

# MISP taxonomies and classification as machine tags

# Table of Contents

PAP	1
accessnow	2
admiralty-scale	6
adversary	7
analyst-assessment	9
binary-class	12
circl	13
csirt_case_classification	15
ddos	17
de-vs	18
dhs-ciip-sectors	18
diamond-model	20
dni-ism	21
domain-abuse	28
ecsirt	29
enisa	32
estimative-language	47
eu-marketop-and-publicadmin	48
euci	50
europol-event	51
europol-incident	59
event-assessment	61
fr-classif	62
iep	63
information-security-indicators	67
kill-chain	76
malware_classification	78
misp	80
ms-caro-malware	82
ms-caro-malware-full	92
nato	153
open_threat	154
osint	161
passivetotal	163
rt_event_status	164
stealth_malware	165
stealth_malware	165
stix-ttp	166

targeted-threat-index .....	168
tlp .....	170
tor .....	172
veris .....	172
vocabulaire-des-probabilites-estimatives .....	255



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.

## 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.

PAP - was designed to indicate how the received information can be used.

## 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.

## **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

## **anti-corruption-transparency**

### **accessnow:anti-corruption-transparency**

Anti-Corruption and transparency

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

## **anti-war-violence**

### **accessnow:anti-war-violence**

Anti-War / Anti-Violence

The organization campaigns, or takes other actions against war

## **culture**

### **accessnow:culture**

Culture

The organization campaigns or acts to promote cultural events Humanitarian Aid/Need Issues: relates to improving life for individuals in the developing world (right to shelter, right to education, right to food, right to water)

## **economic-change**

### **accessnow:economic-change**

Economic Change

Issues of economic policy, wealth distribution, etc.

## **education**

### **accessnow:education**

Education

The organization is concerned with some form of education

## **election-monitoring**

### **accessnow:election-monitoring**

Election Monitoring

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

## **environment**

### **accessnow:environment**

Environment

The organization campaigns or acts to protect the environment

## **freedom-expression**

### **accessnow:freedom-expression**

Freedom of Expression

The organization is concerned with freedom of speech issues

## **freedom-tool-development**

### **accessnow:freedom-tool-development**

Freedom Tool Development

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

# **funding**

## **accessnow:funding**

Funding

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

# **health**

## **accessnow:health**

Health Issues

The organization prevents epidemic illness or acts on curing them

# **human-rights**

## **accessnow:human-rights**

Human Rights Issues

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

# **internet-telecom**

## **accessnow:internet-telecom**

Internet and Telecoms

Issues of digital rights in electronic communications

# **lgbt-gender-sexuality**

## **accessnow:lgbt-gender-sexuality**

LGBT / Gender / Sexuality

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

# **policy**

## **accessnow:policy**

Policy

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

## **politics**

### **accessnow:politics**

Politics

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

## **privacy**

### **accessnow:privacy**

Privacy

Issues relating to the individual's reasonable right to privacy

## **rapid-response**

### **accessnow:rapid-response**

Rapid Response

The organization provides rapid response type capability for civil society

## **refugees**

### **accessnow:refugees**

Refugees

Issues relating to displaced people

## **security**

### **accessnow:security**

Security

Issues relating to physical or information security

## **womens-right**



## **accessnow:womens-right**

Women's Rights

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

## **youth-rights**

### **accessnow:youth-rights**

Youth Rights

Issues of particular relevance to youth

## **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 (also called the NATO System) is used to rank the reliability of a source and the credibility of an information.

## **source-reliability**

### **admiralty-scale:source-reliability="a"**

Completely reliable

### **admiralty-scale:source-reliability="b"**

Usually reliable

### **admiralty-scale:source-reliability="c"**

Fairly reliable

### **admiralty-scale:source-reliability="d"**

Not usually reliable

### **admiralty-scale:source-reliability="e"**

Unreliable

**admiralty-scale:source-reliability="f"**

Reliability cannot be judged

## information-credibility

**admiralty-scale:information-credibility="1"**

Confirmed by other sources

**admiralty-scale:information-credibility="2"**

Probably true

**admiralty-scale:information-credibility="3"**

Possibly true

**admiralty-scale:information-credibility="4"**

Doubtful

**admiralty-scale:information-credibility="5"**

Improbable

**admiralty-scale:information-credibility="6"**

Truth cannot be judged

## 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-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

## **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-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

## 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

### **analyst-assessment:experience="less-than-1-year"**

Less than 1 year

### **analyst-assessment:experience="between-1-and-5-years"**

Between 1 and 5 years

### **analyst-assessment:experience="between-5-and-10-years"**

Between 5 and 10 years

### **analyst-assessment:experience="between-10-and-20-years"**

Between 10 and 20 years

**analyst-assessment:experience="more-than-20-years"**

More than 20 years

## **binary-reversing-arch**

**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**

**analyst-assessment:binary-reversing-experience="less-than-1-year"**

Less than 1 year

**analyst-assessment:binary-reversing-experience="between-1-and-5-years"**

Between 1 and 5 years

**analyst-assessment:binary-reversing-experience="between-5-and-10-years"**

Between 5 and 10 years

**analyst-assessment:binary-reversing-experience="between-10-and-20-years"**

Between 10 and 20 years

**analyst-assessment:binary-reversing-experience="more-than-20-years"**

More than 20 years

## **OS**

### **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**

### **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**

### **analyst-assessment:web-experience="less-than-1-year"**

Less than 1 year

**analyst-assessment:web-experience="between-1-and-5-years"**

Between 1 and 5 years

**analyst-assessment:web-experience="between-5-and-10-years"**

Between 5 and 10 years

**analyst-assessment:web-experience="between-10-and-20-years"**

Between 10 and 20 years

**analyst-assessment:web-experience="more-than-20-years"**

More than 20 years

## crypto-experience

**analyst-assessment:crypto-experience="less-than-1-year"**

Less than 1 year

**analyst-assessment:crypto-experience="between-1-and-5-years"**

Between 1 and 5 years

**analyst-assessment:crypto-experience="between-5-and-10-years"**

Between 5 and 10 years

**analyst-assessment:crypto-experience="between-10-and-20-years"**

Between 10 and 20 years

**analyst-assessment:crypto-experience="more-than-20-years"**

More than 20 years

## 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.

# type

## **binary-class:type="good"**

Known Good/Safe

## **binary-class:type="malicious"**

Known Bad/Malicious

## **binary-class:type="unknown"**

Not yet known

# 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="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="malware"**

Malware

**circl:incident-classification="XSS"**

XSS

**circl:incident-classification="vulnerability"**

Vulnerability

**circl:incident-classification="fastflux"**

Fastflux

**circl:incident-classification="sql-injection"**

SQL Injection

**circl:incident-classification="information-leak"**

Information leak

**circl:incident-classification="scam"**

Scam

## **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

## 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

## 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.

DDoS - taxonomy supports the description of Denial of Service attacks and especially the types they belong too.

## type

**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

**de-vs:Einstufung="GEHEIM"**

GEHEIM

**de-vs:Einstufung="VS-VERTRAULICH"**

VS-VERTRAULICH

**de-vs:Einstufung="VS-NfD"**

VS-NUR FÜR DEN DIENSTGEBRAUCH

## Schutzwort

**de-vs:Schutzwort="Dummy"**

Dummy

## 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

**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, a phase-based model developed by Lockheed Martin, aims to help categorise and identify the stage of an attack.

## 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., command-and-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

## **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.

# 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

## **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

## **notice**

### **dni-ism:notice="FISA"**

FISA Warning statement

### **dni-ism:notice="IMC"**

IMCON Warning statement

### **dni-ism:notice="CNWDI"**

Controlled 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

## **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

## 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

## 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. Use europol-incident to tag abuse-activity

## domain-access-method

**domain-abuse:domain-access-method="criminal-registration"**

Criminal registration

**domain-abuse:domain-access-method="compromised-webserver"**

Compromised webserver

**domain-abuse:domain-access-method="compromised-dns"**

Compromised DNS

**domain-abuse:domain-access-method="sinkhole"**

Sinkhole

## domain-status

**domain-abuse:domain-status="active"**

Registered & active

**domain-abuse:domain-status="inactive"**

Registered & inactive

**domain-abuse:domain-status="suspended"**

Registered & suspended

**domain-abuse:domain-status="not-registered"**

Not registered

**domain-abuse:domain-status="not-registrable"**

Not registrable

**domain-abuse:domain-status="grace-period"**

Grace period

## 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.



## **abusive-content**

**ecsirt:abusive-content="spam"**

spam

## **malicious-code**

**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**

**ecsirt:information-gathering="scanner"**

scanner

## **intrusion-attempts**

**ecsirt:intrusion-attempts="exploit"**

exploit

**ecsirt:intrusion-attempts="brute-force"**

brute-force

**ecsirt:intrusion-attempts="ids-alert"**

ids alerts

## **intrusions**

**ecsirt:intrusions="defacement"**

defacement

**ecsirt:intrusions="compromised"**

compromised

**ecsirt:intrusions="backdoor"**

backdoor

## **availability**

**ecsirt:availability="ddos"**

ddos

## **information-security**

### **information-content-security**

**ecsirt:information-content-security="dropzone"**

dropzone

## **vulnerable**

**ecsirt:vulnerable="vulnerable-service"**

Vulnerable service

## **fraud**

**ecsirt:fraud="phishing"**

phishing

## other

**ecsirt:other="blacklist"**

blacklist

**ecsirt:other="unknown"**

unknown

## test

**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

**enisa:physical-attack="fraud"**

Fraud

**enisa:physical-attack="fraud-by-employees"**

Fraud committed by employees

**enisa:physical-attack="sabotage"**

Sabotage

**enisa:physical-attack="vandalism"**

Vandalism

**enisa:physical-attack="theft"**

Theft (of devices, storage media and documents)

## **enisa:physical-attack="theft-of-mobile-devices"**

Theft of mobile devices (smartphones/ tablets)

## **enisa:physical-attack="theft-of-fixed-hardware"**

Theft of fixed hardware

## **enisa:physical-attack="theft-of-documents"**

Theft of documents

## **enisa:physical-attack="theft-of-backups"**

Theft of backups

## **enisa:physical-attack="information-leak-or-unauthorised-sharing"**

Information leak /sharing

## **enisa:physical-attack="unauthorised-physical-access-or-unauthorised-entry-to-premises"**

Unauthorized physical access / Unauthorised entry to premises

## **enisa:physical-attack="coercion-or-extortion-or-corruption"**

Coercion, extortion or corruption

## **enisa:physical-attack="damage-from-the-wafare"**

Damage from the warfare

## **enisa:physical-attack="terrorist-attack"**

Terrorist attack

## **unintentional-damage**

### **enisa:unintentional-damage="information-leak-or-sharing-due-to-human-error"**

Information leak /sharing due to human error

### **enisa:unintentional-damage="accidental-leaks-or-sharing-of-data-by-employees"**

Accidental leaks/sharing of data by employees

**enisa:unintentional-damage="leaks-of-data-via-mobile-applications"**

Leaks of data via mobile applications

**enisa:unintentional-damage="leaks-of-data-via-web-applications"**

Leaks of data via Web applications

**enisa:unintentional-damage="leaks-of-information-transferred-by-network"**

Leaks of information transferred by network

**enisa:unintentional-damage="erroneous-use-or-administration-of-devices-and-systems"**

Erroneous use or administration of devices and systems

**enisa:unintentional-damage="loss-of-information-due-to-maintenance-errors-or-operators-errors"**

Loss of information due to maintenance errors / operators' errors

**enisa:unintentional-damage="loss-of-information-due-to-configuration-or-installation error"**

Loss of information due to configuration/ installation error

**enisa:unintentional-damage="increasing-recovery-time"**

Increasing recovery time

**enisa:unintentional-damage="lost-of-information-due-to-user-errors"**

Loss of information due to user errors

**enisa:unintentional-damage="using-information-from-an-unreliable-source"**

Using information from an unreliable source

**enisa:unintentional-damage="unintentional-change-of-data-in-an-information-system"**

Unintentional change of data in an information system

**enisa:unintentional-damage="inadequate-design-and-planning-or-improper-adaptation"**

Inadequate design and planning or improper adaptation

**enisa:unintentional-damage="damage-caused-by-a-third-party"**

Damage caused by a third party

**enisa:unintentional-damage="security-failure-caused-by-third-party"**

Security failure caused by third party

**enisa:unintentional-damage="damages-resulting-from-penetration-testing"**

Damages resulting from penetration testing

**enisa:unintentional-damage="loss-of-information-in-the-cloud"**

Loss of information in the cloud

**enisa:unintentional-damage="loss-of-(integrity-of)-sensitive-information"**

Loss of (integrity of) sensitive information

**enisa:unintentional-damage="loss-of-integrity-of-certificates"**

Loss of integrity of certificates

**enisa:unintentional-damage="loss-of-devices-and-storage-media-and-documents"**

Loss of devices, storage media and documents

**enisa:unintentional-damage="loss-of-devices-or-mobile-devices"**

Loss of devices/ mobile devices

**enisa:unintentional-damage="loss-of-storage-media"**

Loss of storage media

**enisa:unintentional-damage="loss-of-documentation-of-IT-Infrastructure"**

Loss of documentation of IT Infrastructure

**enisa:unintentional-damage="destruction-of-records"**

Destruction of records

**enisa:unintentional-damage="infection-of-removable-media"**

Infection of removable media

**enisa:unintentional-damage="abuse-of-storage"**

Abuse of storage

## **disaster**

**enisa:disaster="disaster"**

Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy snowfalls, heavy winds)

