

MISP and ATT&CK - an evolving integration

Using ATT&CK as the corner stone for improving the modeling of adversaries
in an Open Source TIP



CIRCL

Computer Incident
Response Center
Luxembourg



MISP
Threat Sharing

Team CIRCL

<https://www.misp-project.org/>

Twitter: @MISPProject

20190509 - TLP:WHITE

MISP and ATT&CK - a love story

The MISP threat sharing platform is a free and open source software enabling **information sharing, collaboration, automation and modeling of a wide gamut of intelligence.**



The screenshot shows a tweet from the account MISP (@MISPProject). The tweet text reads: "MISP galaxies now include the nifty @MITREattack model [github.com /MISP/misp-gala](https://github.com/MISP/misp-gala) ... you can use it directly in MISP. @jwunder @deltalimasierra". Below the text is a link preview for "MISP/misp-galaxy" with a description: "Clusters and elements to attach to MISP events or attributes (like threat actors) - MISP/misp-galaxy" and the URL "github.com". The tweet is dated "6:29 PM - 17 Aug 2017" and has "38 Retweets" and "39 Likes". At the bottom of the tweet are several profile picture icons of users who interacted with the tweet.

MISP
@MISPProject

Following

MISP galaxies now include the nifty
[@MITREattack](#) model [github.com /MISP/misp-gala](https://github.com/MISP/misp-gala) ... you can use it directly in
MISP. [@jwunder](#) [@deltalimasierra](#)

 **MISP/misp-galaxy**
Clusters and elements to attach to MISP events or attributes (like threat actors) - MISP/misp-galaxy
github.com

6:29 PM - 17 Aug 2017

38 Retweets 39 Likes

Generalised contextualisation model

- MISP already had a system in place allowing users to contextualise data using a **shared library of knowledge base elements called galaxies**.
- The initial implementation (in August 2017) of ATT&CK was a regular galaxy.
- Users could already share and filter by techniques and tactics out-of-the-box using ATT&CK.

Improved UI mimicing ATT&CK navigator

- After the first ATT&CK community workshop in Luxembourg (24-25 May 2018), the release and presentation of **navigator** opened up our eyes.
- Users got to use a familiar UI, representing the kill-chain elements in a meaningful way.

mitre-pre-attack	mitre-mobile-attack	mitre-attack	Submit							
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	
	Exchange		Control	History	Registry	Discovery		System	Command and Control Channel	
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop	Data from	Exfiltration Over	
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery				
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Group Discovery				
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery				
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry				
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Keychain	Remote System Discovery				
	Local Job									

CAPEC-158:
 Network sniffing refers to using the network interface of a host to capture information sent over a wired or wireless connection. This can be done by a network interface into promiscuous mode to passively sniff the network, or use span ports to capture a larger amount of traffic.
 Data captured via this technique may include user credentials, passwords, or other sensitive information. Techniques for network sniffing, such as [LLMNR/NBT-NS Poisoning](https://www.exploit-db.com/exploits/11171), can also be used to capture credentials to web services by redirecting traffic to an adversary.
 Network sniffing may also reveal configuration details, such as IP addresses, version numbers, and other network characteristics (e.g., MAC addresses, VLAN IDs) necessary for follow-on Lateral Movement and other techniques.

Introducing ATT&CK statistics

- A global and per-event ATT&CK visualisation to quickly grasp the techniques and tactics used.

mitre-pre-attack	mitre-mobile-attack	mitre-attack					
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Software Discovery
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Model
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInIt DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation Services
Spearphishing Attachment	Control Panel Items	AppInIt DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Sessions
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash
Spearphishing via Service	Execution Through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Hash
Supply Chain Compromise	Execution Through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote System Discovery
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote System Discovery
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote System Discovery
5 of 9	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Removable Media
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking
	Launchctl	Component Object Model	Image File Execution Options	DLL Search Order Hijacking	Keychain	Remote System Discovery	Shared Volumes

Pivoting from any galaxy such as threat actors, sectors, tools, ...

threat-actor: Lazarus Group

Cluster ID	108651
Name	Lazarus Group
Parent Galaxy	Threat Actor
Description	Since 2009, HIDDEN COBRA actors have leveraged their capabilities to target and compromise a range of victims; some intrusions have resulted in the exfiltration of data while others have been disruptive in nature. Commercial reporting has referred to this activity as Lazarus Group and Guardians of Peace. Tools and capabilities used by HIDDEN COBRA actors include DDoS botnets, keyloggers, remote access tools (RATs), and wiper malware. Variants of malware and tools used by HIDDEN COBRA actors include Destover, Duuzer, and Hangman.
UUID	68391641-859f-4a9a-9a1e-3e5cf71ec376
Collection UUID	7cdf317-a673-4474-84ec-4f1754947823
Source	MISP Project
Authors	Alexandre Dulaunoy, Florian Roth, Thomas Schreck, Timo Steffens, Various
Connector tag	misp-galaxy:threat-actor="Lazarus Group"
Events	50 event(s)

Toggle ATT&CK Matrix

[mitre-pre-attack](#) [mitre-mobile-attack](#) [mitre-attack](#)

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral n
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScr
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Applicatio Software
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distribute Model
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	Appnlit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation Services
Spearphishing Attachment	Control Panel Items	Appnlit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Sc
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential	Network Softwa	Pass the

Community extension for ATT&CK-like galaxies

- Seeing an interest into **modeling other concerns similarly to the ATT&CK model**, MISP added an option to create your own ATT&CK-like matrices.

Election guidelines ▾

example-of-threats

Setup party/candidate registration	Setup electoral rolls	Campaign campaign IT	All phases government IT
DoS or overload of party/campaign registration, causing them to miss the deadline	Deleting or tampering with voter data	Hacking campaign websites (defacement, DoS)	DoS or overload of government websites
Fabricated signatures from sponsor	DoS or overload of voter registration system, suppressing voters	Hacking candidate laptops or email accounts	Hacking campaign websites, spreading misinformation or the election process, registered parties/candidates, or results
Tampering with registrations	Identity fraud during voter registration	Hacking candidate laptops or email accounts	Hacking/misconfiguration of government servers, communication networks, or endpoints

fraud-tactics

Initiation	Target Compromise	Perform Fraud	Obtain Fraudulent Assets
ATM Shimming	ATM Black Box Attack	Business Email Compromise	Compromised Account Credentials
ATM skimming	Account-Checking Services	CxO Fraud	Compromised Intellectual Property (IP)
POS Skimming	Account-Checking Services	Insider Trading	Compromised Payment Cards
Phishing	Malware	Scam	Compromised Personally Identifiable Information (PII)

Future

- We saw **an increase of ATT&CK contextualisation** in different information sharing communities relying on MISP.
- **Sighting and the sharing of metrics** among information sharing communities is becoming a requirement.
- Introducing CAR in MISP is the logical next step pending the evolution of CAR.

Contact

- Getting started with information sharing, want to provide feedback about MISP or discover open source tooling, don't hesitate to contact us:
- Contact: info@circl.lu
- <https://www.circl.lu/>
- <https://github.com/MISP> -
<https://twitter.com/MISPProject>
- <https://github.com/CIRCL> -
<https://www.misp-project.org/galaxy.html>