:partner:country="TZ"

Tanzania, United Republic of

veris:actor:partner:country="UA"

Ukraine

veris:actor:partner:country="UG"

Uganda

veris:actor:partner:country="UM"

United States Minor Outlying Islands

veris:actor:partner:country="US"

United States of America

veris:actor:partner:country="UY"

Uruguay

veris:actor:partner:country="UZ"

Uzbekistan

veris:actor:partner:country="Unknown"

Unknown

veris:actor:partner:country="VA"

Holy See

veris:actor:partner:country="VC"

Saint Vincent and the Grenadines

veris:actor:partner:country="VE"

Venezuela (Bolivarian Republic of)

veris:actor:partner:country="VG"

British Virgin Islands

veris:actor:partner:country="VI"

United States Virgin Islands

veris:actor:partner:country="VN"

Viet Nam

veris:actor:partner:country="VU"

Vanuatu

veris:actor:partner:country="WF"

Wallis and Futuna Islands

veris:actor:partner:country="WS"

Samoa

veris:actor:partner:country="YE"

Yemen

veris:actor:partner:country="YT"

Mayotte

veris:actor:partner:country="ZA"

South Africa

veris:actor:partner:country="ZM"

Zambia

veris:actor:partner:country="ZW"

Zimbabwe

actor:partner:motive

veris:actor:partner:motive="Convenience"

Convenience of expediency

veris:actor:partner:motive="Espionage"

Espionage or competitive advantage

veris:actor:partner:motive="Fear"

Fear or duress

veris:actor:partner:motive="Financial"

Financial or personal gain

veris:actor:partner:motive="Fun"

Fun, curiosity, or pride

veris:actor:partner:motive="Grudge"

Grudge or personal offense

veris:actor:partner:motive="Ideology"

Ideology or protest

veris:actor:partner:motive="NA"

Not Applicable (unintentional action)

veris:actor:partner:motive="Other"

Other

veris:actor:partner:motive="Secondary"

Aid in a different attack

veris:actor:partner:motive="Unknown"

Unknown

asset:assets:variety

veris:asset:assets:variety="E - Other"

Embedded - Variety known but not listed

veris:asset:assets:variety="E - Telematics"

Embedded - A dedicated device that affects the real world

veris:asset:assets:variety="E - Telemetry"

Embedded - A dedicated device that collects data about the physical world

veris:asset:assets:variety="E - Unknown"

Embedded - Variety not known

veris:asset:assets:variety="M - Disk drive"

Media - Hard disk drive

veris:asset:assets:variety="M - Disk media"

Media - Disk media (e.g., CDs, DVDs)

veris:asset:assets:variety="M - Documents"

Media - Documents

veris:asset:assets:variety="M - Fax"

Media - The output of a fax machine

veris:asset:assets:variety="M - Flash drive"

Media - Flash drive or card

veris:asset:assets:variety="M - Other"

Media - Variety known but not listed

veris:asset:assets:variety="M - Payment card"

Media - Payment card (e.g., magstripe, EMV)

veris:asset:assets:variety="M - Smart card"

Media - Identity smart card

veris:asset:assets:variety="M - Tapes"

Media - Backup tapes

veris:asset:assets:variety="M - Unknown"

Media - Variety not known

veris:asset:assets:variety="N - Access reader"

Network - Access control reader (e.g., badge, biometric)

veris:asset:assets:variety="N - Broadband"

Network - Mobile broadband network

veris:asset:assets:variety="N - Camera"

Network - Camera or surveillance system

veris:asset:assets:variety="N - Firewall"

Network - Firewall

veris:asset:assets:variety="N - HSM"

Network - Hardware security module (HSM)

veris:asset:assets:variety="N - IDS"

Network - IDS or IPs

veris:asset:assets:variety="N - LAN"

Network - Wired LAN

veris:asset:assets:variety="N - NAS"

Network - Network area storage (NAS)

veris:asset:assets:variety="N - Other"

Network - Variety known but not listed

veris:asset:assets:variety="N - PBX"

Network - Private branch exchange (PBX)

veris:asset:assets:variety="N - PLC"

Network - Programmable logic controller (PLC)

veris:asset:assets:variety="N - Private WAN"

Network - Private WAN

veris:asset:assets:variety="N - Public WAN"

Network - Public WAN

veris:asset:assets:variety="N - RTU"

Network - Remote terminal unit (RTU)

veris:asset:assets:variety="N - Router or switch"

Network - Router or switch

veris:asset:assets:variety="N - SAN"

Network - Storage area network (SAN)

veris:asset:assets:variety="N - Telephone"

Network - Telephone

veris:asset:assets:variety="N - Unknown"

Network - Variety not known

veris:asset:assets:variety="N - VoIP adapter"

Network - VoIP adapter

veris:asset:assets:variety="N - WLAN"

Network - Wireless LAN

veris:asset:assets:variety="Other"

Asset type known but not User Device, Server, Public Terminal, Server, People, Network, or Media

veris:asset:assets:variety="P - Auditor"

People - Auditor

veris:asset:assets:variety="P - Call center"

People - Call center

veris:asset:assets:variety="P - Cashier"

People - Cashier

veris:asset:assets:variety="P - Customer"

People - Customer

veris:asset:assets:variety="P - Developer"

People - Developer

veris:asset:assets:variety="P - End-user"

People - End-user

veris:asset:assets:variety="P - Executive"

People - Executive

veris:asset:assets:variety="P - Finance"

People - Finance

veris:asset:assets:variety="P - Former employee"

People - Former employee

veris:asset:assets:variety="P - Guard"