**enisa:disaster="fire"**

Fire

**enisa:disaster="pollution-dust-corrosion"**

Pollution, dust, corrosion

**enisa:disaster="thunderstrike"**

Thunderstrike

**enisa:disaster="water"**

Water

**enisa:disaster="explosion"**

Explosion

**enisa:disaster="dangerous-radiation-leak"**

Dangerous radiation leak

**enisa:disaster="unfavourable-climatic-conditions"**

Unfavourable climatic conditions

**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

**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

**enisa:disaster="threats-from-space-or-electromagnetic-storm"**

Threats from space / Electromagnetic storm

**enisa:disaster="wildlife"**

Wildlife

## **failures-malfunction**

**enisa:failures-malfunction="failure-of-devices-or-systems"**

Failure of devices or systems

**enisa:failures-malfunction="failure-of-data-media"**

Failure of data media

**enisa:failures-malfunction="hardware-failure"**

Hardware failure

**enisa:failures-malfunction="failure-of-applications-and-services"**

Failure of applications and services

**enisa:failures-malfunction="failure-of-parts-of-devices-connectors-plug-ins"**

Failure of parts of devices (connectors, plug-ins)

**enisa:failures-malfunction="failure-or-disruption-of-communication-links-communication networks"**

Failure or disruption of communication links (communication networks)

**enisa:failures-malfunction="failure-of-cable-networks"**

Failure of cable networks

**enisa:failures-malfunction="failure-of-wireless-networks"**

Failure of wireless networks



**enisa:failures-malfunction="failure-of-mobile-networks"**

Failure of mobile networks

**enisa:failures-malfunction="failure-or-disruption-of-main-supply"**

Failure or disruption of main supply

**enisa:failures-malfunction="failure-or-disruption-of-power-supply"**

Failure or disruption of power supply

**enisa:failures-malfunction="failure-of-cooling-infrastructure"**

Failure of cooling infrastructure

**enisa:failures-malfunction="failure-or-disruption-of-service-providers-supply-chain"**

Failure or disruption of service providers (supply chain)

**enisa:failures-malfunction="malfunction-of-equipment-devices-or-systems"**

Malfunction of equipment (devices or systems)

## **outages**

**enisa:outages="absence-of-personnel"**

Absence of personnel

**enisa:outages="strike"**

Strike

**enisa:outages="loss-of-support-services"**

Loss of support services

**enisa:outages="internet-outage"**

Internet outage

**enisa:outages="network-outage"**

Network outage

**enisa:outages="outage-of-cable-networks"**

Outage of cable networks

**enisa:outages="Outage-of-short-range-wireless-networks"**

Outage of short-range wireless networks

**enisa:outages="outages-of-long-range-wireless-networks"**

Outages of long-range wireless networks

## **eavesdropping-interception-hijacking**

**enisa:eavesdropping-interception-hijacking="war-driving"**

War driving

**enisa:eavesdropping-interception-hijacking="intercepting-compromising-emissions"**

Intercepting compromising emissions

**enisa:eavesdropping-interception-hijacking="interception-of-information"**

Interception of information

**enisa:eavesdropping-interception-hijacking="corporate-espionage"**

Corporate espionage

**enisa:eavesdropping-interception-hijacking="nation-state-espionage"**

Nation state espionage

**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

**enisa:eavesdropping-interception-hijacking="interfering-radiation"**

Interfering radiation

**enisa:eavesdropping-interception-hijacking="replay-of-messages"**

Replay of messages

**enisa:eavesdropping-interception-hijacking="network-reconnaissance-network-traffic-manipulation-and-information-gathering"**

Network Reconnaissance, Network traffic manipulation and Information gathering

**enisa:eavesdropping-interception-hijacking="man-in-the-middle-session-hijacking"**

Man in the middle/ Session hijacking

## **nefarious-activity-abuse**

**enisa:nefarious-activity-abuse="identity-theft-identity-fraud-account)"**

Identity theft (Identity Fraud/ Account)

**enisa:nefarious-activity-abuse="credentials-stealing-trojans"**

Credentials-stealing trojans

**enisa:nefarious-activity-abuse="receiving-unsolicited-e-mail"**

Receiving unsolicited E-mail

**enisa:nefarious-activity-abuse="spam"**

SPAM

**enisa:nefarious-activity-abuse="unsolicited-infected-e-mails"**

Unsolicited infected e-mails

**enisa:nefarious-activity-abuse="denial-of-service"**

Denial of service

**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)

**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)

**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)

**enisa:nefarious-activity-abuse="malicious-code-software-activity"**

Malicious code/ software/ activity

**enisa:nefarious-activity-abuse="search-engine-poisoning"**

Search Engine Poisoning

**enisa:nefarious-activity-abuse="exploitation-of-fake-trust-of-social-media"**

Exploitation of fake trust of social media

**enisa:nefarious-activity-abuse="worms-trojans"**

Worms/ Trojans

**enisa:nefarious-activity-abuse="rootkits"**

Rootkits

**enisa:nefarious-activity-abuse="mobile-malware"**

Mobile malware

**enisa:nefarious-activity-abuse="infected-trusted-mobile-apps"**

Infected trusted mobile apps

**enisa:nefarious-activity-abuse="elevation-of-privileges"**

Elevation of privileges

**enisa:nefarious-activity-abuse="web-application-attacks-injection-attacks-code-injection-SQL-XSS"**

Web application attacks / injection attacks (Code injection: SQL, XSS)

**enisa:nefarious-activity-abuse="spyware-or-deceptive-adware"**

Spyware or deceptive adware

**enisa:nefarious-activity-abuse="viruses"**

Viruses

**enisa:nefarious-activity-abuse="rogue-security-software-rogueware-scareware"**

Rogue security software/ Rogueware / Scareware

**enisa:nefarious-activity-abuse="ransomware"**

Ransomware

**enisa:nefarious-activity-abuse="exploits-exploit-kits"**

Exploits/Exploit Kits

**enisa:nefarious-activity-abuse="social-engineering"**

Social Engineering

**enisa:nefarious-activity-abuse="phishing-attacks"**

Phishing attacks

**enisa:nefarious-activity-abuse="spear-phishing-attacks"**

Spear phishing attacks

**enisa:nefarious-activity-abuse="abuse-of-information-leakage"**

Abuse of Information Leakage

**enisa:nefarious-activity-abuse="leakage-affecting-mobile-privacy-and-mobile-applications"**

Leakage affecting mobile privacy and mobile applications

**enisa:nefarious-activity-abuse="leakage-affecting-web-privacy-and-web-applications"**

Leakage affecting web privacy and web applications

**enisa:nefarious-activity-abuse="leakage-affecting-network-traffic"**

Leakage affecting network traffic

**enisa:nefarious-activity-abuse="leakage-affecting-cloud-computing"**

Leakage affecting cloud computing

**enisa:nefarious-activity-abuse="generation-and-use-of-rogue-certificates"**

Generation and use of rogue certificates

**enisa:nefarious-activity-abuse="loss-of-integrity-of-sensitive-information"**

Loss of (integrity of) sensitive information

**enisa:nefarious-activity-abuse="man-in-the-middle-session-hijacking"**

Man in the middle / Session hijacking

**enisa:nefarious-activity-abuse="social-engineering-via-signed-malware"**

Social Engineering / signed malware

**enisa:nefarious-activity-abuse="fake-SSL-certificates"**

Fake SSL certificates

**enisa:nefarious-activity-abuse="manipulation-of-hardware-and-software"**

Manipulation of hardware and software

**enisa:nefarious-activity-abuse="anonymous-proxies"**

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)

**enisa:nefarious-activity-abuse="abuse-of-vulnerabilities-0-day-vulnerabilities"**

Abuse of vulnerabilities, 0-day 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)

**enisa:nefarious-activity-abuse="access-to-device-software"**

Access to device software

**enisa:nefarious-activity-abuse="alternation-of-software"**

Alternation of software

**enisa:nefarious-activity-abuse="rogue-hardware"**

Rogue hardware

**enisa:nefarious-activity-abuse="manipulation-of-information"**

Manipulation of information

**enisa:nefarious-activity-abuse="repudiation-of-actions"**

Repudiation of actions

**enisa:nefarious-activity-abuse="address-space-hijacking-IP-prefixes"**

Address space hijacking (IP prefixes)

**enisa:nefarious-activity-abuse="routing-table-manipulation"**

Routing table manipulation

**enisa:nefarious-activity-abuse="DNS-poisoning-or-DNS-spoofing-or-DNS-Manipulations"**

DNS poisoning / DNS spoofing / DNS Manipulations

**enisa:nefarious-activity-abuse="falsification-of-record"**

Falsification of record

**enisa:nefarious-activity-abuse="autonomous-system-hijacking"**

Autonomous System hijacking

**enisa:nefarious-activity-abuse="autonomous-system-manipulation"**

Autonomous System manipulation

**enisa:nefarious-activity-abuse="falsification-of-configurations"**

Falsification of configurations

**enisa:nefarious-activity-abuse="misuse-of-audit-tools"**

Misuse of audit tools

**enisa:nefarious-activity-abuse="misuse-of-information-or-information systems-including-mobile-apps"**

Misuse of information/ information systems (including mobile apps)

**enisa:nefarious-activity-abuse="unauthorized-activities"**

Unauthorized activities

**enisa:nefarious-activity-abuse="Unauthorised-use-or-administration-of devices-and-systems"**

Unauthorised use or administration of devices and systems

**enisa:nefarious-activity-abuse="unauthorised-use-of-software"**

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)

**enisa:nefarious-activity-abuse="network-intrusion"**

Network Intrusion

**enisa:nefarious-activity-abuse="unauthorized-changes-of-records"**

Unauthorized changes of records

**enisa:nefarious-activity-abuse="unauthorized-installation-of-software"**

Unauthorized 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)



**enisa:nefarious-activity-abuse="compromising-confidential-information-like-data-breaches"**

Compromising confidential information (data breaches)

**enisa:nefarious-activity-abuse="hoax"**

Hoax

**enisa:nefarious-activity-abuse="false-rumour-and-or-fake-warning"**

False rumour and/or fake warning

**enisa:nefarious-activity-abuse="remote-activity-execution"**

Remote activity (execution)

**enisa:nefarious-activity-abuse="remote-command-execution"**

Remote Command Execution

**enisa:nefarious-activity-abuse="remote-access-tool"**

Remote Access Tool (RAT)

**enisa:nefarious-activity-abuse="botnets-remote-activity"**

Botnets / Remote activity

**enisa:nefarious-activity-abuse="targeted-attacks"**

Targeted attacks (APTs etc.)

**enisa:nefarious-activity-abuse="mobile-malware"**

Mobile malware

**enisa:nefarious-activity-abuse="spear-phishing-attacks"**

Spear phishing attacks

**enisa:nefarious-activity-abuse="installation-of-sophisticated-and-targeted-malware"**

Installation of sophisticated and targeted malware

**enisa:nefarious-activity-abuse="watering-hole-attacks"**

Watering Hole attacks

**enisa:nefarious-activity-abuse="failed-business-process"**

Failed business process

**enisa:nefarious-activity-abuse="brute-force"**

Brute force

**enisa:nefarious-activity-abuse="abuse-of-authorizations"**

Abuse of authorizations

## legal

**enisa:legal="violation-of-rules-and-regulations-breach-of-legislation"**

Violation of rules and regulations / Breach of legislation

**enisa:legal="failure-to-meet-contractual-requirements"**

Failure to meet contractual requirements

**enisa:legal="failure-to-meet-contractual-requirements-by-third-party"**

Failure to meet contractual requirements by third party

**enisa:legal="unauthorized-use-of-IPR-protected-resources"**

Unauthorized use of IPR protected resources

**enisa:legal="illegal-usage-of-file-sharing-services"**

Illegal usage of File Sharing services

**enisa:legal="abuse-of-personal-data"**

Abuse of personal data

**enisa:legal="judiciary-decisions-or-court-order"**

Judiciary decisions/court order

## 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)

## likelihood-probability

**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%

**estimative-language:likelihood-probability="unlikely"**

Unlikely - improbable (improbably) - 20-45%

**estimative-language:likelihood-probability="roughly-even-chance"**

Roughly even change - roughly even odds - 45-55%

**estimative-language:likelihood-probability="likely"**

Likely - probable (probably) - 55-80%

**estimative-language:likelihood-probability="very-likely"**

Very likely - highly probable - 80-95%

**estimative-language:likelihood-probability="almost-certain"**

Almost certain(ly) - nearly certain - 95-99%

## 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

## 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.

### TS-UE/EU-TS

**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

**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

**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

## **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**

### **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**

### **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**

### **europol-event:hosting-malware-webpage**

Hosting of malware on web page

Web page disseminating one or various types of malware.

## **c&c-server-hosting**

### **europol-event:c&c-server-hosting**

Hosting of malware on web page

Web page disseminating one or various types of malware.

## **worm-spreading**

### **europol-event:worm-spreading**

Replication and spreading of a worm

System infected by a worm trying to infect other systems.

## **connection-malware-port**

### **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**

### **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**

### **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**

### **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**

### **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**

### **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**

### **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**

### **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**

### **europol-event:system-probe**

System probe

Single system scan searching for open ports or services using these ports for responding.



## **network-scanning**

### **europol-event:network-scanning**

Network scanning

Scanning a network aimed at identifying systems which are active in the same network.

## **dns-zone-transfer**

### **europol-event:dns-zone-transfer**

DNS zone transfer

Transfer of a specific DNS zone.

## **wiretapping**

### **europol-event:wiretapping**

Wiretapping

Logical or physical interception of communications.

## **dissemination-phishing-emails**

### **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**

### **europol-event:hosting-phishing-sites**

Hosting phishing sites

Hosting web sites for phishing purposes.

## **aggregation-information-phishing-schemes**

### **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**

### **europol-event:exploit-attempt**

Exploit attempt

Unsuccessful use of a tool exploiting a specific vulnerability of the system.

