Module 3:

Storing and Analyzing ATT&CK® Mapped Data

Jackie Lasky

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Approved for Public Release; Distribution Unlimited. Public Release Case Number 23-4342

Module 3 Agenda

Lesson 3.1:Storing and Displaying ATT&CK mapped Data

Lesson 3.2: Expressing ATT&CK mapped Data

Lesson 3.3: Analyzing ATT&CK mapped Data

Lesson 3.4: Compare Layers in ATT&CK Navigator

Lesson 3.1
Storing and Displaying ATT&CK® Mapped Data

Lesson 3.1 Objectives

1 Consider who (or what) will be consuming the mapped CTI

2 Identify the most effective storage platform for your environment and requirements

Storing ATT&CK Mapped Data: Considerations

Who's consuming it?

Human or machine?

What are the intelligence requirements? How will you provide context?

Include full text?

How detailed will it be?

Just a Technique/ sub-technique, or a Procedure?

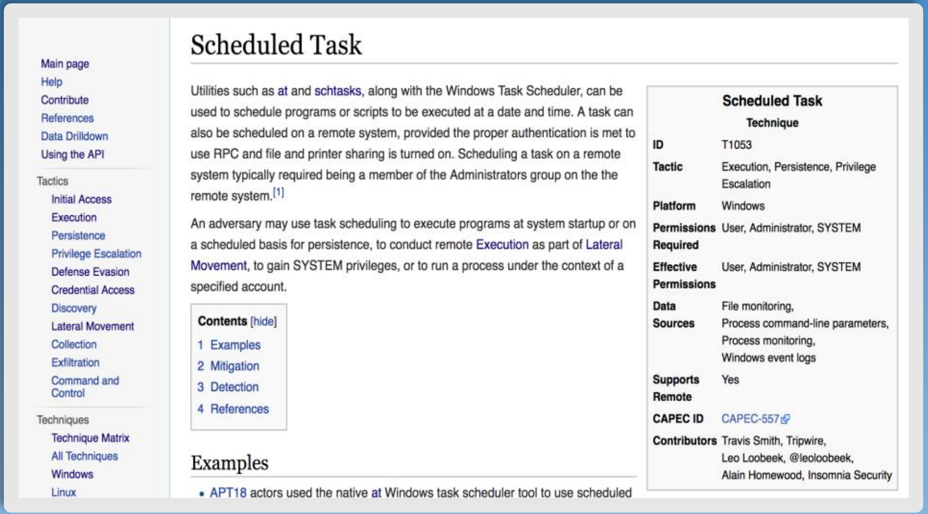
How will you capture that detail?

- (Free text?) How will you link it to other CTI?
- Incident, group, campaign, indicator?

How will you import and export data?

What format will you use?

Storing and Displaying ATT&CK Mapped Data



Main page
Help
Contribute
References
Data Drilldown
Using the API

Tactics

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

Techniques

- Technique Matrix
- All Techniques
- Windows
- Linux

Scheduled Task

Utilities such as at and schtasks, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically required being a member of the Administrators group on the the remote system.[1]

An adversary may use task scheduling to execute programs at system startup or on a scheduled basis for persistence, to conduct remote Execution as part of Lateral Movement, to gain SYSTEM privileges, or to run a process under the context of a specified account.

Contents [hide]