People - Guard

veris:asset:assets:variety="P - Helpdesk"

People - Helpdesk

veris:asset:assets:variety="P - Human resources"

People - Human resources

veris:asset:assets:variety="P - Maintenance"

People - Maintenance

veris:asset:assets:variety="P - Manager"

People - Manager

veris:asset:assets:variety="P - Other"

People - Variety known but not listed

veris:asset:assets:variety="P - Partner"

People - Partner

veris:asset:assets:variety="P - System admin"

People - Administrator

veris:asset:assets:variety="P - Unknown"

People - Variety not known

veris:asset:assets:variety="S - Authentication"

Server - Authentication

veris:asset:assets:variety="S - Backup"

Server - Backup

veris:asset:assets:variety="S - Code repository"

Server - Code repository

veris:asset:assets:variety="S - Configuration or patch management"

Servers maintaining or deploying configurations or patches to other assets

veris:asset:assets:variety="S - DCS"

Server - Distributed control system (DCS)

veris:asset:assets:variety="S - DHCP"

Server - DHCP

veris:asset:assets:variety="S - DNS"

Server - DNS

veris:asset:assets:variety="S - Database"

Server - Database

veris:asset:assets:variety="S - Directory"

Server - Directory (LDAP, AD)

veris:asset:assets:variety="S - File"

Server - File

veris:asset:assets:variety="S - ICS"

Server - Industrial Control System (ICS). Includes Supervisory Control And Data Acquisition (SCADA) systems.

veris:asset:assets:variety="S - Log"

Server - Log or event management

veris:asset:assets:variety="S - Mail"

Server - Mail

veris:asset:assets:variety="S - Mainframe"

Server - Mainframe

veris:asset:assets:variety="S - Other"

Server - Variety known but not listed

veris:asset:assets:variety="S - POS controller"

Server - POS controller

veris:asset:assets:variety="S - Payment switch"

Server - Payment switch or gateway

veris:asset:assets:variety="S - Print"

Server - Print

veris:asset:assets:variety="S - Proxy"

Server - Proxy

veris:asset:assets:variety="S - Remote access"

Server - Remote access

veris:asset:assets:variety="S - Unknown"

Server - Variety not known

veris:asset:assets:variety="S - VM host"

Server - Virtual Host

veris:asset:assets:variety="S - Web application"

Server - Web application

veris:asset:assets:variety="T - ATM"

Public Terminal - Automated Teller Machine (ATM)

veris:asset:assets:variety="T - Gas terminal"

Public Terminal - Gas "pay-at-the-pump" terminal

veris:asset:assets:variety="T - Kiosk"

Public Terminal - Self-service kiosk

veris:asset:assets:variety="T - Other"

Public Terminal - Variety known but not listed

veris:asset:assets:variety="T - PED pad"

Public Terminal - Detached PIN pad or card reader

veris:asset:assets:variety="T - Unknown"

Public Terminal - Variety not known

veris:asset:assets:variety="U - Auth token"

User Device - Authentication token or device

veris:asset:assets:variety="U - Desktop"

User Device - Desktop or workstation

veris:asset:assets:variety="U - Laptop"

User Device - Laptop

veris:asset:assets:variety="U - Media"

User Device - Media player or recorder

veris:asset:assets:variety="U - Mobile phone"

User Device - Mobile phone or smartphone

veris:asset:assets:variety="U - Other"

User Device - Variety known but not listed

veris:asset:assets:variety="U - POS terminal"

User Device - POS terminal

veris:asset:assets:variety="U - Peripheral"

User Device - Peripheral (e.g., printer, copier, fax)

veris:asset:assets:variety="U - Tablet"

User Device - Tablet

veris:asset:assets:variety="U - Telephone"

User Device - Telephone

veris:asset:assets:variety="U - Unknown"

User Device - Variety not known

veris:asset:assets:variety="U - VoIP phone"

User Device - VoIP phone

veris:asset:assets:variety="Unknown"

Unknown type of asset

attribute:availability:variety

veris:attribute:availability:variety="Acceleration"

Acceleration

veris:attribute:availability:variety="Degradation"

Performance degradation

veris:attribute:availability:variety="Destruction"

Destruction

veris:attribute:availability:variety="Interruption"

Interruption

veris:attribute:availability:variety="Loss"

Loss

veris:attribute:availability:variety="Obscuration"

Conversion or obscuration

veris:attribute:availability:variety="Other"

Other

veris:attribute:availability:variety="Unknown"

Unknown

attribute:confidentiality:data_disclosure

veris:attribute:confidentiality:data_disclosure="No"

No

veris:attribute:confidentiality:data_disclosure="Potentially"

Potentially (at risk)

veris:attribute:confidentiality:data_disclosure="Unknown"

Unknown

veris:attribute:confidentiality:data_disclosure="Yes"

Yes (confirmed)

attribute:confidentiality:data_victim

veris:attribute:confidentiality:data_victim="Customer"

Customer

veris:attribute:confidentiality:data_victim="Employee"

Employee

veris:attribute:confidentiality:data_victim="Other"

Other

veris:attribute:confidentiality:data_victim="Partner"

Partner

veris:attribute:confidentiality:data_victim="Patient"

Patient

veris:attribute:confidentiality:data_victim="Student"

Student

veris:attribute:confidentiality:data_victim="Unknown"

Unknown

attribute:confidentiality:state

veris:attribute:confidentiality:state="Other"

Data state known but not listed.

veris:attribute:confidentiality:state="Printed"

Data printed in human-readable format

veris:attribute:confidentiality:state="Processed"

Processed

veris:attribute:confidentiality:state="Stored"