## **sql-injection-attempt**

### **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**

### **europol-event:xss-attempt**

XSS attempt

Unsuccessful attempts to perform attacks by using cross-site scripting techniques.

## **file-inclusion-attempt**

### **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**

### **europol-event:brute-force-attempt**

Brute force attempt

Unsuccessful login attempt by using sequential credentials for gaining access to the system.

## **password-cracking-attempt**

### **europol-event:password-cracking-attempt**

Password cracking attempt

Attempt to acquire access credentials by breaking the protective cryptographic keys.

## **dictionary-attack-attempt**

### **europol-event:dictionary-attack-attempt**

Dictionary attack attempt

Unsuccessful login attempt by using system access credentials previously loaded into a dictionary.

## **exploit**

### **europol-event:exploit**

Use of a local or remote exploit

Successful use of a tool exploiting a specific vulnerability of the system.

## **sql-injection**

### **europol-event:sql-injection**

SQL injection

Manipulation or reading of information contained in a database by using the SQL injection technique.

## **XSS**

### **europol-event:xss**

XSS

Attacks performed with the use of cross-site scripting techniques.

## **file-inclusion**

### **europol-event:file-inclusion**

File inclusion

Inclusion of files into a system under attack with the use of file inclusion techniques.

## **control-system-bypass**

## **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**

### **europol-event:theft-access-credentials**

Theft of access credentials

Unauthorised access to a system or component by using stolen access credentials.

## **unauthorized-access-system**

### **europol-event:unauthorized-access-system**

Unauthorised access to a system

Unauthorised access to a system or component.

## **unauthorized-access-information**

### **europol-event:unauthorized-access-information**

Unauthorised access to information

Unauthorised access to a set of information.

## **data-exfiltration**

### **europol-event:data-exfiltration**

Data exfiltration

Unauthorised access to and sharing of a specific set of information.

## **modification-information**

### **europol-event:modification-information**

Modification of information

Unauthorised changes to a specific set of information.

## **deletion-information**

### **europol-event:deletion-information**

Deletion of information

Unauthorised deleting of a specific set of information.

## **illegitimate-use-resources**

### **europol-event:illegitimate-use-resources**

Misuse or unauthorised use of resources

Use of institutional resources for purposes other than those intended.

## **illegitimate-use-name**

### **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**

### **europol-event:email-flooding**

Email flooding

Sending an unusually large quantity of email messages.

## **spam**

### **europol-event:spam**

Sending an unsolicited message

Sending an email message that was unsolicited or unwanted by the recipient.

## **copyrighted-content**

### **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

### 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

### europol-event:unspecified

Other unspecified event

Other unlisted events.

## undetermined

### 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

### europol-incident:malware="distribution"

Distribution

### europol-incident:malware="c&c"

C&C

**europol-incident:malware="undetermined"**

Undetermined

## **availability**

**europol-incident:availability="dos-ddos"**

DoS/DDoS

**europol-incident:availability="sabotage"**

Sabotage

## **information-gathering**

**europol-incident:information-gathering="scanning"**

Scanning

**europol-incident:information-gathering="sniffing"**

Sniffing

**europol-incident:information-gathering="phishing"**

Phishing

## **intrusion-attempt**

**europol-incident:intrusion-attempt="exploitation-vulnerability"**

Exploitation of vulnerability

**europol-incident:intrusion-attempt="login-attempt"**

Login attempt

## **intrusion**

**europol-incident:intrusion="exploitation-vulnerability"**

Exploitation of vulnerability

**europol-incident:intrusion="compromising-account"**

Compromising an account

## information-security

**europol-incident:information-security="unauthorized-access"**

Unauthorised access

**europol-incident:information-security="unauthorized-modification"**

Unauthorised modification/deletion

## fraud

**europol-incident:fraud="illegitimate-use-resources"**

Misuse or unauthorised use of resources

**europol-incident:fraud="illegitimate-use-name"**

Illegitimate use of the name of a third party

## abusive-content

**europol-incident:abusive-content="spam"**

SPAM

**europol-incident:abusive-content="copyright"**

Copyright

**europol-incident:abusive-content="content-forbidden-by-law"**

Dissemination of content forbidden by law.

## other

**europol-incident:other="other"**

Other

## 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

### **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

## 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-defense

**fr-classif:classifiedes-defense="TRES\_SECRET\_DEFENSE"**

TRES SECRET DEFENSE

**fr-classif:classifiedes-defense="SECRET\_DEFENSE"**

SECRET DEFENSE

**fr-classif:classifiedes-defense="CONFIDENTIEL\_DEFENSE"**

CONFIDENTIEL DEFENSE

## non-classifiedes-defense

**fr-classif:non-classifiedes-defense="SECRET"**

SECRET

**fr-classif:non-classifiedes-defense="CONFIDENTIEL"**

CONFIDENTIEL

**fr-classif:non-classifiedes-defense="DIFFUSION\_RESTREINTE"**

DIFFUSION RESTREINTE

## non-classifiedes

**fr-classif:non-classifiedes="NON-CLASSIFIEES"**

NON CLASSIFIEES

## 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

## id

**iep:id="\$text"**

An id value is required

## **version**

**iep:version="\$text"**

A version value is required

## **name**

**iep:name="\$text"**

A name value is required

## **start-date**

**iep:start-date="\$text"**

A start-date value is required

## **end-date**

**iep:end-date="\$text"**

An end-date value is required

## **reference**

**iep:reference="\$text"**

A reference value is required

## **commercial-use**

**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**

**iep:external-reference="\$text"**

An external-reference value is required

## **encrypt-in-transit**

### **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**

### **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**

### **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**

### **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**

### **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**

### **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**

### **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**

### **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.

## **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**

### **information-security-indicators:IEX="FGY.1"**

Forged domain or brand names impersonating or imitating legitimate and genuine names

### **information-security-indicators:IEX="FGY.2"**

Wholly or partly forged websites (excluding parking pages) spoiling company's image or business

### **information-security-indicators:IEX="SPM.1"**

Not requested received bulk messages (spam) targeting organization's registered users

### **information-security-indicators:IEX="PHI.1"**

Phishing targeting company's customers' workstations spoiling company's image or business

### **information-security-indicators:IEX="PHI.2"**

Spear phishing or whaling carried out using social engineering and targeting organization's specific registered users

### **information-security-indicators:IEX="INT.1"**

Intrusion attempts on externally accessible servers

### **information-security-indicators:IEX="INT.2"**

Intrusion on externally accessible servers

### **information-security-indicators:IEX="INT.3"**

Intrusions on internal servers

### **information-security-indicators:IEX="DFC.1"**

Obvious and visible websites defacements

### **information-security-indicators:IEX="MIS.1"**

Servers resources misappropriation by external attackers

### **information-security-indicators:IEX="DOS.1"**

Denial of service attacks on websites

### **information-security-indicators:IEX="MLW.1"**

Attempts to install malware on workstations

### **information-security-indicators:IEX="MLW.2"**

Attempts to install malware on servers

### **information-security-indicators:IEX="MLW.3"**

Malware installed on workstations

### **information-security-indicators:IEX="MLW.4"**

Malware installed on internal servers

### **information-security-indicators:IEX="PHY.1"**

Human intrusion into the organization's perimeter

## **IMF**

### **information-security-indicators:IMF="BRE.1"**

Workstations accidental breakdowns or malfunctions

### **information-security-indicators:IMF="BRE.2"**

Servers accidental breakdowns or malfunctions

### **information-security-indicators:IMF="BRE.3"**

Mainframes accidental breakdowns or malfunctions

### **information-security-indicators:IMF="BRE.4"**

Networks accidental breakdowns or malfunctions

### **information-security-indicators:IMF="MDL.1"**

Delivery of email to wrong recipient

### **information-security-indicators:IMF="LOM.1"**

Loss (or theft) of mobile devices belonging to the organization

### **information-security-indicators:IMF="LOG.1"**

Downtime or malfunction of the log production function with possible legal impact

### **information-security-indicators:IMF="LOG.2"**

Absence of possible tracking of the person involved in a security event with possible legal impact

### **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

## **IDB**

### **information-security-indicators>IDB="UID.1"**

User impersonation

### **information-security-indicators>IDB="RGH.1"**

Privilege escalation by exploitation of software or configuration vulnerability on an externally



accessible server

### **information-security-indicators:IDB="RGH.2"**

Privilege escalation on a server or central application by social engineering

### **information-security-indicators:IDB="RGH.3"**

Use on a server or central application of administrator rights illicitly granted by an administrator

### **information-security-indicators:IDB="RGH.4"**

Use on a server or central application of time-limited granted rights after the planned period

### **information-security-indicators:IDB="RGH.5"**

Abuse of privileges by an administrator on a server or central application

### **information-security-indicators:IDB="RGH.6"**

Abuse of privileges by an operator or a plain user on a server or central application

### **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

### **information-security-indicators:IDB="MIS.1"**

Server resources misappropriation by an internal source

### **information-security-indicators:IDB="IAC.1"**

Access to hacking Website

### **information-security-indicators:IDB="LOG.1"**

Deactivating of logs recording by an administrator

## **IWH**

### **information-security-indicators:IWH="VNP.1"**

Exploitation of a software vulnerability without available patch

## **information-security-indicators:IWH="VNP.2"**

Exploitation of a non-patched software vulnerability

## **information-security-indicators:IWH="VNP.3"**

Exploitation of a poorly-patched software vulnerability

## **information-security-indicators:IWH="VCN.1"**

Exploitation of a configuration flaw

## **information-security-indicators:IWH="UKN.1"**

Not categorized security incidents

## **information-security-indicators:IWH="UNA.1"**

Security incidents on non-inventoried and/or not managed assets

## **VBH**

### **information-security-indicators:VBH="PRC.1"**

Server accessed by an administrator with unsecure protocols

### **information-security-indicators:VBH="PRC.2"**

P2P client in a workstation

### **information-security-indicators:VBH="PRC.3"**

VoIP clients in a workstation

### **information-security-indicators:VBH="PRC.4"**

Outbound connection dangerously set up

### **information-security-indicators:VBH="PRC.5"**

Not compliant laptop computer used to establish a connection

### **information-security-indicators:VBH="PRC.6"**

Other unsecure protocols used

**information-security-indicators:VBH="IAC.1"**

Outbound controls bypassed to access Internet

**information-security-indicators:VBH="IAC.2"**

Anonymization site used to access Internet

**information-security-indicators:VBH="FTR.1"**

Files recklessly downloaded

**information-security-indicators:VBH="FTR.2"**

Personal public instant messaging account used for business file exchanges

**information-security-indicators:VBH="FTR.3"**

Personal public messaging account used for business file exchanges

**information-security-indicators:VBH="WTI.1"**

Workstations accessed in administrator mode

**information-security-indicators:VBH="WTI.2"**

Personal storage devices used

**information-security-indicators:VBH="WTI.3"**

Personal devices used without compartmentalization (BYOD)

**information-security-indicators:VBH="WTI.4"**

Not encrypted sensitive files exported

**information-security-indicators:VBH="WTI.5"**

Personal software used

**information-security-indicators:VBH="WTI.6"**

Mailbox or Internet access with admin mode

**information-security-indicators:VBH="PSW.1"**

Weak passwords used

## **information-security-indicators:VBH="PSW.2"**

Passwords not changed

## **information-security-indicators:VBH="PSW.3"**

Administrator passwords not changed

## **information-security-indicators:VBH="RGH.1"**

Not compliant user rights granted illicitly by an administrator

## **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

## **information-security-indicators:VBH="HUW.2"**

Human weakness exploited by exchanges meant to entice or appeal to tell some secrets to be used later

## **VSW**

### **information-security-indicators:VSW="WSR.1"**

Web applications software vulnerabilities

### **information-security-indicators:VSW="OSW.1"**

OS software vulnerabilities regarding servers

### **information-security-indicators:VSW="WBR.1"**

Web browsers software vulnerabilities

## **VCF**

### **information-security-indicators:VCF="DIS.1"**

Dangerous or illicit services on externally accessible servers

### **information-security-indicators:VCF="LOG.1"**

Insufficient size of the space allocated for logs

### **information-security-indicators:VCF="FWR.1"**

Weak firewall filtering rules

### **information-security-indicators:VCF="WTI.1"**

Workstation wrongly configured

### **information-security-indicators:VCF="WTI.2"**

Autorun feature enabled on workstations

### **information-security-indicators:VCF="UAC.1"**

Access rights configuration not compliant with the security policy

### **information-security-indicators:VCF="UAC.2"**

Not compliant access rights on logs

### **information-security-indicators:VCF="UAC.3"**

Generic and shared administrator accounts

### **information-security-indicators:VCF="UAC.4"**

Accounts without owners

### **information-security-indicators:VCF="UAC.5"**

Inactive accounts

## **VTC**

### **information-security-indicators:VTC="BKP.1"**

Malfunction of server-hosted sensitive data safeguards

### **information-security-indicators:VTC="IDS.1"**

Full unavailability of IDS/IPS

### **information-security-indicators:VTC="WFI.1"**

Wi-Fi devices installed on the network without any official authorization

### **information-security-indicators:VTC="RAP.1"**

Remote access points used to gain unauthorized access

### **information-security-indicators:VTC="NRG.1"**

Devices or servers connected to the organization's network without being registered and managed

### **information-security-indicators:VTC="PHY.1"**

Not operational physical access control means

## **VOR**

### **information-security-indicators:VOR="DSC.1"**

Discovery of attacks

### **information-security-indicators:VOR="VNP.1"**

Excessive time of window of risk exposure

### **information-security-indicators:VOR="VNP.2"**

Rate of not patched systems

### **information-security-indicators:VOR="VNR.1"**

Rate of not reconfigured systems

### **information-security-indicators:VOR="RCT.1"**

Reaction plans launched without experience feedback

### **information-security-indicators:VOR="RCT.2"**

Reaction plans unsuccessfully launched

### **information-security-indicators:VOR="PRT.1"**

Launch of new IT projects without information classification

### **information-security-indicators:VOR="PRT.2"**

Launch of new specific IT projects without risk analysis

## **information-security-indicators:VOR="PRT.3"**

Launch of new IT projects of a standard type without identification of vulnerabilities and threats

