

MISP and ATT&CK

How matrix-like models are changing MISP

Team CIRCL



25th October 2019 - attack-community.org



WHAT CHANGED SINCE THE LAST WORKSHOP?

- ATT&CK has been steadily on the rise
- We have observed 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 own **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?

SEARCHING OUR DATA-SET FOR ATT&CK-LIKE MATRIX HEATMAPS

■ The full dataset for a given time in an instance

Initial access (CT items)	Execution (CT items)	Persistence (CT items)	Privilege escalation (CT items)	Defense evasion (CT items)	Credential access (CT items)	Discovery (CT items)	Lateral movement (CT items)	Collection (CT items)	Exfiltration (CT items)	Command and control (CT items)
Spezifischer Link	Command-Line Interface	Hidden Files and Directories	Process Injection	Obfuscated Files or Information	Credentials in Files	System Information Discovery	Exploitation of Remote Services	Screen Capture	Data Encrypted	Standard Application Layer Protocol
Spezifischer Attachment	User Execution	Registry Run Keys / Startup Folder	Access Token Manipulation	File Deletion	Brute Force	File and Directory Discovery	Increase File Copy	Automated Collection	Exfiltration Over Command and Control Channel	Commonly Used Port
Drive-by-Compromise	PowerShell	Component Object Model Hijacking	DLL Search Order Hijacking	Deobfuscate/Decode Files or Information	Credential Dumping	Account Discovery	AppletScript	Data Staged	Automated Exfiltration	Custom Command and Control Protocol
Exploit Public-Facing Application	Service Execution	DLL Search Order Hijacking	Hoisting	Hidden Files and Directories	Hoisting	Password Policy Discovery	Application Deployment Software	Data from Local System	Data Compressed	Data Encrypted
VMI Accounts	CMSTP	Hoisting	New Service	DLL Side-Loading	Input Capture	Process Discovery	Distributed Component Object Model	Data from Network Shared Drive	Data Transfer Size Limits	Data Obfuscation
External Remote Services	Execution Through Mobile Load	New Service	Scheduled Task	Process Injection	Account Manipulation	Query Registry	Logon Scripts	Data from Removable Media	Exfiltration Over Alternative Protocol	Uncommonly Used Port
Hardware Additions	Runnable	Scheduled Task	Valid Accounts	Access Token Manipulation	Back History	System Network Configuration Discovery	Pass the Hash	Input Capture	Exfiltration Over Other Network Medium	Custom Cryptographic Protocol
Replication Through Removable Media	Scheduled Task	VMI Accounts	Web Shell	CMSTP	Credentials in Registry	System Configuration Discovery	Pass the Ticket	Audio Capture	Exfiltration Over Physical Medium	Fallback Channels
Spezifischer via Service	Scripting	Web Shell	Accessibility Features	Clear Command History	Exploitation for Credential Access	System Time Discovery	Remote Desktop Protocol	Clipboard Data	Scheduled Transfer	Multi-stage Channels
Supply Chain Compromise	Windows Management Instrumentation	task_profile and taskco	AppCert DLLs	Code Signing	Foiled Authentication	Application Window Discovery	Remote Services	Data from Information Repositories		Multi-Step Encryption
Trusted Relationship	AppletScript	Accessibility Features	Applet DLLs	Component Object Model Hijacking	Input Prompt	Browser Bookmarks Discovery	Replication Through Removable Media	Email Collection		Remote File Copy
	Compiled HTML File	Account Manipulation	Application Shimming	DLL Search Order Hijacking	KernelEvasion	Domain Trust Discovery	SSH Hijacking	Man in the Browser		Standard Cryptographic Protocol
	Control Panel Items	AppCert DLLs	Bypass User Account Control	Disabling Security Tools	Keychain	Network Service Scanning	Shared Webroot	Video Capture		Communication Through Removable Media
	Dynamic Data Exchange	Applet DLLs	Dylib Hijacking	FBI Permissions	LLMNR/BTNS Poisoning	Network Share Discovery	Task Shared Content			Connection Proxy

