Turning data into actionable intelligence

advanced features in MISP supporting your analysts and tools

Team CIRCL

MISP Summit 2019
20191021

What changed since the last workshop?

- 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

New ATT&CK sighting reporting format

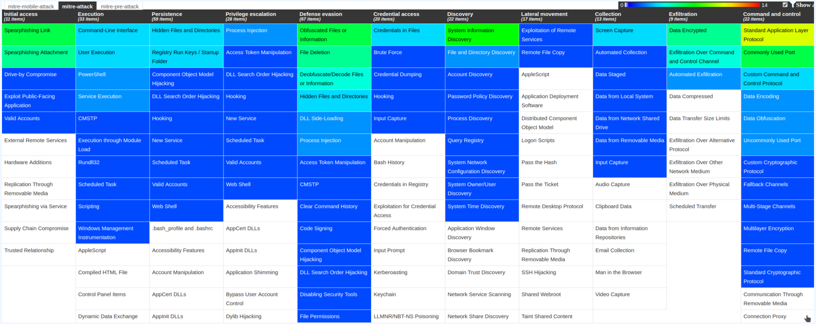
- Result of discussions with Mitre
- MISP server hosts can now decide to export an **enumeration of the patterns** used based on the data-set
- Subject to all regular **restSearch filtering methods** (time, organisation, context, etc)
- Export returns the data-set in Mitre's owns **ATT&CK sighting format**

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?

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

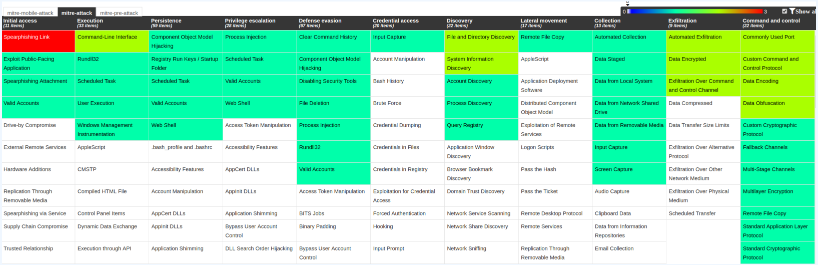
- The full dataset for a given time in an instance



Initial access (11 items)	Execution (33 items)	Persistence (59 items)	Privilege escalation (28 items)	Defense evasion (67 items)	Credential access (20 items)	Discovery (22 items)	Lateral movement (17 items)	Collection (13 items)	Exfiltration (9 items)	Command and control (22 items)
Spearphishing 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
Spearphishing Attachment	User Execution	Registry Run Keys / Startup Folder	Access Token Manipulation	File Deletion	Brute Force	File and Directory Discovery	Remote 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	AppleScript	Data Staged	Automated Exfiltration	Custom Command and Control Protocol
Exploit Public-Facing Application	Service Execution	DLL Search Order Hijacking	Hooking	Hidden Files and Directories	Hooking	Password Policy Discovery	Application Deployment Software	Data from Local System	Data Compressed	Data Encoding
Valid Accounts	CMSTP	Hooking	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 Module 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	Rundll32	Scheduled Task	Valid Accounts	Access Token Manipulation	Bash History	System Network Configuration Discovery	Pass the Hash	Input Capture	Exfiltration Over Other Network Medium	Custom Cryptographic Protocol
Replication Through Removable Media	Scheduled Task	Valid Accounts	Web Shell	CMSTP	Credentials in Registry	System Owner/User Discovery	Pass the Ticket	Audio Capture	Exfiltration Over Physical Medium	Fallback Channels
Spearphishing 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	.bash_profile and .bashrc	AppCert DLLs	Code Signing	Forced Authentication	Application Window Discovery	Remote Services	Data from Information Repositories		Multilayer Encryption
Trusted Relationship	AppleScript	Accessibility Features	AppInit DLLs	Component Object Model Hijacking	Input Prompt	Browser Bookmark Discovery	Replication Through Removable Media	Email Collection		Remote File Copy
	Compiled HTML File	Account Manipulation	Application Shimming	DLL Search Order Hijacking	Kerberoasting	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	AppInit DLLs	Dylib Hijacking	File Permissions	LLMNR/NBT-NS Poisoning	Network Share Discovery	Taint 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 *(11 items)*	Execution *(33 items)*	Persistence *(59 items)*	Privilege escalation *(28 items)*	Defense evasion *(67 items)*	Credential access *(20 items)*	Discovery *(22 items)*	Lateral movement *(17 items)*	Collection *(13 items)*	Exfiltration *(9 items)*	Command and control *(22 items)*
Spearphishing Link	Command-Line Interface	Component Object Model Hijacking	Process Injection	Clear Command History	Input Capture	File and Directory Discovery	Remote File Copy	Automated Collection	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Rundll32	Registry Run Keys / Startup Folder	Scheduled Task	Component Object Model Hijacking	Account Manipulation	System Information Discovery	AppleScript	Data Staged	Data Encrypted	Custom Command and Control Protocol
Spearphishing Attachment	Scheduled Task	Scheduled Task	Valid Accounts	Disabling Security Tools	Bash History	Account Discovery	Application Deployment Software	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Valid Accounts	User Execution	Valid 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	.bash_profile and .bashrc	Accessibility Features	Rundll32	Credentials in Files	Application Window Discovery	Logon Scripts	Input Capture	Exfiltration Over Alternative Protocol	Fallback Channels
Hardware Additions	CMSTP	Accessibility Features	AppCert DLLs	Valid 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	AppInit DLLs	Access Token Manipulation	Exploitation for Credential Access	Domain Trust Discovery	Pass the Ticket	Audio Capture	Exfiltration Over Physical Medium	Multilayer Encryption
Spearphishing 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	AppInit 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