## **IMP**

### **information-security-indicators:IMP="COS.1"**

Average cost to tackle a critical security incident

### **information-security-indicators:IMP="TIM.1"**

Average time of Websites downtime due to whole security incidents

### **information-security-indicators:IMP="TIM.2"**

Average time of Websites downtime due to successful malicious attacks

### **information-security-indicators:IMP="TIM.3"**

Average time of Websites downtime due to malfunctions or unintentional security incidents

## **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.



# 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.

## 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

## 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.

## **contributor**

**misp:contributor="pgpfingerprint"**

OpenPGP Fingerprint

## **confidence-level**

**misp:confidence-level="completely-confident"**

Completely confident

**misp:confidence-level="usually-confident"**

Usually confident

**misp:confidence-level="fairly-confident"**

Fairly confident

**misp:confidence-level="rarely-confident"**

Rarely confident

**misp:confidence-level="unconfident"**

Unconfident

**misp:confidence-level="confidence-cannot-be-evaluated"**

Confidence cannot be evaluated

## threat-level

**misp:threat-level="no-risk"**

No risk

**misp:threat-level="low-risk"**

Low risk

**misp:threat-level="medium-risk"**

Medium risk

**misp:threat-level="high-risk"**

High risk

## should-not-sync

## expansion

**misp:expansion="block"**

block

## 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

**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="BrowserModifier"**

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**

### **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="BrowserModifier"**

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="Spoofers"**

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 rootkit-enabled 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="GhostAdmin"**

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"**

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="Salinity"**

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-of-service (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="Nugel"**

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="Swinnag"**

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 arbitrary 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"**

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 malware 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="Kradbare"**

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"**

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, Tamper with root certificate trust, Modifies the system hosts file, Modifies your system DNS settings, Disables anti-virus products, Tamper 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.

# 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.

## 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

## 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](#).

## 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="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="expansion"**

Expansion

## **lifetime**

**osint:lifetime="perpetual"**

Perpetual

**osint:lifetime="ephemeral"**

Ephemeral

## **certainty**

**osint:certainty="100"**

100% Certainty

**osint:certainty="93"**

93% Almost certain

**osint:certainty="75"**

75% Probable

**osint:certainty="50"**

50% Chances about even

**osint:certainty="30"**

30% Probably not

**osint:certainty="7"**

7% Almost certainly not

**osint:certainty="0"**

0% Impossibility

## 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

## class

**passivetotal:class="malicious"**

Malicious

**passivetotal:class="suspicious"**

Malicious

**passivetotal:class="non-malicious"**

Non Malicious

**passivetotal:class="unknown"**

Unknown

## dynamic-dns

**passivetotal:dynamic-dns="yes"**

Yes

**passivetotal:dynamic-dns="no"**

No

## 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.

## 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

## 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](#).

### 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.

## 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](#).

## 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"**

Government & 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="authentication-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.

Monitoring a Malware Menagerie" along with Katie Kleemola and Greg Wiseman.

## targeting-sophistication-base-value

### **targeted-threat-index:targeting-sophistication-base-value="not-targeted"**

Not targeted, e.g. spam or financially motivated malware.

## **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.

## **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.

## **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.

## **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.

## **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.

## **technical-sophistication-multiplier**

### **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.

### **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.

## **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.

## **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.

## **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.

## **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.

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.

## **red**

### **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

## **t1p: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

## **t1p: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

## **t1p: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

## **t1p: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

# 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)

## iso\_currency\_code

### **veris:iso\_currency\_code="DZD"**

DZD - Algerian Dinar

### **veris:iso\_currency\_code="NAD"**

NAD - Namibia Dollar

### **veris:iso\_currency\_code="GHS"**

GHS - Ghana Cedi

**veris:iso\_currency\_code="EGP"**

EGP - Egyptian Pound

**veris:iso\_currency\_code="BGN"**

BGN - Bulgarian Lev

**veris:iso\_currency\_code="PAB"**

PAB - Balboa

**veris:iso\_currency\_code="BOB"**

BOB - Boliviano

**veris:iso\_currency\_code="DKK"**

DKK - Danish Krone

**veris:iso\_currency\_code="BWP"**

BWP - Pula

**veris:iso\_currency\_code="LBP"**

LBP - Lebanese Pound

**veris:iso\_currency\_code="TZS"**

TZS - Tanzanian Shilling

**veris:iso\_currency\_code="VND"**

VND - Dong

**veris:iso\_currency\_code="AOA"**

AOA - Kwanza

**veris:iso\_currency\_code="KHR"**

KHR - Riel

**veris:iso\_currency\_code="MYR"**

MYR - Malaysian Ringgit



**veris:iso\_currency\_code="KYD"**

KYD - Cayman Islands Dollar

**veris:iso\_currency\_code="LYD"**

LYD - Libyan Dinar

**veris:iso\_currency\_code="UAH"**

UAH - Hryvnia

**veris:iso\_currency\_code="JOD"**

JOD - Jordanian Dinar

**veris:iso\_currency\_code="AWG"**

AWG - Aruban Florin

**veris:iso\_currency\_code="SAR"**

SAR - Saudi Riyal

**veris:iso\_currency\_code="EUR"**

EUR - Euro

**veris:iso\_currency\_code="HKD"**

HKD - Hong Kong Dollar

**veris:iso\_currency\_code="CHF"**

CHF - Swiss Franc

**veris:iso\_currency\_code="GIP"**

GIP - Gibraltar Pound

**veris:iso\_currency\_code="BYR"**

BYR - Belarussian Ruble

**veris:iso\_currency\_code="ALL"**

ALL - Lek

**veris:iso\_currency\_code="MRO"**

MRO - Ouguiya

**veris:iso\_currency\_code="HRK"**

HRK - Croatian Kuna

**veris:iso\_currency\_code="DJF"**

DJF - Djibouti Franc

**veris:iso\_currency\_code="SZL"**

SZL - Lilangeni

**veris:iso\_currency\_code="THB"**

THB - Baht

**veris:iso\_currency\_code="XAF"**

XAF - CFA Franc BEAC

**veris:iso\_currency\_code="BND"**

BND - Brunei Dollar

**veris:iso\_currency\_code="ISK"**

ISK - Iceland Krona

**veris:iso\_currency\_code="UYU"**

UYU - Peso Uruguayo

**veris:iso\_currency\_code="NIO"**

NIO - Cordoba Oro

**veris:iso\_currency\_code="LAK"**

LAK - Kip

**veris:iso\_currency\_code="SYP"**

SYP - Syrian Pound

**veris:iso\_currency\_code="MAD"**

MAD - Moroccan Dirham

**veris:iso\_currency\_code="MZN"**

MZN - Mozambique Metical

**veris:iso\_currency\_code="PHP"**

PHP - Philippine Peso

**veris:iso\_currency\_code="ZAR"**

ZAR - South African Rand

**veris:iso\_currency\_code="NPR"**

NPR - Nepalese Rupee

**veris:iso\_currency\_code="NGN"**

NGN - Naira

**veris:iso\_currency\_code="ZWD"**

ZWD - Zimbabwean Dollar A/06

**veris:iso\_currency\_code="CRC"**

CRC - Costa Rican Colon

**veris:iso\_currency\_code="AED"**

AED - UAE Dirham

**veris:iso\_currency\_code="GBP"**

GBP - Pound Sterling

**veris:iso\_currency\_code="MWK"**

MWK - Kwacha

**veris:iso\_currency\_code="LKR"**

LKR - Sri Lanka Rupee

**veris:iso\_currency\_code="PKR"**

PKR - Pakistan Rupee

**veris:iso\_currency\_code="HUF"**

HUF - Forint

**veris:iso\_currency\_code="BMD"**

BMD - Bermudian Dollar

**veris:iso\_currency\_code="LSL"**

LSL - Loti

**veris:iso\_currency\_code="MNT"**

MNT - Tugrik

**veris:iso\_currency\_code="AMD"**

AMD - Armenian Dram

**veris:iso\_currency\_code="UGX"**

UGX - Uganda Shilling

**veris:iso\_currency\_code="QAR"**

QAR - Qatari Rial

**veris:iso\_currency\_code="XDR"**

XDR - SDR (Special Drawing Right)