Stored

veris:attribute:confidentiality:state="Stored encrypted"

Stored encrypted

veris:attribute:confidentiality:state="Stored unencrypted"

Stored unencrypted

veris:attribute:confidentiality:state="Transmitted"

Transmitted

veris:attribute:confidentiality:state="Transmitted encrypted"

Transmitted encrypted

veris:attribute:confidentiality:state="Transmitted unencrypted"

Transmitted unencrypted

veris:attribute:confidentiality:state="Unknown"

Data stat not known

attribute:integrity:variety

veris:attribute:integrity:variety="Alter behavior"

Influence or alter human behavior

veris:attribute:integrity:variety="Created account"

Created new user account

veris:attribute:integrity:variety="Defacement"

Deface content

veris:attribute:integrity:variety="Fraudulent transaction"

Initiate fraudulent transaction

veris:attribute:integrity:variety="Hardware tampering"

Hardware tampering or physical alteration

veris:attribute:integrity:variety="Log tampering"

Log tampering or modification

veris:attribute:integrity:variety="Misrepresentation"

Misrepresentation

veris:attribute:integrity:variety="Modify configuration"

Modified configuration or services

veris:attribute:integrity:variety="Modify data"

Modified stored data or content

veris:attribute:integrity:variety="Modify privileges"

Modified privileges or permissions

veris:attribute:integrity:variety="Other"

Other

veris:attribute:integrity:variety="Repurpose"

Repurposed asset for unauthorized function

veris:attribute:integrity:variety="Software installation"

Software installation or code modification

veris:attribute:integrity:variety="Unknown"

Unknown

impact:loss:rating

veris:impact:loss:rating="Major"

Major

veris:impact:loss:rating="Minor"

Minor

veris:impact:loss:rating="Moderate"

Moderate

veris:impact:loss:rating="None"

None

veris:impact:loss:rating="Unknown"

Unknown

impact:loss:variety

veris:impact:loss:variety="Asset and fraud"

Asset and fraud-related losses

veris:impact:loss:variety="Brand damage"

Brand and market damage

veris:impact:loss:variety="Business disruption"

Business disruption

veris:impact:loss:variety="Competitive advantage"

Loss of competitive advantage

veris:impact:loss:variety="Legal and regulatory"

Legal and regulatory costs

veris:impact:loss:variety="Operating costs"

Increased operating costs

veris:impact:loss:variety="Other"

Impact variety known but not listed.

veris:impact:loss:variety="Response and recovery"

Response and recovery costs

timeline:compromise:unit

veris:timeline:compromise:unit="Days"

Days

veris:timeline:compromise:unit="Hours"

Hours

veris:timeline:compromise:unit="Minutes"

Minutes

veris:timeline:compromise:unit="Months"

Months

veris:timeline:compromise:unit="NA"

Compromise does not apply in the context of the security event.

veris:timeline:compromise:unit="Never"

Never

veris:timeline:compromise:unit="Seconds"

Seconds

veris:timeline:compromise:unit="Unknown"

Unknown

veris:timeline:compromise:unit="Weeks"

Weeks

veris:timeline:compromise:unit="Years"

Years

timeline:containment:unit

veris:timeline:containment:unit="Days"

Days

veris:timeline:containment:unit="Hours"

Hours

veris:timeline:containment:unit="Minutes"

Minutes

veris:timeline:containment:unit="Months"

Months

veris:timeline:containment:unit="NA"

Containment does not apply in the context of the security event.

veris:timeline:containment:unit="Never"

Never

veris:timeline:containment:unit="Seconds"

Seconds

veris:timeline:containment:unit="Unknown"

Unknown

veris:timeline:containment:unit="Weeks"

Weeks

veris:timeline:containment:unit="Years"

Years

timeline:discovery:unit

veris:timeline:discovery:unit="Days"

Days

veris:timeline:discovery:unit="Hours"

Hours

veris:timeline:discovery:unit="Minutes"

Minutes

veris:timeline:discovery:unit="Months"

Months

veris:timeline:discovery:unit="NA"

Discovery does not apply in the context of the security event.

veris:timeline:discovery:unit="Never"

Never

veris:timeline:discovery:unit="Seconds"

Seconds

veris:timeline:discovery:unit="Unknown"

Unknown

veris:timeline:discovery:unit="Weeks"

Weeks

veris:timeline:discovery:unit="Years"

Years

timeline:exfiltration:unit

veris:timeline:exfiltration:unit="Days"

Days

veris:timeline:exfiltration:unit="Hours"

Hours

veris:timeline:exfiltration:unit="Minutes"

Minutes

veris:timeline:exfiltration:unit="Months"

Months

veris:timeline:exfiltration:unit="NA"

Exfiltration does not apply in the context of the security event.

veris:timeline:exfiltration:unit="Never"

Never

veris:timeline:exfiltration:unit="Seconds"

Seconds

veris:timeline:exfiltration:unit="Unknown"

Unknown

veris:timeline:exfiltration:unit="Weeks"

Weeks

veris:timeline:exfiltration:unit="Years"

Years

victim:revenue:iso_currency_code

veris:victim:revenue:iso_currency_code="AED"

AED - UAE Dirham

veris:victim:revenue:iso_currency_code="AFN"

AFN - Afghani

veris:victim:revenue:iso_currency_code="ALL"

ALL - Lek

veris:victim:revenue:iso_currency_code="AMD"

AMD - Armenian Dram

veris:victim:revenue:iso_currency_code="ANG"

ANG - Netherlands Antillean Guilder

veris:victim:revenue:iso_currency_code="AOA"

