# 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

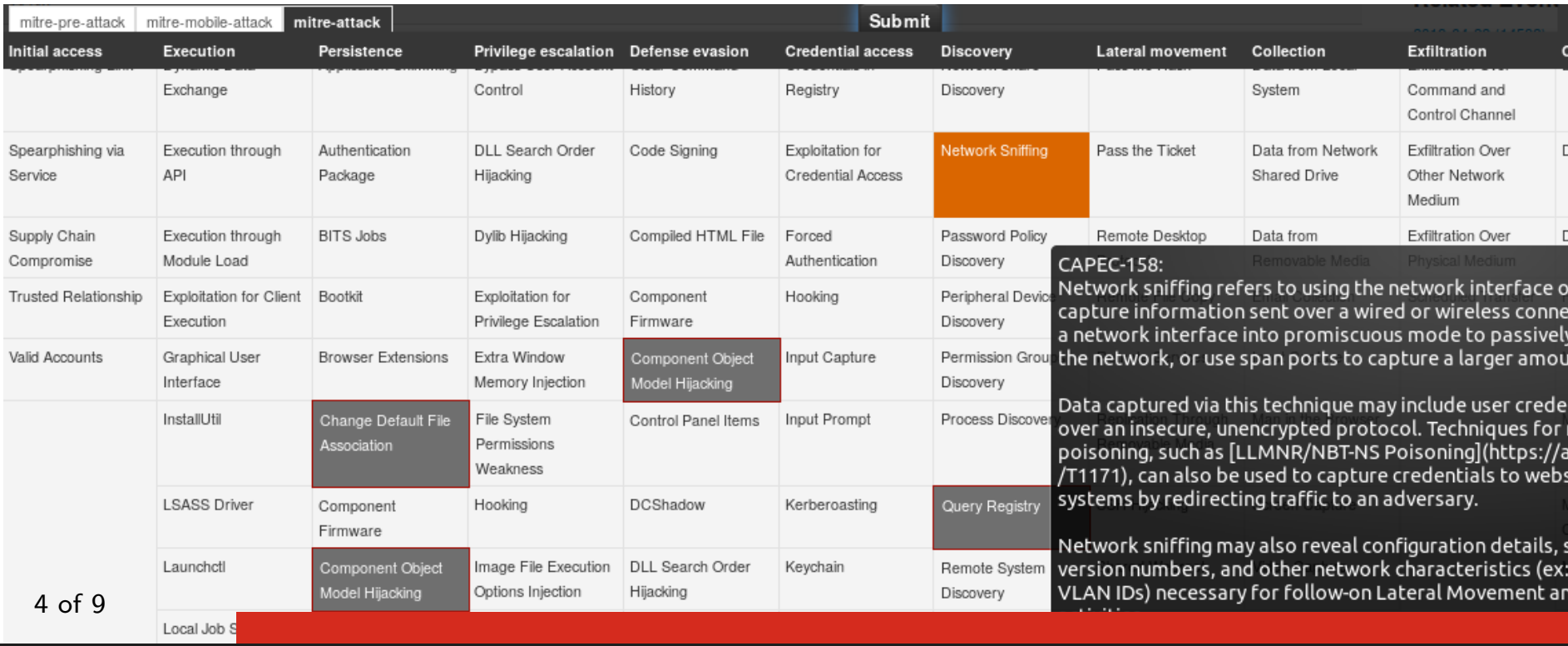
The MISP threat sharing platform is a free and open source software enabling **information sharing, collaboration, automation and modeling of a wide gamut of intelligence**.

# 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 familar UI, representing the kill-chain elements in a meaningful way.



# 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 m |
|---|---|---|---|---|---|---|---|
| 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 | AppInit DLLs | Bypass User Account Control | Credential Dumping | File and Directory Discovery | Exploitati Services |
| Spearphishing Attachment | Control Panel Items | AppInit 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 Access | Network Sniffing | Pass the |
| Supply Chain Compromise | Execution through Module Load | BITS Jobs | Dylib Hijacking | Compiled HTML File | Forced Authentication | Password Policy Discovery | Remote |
| Trusted Relationship | Exploitation for Client Execution | Bootkit | Exploitation for Privilege Escalation | Component Firmware | Hooking | Peripheral Device Discovery | Remote |
| Valid Accounts | Graphical User Interface | Browser Extensions | Extra Window Memory Injection | Component Object Model Hijacking | Input Capture | Permission Groups Discovery | Remote |
| | InstallUtil | Change Default File Association | File System Permissions Weakness | Control Panel Items | Input Prompt | Process Discovery | Replicatio Removal |
| | LSASS Driver | Component Firmware | Hooking | DCShadow | Kerberoasting | Query Registry | SSH Hija |
| | Launchctl | Component Object Model | Image File Execution Options | DLL Search Order Hijacking | Keychain | Remote System Discovery | Shared W |

# 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** | 7cdff317-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 m |
|---|---|---|---|---|---|---|---|
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | AppleScri |
| 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 | AppInit DLLs | Bypass User Account Control | Credential Dumping | File and Directory Discovery | Exploitati Services |
| Spearphishing Attachment | Control Panel Items | AppInit 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 Sniffing | Pass the |
| Supply C | | | | | | | |

# 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 \| governement 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 on 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`