**veris:iso\_currency\_code="JMD"**

JMD - Jamaican Dollar

**veris:iso\_currency\_code="GEL"**

GEL - Lari

**veris:iso\_currency\_code="SHP"**

SHP - Saint Helena Pound

**veris:iso\_currency\_code="AFN"**

AFN - Afghani

**veris:iso\_currency\_code="SBD"**

SBD - Solomon Islands Dollar

**veris:iso\_currency\_code="KPW"**

KPW - North Korean Won

**veris:iso\_currency\_code="TRY"**

TRY - Turkish Lira

**veris:iso\_currency\_code="BDT"**

BDT - Taka

**veris:iso\_currency\_code="YER"**

YER - Yemeni Rial

**veris:iso\_currency\_code="HTG"**

HTG - Gourde

**veris:iso\_currency\_code="XOF"**

XOF - CFA Franc BCEAO

**veris:iso\_currency\_code="MGA"**

MGA - Malagasy Ariary

**veris:iso\_currency\_code="ANG"**

ANG - Netherlands Antillean Guilder

**veris:iso\_currency\_code="LRD"**

LRD - Liberian Dollar

**veris:iso\_currency\_code="RWF"**

RWF - Rwanda Franc

**veris:iso\_currency\_code="NOK"**

NOK - Norwegian Krone

**veris:iso\_currency\_code="MOP"**

MOP - Pataca

**veris:iso\_currency\_code="INR"**

INR - Indian Rupee

**veris:iso\_currency\_code="MXN"**

MXN - Mexican Peso

**veris:iso\_currency\_code="CZK"**

CZK - Czech Koruna

**veris:iso\_currency\_code="TJS"**

TJS - Somoni

**veris:iso\_currency\_code="TWD"**

TWD - New Taiwan Dollar

**veris:iso\_currency\_code="BTN"**

BTN - Ngultrum

**veris:iso\_currency\_code="COP"**

COP - Colombian Peso

**veris:iso\_currency\_code="TMT"**

TMT - Turkmenistan New Manat

**veris:iso\_currency\_code="MUR"**

MUR - Mauritius Rupee

**veris:iso\_currency\_code="IDR"**

IDR - Rupiah

**veris:iso\_currency\_code="HNL"**

HNL - Lempira

**veris:iso\_currency\_code="XPF"**

XPF - CFP Franc

**veris:iso\_currency\_code="FJD"**

FJD - Fiji Dollar

**veris:iso\_currency\_code="ETB"**

ETB - Ethiopian Birr

**veris:iso\_currency\_code="PEN"**

PEN - Nuevo Sol

**veris:iso\_currency\_code="BZD"**

BZD - Belize Dollar

**veris:iso\_currency\_code="ILS"**

ILS - New Israeli Sheqel

**veris:iso\_currency\_code="DOP"**

DOP - Dominican Peso

**veris:iso\_currency\_code="GGP"**

GGP - Guernsey pound

**veris:iso\_currency\_code="MDL"**

MDL - Moldovan Leu

**veris:iso\_currency\_code="BSD"**

BSD - Bahamian Dollar

**veris:iso\_currency\_code="SPL"**

SPL - Seborga Luigino

**veris:iso\_currency\_code="SEK"**

SEK - Swedish Krona

**veris:iso\_currency\_code="ZMK"**

ZMK - Zambian Kwacha

**veris:iso\_currency\_code="JEP"**

JEP - Jersey pound

**veris:iso\_currency\_code="AUD"**

AUD - Australian Dollar

**veris:iso\_currency\_code="SRD"**

SRD - Surinam Dollar

**veris:iso\_currency\_code="CUP"**

CUP - Cuban Peso

**veris:iso\_currency\_code="BBD"**

BBD - Barbados Dollar

**veris:iso\_currency\_code="KMF"**

KMF - Comoro Franc

**veris:iso\_currency\_code="KRW"**

KRW - South Korean Won

**veris:iso\_currency\_code="GMD"**

GMD - Dalasi

**veris:iso\_currency\_code="VEF"**

VEF - Bolivar

**veris:iso\_currency\_code="IMP"**

IMP - Isle of Man Pound



**veris:iso\_currency\_code="CUC"**

CUC - Peso Convertible

**veris:iso\_currency\_code="TVD"**

TVD - Tuvalu Dollar

**veris:iso\_currency\_code="CLP"**

CLP - Chilean Peso

**veris:iso\_currency\_code="LTL"**

LTL - Lithuanian Litas

**veris:iso\_currency\_code="CDF"**

CDF - Congolese Franc

**veris:iso\_currency\_code="XCD"**

XCD - East Caribbean Dollar

**veris:iso\_currency\_code="KZT"**

KZT - Tenge

**veris:iso\_currency\_code="RUB"**

RUB - Russian Ruble

**veris:iso\_currency\_code="TTD"**

TTD - Trinidad and Tobago Dollar

**veris:iso\_currency\_code="OMR"**

OMR - Rial Omani

**veris:iso\_currency\_code="BRL"**

BRL - Brazilian Real

**veris:iso\_currency\_code="MMK"**

MMK - Kyat

**veris:iso\_currency\_code="PLN"**

PLN - Zloty

**veris:iso\_currency\_code="PYG"**

PYG - Guarani

**veris:iso\_currency\_code="KES"**

KES - Kenyan Shilling

**veris:iso\_currency\_code="SVC"**

SVC - El Salvador Colon

**veris:iso\_currency\_code="MKD"**

MKD - Denar

**veris:iso\_currency\_code="AZN"**

AZN - Azerbaijanian Manat

**veris:iso\_currency\_code="TOP"**

TOP - Pa'anga

**veris:iso\_currency\_code="MVR"**

MVR - Rufiyaa

**veris:iso\_currency\_code="VUV"**

VUV - Vatu

**veris:iso\_currency\_code="GNF"**

GNF - Guinea Franc

**veris:iso\_currency\_code="WST"**

WST - Tala

**veris:iso\_currency\_code="IQD"**

IQD - Iraqi Dinar

**veris:iso\_currency\_code="ERN"**

ERN - Nakfa

**veris:iso\_currency\_code="BAM"**

BAM - Convertible Mark

**veris:iso\_currency\_code="SCR"**

SCR - Seychelles Rupee

**veris:iso\_currency\_code="CAD"**

CAD - Canadian Dollar

**veris:iso\_currency\_code="CVE"**

CVE - Cape Verde Escudo

**veris:iso\_currency\_code="KWD"**

KWD - Kuwaiti Dinar

**veris:iso\_currency\_code="BIF"**

BIF - Burundi Franc

**veris:iso\_currency\_code="PGK"**

PGK - Kina

**veris:iso\_currency\_code="SOS"**

SOS - Somali Shilling

**veris:iso\_currency\_code="SGD"**

SGD - Singapore Dollar

**veris:iso\_currency\_code="UZS"**

UZS - Uzbekistan Sum

**veris:iso\_currency\_code="STD"**

STD - Dobra

**veris:iso\_currency\_code="IRR"**

IRR - Iranian Rial

**veris:iso\_currency\_code="CNY"**

CNY - Yuan Renminbi

**veris:iso\_currency\_code="SLL"**

SLL - Leone

**veris:iso\_currency\_code="TND"**

TND - Tunisian Dinar

**veris:iso\_currency\_code="GYD"**

GYD - Guyana Dollar

**veris:iso\_currency\_code="NZD"**

NZD - New Zealand Dollar

**veris:iso\_currency\_code="FKP"**

FKP - Falkland Islands Pound

**veris:iso\_currency\_code="LVL"**

LVL - Latvian Lats

**veris:iso\_currency\_code="USD"**

USD - US Dollar

**veris:iso\_currency\_code="KGS"**

KGS - Som

**veris:iso\_currency\_code="ARS"**

ARS - Argentine Peso

**veris:iso\_currency\_code="RON"**

RON - New Romanian Leu

**veris:iso\_currency\_code="GTQ"**

GTQ - Quetzal

**veris:iso\_currency\_code="RSD"**

RSD - Serbian Dinar

**veris:iso\_currency\_code="BHD"**

BHD - Bahraini Dinar

**veris:iso\_currency\_code="JPY"**

JPY - Yen

**veris:iso\_currency\_code="SDG"**

SDG - Sudanese Pound

## **confidence**

**veris:confidence="High"**

High confidence

**veris:confidence="None"**

No confidence

**veris:confidence="Medium"**

Medium confidence

**veris:confidence="Low"**

Low confidence

## **targeted**

**veris:targeted="Targeted"**

Targeted: victim chosen as target then actor determined what weaknesses could be exploited

**veris:targeted="NA"**

Not applicable

**veris:targeted="Opportunistic"**

Opportunistic: victim attacked because they exhibited a weakness the actor knew how to exploit

**veris:targeted="Unknown"**

Unknown

## **discovery\_method**

**veris:discovery\_method="Int - financial audit"**

Internal - financial audit and reconciliation process

**veris:discovery\_method="Ext - found documents"**

External - Found documents

**veris:discovery\_method="Unknown"**

Unknown

**veris:discovery\_method="Ext - audit"**

External - security audit or scan

**veris:discovery\_method="Ext - incident response"**

External - Notified while investigating another incident

**veris:discovery\_method="Ext - unknown"**

External - unknown

**veris:discovery\_method="Other"**

Other

**veris:discovery\_method="Int - NIDS"**

Internal - network IDS or IPS alert

**veris:discovery\_method="Ext - emergency response team"**

External - Emergency response team

**veris:discovery\_method="Ext - fraud detection"**

External - fraud detection (e.g., CPP)

**veris:discovery\_method="Int - incident response"**

Internal - discovered while responding to another (separate) incident

**veris:discovery\_method="Ext - customer"**

External - reported by customer or partner affected by the incident

**veris:discovery\_method="Prt - audit"**

Partner - Audit performed by a partner organization

**veris:discovery\_method="Int - IT review"**

Internal - Informal IT review

**veris:discovery\_method="Int - log review"**

Internal - log review process or SIEM

**veris:discovery\_method="Int - unknown"**

Internal - unknown

**veris:discovery\_method="Ext - suspicious traffic"**

External - Report of suspicious traffic

**veris:discovery\_method="Int - HIDS"**

Internal - host IDS or file integrity monitoring

**veris:discovery\_method="Prt - Other"**

Partner - Other

**veris:discovery\_method="Ext - monitoring service"**

External - managed security event monitoring service

**veris:discovery\_method="Prt - antivirus"**

Partner - Notified by antivirus company but not through AV product

## **veris:discovery\_method="Prt - Unknown"**

Partner - Unknown

## **veris:discovery\_method="Int - security alarm"**

Internal - physical security system alarm

## **veris:discovery\_method="Ext - law enforcement"**

Internal - notified by law enforcement or government agency

## **veris:discovery\_method="Int - antivirus"**

Internal - antivirus alert

## **veris:discovery\_method="Int - infrastructure monitoring"**

Internal - Infrastructure monitoring

## **veris:discovery\_method="Prt - incident response"**

Partner - notified while investigating another incident

## **veris:discovery\_method="Int - data loss prevention"**

Internal - Data loss prevention software

## **veris:discovery\_method="Int - fraud detection"**

Internal - fraud detection mechanism

## **veris:discovery\_method="Prt - monitoring service"**

Partner - Reported by a monitoring service

## **veris:discovery\_method="Int - reported by employee"**

Internal - reported by employee who saw something odd

## **veris:discovery\_method="Ext - actor disclosure"**

External - disclosed by threat agent (e.g., public brag, private blackmail)

## **cost\_corrective\_action**



**veris:cost\_corrective\_action="Simple and cheap"**

Simple and cheap

**veris:cost\_corrective\_action="Unknown"**

Unknown

**veris:cost\_corrective\_action="Something in-between"**

Something in-between

**veris:cost\_corrective\_action="Difficult and expensive"**

Difficult and expensive

## **security\_incident**

**veris:security\_incident="Suspected"**

Suspected

**veris:security\_incident="Confirmed"**

Yes - Confirmed

**veris:security\_incident="Near miss"**

Near miss (actions did not compromise asset)

**veris:security\_incident="False positive"**

False positive (response triggered, but no incident)

## **country**

**veris:country="BD"**

Bangladesh

**veris:country="BE"**

Belgium

**veris:country="BF"**

Burkina Faso

**veris:country="BG"**

Bulgaria

**veris:country="BA"**

Bosnia and Herzegovina

**veris:country="BB"**

Barbados

**veris:country="WF"**

Wallis and Futuna Islands

**veris:country="BL"**

Saint-Barthelemy

**veris:country="BM"**

Bermuda

**veris:country="BN"**

Brunei Darussalam

**veris:country="BO"**

Bolivia

**veris:country="BH"**

Bahrain

**veris:country="BI"**

Burundi

**veris:country="BJ"**

Benin

**veris:country="BT"**

Bhutan

**veris:country="JM"**

Jamaica

**veris:country="BV"**

Bouvet Island

**veris:country="BW"**

Botswana

**veris:country="WS"**

Samoa

**veris:country="BQ"**

Bonaire, Saint Eustatius and Saba

**veris:country="BR"**

Brazil

**veris:country="BS"**

Bahamas

**veris:country="JE"**

Jersey

**veris:country="BY"**

Belarus

**veris:country="BZ"**

Belize

**veris:country="RU"**

Russian Federation

**veris:country="RW"**

Rwanda

**veris:country="RS"**

Serbia

**veris:country="TL"**

Timor-Leste

**veris:country="RE"**

Reunion

**veris:country="TM"**

Turkmenistan

**veris:country="Unknown"**

Unknown

**veris:country="TJ"**

Tajikistan

**veris:country="RO"**

Romania

**veris:country="TK"**

Tokelau

**veris:country="GW"**

Guinea-Bissau

**veris:country="GU"**

Guam

**veris:country="GT"**

Guatemala

**veris:country="GS"**

South Georgia and the South Sandwich Islands

**veris:country="GR"**

Greece

**veris:country="GQ"**

Equatorial Guinea

**veris:country="GP"**

Guadeloupe

**veris:country="JP"**

Japan

**veris:country="GY"**

Guyana

**veris:country="GG"**

Guernsey

**veris:country="GF"**

French Guiana

**veris:country="GE"**

Georgia

**veris:country="GD"**

Grenada

**veris:country="GB"**

United Kingdom

**veris:country="GA"**

Gabon

**veris:country="SV"**

El Salvador

**veris:country="GN"**

Guinea

**veris:country="GM"**

Gambia

**veris:country="GL"**

Greenland

**veris:country="GI"**

Gibraltar

**veris:country="GH"**

Ghana

**veris:country="OM"**

Oman

**veris:country="TN"**

Tunisia

**veris:country="JO"**

Jordan

**veris:country="HR"**

Croatia

**veris:country="HT"**

Haiti

**veris:country="HU"**

Hungary

**veris:country="HK"**

Hong Kong

**veris:country="HN"**

Honduras

**veris:country="HM"**

Heard Island and McDonal Islands

**veris:country="VE"**

Venezuela (Bolivarian Republic of)

**veris:country="PR"**

Puerto Rico

**veris:country="PS"**

Palestinian Territory, Occupied

**veris:country="PW"**

Palau

**veris:country="PT"**

Portugal

**veris:country="SJ"**

Svalbard and Jan Mayen Islands

**veris:country="PY"**

Paraguay

**veris:country="IQ"**

Iraq

**veris:country="PA"**

Panama

**veris:country="PF"**

French Polynesia

**veris:country="PG"**

Papua New Guinea

**veris:country="PE"**

Peru

**veris:country="PK"**

Pakistan

**veris:country="PH"**

Philippines

**veris:country="PN"**

Pitcairn

**veris:country="PL"**

Poland

**veris:country="PM"**

Saint Pierre and Miquelon

**veris:country="ZM"**

Zambia

**veris:country="EH"**

Western Sahara

**veris:country="EE"**

Estonia

**veris:country="EG"**

Egypt

**veris:country="ZA"**

South Africa



**veris:country="EC"**

Ecuador

**veris:country="IT"**

Italy

**veris:country="VN"**

Viet Nam

**veris:country="SB"**

Solomon Islands

**veris:country="ET"**

Ethiopia

**veris:country="SO"**

Somalia

**veris:country="ZW"**

Zimbabwe

**veris:country="SA"**

Saudi Arabia

**veris:country="ES"**

Spain

**veris:country="ER"**

Eritrea

**veris:country="ME"**

Montenegro

**veris:country="MD"**

Moldova, Republic of

**veris:country="MG"**

Madagascar

**veris:country="MF"**

Saint Martin (French part)

**veris:country="MA"**

Morocco

**veris:country="MC"**

Monaco

**veris:country="UZ"**

Uzbekistan

**veris:country="MM"**

Myanmar

**veris:country="ML"**

Mali

**veris:country="MO"**

Macao

**veris:country="MN"**

Mongolia

**veris:country="MH"**

Marshall Islands

**veris:country="MK"**

Macedonia, The former Yugoslav Republic of

**veris:country="MU"**

Mauritius

**veris:country="MT"**

Malta

**veris:country="MW"**

Malawi

**veris:country="MV"**

Maldives

**veris:country="MQ"**

Martinique

**veris:country="MP"**

Northern Mariana Islands

**veris:country="MS"**

Montserrat

**veris:country="MR"**

Mauritania

**veris:country="IM"**

Isle of Man

**veris:country="UG"**

Uganda

**veris:country="TZ"**

Tanzania, United Republic of

**veris:country="MY"**

Malaysia

**veris:country="MX"**

Mexico

**veris:country="IL"**

Israel

**veris:country="FR"**

France

**veris:country="IO"**

British Virgin Islands

**veris:country="SH"**

Saint Helena

**veris:country="FI"**

Finland

**veris:country="FJ"**

Fiji

**veris:country="FK"**

Faeroe Islands

**veris:country="FM"**

Micronesia (Federated States of)

**veris:country="FO"**

Falkland Islands (Malvinas)

**veris:country="NI"**

Nicaragua

**veris:country="NL"**

Netherlands

**veris:country="NO"**

Norway

**veris:country="NA"**

Namibia

**veris:country="VU"**

Vanuatu

**veris:country="NC"**

New Caledonia

**veris:country="NE"**

Niger

**veris:country="NF"**

Norfolk Island

**veris:country="NG"**

Nigeria

**veris:country="NZ"**

New Zealand

**veris:country="NP"**

Nepal

**veris:country="NR"**

Nauru

**veris:country="NU"**

Niue

**veris:country="CK"**

Cook Islands

**veris:country="CI"**

Cote d'Ivoire

**veris:country="CH"**

Switzerland

**veris:country="CO"**

Colombia

**veris:country="CN"**

China

**veris:country="CM"**

Cameroon

**veris:country="CL"**

Chile

**veris:country="CC"**

Cocos (Keeling) Islands

**veris:country="CA"**

Canada

**veris:country="CG"**

Congo

**veris:country="CF"**

Central African Republic

**veris:country="CD"**

Congo, Democratic Republic of the

**veris:country="CZ"**

Czech Republic

**veris:country="CY"**

Cyprus

**veris:country="CX"**

Christmas Island

**veris:country="CR"**

Costa Rica

**veris:country="CW"**

Curacao

**veris:country="CV"**

Cape Verde

**veris:country="CU"**

Cuba

**veris:country="SZ"**

Swaziland

**veris:country="SY"**

Syrian Arab Republic

**veris:country="SX"**

Sint Maarten (Dutch part)