AOA - Kwanza

veris:victim:revenue:iso_currency_code="ARS"

ARS - Argentine Peso

veris:victim:revenue:iso_currency_code="AUD"

AUD - Australian Dollar

veris:victim:revenue:iso_currency_code="AWG"

AWG - Aruban Florin

veris:victim:revenue:iso_currency_code="AZN"

AZN - Azerbaijanian Manat

veris:victim:revenue:iso_currency_code="BAM"

BAM - Convertible Mark

veris:victim:revenue:iso_currency_code="BBD"

BBD - Barbados Dollar

veris:victim:revenue:iso_currency_code="BDT"

BDT - Taka

veris:victim:revenue:iso_currency_code="BGN"

BGN - Bulgarian Lev

veris:victim:revenue:iso_currency_code="BHD"

BHD - Bahraini Dinar

veris:victim:revenue:iso_currency_code="BIF"

BIF - Burundi Franc

veris:victim:revenue:iso_currency_code="BMD"

BMD - Bermudian Dollar

veris:victim:revenue:iso_currency_code="BND"

BND - Brunei Dollar

veris:victim:revenue:iso_currency_code="BOB"

BOB - Boliviano

veris:victim:revenue:iso_currency_code="BRL"

BRL - Brazilian Real

veris:victim:revenue:iso_currency_code="BSD"

BSD - Bahamian Dollar

veris:victim:revenue:iso_currency_code="BTN"

BTN - Ngultrum

veris:victim:revenue:iso_currency_code="BWP"

BWP - Pula

veris:victim:revenue:iso_currency_code="BYR"

BYR - Belarussian Ruble

veris:victim:revenue:iso_currency_code="BZD"

BZD - Belize Dollar

veris:victim:revenue:iso_currency_code="CAD"

CAD - Canadian Dollar

veris:victim:revenue:iso_currency_code="CDF"

CDF - Congolese Franc

veris:victim:revenue:iso_currency_code="CHF"

CHF - Swiss Franc

veris:victim:revenue:iso_currency_code="CLP"

CLP - Chilean Peso

veris:victim:revenue:iso_currency_code="CNY"

CNY - Yuan Renminbi

veris:victim:revenue:iso_currency_code="COP"

COP - Colombian Peso

veris:victim:revenue:iso_currency_code="CRC"

CRC - Costa Rican Colon

veris:victim:revenue:iso_currency_code="CUC"

CUC - Peso Convertible

veris:victim:revenue:iso_currency_code="CUP"

CUP - Cuban Peso

veris:victim:revenue:iso_currency_code="CVE"

CVE - Cape Verde Escudo

veris:victim:revenue:iso_currency_code="CZK"

CZK - Czech Koruna

veris:victim:revenue:iso_currency_code="DJF"

DJF - Djibouti Franc

veris:victim:revenue:iso_currency_code="DKK"

DKK - Danish Krone

veris:victim:revenue:iso_currency_code="DOP"

DOP - Dominican Peso

veris:victim:revenue:iso_currency_code="DZD"

DZD - Algerian Dinar

veris:victim:revenue:iso_currency_code="EGP"

EGP - Egyptian Pound

veris:victim:revenue:iso_currency_code="ERN"

ERN - Nakfa

veris:victim:revenue:iso_currency_code="ETB"

ETB - Ethiopian Birr

veris:victim:revenue:iso_currency_code="EUR"

EUR - Euro

veris:victim:revenue:iso_currency_code="FJD"

FJD - Fiji Dollar

veris:victim:revenue:iso_currency_code="FKP"

FKP - Falkland Islands Pound

veris:victim:revenue:iso_currency_code="GBP"

GBP - Pound Sterling

veris:victim:revenue:iso_currency_code="GEL"

GEL - Lari

veris:victim:revenue:iso_currency_code="GGP"

GGP - Guernsey pound

veris:victim:revenue:iso_currency_code="GHS"

GHS - Ghana Cedi

veris:victim:revenue:iso_currency_code="GIP"

GIP - Gibraltar Pound

veris:victim:revenue:iso_currency_code="GMD"

GMD - Dalasi

veris:victim:revenue:iso_currency_code="GNF"

GNF - Guinea Franc

veris:victim:revenue:iso_currency_code="GTQ"

GTQ - Quetzal

veris:victim:revenue:iso_currency_code="GYD"

GYD - Guyana Dollar

veris:victim:revenue:iso_currency_code="HKD"

HKD - Hong Kong Dollar

veris:victim:revenue:iso_currency_code="HNL"

HNL - Lempira

veris:victim:revenue:iso_currency_code="HRK"

HRK - Croatian Kuna

veris:victim:revenue:iso_currency_code="HTG"

HTG - Gourde

veris:victim:revenue:iso_currency_code="HUF"

HUF - Forint

veris:victim:revenue:iso_currency_code="IDR"

IDR - Rupiah

veris:victim:revenue:iso_currency_code="ILS"

ILS - New Israeli Sheqel

veris:victim:revenue:iso_currency_code="IMP"

IMP - Isle of Man Pound

veris:victim:revenue:iso_currency_code="INR"

INR - Indian Rupee

veris:victim:revenue:iso_currency_code="IQD"

IQD - Iraqi Dinar

veris:victim:revenue:iso_currency_code="IRR"

IRR - Iranian Rial

veris:victim:revenue:iso_currency_code="ISK"

ISK - Iceland Krona

veris:victim:revenue:iso_currency_code="JEP"

JEP - Jersey pound

veris:victim:revenue:iso_currency_code="JMD"

JMD - Jamaican Dollar

veris:victim:revenue:iso_currency_code="JOD"

