MISP and ATT&CK status

The golden age of matrix-like models

Team MISP Project

23th October 2020 - attack-community.org

What changed since the last workshop?

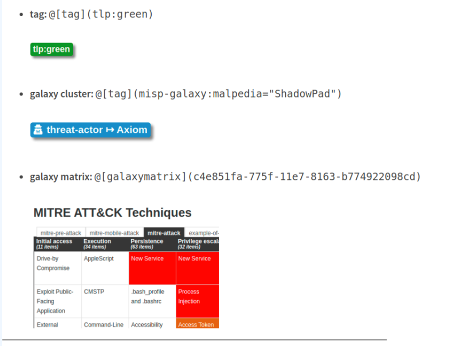
- ATT&CK has been steadily on the rise
- In cyber security MISP information sharing community, ATT&CK is often attached on **more than 70%** of the events
- The **number of matrix-like galaxies increased** in MISP in addition to the ones published by MITRE
  - Including **Telecom** matrix (Bhadra framework), **Election guidelines**, **Misinformation patterns**, **Segregation of Duties (LEA/CSIRT)**, **Financial** (att4ck for fraud), **Office 365** techniques.

MISP updates about ATT&CK

- Various improvements in ATT&CK visualisations and export format such as **attack-sightings**
- **ATT&CK Sub-techniques** are now available MISP
- MITRE ATT&CK **ICS** is available
- Challenges with historical data and ATT&CK techniques. Should MITRE provide UUID mapping tables for new and old/historical techniques?

MISP EVENT REPORT

- Event report[1] is a new convenient mechanism to edit, visualize and share Markdown reports in MISP
- Standardise and **extend the Markdown format** to support references to MISP attributes, objects, galaxies or ATT&CK matrix:



- **tag:** `@[tag](tlp:green)`

  tlp:green

- **galaxy cluster:** `@[tag](misp-galaxy:malpedia="ShadowPad")`

  threat-actor ↦ Axiom

- **galaxy matrix:** `@[galaxymatrix](c4e851fa-775f-11e7-8163-b774922098cd)`

MITRE ATT&CK Techniques

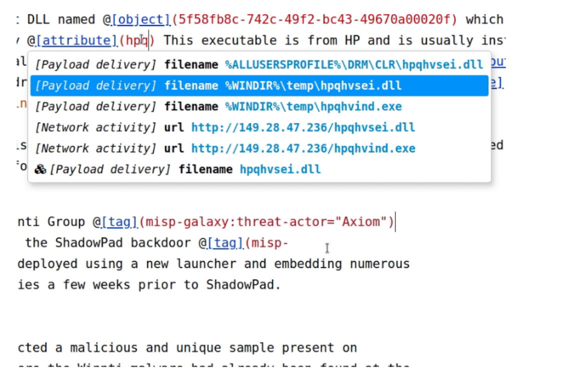
mitre-pre-attack | mitre-mobile-attack | mitre-attack | example-of-

Initial access *(11 items)*	Execution *(34 items)*	Persistence *(63 items)*	Privilege escal *(32 items)*
Drive-by Compromise	AppleScript	New Service	New Service
Exploit Public-Facing Application	CMSTP	.bash_profile and .bashrc	Process Injection
External	Command-Line	Accessibility	Access Token

[1] https://www.misp-project.org/2020/10/16/MISP.2.4.133.released.html

MISP EVENT REPORT

- Overall goal is to provide a standard Markdown format for reports which can be combined with structured elements
- The importance of **fixed references in MITRE ATT&CK is critical** for long-term accessibility to information



```
: DLL named @[object](5f58fb8c-742c-49f2-bc43-49670a00020f) which
/ @[attribute](hpq) This executable is from HP and is usually ins
  [Payload delivery] filename %ALLUSERSPROFILE%\DRM\CLR\hpqhvsei.dll
  [Payload delivery] filename %WINDIR%\temp\hpqhvsei.dll
  [Payload delivery] filename %WINDIR%\temp\hpqhvind.exe
  [Network activity] url http://149.28.47.236/hpqhvsei.dll
  [Network activity] url http://149.28.47.236/hpqhvind.exe
  [Payload delivery] filename hpqhvsei.dll

nti Group @[tag](misp-galaxy:threat-actor="Axiom")
 the ShadowPad backdoor @[tag](misp-
deployed using a new launcher and embedding numerous
ies a few weeks prior to ShadowPad.


cted a malicious and unique sample present on
```

Conclusion

- Bridging the gap between structured and unstructured report is critical. Integrating tram[2] with MISP event report could be an option.
- The matrix-like enhancement from the MISP galaxy format will be added in the default MISP galaxy standard format[3]
- ATT&CK like matrices become more and more common and used, thanks the **continuous work of the community**

[2] https://github.com/mitre-attack/tram

[3] https://www.misp-standard.org/