**veris:country="KG"**

Kyrgyzstan

**veris:country="KE"**

Kenya

**veris:country="SS"**

South Sudan

**veris:country="SR"**

Suriname

**veris:country="KI"**

Kiribati

**veris:country="KH"**

Cambodia

**veris:country="KN"**

Saint Kitts and Nevis

**veris:country="KM"**

Comoros

**veris:country="ST"**

Sao Tome and Principe

**veris:country="SK"**

Slovakia

**veris:country="KR"**

Korea, Republic of

**veris:country="SI"**

Slovenia

**veris:country="KP"**

Korea, Democratic People's Republic of

**veris:country="KW"**

Kuwait

**veris:country="SN"**

Senegal

**veris:country="SM"**

San Marino



**veris:country="SL"**

Sierra Leone

**veris:country="SC"**

Seychelles

**veris:country="KZ"**

Kazakhstan

**veris:country="KY"**

Cayman Islands

**veris:country="SG"**

Singapore

**veris:country="SE"**

Sweden

**veris:country="SD"**

Sudan

**veris:country="DO"**

Dominican Republic

**veris:country="DM"**

Dominica

**veris:country="DJ"**

Djibouti

**veris:country="DK"**

Denmark

**veris:country="VG"**

British Virgin Islands

**veris:country="DE"**

Germany

**veris:country="YE"**

Yemen

**veris:country="Other"**

Other

**veris:country="DZ"**

Algeria

**veris:country="US"**

United States of America

**veris:country="UY"**

Uruguay

**veris:country="YT"**

Mayotte

**veris:country="UM"**

United States Minor Outlying Islands

**veris:country="LB"**

Lebanon

**veris:country="LC"**

Saint Lucia

**veris:country="LA"**

Lao People's Democratic Republic

**veris:country="TV"**

Tuvalu

**veris:country="TW"**

Taiwan, Province of China

**veris:country="TT"**

Trinidad and Tobago

**veris:country="TR"**

Turkey

**veris:country="LK"**

Sri Lanka

**veris:country="LI"**

Liechtenstein

**veris:country="LV"**

Latvia

**veris:country="TO"**

Tonga

**veris:country="LT"**

Lithuania

**veris:country="LU"**

Luxembourg

**veris:country="LR"**

Liberia

**veris:country="LS"**

Lesotho

**veris:country="TH"**

Thailand

**veris:country="TF"**

French Southern Territories

**veris:country="TG"**

Togo

**veris:country="TD"**

Chad

**veris:country="TC"**

Turks and Caicos Islands

**veris:country="LY"**

Libya

**veris:country="VA"**

Holy See

**veris:country="VC"**

Saint Vincent and the Grenadines

**veris:country="AE"**

United Arab Emirates

**veris:country="AD"**

Andorra

**veris:country="AG"**

Antigua and Barbuda

**veris:country="AF"**

Afghanistan

**veris:country="AI"**

Anguilla

**veris:country="VI"**

United States Virgin Islands

**veris:country="IS"**

Iceland

**veris:country="IR"**

Iran (Islamic Republic of)

**veris:country="AM"**

Armenia

**veris:country="AL"**

Albania

**veris:country="AO"**

Angola

**veris:country="AQ"**

Antarctica

**veris:country="AS"**

American Samoa

**veris:country="AR"**

Argentina

**veris:country="AU"**

Australia

**veris:country="AT"**

Austria

**veris:country="AW"**

Aruba

**veris:country="IN"**

India

**veris:country="AX"**

Aland Islands

**veris:country="AZ"**

Azerbaijan

**veris:country="IE"**

Ireland

**veris:country="ID"**

Indonesia

**veris:country="UA"**

Ukraine

**veris:country="QA"**

Qatar

**veris:country="MZ"**

Mozambique

## **impact:overall\_rating**

**veris:impact:overall\_rating="Insignificant"**

Insignificant: Impact absorbed by normal activities

**veris:impact:overall\_rating="Catastrophic"**

Catastrophic: A business-ending event (don't choose this if the victim will continue operations)

**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="Damaging"**

Damaging: Real and serious effect on the "bottom line" and/or long-term ability to generate revenue

## **veris:impact:overall\_rating="Unknown"**

Unknown

## **veris:impact:overall\_rating="Painful"**

Painful: Limited "hard costs", but impact felt through having to deal with the incident rather than conducting normal duties

## **actor:motive**

### **veris:actor:motive="Grudge"**

Grudge or personal offense

### **veris:actor:motive="Financial"**

Financial or personal gain

### **veris:actor:motive="NA"**

Not Applicable (unintentional action)

### **veris:actor:motive="Ideology"**

Ideology or protest

### **veris:actor:motive="Convenience"**

Convenience of expediency

### **veris:actor:motive="Other"**

Other

### **veris:actor:motive="Unknown"**

Unknown

### **veris:actor:motive="Fun"**

Fun, curiosity, or pride

## **veris:actor:motive="Fear"**

Fear or duress

## **veris:actor:motive="Espionage"**

Espionage or competitive advantage

## **veris:actor:motive="Secondary"**

Aid in a different attack

## **asset:management**

### **veris:asset:management="NA"**

Not applicable

### **veris:asset:management="Internal"**

Internally managed

### **veris:asset:management="External"**

Externally managed

### **veris:asset:management="Unknown"**

Unknown

## **asset:variety**

### **veris:asset:variety="M - Flash drive"**

Media - Flash drive or card

### **veris:asset:variety="S - Print"**

Server - Print

### **veris:asset:variety="P - Guard"**

People - Guard

### **veris:asset:variety="S - Database"**

Server - Database



**veris:asset:variety="N - PBX"**

Network - Private branch exchange (PBX)

**veris:asset:variety="M - Other"**

Media - Other/Unknown

**veris:asset:variety="S - Other"**

Server - Other/Unknown

**veris:asset:variety="P - System admin"**

People - Administrator

**veris:asset:variety="S - POS controller"**

Server - POS controller

**veris:asset:variety="T - Other"**

Public Terminal - Other/Unknown

**veris:asset:variety="N - Camera"**

Network - Camera or surveillance system

**veris:asset:variety="S - Unknown"**

Server - Unknown

**veris:asset:variety="S - DHCP"**

Server - DHCP

**veris:asset:variety="U - POS terminal"**

User Device - POS terminal

**veris:asset:variety="N - LAN"**

Network - Wired LAN

**veris:asset:variety="P - Manager"**

People - Manager

**veris:asset:variety="M - Payment card"**

Media - Payment card (e.g., magstripe, EMV)

**veris:asset:variety="N - Public WAN"**

Network - Public WAN

**veris:asset:variety="P - Former employee"**

People - Former employee

**veris:asset:variety="S - Authentication"**

Server - Authentication

**veris:asset:variety="U - Mobile phone"**

User Device - Mobile phone or smartphone

**veris:asset:variety="N - Router or switch"**

Network - Router or switch

**veris:asset:variety="T - Kiosk"**

Public Terminal - Self-service kiosk

**veris:asset:variety="N - HSM"**

Network - Hardware security module (HSM)

**veris:asset:variety="U - Peripheral"**

User Device - Peripheral (e.g., printer, copier, fax)

**veris:asset:variety="S - Code repository"**

Server - Code repository

**veris:asset:variety="S - SCADA"**

Server - SCADA system

**veris:asset:variety="P - End-user"**

People - End-user

**veris:asset:variety="N - SAN"**

Network - Storage area network (SAN)

**veris:asset:variety="T - ATM"**

Public Terminal - Automated Teller Machine (ATM)

**veris:asset:variety="N - RTU"**

Network - Remote terminal unit (RTU)

**veris:asset:variety="Unknown"**

Unknown

**veris:asset:variety="M - Smart card"**

Media - Identity smart card

**veris:asset:variety="N - IDS"**

Network - IDS or IPS

**veris:asset:variety="N - PLC"**

Network - Programmable logic controller (PLC)

**veris:asset:variety="N - Other"**

Network - Other/Unknown

**veris:asset:variety="P - Cashier"**

People - Cashier

**veris:asset:variety="P - Executive"**

People - Executive

**veris:asset:variety="U - Desktop"**

User Device - Desktop or workstation

**veris:asset:variety="U - Tablet"**

User Device - Tablet

**veris:asset:variety="N - Firewall"**

Network - Firewall

**veris:asset:variety="P - Customer"**

People - Customer

**veris:asset:variety="S - Mainframe"**

Server - Mainframe

**veris:asset:variety="S - Directory"**

Server - Directory (LDAP, AD)

**veris:asset:variety="U - Auth token"**

User Device - Authentication token or device

**veris:asset:variety="U - Media"**

User Device - Media player or recorder

**veris:asset:variety="T - Gas terminal"**

Public Terminal - Gas "pay-at-the-pump" terminal

**veris:asset:variety="T - PED pad"**

Public Terminal - Detached PIN pad or card reader

**veris:asset:variety="M - Disk drive"**

Media - Hard disk drive

**veris:asset:variety="S - VM host"**

Server - Virtual Host

**veris:asset:variety="P - Auditor"**

People - Auditor

**veris:asset:variety="U - VoIP phone"**

User Device - VoIP phone

**veris:asset:variety="N - Broadband"**

Network - Mobile broadband network

**veris:asset:variety="U - Other"**

User Device - Other/Unknown

**veris:asset:variety="U - Telephone"**

User Device - Telephone

**veris:asset:variety="P - Call center"**

People - Call center

**veris:asset:variety="N - Private WAN"**

Network - Private WAN

**veris:asset:variety="S - DNS"**

Server - DNS

**veris:asset:variety="P - Helpdesk"**

People - Helpdesk

**veris:asset:variety="N - Telephone"**

Network - Telephone

**veris:asset:variety="U - Laptop"**

User Device - Laptop

**veris:asset:variety="S - Log"**

Server - Log or event management

**veris:asset:variety="P - Finance"**

People - Finance

**veris:asset:variety="P - Human resources"**

People - Human resources

**veris:asset:variety="N - VoIP adapter"**

Network - VoIP adapter

**veris:asset:variety="S - Backup"**

Server - Backup

**veris:asset:variety="P - Partner"**

People - Partner

**veris:asset:variety="P - Maintenance"**

People - Maintenance

**veris:asset:variety="S - Payment switch"**

Server - Payment switch or gateway

**veris:asset:variety="S - DCS"**

Server - Distributed control system (DCS)

**veris:asset:variety="P - Other"**

People - Other/Unknown

**veris:asset:variety="S - Proxy"**

Server - Proxy

**veris:asset:variety="S - Mail"**

Server - Mail

**veris:asset:variety="M - Tapes"**

Media - Backup tapes

**veris:asset:variety="S - Remote access"**

Server - Remote access

**veris:asset:variety="N - Access reader"**

Network - Access control reader (e.g., badge, biometric)

**veris:asset:variety="S - File"**

Server - File

**veris:asset:variety="S - Web application"**

Server - Web application

**veris:asset:variety="M - Documents"**

Media - Documents

**veris:asset:variety="N - WLAN"**

Network - Wireless LAN

**veris:asset:variety="P - Developer"**

People - Developer

**veris:asset:variety="M - Disk media"**

Media - Disk media (e.g., CDs, DVDs)

## **asset:accessibility**

**veris:asset:accessibility="NA"**

Not applicable

**veris:asset:accessibility="Internal"**

Internally accessible

**veris:asset:accessibility="Unknown"**

Unknown

**veris:asset:accessibility="External"**

Publicly accessible

**veris:asset:accessibility="Isolated"**

Internally isolated or restricted environment

## **asset:governance**

**veris:asset:governance="3rd party hosted"**

Hosted by 3rd party

**veris:asset:governance="Unknown"**

Unknown

**veris:asset:governance="3rd party managed"**

Managed by 3rd party

**veris:asset:governance="3rd party owned"**

Owned by 3rd party

**veris:asset:governance="Personally owned"**

Personally owned asset

**veris:asset:governance="Internally isolated"**

Isolated internal asset

## **asset:hosting**

**veris:asset:hosting="External shared"**

Externally hosted in a shared environment

**veris:asset:hosting="External dedicated"**

Externally hosted in a dedicated environment

**veris:asset:hosting="NA"**

Not applicable

**veris:asset:hosting="Internal"**

Internally hosted

**veris:asset:hosting="External"**

Externally hosted (unsure if dedicated or shared)



**veris:asset:hosting="Unknown"**

Unknown

## **asset:ownership**

**veris:asset:ownership="Customer"**

Customer owned

**veris:asset:ownership="Unknown"**

Unknown

**veris:asset:ownership="Victim"**

Victim owned

**veris:asset:ownership="NA"**

Not applicable

**veris:asset:ownership="Employee"**

Employee owned

**veris:asset:ownership="Partner"**

Partner owned

## **asset:cloud**

**veris:asset:cloud="Hosting error"**

Misconfiguration or error by hosting provider

**veris:asset:cloud="User breakout"**

Elevation of privilege by another customer in shared environment

**veris:asset:cloud="Unknown"**

Unknown

**veris:asset:cloud="Other"**

Other

## **veris:asset:cloud="Hosting governance"**

Lack of security process or procedure by hosting provider

## **veris:asset:cloud="Customer attack"**

Penetration of another web site on shared device

## **veris:asset:cloud="Hypervisor"**

Hypervisor break-out attack

## **veris:asset:cloud="Partner application"**

Application vulnerability in partner-developed application

## **victim:employee\_count**

### **veris:victim:employee\_count="1001 to 10000"**

1,001 to 10,000 employees

### **veris:victim:employee\_count="Over 100000"**

Over 100,0001 employees

### **veris:victim:employee\_count="Large"**

Large organizations (over 1,000 employees)