JOD - Jordanian Dinar

veris:victim:revenue:iso_currency_code="JPY"

JPY - Yen

veris:victim:revenue:iso_currency_code="KES"

KES - Kenyan Shilling

veris:victim:revenue:iso_currency_code="KGS"

KGS - Som

veris:victim:revenue:iso_currency_code="KHR"

KHR - Riel

veris:victim:revenue:iso_currency_code="KMF"

KMF - Comoro Franc

veris:victim:revenue:iso_currency_code="KPW"

KPW - North Korean Won

veris:victim:revenue:iso_currency_code="KRW"

KRW - South Korean Won

veris:victim:revenue:iso_currency_code="KWD"

KWD - Kuwaiti Dinar

veris:victim:revenue:iso_currency_code="KYD"

KYD - Cayman Islands Dollar

veris:victim:revenue:iso_currency_code="KZT"

KZT - Tenge

veris:victim:revenue:iso_currency_code="LAK"

LAK - Kip

veris:victim:revenue:iso_currency_code="LBP"

LBP - Lebanese Pound

veris:victim:revenue:iso_currency_code="LKR"

LKR - Sri Lanka Rupee

veris:victim:revenue:iso_currency_code="LRD"

LRD - Liberian Dollar

veris:victim:revenue:iso_currency_code="LSL"

LSL - Loti

veris:victim:revenue:iso_currency_code="LTL"

LTL - Lithuanian Litas

veris:victim:revenue:iso_currency_code="LVL"

LVL - Latvian Lats

veris:victim:revenue:iso_currency_code="LYD"

LYD - Libyan Dinar

veris:victim:revenue:iso_currency_code="MAD"

MAD - Moroccan Dirham

veris:victim:revenue:iso_currency_code="MDL"

MDL - Moldovan Leu

veris:victim:revenue:iso_currency_code="MGA"

MGA - Malagasy Ariary

veris:victim:revenue:iso_currency_code="MKD"

MKD - Denar

veris:victim:revenue:iso_currency_code="MMK"

MMK - Kyat

veris:victim:revenue:iso_currency_code="MNT"

MNT - Tugrik

veris:victim:revenue:iso_currency_code="MOP"

MOP - Pataca

veris:victim:revenue:iso_currency_code="MRO"

MRO - Ouguiya

veris:victim:revenue:iso_currency_code="MUR"

MUR - Mauritius Rupee

veris:victim:revenue:iso_currency_code="MVR"

MVR - Rufiyaa

veris:victim:revenue:iso_currency_code="MWK"

MWK - Kwacha

veris:victim:revenue:iso_currency_code="MXN"

MXN - Mexican Peso

veris:victim:revenue:iso_currency_code="MYR"

MYR - Malaysian Ringgit

veris:victim:revenue:iso_currency_code="MZN"

MZN - Mozambique Metical

veris:victim:revenue:iso_currency_code="NAD"

NAD - Namibia Dollar

veris:victim:revenue:iso_currency_code="NGN"

NGN - Naira

veris:victim:revenue:iso_currency_code="NIO"

NIO - Cordoba Oro

veris:victim:revenue:iso_currency_code="NOK"

NOK - Norwegian Krone

veris:victim:revenue:iso_currency_code="NPR"

NPR - Nepalese Rupee

veris:victim:revenue:iso_currency_code="NZD"

NZD - New Zealand Dollar

veris:victim:revenue:iso_currency_code="OMR"

OMR - Rial Omani

veris:victim:revenue:iso_currency_code="PAB"

PAB - Balboa

veris:victim:revenue:iso_currency_code="PEN"

PEN - Nuevo Sol

veris:victim:revenue:iso_currency_code="PGK"

PGK - Kina

veris:victim:revenue:iso_currency_code="PHP"

PHP - Philippine Peso

veris:victim:revenue:iso_currency_code="PKR"

PKR - Pakistan Rupee

veris:victim:revenue:iso_currency_code="PLN"

PLN - Zloty

veris:victim:revenue:iso_currency_code="PYG"

PYG - Guarani

veris:victim:revenue:iso_currency_code="QAR"

QAR - Qatari Rial

veris:victim:revenue:iso_currency_code="RON"

RON - New Romanian Leu

veris:victim:revenue:iso_currency_code="RSD"

RSD - Serbian Dinar

veris:victim:revenue:iso_currency_code="RUB"

RUB - Russian Ruble

veris:victim:revenue:iso_currency_code="RWF"

RWF - Rwanda Franc

veris:victim:revenue:iso_currency_code="SAR"

SAR - Saudi Riyal

veris:victim:revenue:iso_currency_code="SBD"

SBD - Solomon Islands Dollar

veris:victim:revenue:iso_currency_code="SCR"

SCR - Seychelles Rupee

veris:victim:revenue:iso_currency_code="SDG"

SDG - Sudanese Pound

veris:victim:revenue:iso_currency_code="SEK"

SEK - Swedish Krona

veris:victim:revenue:iso_currency_code="SGD"

SGD - Singapore Dollar

veris:victim:revenue:iso_currency_code="SHP"

SHP - Saint Helena Pound

veris:victim:revenue:iso_currency_code="SLL"

SLL - Leone

veris:victim:revenue:iso_currency_code="SOS"

SOS - Somali Shilling

veris:victim:revenue:iso_currency_code="SPL"

SPL - Seborga Luigino

veris:victim:revenue:iso_currency_code="SRD"

SRD - Surinam Dollar

veris:victim:revenue:iso_currency_code="STD"

STD - Dobra

veris:victim:revenue:iso_currency_code="SVC"

