MISP and ATT&CK

How matrix-like models are changing MISP

Team CIRCL

MISP
Threat Sharing

- ATT&CK has been steadily on the rise
- We have observerd it becoming a **baseline for contextualisation** in several communities
- Relatively **simple** to understand
- Makes the **ingestion** of data based on context much easier
- Its use boosts **analytical use-cases** (risk assessment, threat intelligence)
- This made us think about how we could further capitalise on its success

- Result of discussions with MITRE
- MISP server hosts can now decide to export an **enumeration of the patterns** used based on the data-set
- Subject to all regular **restSearch filtering methods** (time, organisation, context, etc)
- Export returns the data-set in MITRE's owns **ATT&CK sighting format**

Searching our data-set for ATT&CK-like matrix heatmaps

- new standard **restSearch return format**
- Returns **HTML navigator-like heatmap**
- Easy integration into existing web applications
- Make use of all the MISP API filtering options
- Interested in how the rest of your **sector** shapes up?
- Or perhaps different **time** frames?
- Why not both and **compare** them?

- The full dataset for a given time in an instance

■ The full dataset for a given time in an instance

- The advent of ATT&CK had a secondary effect that was somewhat anticipated
- **Francesco Bigarella** from ING showcased **attack4fraud**
  - ► **ATT&CK like matrix**
  - ► Makes use of kill-chain phases
  - ► Enables all of the advantages provided by the framework (such as technique frequency analysis)
- This inspired us to allow for other matrix-like galaxies to be added
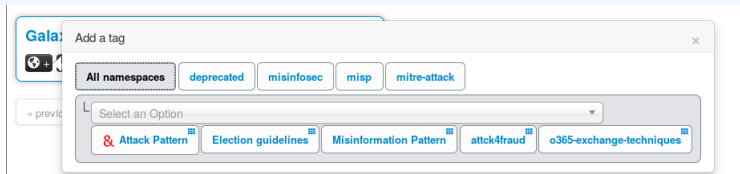
- Several ATT&CK like matrices added since in MISP galaxy
    - **attck4fraud**
    - **Election guidelines**
    - **Office365 exchange techniques**
    - **AM!TT Tactic**[1] (Adversarial Misinformation and Influence Tactics and Techniques) framework for describing disinformation incidents

---

[1]https://github.com/misinfosecproject/amitt_framework

example-of-threats	Email	andras.iklody@gmail.com		
Setup | party/candidate registration *(3 items)*	**Setup | electoral rolls** *(3 items)*	**Campaign | campaign IT** *(4 items)*	**All phases** *(3 items)*
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 ove
Fabricated signatures from sponsor	DoS or overload of voter registration system, suppressing voters	Hacking candidate laptops or email accounts	Hacking ca the election results
Tampering with registrations	Identity fraud during voter registration	Leak of confidential information	Hacking/mi communica
		Misconfiguration of a website	

Select Some Options

Cancel

Recon (10 items)	Compromise (8 items)	Persistence (6 items)	Expa (8 it
AAD - Dump users and groups with Azure AD	AAD - Password Spray: CredKing	End Point - Create Hidden Mailbox Rule	O365
End Point - Search host for Azure Credentials: SharpCloud	AAD - Password Spray: MailSniper	End Point - Persistence throught Outlook Home Page: SensePost Ruler	O365
O365 - Find Open Mailboxes: MailSniper	O365 - 2FA MITM Phishing: evilginx2	End Point - Persistence throught custom Outlook form	O365
O365 - Get Global Address List: MailSniper	O365 - Bruteforce of Autodiscover: SensePost Ruler	O365 - Add Global admin account	O365
O365 - User account enumeration with ActiveSync	O365 - Phishing for credentials	O365 - Add Mail forwarding rule	O365
On-Prem Exchange - Enumerate domain accounts: FindPeople	O365 - Phishing using OAuth app	O365 - Delegate Tenant Admin	O365
On-Prem Exchange - Enumerate domain accounts: OWA & Exchange	On-Prem Exchange - Bruteforce of Autodiscover: SensePost Ruler		On-P
On-Prem Exchange - Enumerate domain accounts: using Skype4B	On-Prem Exchange - Password Spray using Invoke-PasswordSprayOWA, EWS		On-P (EXC
On-Prem Exchange - OWA version discovery			
On-Prem Exchange - Portal Recon			

Select Some Options

Cancel

9

11

misinformation-tactics							
workflow:state="incomplete" x	workflow:todo="review" x						
Strategic Planning (4 items)	Objective Planning (2 items)	Develop People (3 items)	Develop Networks (6 items)	Microtargeting (3 items)	Develop Content (10 items)	Channel Selection (10 items)	Pump Pri (8 items)
5Ds (dismiss, distort, distract, dismay, divide)	Center of Gravity Analysis	Create fake Social Media Profiles / Pages / Groups	Create fake websites	Clickbait	Adapt existing narratives	Backstop personas	Bait legitim influencers
Competing Narratives	Create Master Narratives	Create fake experts	Create funding campaigns	Paid targeted ads	Conspiracy narratives	Facebook	Demand unsurmou
Facilitate State Propaganda		Create fake or imposter news sites	Create hashtag	Promote online funding	Create competing narratives	Instagram	Deny invol
Leverage Existing Narratives			Cultivate useful idiots		Create fake research	LinkedIn	Kernel of T
			Hijack legitimate account		Create fake videos and images	Manipulate online polls	Search En Optimizati
			Use concealment		Distort facts	Pinterest	Seed disto
					Generate information pollution	Reddit	Use SMS/ Chat apps
					Leak altered documents	Twitter	Use fake e
					Memes	WhatsApp	
					Trial content	YouTube	

CONCLUSION

- The matrix-like enhancement from the MISP galaxy format will be added in the default MISP galaxy standard format[2]
- MITRE ATT&CK sighting export in MISP was a first step to automate sharing of sightings ($\rightarrow$ public/private repository of sightings)
- ATT&CK like matrices become more and more common, thanks the **continuous work of the community**

---

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