### **veris:victim:employee\_count="Unknown"**

Unknown number of employees

### **veris:victim:employee\_count="50001 to 100000"**

50,001 to 100,000 employees

### **veris:victim:employee\_count="101 to 1000"**

101 to 1,000 employees

### **veris:victim:employee\_count="25001 to 50000"**

25,001 to 50,000 employees

**veris:victim:employee\_count="10001 to 25000"**

10,001 to 25,000 employees

**veris:victim:employee\_count="Small"**

Small organizations (1,000 employees or less)

**veris:victim:employee\_count="1 to 10"**

1 to 10 employees

**veris:victim:employee\_count="11 to 100"**

11 to 100 employees

## **timeline:unit**

**veris:timeline:unit="Months"**

Months

**veris:timeline:unit="Seconds"**

Seconds

**veris:timeline:unit="NA"**

NA

**veris:timeline:unit="Never"**

Never

**veris:timeline:unit="Days"**

Days

**veris:timeline:unit="Years"**

Years

**veris:timeline:unit="Hours"**

Hours

**veris:timeline:unit="Unknown"**

Unknown

**veris:timeline:unit="Weeks"**

Weeks

**veris:timeline:unit="Minutes"**

Minutes

## **impact:loss:rating**

**veris:impact:loss:rating="Unknown"**

Unknown

**veris:impact:loss:rating="Major"**

Major

**veris:impact:loss:rating="Moderate"**

Moderate

**veris:impact:loss:rating="None"**

None

**veris:impact:loss:rating="Minor"**

Minor

## **impact:loss:variety**

**veris:impact:loss:variety="Legal and regulatory"**

Legal and regulatory costs

**veris:impact:loss:variety="Asset and fraud"**

Asset and fraud-related losses

**veris:impact:loss:variety="Business disruption"**

Business disruption

**veris:impact:loss:variety="Response and recovery"**

Response and recovery costs

**veris:impact:loss:variety="Competitive advantage"**

Loss of competitive advantage

**veris:impact:loss:variety="Operating costs"**

Increased operating costs

**veris:impact:loss:variety="Brand damage"**

Brand and market damage

**attribute:integrity:variety**

**veris:attribute:integrity:variety="Misrepresentation"**

Misrepresentation

**veris:attribute:integrity:variety="Modify data"**

Modified stored data or content

**veris:attribute:integrity:variety="Unknown"**

Unknown

**veris:attribute:integrity:variety="Created account"**

Created new user account

**veris:attribute:integrity:variety="Defacement"**

Deface content

**veris:attribute:integrity:variety="Log tampering"**

Log tampering or modification

**veris:attribute:integrity:variety="Modify privileges"**

Modified privileges or permissions

## **veris:attribute:integrity:variety="Software installation"**

Software installation or code modification

## **veris:attribute:integrity:variety="Other"**

Other

## **veris:attribute:integrity:variety="Fraudulent transaction"**

Initiate fraudulent transaction

## **veris:attribute:integrity:variety="Alter behavior"**

Influence or alter human behavior

## **veris:attribute:integrity:variety="Hardware tampering"**

Hardware tampering or physical alteration

## **veris:attribute:integrity:variety="Modify configuration"**

Modified configuration or services

## **veris:attribute:integrity:variety="Repurpose"**

Repurposed asset for unauthorized function

## **attribute:availability:variety**

### **veris:attribute:availability:variety="Acceleration"**

Acceleration

### **veris:attribute:availability:variety="Interruption"**

Interruption

### **veris:attribute:availability:variety="Loss"**

Loss

### **veris:attribute:availability:variety="Unknown"**

Unknown

**veris:attribute:availability:variety="Degradation"**

Performance degradation

**veris:attribute:availability:variety="Other"**

Other

**veris:attribute:availability:variety="Obscuration"**

Conversion or obscuration

**veris:attribute:availability:variety="Destruction"**

Destruction

**attribute:confidentiality:data\_victim**

**veris:attribute:confidentiality:data\_victim="Customer"**

Customer

**veris:attribute:confidentiality:data\_victim="Patient"**

Patient

**veris:attribute:confidentiality:data\_victim="Unknown"**

Unknown

**veris:attribute:confidentiality:data\_victim="Other"**

Other

**veris:attribute:confidentiality:data\_victim="Student"**

Student

**veris:attribute:confidentiality:data\_victim="Employee"**

Employee

**veris:attribute:confidentiality:data\_victim="Partner"**

Partner

## **attribute:confidentiality:state**

**veris:attribute:confidentiality:state="Unknown"**

Unknown

**veris:attribute:confidentiality:state="Transmitted encrypted"**

Transmitted encrypted

**veris:attribute:confidentiality:state="Transmitted unencrypted"**

Transmitted unencrypted

**veris:attribute:confidentiality:state="Stored"**

Stored

**veris:attribute:confidentiality:state="Transmitted"**

Transmitted

**veris:attribute:confidentiality:state="Processed"**

Processed

**veris:attribute:confidentiality:state="Stored encrypted"**

Stored encrypted

**veris:attribute:confidentiality:state="Stored unencrypted"**

Stored unencrypted

## **attribute:confidentiality:data\_disclosure**

**veris:attribute:confidentiality:data\_disclosure="Unknown"**

Unknown

**veris:attribute:confidentiality:data\_disclosure="Yes"**

Yes (confirmed)

**veris:attribute:confidentiality:data\_disclosure="Potentially"**

Potentially (at risk)



**veris:attribute:confidentiality:data\_disclosure="No"**

No

## **actor:internal:job\_change**

**veris:actor:internal:job\_change="Lateral move"**

Lateral move

**veris:actor:internal:job\_change="Job eval"**

Recent poor job evaluation

**veris:actor:internal:job\_change="Unknown"**

Unknown

**veris:actor:internal:job\_change="Personal issues"**

Personal issues

**veris:actor:internal:job\_change="Let go"**

Fired, laid off, or let go

**veris:actor:internal:job\_change="Reprimanded"**

Recently reprimanded

**veris:actor:internal:job\_change="Hired"**

Recently hired

**veris:actor:internal:job\_change="Passed over"**

Recently passed over for promotion

**veris:actor:internal:job\_change="Demoted"**

Recently demoted or hours reduced

**veris:actor:internal:job\_change="Promoted"**

Recently promoted

**veris:actor:internal:job\_change="Resigned"**

Recently resigned

**veris:actor:internal:job\_change="Other"**

Other

## **actor:internal:variety**

**veris:actor:internal:variety="End-user"**

End-user or regular employee

**veris:actor:internal:variety="Human resources"**

Human resources staff

**veris:actor:internal:variety="Finance"**

Finance or accounting staff

**veris:actor:internal:variety="Unknown"**

Unknown

**veris:actor:internal:variety="Helpdesk"**

Helpdesk staff

**veris:actor:internal:variety="Executive"**

Executive or upper management

**veris:actor:internal:variety="Cashier"**

Cashier, teller, or waiter

**veris:actor:internal:variety="Manager"**

Manager or supervisor

**veris:actor:internal:variety="Guard"**

Security guard

**veris:actor:internal:variety="Other"**

Other

**veris:actor:internal:variety="Auditor"**

Auditor

**veris:actor:internal:variety="Maintenance"**

Maintenance or janitorial staff

**veris:actor:internal:variety="Call center"**

Call center staff

**veris:actor:internal:variety="System admin"**

System or network administrator

**veris:actor:internal:variety="Developer"**

Software developer

**actor:external:variety**

**veris:actor:external:variety="Customer"**

Customer (B2C)

**veris:actor:external:variety="Organized crime"**

Organized or professional criminal group

**veris:actor:external:variety="Acquaintance"**

Relative or acquaintance of employee

**veris:actor:external:variety="Competitor"**

Competitor

**veris:actor:external:variety="Unaffiliated"**

Unaffiliated person(s)

## **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="Activist"**

Activist group

## **veris:actor:external:variety="Terrorist"**

Terrorist group

## **veris:actor:external:variety="Auditor"**

Auditor

## **veris:actor:external:variety="Unknown"**

Unknown

## **veris:actor:external:variety="State-affiliated"**

State-sponsored or affiliated group

## **veris:actor:external:variety="Other"**

Other

## **action:malware:vector**

### **veris:action:malware:vector="Remote injection"**

Remotely injected by agent (i.e. via SQLi)

### **veris:action:malware:vector="Software update"**

Included in automated software update

**veris:action:malware:vector="Instant messaging"**

Instant Messaging

**veris:action:malware:vector="Email attachment"**

Email via user-executed attachment

**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="Removable media"**

Removable storage media or devices

**veris:action:malware:vector="Web drive-by"**

Web via auto-executed or "drive-by" infection

**veris:action:malware:vector="Email link"**

Email via embedded link

**veris:action:malware:vector="Network propagation"**

Network propagation

**veris:action:malware:vector="Unknown"**

Unknown

**veris:action:malware:vector="Email autoexecute"**

Email via automatic execution

**veris:action:malware:vector="Web download"**

Web via user-executed or downloaded content

**veris:action:malware:vector="Other"**

Other

## **action:malware:variety**

**veris:action:malware:variety="Spam"**

Send spam

**veris:action:malware:variety="Unknown"**

Unknown

**veris:action:malware:variety="Packet sniffer"**

Packet sniffer (capture data from network)

**veris:action:malware:variety="Backdoor"**

Backdoor (enable remote access)

**veris:action:malware:variety="Exploit vuln"**

Exploit vulnerability in code (vs misconfig or weakness)

**veris:action:malware:variety="Other"**

Other

**veris:action:malware:variety="Password dumper"**

Password dumper (extract credential hashes)

**veris:action:malware:variety="Scan network"**

Scan or footprint network

**veris:action:malware:variety="Downloader"**

Downloader (pull updates or other malware)

**veris:action:malware:variety="Adminware"**

System or network utilities (e.g., PsTools, Netcat)

**veris:action:malware:variety="Click fraud"**

Click fraud or Bitcoin mining

**veris:action:malware:variety="Adware"**

Adware

**veris:action:malware:variety="C2"**

Command and control (C2)

**veris:action:malware:variety="Worm"**

Worm (propagate to other systems or devices)

**veris:action:malware:variety="Spyware/Keylogger"**

Spyware, keylogger or form-grabber (capture user input or activity)

**veris:action:malware:variety="Brute force"**

Brute force attack

**veris:action:malware:variety="Capture app data"**

Capture data from application or system process

**veris:action:malware:variety="Ram scraper"**

Ram scraper or memory parser (capture data from volatile memory)

**veris:action:malware:variety="Disable controls"**

Disable or interfere with security controls

**veris:action:malware:variety="Capture stored data"**

Capture data stored on system disk

**veris:action:malware:variety="Ransomware"**

Ransomware (encrypt or seize stored data)

**veris:action:malware:variety="Export data"**

Export data to another site or system

**veris:action:malware:variety="Client-side attack"**

Client-side or browser attack (e.g., redirection, XSS, MitB)

**veris:action:malware:variety="SQL injection"**

SQL injection attack

**veris:action:malware:variety="Rootkit"**

Rootkit (maintain local privileges and stealth)

**veris:action:malware:variety="Destroy data"**

Destroy or corrupt stored data

**veris:action:malware:variety="DoS"**

DoS attack

## **action:social:vector**

**veris:action:social:vector="In-person"**

In-person

**veris:action:social:vector="Social media"**

Social media or networking

**veris:action:social:vector="Documents"**

Documents

**veris:action:social:vector="Unknown"**

Unknown

**veris:action:social:vector="SMS"**

SMS or texting

**veris:action:social:vector="Phone"**

Phone

**veris:action:social:vector="Website"**

Website



**veris:action:social:vector="Other"**

Other

**veris:action:social:vector="IM"**

Instant messaging

**veris:action:social:vector="Removable media"**

Removable storage media

**veris:action:social:vector="Email"**

Email

**veris:action:social:vector="Software"**

Software

**action:social:target**

**veris:action:social:target="Customer"**

Customer (B2C)

**veris:action:social:target="End-user"**

End-user or regular employee

**veris:action:social:target="Human resources"**

Human resources staff

**veris:action:social:target="Finance"**

Finance or accounting staff

**veris:action:social:target="Unknown"**

Unknown

**veris:action:social:target="Helpdesk"**

Helpdesk staff

**veris:action:social:target="Executive"**

Executive or upper management

**veris:action:social:target="Cashier"**

Cashier, teller or waiter

**veris:action:social:target="Manager"**

Manager or supervisor

**veris:action:social:target="Former employee"**

Former employee

**veris:action:social:target="Guard"**

Security guard

**veris:action:social:target="Other"**

Other

**veris:action:social:target="Auditor"**

Auditor

**veris:action:social:target="Maintenance"**

Maintenance or janitorial staff

**veris:action:social:target="Call center"**

Call center staff

**veris:action:social:target="Partner"**

Partner (B2B)

**veris:action:social:target="System admin"**

System or network administrator

**veris:action:social:target="Developer"**

Software developer

## **action:social:variety**

### **veris:action:social:variety="Scam"**

Online scam or hoax (e.g., scareware, 419 scam, auction fraud)

### **veris:action:social:variety="Phishing"**

Phishing (or any type of \*ishing)

### **veris:action:social:variety="Elicitation"**

Elicitation (subtle extraction of info through conversation)

### **veris:action:social:variety="Unknown"**

Unknown

### **veris:action:social:variety="Spam"**

Spam (unsolicited or undesired email and advertisements)

### **veris:action:social:variety="Influence"**

Influence tactics (Leveraging authority or obligation, framing, etc)