SVC - El Salvador Colon

veris:victim:revenue:iso_currency_code="SYP"

SYP - Syrian Pound

veris:victim:revenue:iso_currency_code="SZL"

SZL - Lilangeni

veris:victim:revenue:iso_currency_code="THB"

THB - Baht

veris:victim:revenue:iso_currency_code="TJS"

TJS - Somoni

veris:victim:revenue:iso_currency_code="TMT"

TMT - Turkmenistan New Manat

veris:victim:revenue:iso_currency_code="TND"

TND - Tunisian Dinar

veris:victim:revenue:iso_currency_code="TOP"

TOP - Pa’anga

veris:victim:revenue:iso_currency_code="TRY"

TRY - Turkish Lira

veris:victim:revenue:iso_currency_code="TTD"

TTD - Trinidad and Tobago Dollar

veris:victim:revenue:iso_currency_code="TVD"

TVD - Tuvalu Dollar

veris:victim:revenue:iso_currency_code="TWD"

TWD - New Taiwan Dollar

veris:victim:revenue:iso_currency_code="TZS"

TZS - Tanzanian Shilling

veris:victim:revenue:iso_currency_code="UAH"

UAH - Hryvnia

veris:victim:revenue:iso_currency_code="UGX"

UGX - Uganda Shilling

veris:victim:revenue:iso_currency_code="USD"

USD - US Dollar

veris:victim:revenue:iso_currency_code="UYU"

UYU - Peso Uruguayo

veris:victim:revenue:iso_currency_code="UZS"

UZS - Uzbekistan Sum

veris:victim:revenue:iso_currency_code="VEF"

VEF - Bolivar

veris:victim:revenue:iso_currency_code="VND"

VND - Dong

veris:victim:revenue:iso_currency_code="VUV"

VUV - Vatu

veris:victim:revenue:iso_currency_code="WST"

WST - Tala

veris:victim:revenue:iso_currency_code="XAF"

XAF - CFA Franc BEAC

veris:victim:revenue:iso_currency_code="XCD"

XCD - East Caribbean Dollar

veris:victim:revenue:iso_currency_code="XDR"

XDR - SDR (Special Drawing Right)

veris:victim:revenue:iso_currency_code="XOF"

XOF - CFA Franc BCEAO

veris:victim:revenue:iso_currency_code="XPF"

XPF - CFP Franc

veris:victim:revenue:iso_currency_code="YER"

YER - Yemeni Rial

veris:victim:revenue:iso_currency_code="ZAR"

ZAR - South African Rand

veris:victim:revenue:iso_currency_code="ZMK"

ZMK - Zambian Kwacha

veris:victim:revenue:iso_currency_code="ZWD"

ZWD - Zimbabwean Dollar A/06

attribute:availability:duration:unit

veris:attribute:availability:duration:unit="Days"

Days

veris:attribute:availability:duration:unit="Hours"

Hours

veris:attribute:availability:duration:unit="Minutes"

Minutes

veris:attribute:availability:duration:unit="Months"

Months

veris:attribute:availability:duration:unit="NA"

NA

veris:attribute:availability:duration:unit="Never"

Never

veris:attribute:availability:duration:unit="Seconds"

Seconds

veris:attribute:availability:duration:unit="Unknown"

Unknown

veris:attribute:availability:duration:unit="Weeks"

Weeks

veris:attribute:availability:duration:unit="Years"

Years

attribute:confidentiality:data:variety

veris:attribute:confidentiality:data:variety="Bank"

Bank account data

veris:attribute:confidentiality:data:variety="Classified"

Classified information

veris:attribute:confidentiality:data:variety="Copyrighted"

Copyrighted material

veris:attribute:confidentiality:data:variety="Credentials"

Authentication credentials (e.g., pwds, OTPs, biometrics)

veris:attribute:confidentiality:data:variety="Digital certificate"

Digital certificate

veris:attribute:confidentiality:data:variety="Internal"

Sensitive internal data (e.g., plans, reports, emails)

veris:attribute:confidentiality:data:variety="Medical"

Medical records

veris:attribute:confidentiality:data:variety="Other"

Other

veris:attribute:confidentiality:data:variety="Payment"

Payment card data (e.g., PAN, PIN, CVV2, Expiration)

veris:attribute:confidentiality:data:variety="Personal"

Personal or identifying information (e.g., addr, ID#, credit score)

veris:attribute:confidentiality:data:variety="Secrets"

Trade secrets

veris:attribute:confidentiality:data:variety="Source code"

Source code

veris:attribute:confidentiality:data:variety="System"

System information (e.g., config info, open services)

veris:attribute:confidentiality:data:variety="Unknown"

Unknown

veris:attribute:confidentiality:data:variety="Virtual currency"

Virtual currency

vmray

vmray namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

VMRay taxonomies to map VMRay Thread Identifier scores and artifacts.

verdict

vmray:verdict="malicious"

Malicious

vmray:verdict="suspicious"

Suspicious

vmray:verdict="clean"

Clean

vmray:verdict="n/a"

N/A

vti_analysis_score

vmray:vti_analysis_score="-1/5"

-1/5

vmray:vti_analysis_score="1/5"

1/5

vmray:vti_analysis_score="2/5"

2/5

vmray:vti_analysis_score="3/5"

3/5

vmray:vti_analysis_score="4/5"

4/5

vmray:vti_analysis_score="5/5"

5/5

artifact

vmray:artifact="ioc"

is IOC

vocabulaire-des-probabilites-estimatives

vocabulaire-des-probabilites-estimatives namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Ce vocabulaire attribue des valeurs en pourcentage à certains énoncés de probabilité