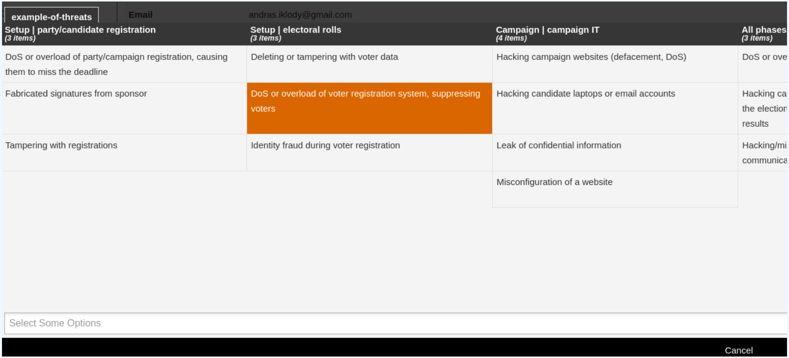
ATT&CK MATRICES AS A STANDARDISED METHODOLOGY

- 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
  - **Election guidelines**
  - **Office 365 exchange techniques**

Election guidelines

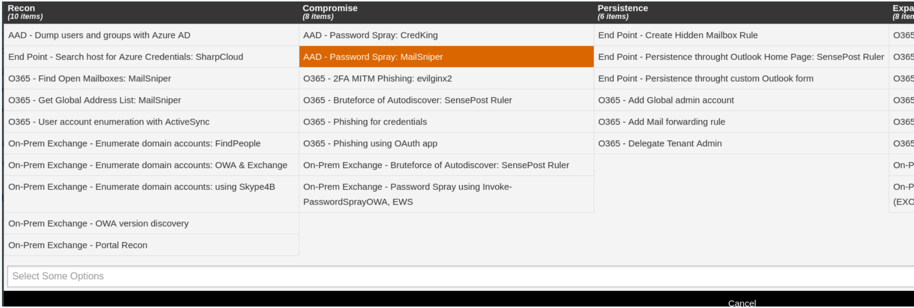


example-of-threats

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	

OFFICE 365 TECHNIQUES



Recon *(10 items)*	Compromise *(8 items)*	Persistence *(6 items)*	Expa *(8 item*
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			