### **veris:action:social:variety="Propaganda"**

Propaganda or disinformation

### **veris:action:social:variety="Forgery"**

Forgery or counterfeiting (fake hardware, software, documents, etc)

### **veris:action:social:variety="Bribery"**

Bribery or solicitation

### **veris:action:social:variety="Other"**

Other

### **veris:action:social:variety="Pretexting"**

Pretexting (dialogue leveraging invented scenario)

**veris:action:social:variety="Extortion"**

Extortion or blackmail

**veris:action:social:variety="Baiting"**

Baiting (planting infected media)

**action:environmental:variety**

**veris:action:environmental:variety="Hazmat"**

Hazardous material

**veris:action:environmental:variety="Temperature"**

Extreme temperature

**veris:action:environmental:variety="Unknown"**

Unknown

**veris:action:environmental:variety="Hurricane"**

Hurricane

**veris:action:environmental:variety="Ice"**

Ice and snow

**veris:action:environmental:variety="Meteorite"**

Meteorite

**veris:action:environmental:variety="Other"**

Other

**veris:action:environmental:variety="Pathogen"**

Pathogen

**veris:action:environmental:variety="Landslide"**

Landslide

**veris:action:environmental:variety="Tornado"**

Tornado

**veris:action:environmental:variety="Leak"**

Water leak

**veris:action:environmental:variety="Earthquake"**

Earthquake

**veris:action:environmental:variety="Particulates"**

Particulate matter (e.g., dust, smoke)

**veris:action:environmental:variety="Power failure"**

Power failure or fluctuation

**veris:action:environmental:variety="EMI"**

Electromagnetic interference (EMI)

**veris:action:environmental:variety="Humidity"**

Humidity

**veris:action:environmental:variety="Tsunami"**

Tsunami

**veris:action:environmental:variety="ESD"**

Electrostatic discharge (ESD)

**veris:action:environmental:variety="Deterioration"**

Deterioration and degradation

**veris:action:environmental:variety="Volcano"**

Volcanic eruption

**veris:action:environmental:variety="Lightning"**

Lightning

**veris:action:environmental:variety="Wind"**

Wind

**veris:action:environmental:variety="Flood"**

Flood

**veris:action:environmental:variety="Vermin"**

Vermin

**veris:action:environmental:variety="Fire"**

Fire

## **action:error:vector**

**veris:action:error:vector="Random error"**

Random error (no reason, no fault)

**veris:action:error:vector="Carelessness"**

Carelessness

**veris:action:error:vector="Other"**

Other

**veris:action:error:vector="Unknown"**

Unknown

**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="Inadequate personnel"**

Inadequate or insufficient personnel

## **action:error:variety**

**veris:action:error:variety="Disposal error"**

Disposal error

**veris:action:error:variety="Omission"**

Omission (something intended, but not done)

**veris:action:error:variety="Loss"**

Loss or misplacement

**veris:action:error:variety="Unknown"**

Unknown

**veris:action:error:variety="Maintenance error"**

Maintenance error

**veris:action:error:variety="Misinformation"**

Misinformation (unintentionally giving false info)

**veris:action:error:variety="Physical accidents"**

Physical accidents (e.g., drops, bumps, spills)

**veris:action:error:variety="Publishing error"**

Publishing error (private info to public doc or site)

**veris:action:error:variety="Malfunction"**

Technical malfunction or glitch

**veris:action:error:variety="Capacity shortage"**

Poor capacity planning

**veris:action:error:variety="Other"**

Other

## **veris:action:error:variety="Programming error"**

Programming error (flaws or bugs in custom code)

## **veris:action:error:variety="Data entry error"**

Data entry error

## **veris:action:error:variety="Gaffe"**

Gaffe (social or verbal slip)

## **veris:action:error:variety="Misconfiguration"**

Misconfiguration

## **veris:action:error:variety="Misdelivery"**

Misdelivery (send wrong info or to wrong recipient)

## **veris:action:error:variety="Classification error"**

Classification or labeling error

## **action:misuse:vector**

### **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="LAN access"**

Local network access within corporate facility

### **veris:action:misuse:vector="Unknown"**

Unknown

### **veris:action:misuse:vector="Non-corporate"**

Non-corporate facilities or networks



**veris:action:misuse:vector="Other"**

Other

## **action:misuse:variety**

**veris:action:misuse:variety="Unapproved software"**

Use of unapproved software or services

**veris:action:misuse:variety="Illicit content"**

Storage or distribution of illicit content

**veris:action:misuse:variety="Unapproved workaround"**

Unapproved workaround or shortcut

**veris:action:misuse:variety="Unapproved hardware"**

Use of unapproved hardware or devices

**veris:action:misuse:variety="Unknown"**

Unknown

**veris:action:misuse:variety="Email misuse"**

Inappropriate use of email or IM

**veris:action:misuse:variety="Possession abuse"**

Abuse of physical access to asset

**veris:action:misuse:variety="Other"**

Other

**veris:action:misuse:variety="Net misuse"**

Inappropriate use of network or Web access

**veris:action:misuse:variety="Data mishandling"**

Handling of data in an unapproved manner

**veris:action:misuse:variety="Privilege abuse"**

Abuse of system access privileges

**veris:action:misuse:variety="Knowledge abuse"**

Abuse of private or entrusted knowledge

## **action:hacking:vector**

**veris:action:hacking:vector="Physical access"**

Physical access or connection (i.e., at keyboard or via cable)

**veris:action:hacking:vector="Command shell"**

Remote shell

**veris:action:hacking:vector="Unknown"**

Unknown

**veris:action:hacking:vector="Backdoor or C2"**

Backdoor or command and control channel

**veris:action:hacking:vector="Web application"**

Web application

**veris:action:hacking:vector="Desktop sharing"**

Graphical desktop sharing (RDP, VNC, PCAnywhere, Citrix)

**veris:action:hacking:vector="3rd party desktop"**

3rd party online desktop sharing (LogMeIn, Go2Assist)

**veris:action:hacking:vector="Partner"**

Partner connection or credential

**veris:action:hacking:vector="VPN"**

VPN

**veris:action:hacking:vector="Other"**

Other

## **action:hacking:variety**

**veris:action:hacking:variety="XSS"**

Cross-site scripting

**veris:action:hacking:variety="HTTP Response Splitting"**

HTTP Response Splitting

**veris:action:hacking:variety="Unknown"**

Unknown

**veris:action:hacking:variety="Buffer overflow"**

Buffer overflow

**veris:action:hacking:variety="Format string attack"**

Format string attack

**veris:action:hacking:variety="LDAP injection"**

LDAP injection

**veris:action:hacking:variety="SSI injection"**

SSI injection

**veris:action:hacking:variety="MitM"**

Man-in-the-middle attack

**veris:action:hacking:variety="Path traversal"**

Path traversal

**veris:action:hacking:variety="URL redirector abuse"**

URL redirector abuse

**veris:action:hacking:variety="Use of backdoor or C2"**

Use of Backdoor or C2 channel

**veris:action:hacking:variety="Mail command injection"**

Mail command injection

**veris:action:hacking:variety="Virtual machine escape"**

Virtual machine escape

**veris:action:hacking:variety="OS commanding"**

OS commanding

**veris:action:hacking:variety="Soap array abuse"**

Soap array abuse

**veris:action:hacking:variety="Footprinting"**

Footprinting and fingerprinting

**veris:action:hacking:variety="Cryptanalysis"**

Cryptanalysis

**veris:action:hacking:variety="SQLi"**

SQL injection

**veris:action:hacking:variety="XML external entities"**

XML external entities

**veris:action:hacking:variety="Abuse of functionality"**

Abuse of functionality

**veris:action:hacking:variety="XML injection"**

XML injection

**veris:action:hacking:variety="Routing detour"**

Routing detour

**veris:action:hacking:variety="HTTP response smuggling"**

HTTP response smuggling

**veris:action:hacking:variety="Forced browsing"**

Forced browsing or predictable resource location

**veris:action:hacking:variety="Cache poisoning"**

Cache poisoning

**veris:action:hacking:variety="Null byte injection"**

Null byte injection

**veris:action:hacking:variety="Reverse engineering"**

Reverse engineering

**veris:action:hacking:variety="Brute force"**

Brute force or password guessing attacks

**veris:action:hacking:variety="Fuzz testing"**

Fuzz testing

**veris:action:hacking:variety="Offline cracking"**

Offline password or key cracking (e.g., rainbow tables, Hashcat, JtR)

**veris:action:hacking:variety="CSRF"**

Cross-site request forgery

**veris:action:hacking:variety="XML entity expansion"**

XML entity expansion

**veris:action:hacking:variety="RFI"**

Remote file inclusion

**veris:action:hacking:variety="Session fixation"**

Session fixation

**veris:action:hacking:variety="Integer overflows"**

Integer overflows

**veris:action:hacking:variety="XQuery injection"**

XQuery injection

**veris:action:hacking:variety="Pass-the-hash"**

Pass-the-hash

**veris:action:hacking:variety="XML attribute blowup"**

XML attribute blowup

**veris:action:hacking:variety="Session prediction"**

Credential or session prediction

**veris:action:hacking:variety="Use of stolen creds"**

Use of stolen authentication credentials

**veris:action:hacking:variety="HTTP request smuggling"**

HTTP request smuggling

**veris:action:hacking:variety="XPath injection"**

XPath injection

**veris:action:hacking:variety="Other"**

Other

**veris:action:hacking:variety="DoS"**

Denial of service

**veris:action:hacking:variety="Special element injection"**

Special element injection

**veris:action:hacking:variety="HTTP request splitting"**

HTTP request splitting

**veris:action:hacking:variety="Session replay"**

Session replay

**action:physical:vector**

**veris:action:physical:vector="Personal vehicle"**

Personal vehicle

**veris:action:physical:vector="Visitor privileges"**

Given temporary visitor access

**veris:action:physical:vector="Public facility"**

Public facility or area

**veris:action:physical:vector="Victim grounds"**

Victim outdoor grounds

**veris:action:physical:vector="Uncontrolled location"**

The location was uncontrolled (public)

**veris:action:physical:vector="Partner vehicle"**

Partner vehicle (e.g., delivery truck)

**veris:action:physical:vector="Victim work area"**

Victim private or work area (e.g., office space)

**veris:action:physical:vector="Victim secure area"**

Victim high security area (e.g., server room, R&D labs)

**veris:action:physical:vector="Partner facility"**

Partner facility or area

**veris:action:physical:vector="Personal residence"**

Personal residence

## **veris:action:physical:vector="Other"**

Other

## **veris:action:physical:vector="Public vehicle"**

Public vehicle (e.g., plane, taxi)

## **veris:action:physical:vector="Unknown"**

Unknown

## **veris:action:physical:vector="Victim public area"**

Victim public or customer area (e.g., lobby, storefront)

## **veris:action:physical:vector="Privileged access"**

Held privileged access to location

## **action:physical:variety**

### **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="Tampering"**

Tampering (alter physical form or function)

### **veris:action:physical:variety="Unknown"**

Unknown

### **veris:action:physical:variety="Theft"**

Theft (taking assets without permission)

### **veris:action:physical:variety="Connection"**

Connection



## **veris:action:physical:variety="Surveillance"**

Surveillance (monitoring and observation)

## **veris:action:physical:variety="Assault"**

Assault (threats or acts of physical violence)

## **veris:action:physical:variety="Other"**

Other

## **veris:action:physical:variety="Wiretapping"**

Wiretapping (Physical tap to comms line)

## **veris:action:physical:variety="Bypassed controls"**

Bypassed physical barriers or controls

## **veris:action:physical:variety="Disabled controls"**

Disabled physical barriers or controls

## **veris:action:physical:variety="Destruction"**

Destruction (deliberate damaging or disabling)

## **attribute:confidentiality:data:variety**

### **veris:attribute:confidentiality:data:variety="Source code"**

Source code

### **veris:attribute:confidentiality:data:variety="Personal"**

Personal or identifying information (e.g., addr, ID#, credit score)

### **veris:attribute:confidentiality:data:variety="Unknown"**

Unknown

### **veris:attribute:confidentiality:data:variety="Medical"**

Medical records

**veris:attribute:confidentiality:data:variety="Classified"**

Classified information

**veris:attribute:confidentiality:data:variety="System"**

System information (e.g., config info, open services)

**veris:attribute:confidentiality:data:variety="Digital certificate"**

Digital certificate

**veris:attribute:confidentiality:data:variety="Secrets"**

Trade secrets

**veris:attribute:confidentiality:data:variety="Internal"**

Sensitive internal data (e.g., plans, reports, emails)

**veris:attribute:confidentiality:data:variety="Virtual currency"**

Virtual currency

**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="Other"**

Other

**veris:attribute:confidentiality:data:variety="Payment"**

Payment card data (e.g., PAN, PIN, CVV2, Expiration)

**veris:attribute:confidentiality:data:variety="Bank"**

Bank account data

**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

## degré-de-probabilité

### **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 %)

### **vocabulaire-des-probabilites-estimatives:degré-de- probabilité="probablement-pas"**

Probablement pas - Invraisemblable Peu probable - 30 % (marge d'erreur d'environ 10 %)

### **vocabulaire-des-probabilites-estimatives:degré-de-probabilité="chances-à- peu-près-égales"**

Chances à peu près égales - une chance sur deux - 50% (marge d'erreur d'environ 10 %)

### **vocabulaire-des-probabilites-estimatives:degré-de-probabilité="probable"**

Probable - Vraisemblable Probable - 75 % (marge d'erreur d'environ 12 %)

### **vocabulaire-des-probabilites-estimatives:degré-de-probabilité="quasi- certaine"**

Quasi certaine - Certain Presque certain Très probable - 93% (marge d'erreur d'environ 6 %)