Exclusive flag set which means the values or predicate below must be set exclusively.

degré-de-probabilité

Le tableau suivant attribue des valeurs en pourcentage à certains énoncés de probabilité. Les pourcentages sont tirés de l'ouvrage de Sherman Kent intitulé « Words of Estimative Probability » publié par le Centre for the Study of Intelligence de la CIA en 1964. 0% exprime une impossibilité et 100% exprime une certitude.

vocabulaire-des-probabilites-estimatives:degré-de-probabilité="presque-aucune-chance"

Presque aucune chance - Quasi impossible Presque impossible Minces chances Très douteux Très peu probable Très improbable Improbable Peu de chances - 7 % (marge d'erreur d'environ 5 %)

Associated numerical value="7"

vocabulaire-des-probabilites-estimatives:degré-de-probabilité="probablement-pas"

Probablement pas - Invraisemblable Peu probable - 30 % (marge d'erreur d'environ 10 %)

Associated numerical value="30"

vocabulaire-des-probabilites-estimatives:degré-de-probabilité="chances-à-peu-près-egales"

Chances à peu près égales - une chance sur deux - 50% (marge d'erreur d'environ 10 %)

Associated numerical value="50"

vocabulaire-des-probabilites-estimatives:degré-de-probabilité="probable"

Probable - Vraisemblable Probable - 75 % (marge d'erreur d'environ 12 %)

Associated numerical value="75"

vocabulaire-des-probabilites-estimatives:degré-de-probabilité="quasi-certaine"

Quasi certaine - Certain Presque certain Très probable - 93% (marge d'erreur d'environ 6 %)

Associated numerical value="93"

workflow

workflow namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Workflow support language is a common language to support intelligence analysts to perform their analysis on data and information.

todo

Todo are the actions to be performed by one or more analyst(s) to apply cognitive methods, evaluation(s), weightening information, to validate hypothesis or complete additional tasks to improve the overall information or data being tagged with a todo.

workflow:todo="expansion"

Expansion need to be applied to expand the information tagged

workflow:todo="review"

Additional review is required to reach a certain level of validation of the information tagged

workflow:todo="review-for-privacy"

Additional review is required to ensure privacy of the information tagged

workflow:todo="review-before-publication"

Review is required before publishing the information tagged

workflow:todo="release-requested"

Release of the information tagged is requested (often after the review process

workflow:todo="review-for-false-positive"

Review the the information tagged to limit the number of false-positives and potentially remove any IDS/automation flag to avoid automation of the false-positives

workflow:todo="review-the-source-credibility"

Review the source credibility and add the corresponding marking like admiralty-scale on the origin

workflow:todo="add-missing-misp-galaxy-cluster-values"

Add potential MISP galaxy cluster values missing about the information tagged

workflow:todo="create-missing-misp-galaxy-cluster"

Create missing MISP galaxy cluster about the information tagged

workflow:todo="create-missing-misp-galaxy-cluster-relationship"

create missing MISP galaxy cluster relationships (e.g. relationships between MISP clusters)

workflow:todo="create-missing-misp-galaxy"

Create missing MISP galaxy at large about the information tagged (e.g. a new category of malware or activity)

workflow:todo="create-missing-relationship"

Create missing relationship about the information tagged (e.g. create new relationship between MISP objects)

workflow:todo="add-context"

Add contextual information about the information tagged

workflow:todo="add-tagging"

Add adequate tagging and classification about the information tagged

workflow:todo="check-passive-dns-for-shared-hosting"

Check Passive DNS (or similar techniques) to review if the information tagged is used within shared hosting

workflow:todo="review-classification"

Review the classification of the information tagged to ensure adequate marking of the information before publication

workflow:todo="review-the-grammar"

Review the grammar of the information tagged to improve the overall quality

workflow:todo="do-not-delete"

Element that should not be deleted (without asking)

workflow:todo="add-mitre-attack-cluster"

Describe cyber adversary behavior using MITRE ATT&CK

workflow:todo="additional-task"

Used to point an additional task that can not be describe by the rest of the taxonomy and need to be done

workflow:todo="create-event"

A new MISP event need to be created from the tag reference

workflow:todo="preserve-evidence"

Preseve evidence mentioned in the information tagged

state

State are the different states of the information or data being tagged.

Exclusive flag set which means the values or predicate below must be set exclusively.

workflow:state="incomplete"

Incomplete means that the information tagged is incomplete and has potential to be completed by other analysts, technical processes or the current analysts performing the analysis.

workflow:state="complete"

Complete means that the information tagged reach a state of completeness with the current capabilities of the analyst.

workflow:state="draft"

Draft means the information tagged can be released as a preliminary version or outline.

workflow:state="ongoing"

Analyst is currently working on this analysis. To remove when there is no more work to be done by the analyst.

workflow:state="rejected"

Analyst rejected the process. The object will not reach state of completeness.

Mapping of taxonomies

Analysts relying on taxonomies don't always know the appropriate namespace to use but know which value to use for classification. The MISP mapping taxonomy allows to map a single classification into a series of machine-tag synonyms.