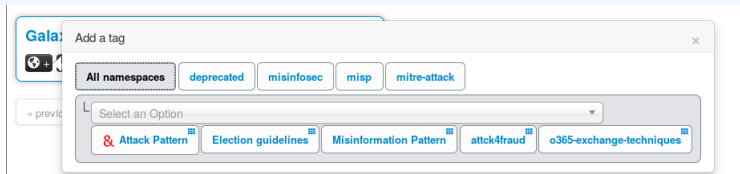
SEARCHING OUR DATA-SET FOR ATT&CK-LIKE MATRIX HEATMAPS

- The full dataset for a given time in an instance

Initial access (21 items)	Execution (21 items)	Persistence (21 items)	Privilege escalation (21 items)	Defensive evasion (21 items)	Credential access (21 items)	Discovery (21 items)	Lateral movement (21 items)	Collection (21 items)	Exfiltration (21 items)	Command and control (21 items)
Spinephishing Link	Command-Line Interface	Component Object Model Hijacking	Process Injection	Clean Command History	Input Capture	File and Directory Discovery	Remote File Copy	Automated Collection	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Shell/BI	Registry Run Keys / Startup Folder	Scheduled Task	Component Object Model Hijacking	Account Manipulation	System Information Discovery	AppleScript	Data Stager	Data Encrypted	Custom Command and Control Protocol
Spinephishing Attachment	Scheduled Task	Scheduled Task	WMI Accounts	Disabling Security Tools	Batch History	Account Discovery	Application Deployment Software	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
WMI Accounts	User Execution	WMI Accounts	Web Shell	File Deletion	Brute Force	Process Discovery	Distributed Component Object Model	Data from Network Shared Drive	Data Compressed	Data Obfuscation
Drive-by Compromise	Windows Management Instrumentation	Web Shell	Access Token Manipulation	Process Injection	Credential Dumping	Query Registry	Exploitation of Remote Services	Data from Removable Media	Data Transfer Size Limits	Custom Cryptographic Protocol
External Remote Services	AppleScript	batch_profile and batch	Accessibility Features	Shell/BI	Credentials in Files	Application Window Discovery	Logon Scripts	Input Capture	Exfiltration Over Alternative Protocol	Fallback Channels
Hardware Additions	CMSTP	Accessibility Features	AppCert DLLs	WMI Accounts	Credentials in Registry	Browser Bookmark Discovery	Pass the Hash	Screen Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Replication Through Removable Media	Compiled HTML File	Account Manipulation	Applet DLLs	Access Token Manipulation	Exploitation for Credential Access	Domain Trust Discovery	Pass the Ticket	Audio Capture	Exfiltration Over Physical Medium	Multi-layer Encryption
Spinephishing via Service	Control Panel Items	AppCert DLLs	Application Shimming	BITS Jobs	Forced Authentication	Network Service Scanning	Remote Desktop Protocol	Clipboard Data	Scheduled Transfer	Remote File Copy
Supply Chain Compromise	Dynamic Data Exchange	Applet DLLs	Bypass User Account Control	Binary Padding	Hooking	Network Share Discovery	Remote Services	Data from Information Repositories		Standard Application Layer Protocol
Trusted Relationship	Execution through API	Application Shimming	DLL Search Order Hijacking	Bypass User Account Control	Input Prompt	Network Sniffing	Replication Through Removable Media	Email Collection		Standard Cryptographic Protocol

ATT&CK MATRICES AS A STANDARDISED METHODOLOGY

- 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



ATT&CK MATRICES AS A STANDARDISED METHODOLOGY OUTCOMES

- 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

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

ELECTION GUIDELINES

example-of-threats	Email	andras.klody@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 elector results	
Tampering with registrations	Identity fraud during voter registration	Leak of confidential information	Hacking/mi communica	
		Misconfiguration of a website		
Select Some Options				
Cancel				

OFFICE 365 TECHNIQUES

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

Cancel

AM!TT TACTIC (ADVERSARIAL MISINFORMATION AND INFLUENCE TACTICS AND TECHNIQUES)

misinformation-tactics							
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 unsumrou
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 ER 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	

- The matrix-like enhancement from the MISP galaxy format will be added in the default MISP galaxy standard format²
- MITRE ATT&CK sighting export in MISP was a first step to automate sharing of sightings (→ 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/>