Table 1. Mapping table - **Adware**

Adware
veris:action:malware:variety="Adware"
malware_classification:malware-category="Adware"
ms-caro-malware:malware-type="Adware"

Table 2. Mapping table - **Brute Force**

Brute Force
ecsirt:intrusion-attempts="brute-force"
veris:action:malware:variety="Brute force"
europol-event:brute-force-attempt
enisa:nefarious-activity-abuse="brute-force"

Table 3. Mapping table - **DDoS**

DDoS
rsit:availability="dos"
rsit:availability="ddos"
rsit:vulnerable="ddos-amplifier"
ecsirt:availability="ddos"
europol-incident:availability="dos-ddos"
ms-caro-malware:malware-type="DDoS"
circl:incident-classification="denial-of-service"
enisa:nefarious-activity-abuse="denial-of-service"

Table 4. Mapping table - **Downloader**

Downloader
veris:action:malware:variety="Downloader"
malware_classification:malware-category="Downloader"

Table 5. Mapping table - **Remote Access Tool**

Remote Access Tool
enisa:nefarious-activity-abuse="remote-access-tool"

ms-caro-malware:malware-type="RemoteAccess"

Table 6. Mapping table - **SQLi**

SQLi
circl:incident-classification="sql-injection"
veris:action:malware:variety="SQL injection"
veris:action:hacking:variety="SQLi"
enisa:nefarious-activity-abuse="web-application-attacks-injection-attacks-code-injection-SQL-XSS"
europol-event:sql-injection

Table 7. Mapping table - **Spyware**

Spyware
veris:action:malware:variety="Spyware/Keylogger"
malware_classification:malware-category="Spyware"
ms-caro-malware:malware-type="Spyware"
enisa:nefarious-activity-abuse="spyware-or-deceptive-adware"

Table 8. Mapping table - **Trojan**

Trojan
malware_classification:malware-category="Trojan"
ms-caro-malware:malware-type="Trojan"
ecsirt:malicious-code="trojan"

Table 9. Mapping table - **Virus**

Virus
malware_classification:malware-category="Virus"
ms-caro-malware:malware-type="Virus"
ecsirt:malicious-code="virus"

Table 10. Mapping table - **Worm**

Worm
veris:action:malware:variety="Worm"
malware_classification:malware-category="Worm"
ms-caro-malware:malware-type="Worm"
ecsirt:malicious-code="worm"

Table 11. Mapping table - **backdoor**

backdoor

ecsirt:intrusions="backdoor"
veris:action:malware:variety="Backdoor"
ms-caro-malware:malware-type="Backdoor"

Table 12. Mapping table - **brute force**

brute force
rsit:intrusion-attempts="brute-force"
ecsirt:intrusion-attempts="brute-force"
veris:action:malware:variety="Brute force"
europol-event:brute-force-attempt
enisa:nefarious-activity-abuse="brute-force"

Table 13. Mapping table - **c&c**

c&c
rsit:malicious-code="c2-server"
ecsirt:malicious-code="c&c"
europol-incident:malware="c&c"
europol-event:c&c-server-hosting
veris:action:malware:variety="C2"

Table 14. Mapping table - **content**

content
rsit:abusive-content="harmful-speech"
rsit:abusive-content="violence"
rsit:fraud="copyright"
rsit:fraud="masquerade"

Table 15. Mapping table - **exploit**

exploit
rsit:intrusion-attempts="exploit"
veris:action:malware:variety="Exploit vuln"
ecsirt:intrusion-attempts="exploit"
europol-event:exploit
europol-incident:intrusion="exploitation-vulnerability"
ms-caro-malware:malware-type="Exploit"

Table 16. Mapping table - **malware**

malware
rsit:malicious-code="malware-distribution"
rsit:malicious-code="malware-configuration"
ecsirt:malicious-code="malware"
circl:incident-classification="malware"

Table 17. Mapping table - **other**

other
rsit:other="other"

Table 18. Mapping table - **phishing**

phishing
rsit:fraud="phishing"
circl:incident-classification="phishing"
ecsirt:fraud="phishing"
veris:action:social:variety="Phishing"
europol-incident:information-gathering="phishing"
enisa:nefarious-activity-abuse="phishing-attacks"

Table 19. Mapping table - **ransomware**

ransomware
ecsirt:malicious-code="ransomware"
enisa:nefarious-activity-abuse="ransomware"
malware_classification:malware-category="Ransomware"
ms-caro-malware:malware-type="Ransom"
veris:action:malware:variety="Ransomware"

Table 20. Mapping table - **rootkit**

rootkit
veris:action:malware:variety="Rootkit"
enisa:nefarious-activity-abuse="rootkits"
malware_classification:malware-category="Rootkit"

Table 21. Mapping table - **scan**

scan
rsit:information-gathering="scanner"
circl:incident-classification="scan"

ecsirt:information-gathering="scanner"
europol-incident:information-gathering="scanning"

Table 22. Mapping table - **scan network**

scan network
veris:action:malware:variety="Scan network"
europol-event:network-scanning

Table 23. Mapping table - **spam**

spam
rsit:abusive-content="spam"
circl:incident-classification="spam"
ecsirt:abusive-content="spam"
enisa:nefarious-activity-abuse="spam"
europol-event:spam
europol-incident:abusive-content="spam"
veris:action:malware:variety="Spam"
veris:action:social:variety="Spam"

Table 24. Mapping table - **test**

test
rsit:test="test"

Table 25. Mapping table - **tlp-amber**

tlp-amber
tlp:amber
iep:traffic-light-protocol="AMBER"

Table 26. Mapping table - **tlp-green**

tlp-green
tlp:green
iep:traffic-light-protocol="GREEN"

Table 27. Mapping table - **tlp-red**

tlp-red
tlp:red
iep:traffic-light-protocol="RED"

Table 28. Mapping table - **tlp-white**

tlp-white
tlp:white
iep:traffic-light-protocol="WHITE"

Table 29. Mapping table - **xss**

xss
circl:incident-classification="XSS"
europol-event:xss