1 Examples
2 Mitigation
3 Detection
4 References

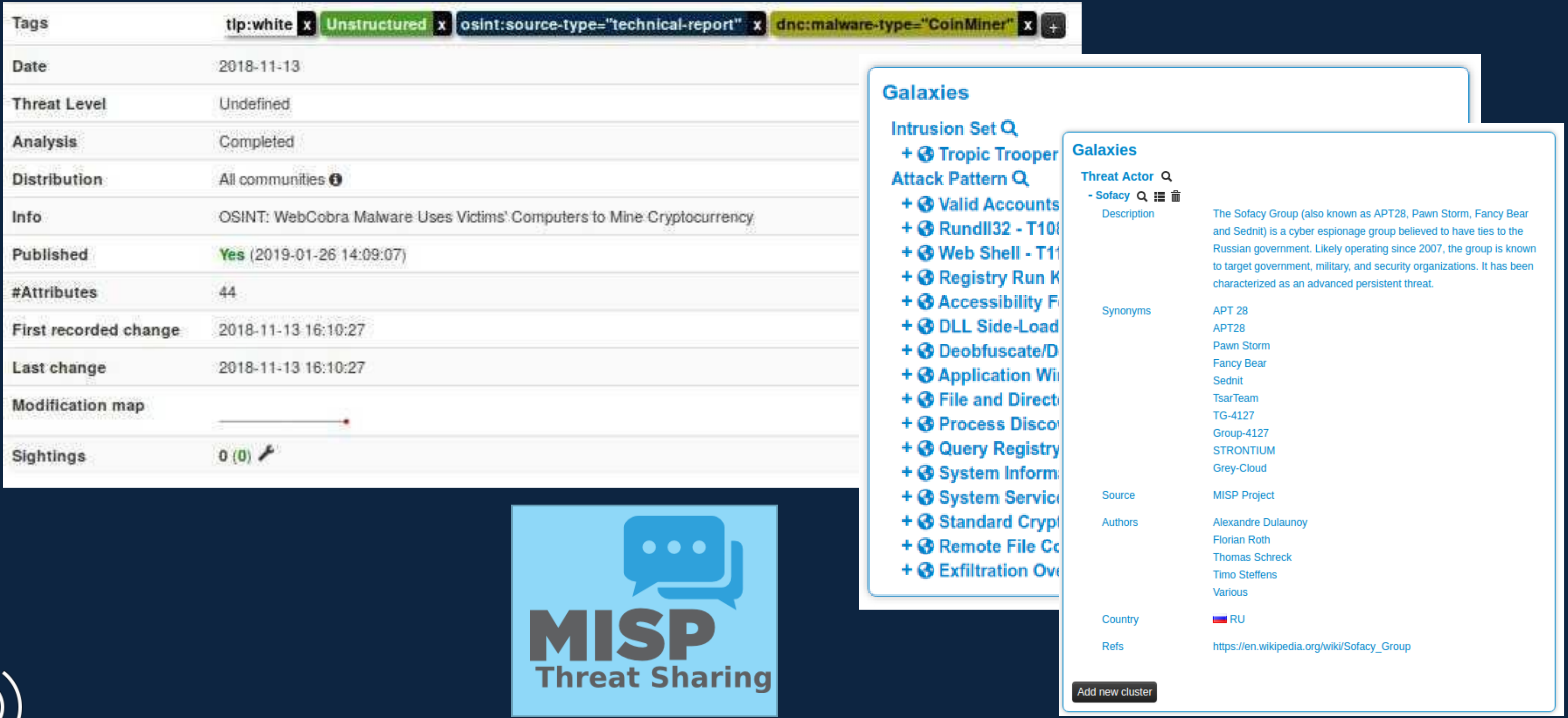
Scheduled Task
Technique

ID	T1053
Tactic	Execution, Persistence, Privilege Escalation
Platform	Windows
Permissions Required	User, Administrator, SYSTEM
Effective Permissions	User, Administrator, SYSTEM
Data Sources	File monitoring, Process command-line parameters, Process monitoring, Windows event logs
Supports Remote	Yes
CAPEC ID	CAPEC-557
Contributors	Travis Smith, Tripwire, Leo Loobeek, @leoloobeek, Alain Homewood, Insomnia Security

Examples

- APT18 actors used the native at Windows task scheduler tool to use scheduled

Storing and Displaying ATT&CK Mapped Data



Tags	tlp:white x Unstructured x osint:source-type="technical-report" x dnc:malware-type="CoinMiner" x +
Date	2018-11-13
Threat Level	Undefined
Analysis	Completed
Distribution	All communities
Info	OSINT: WebCobra Malware Uses Victims' Computers to Mine Cryptocurrency
Published	Yes (2019-01-26 14:09:07)
#Attributes	44
First recorded change	2018-11-13 16:10:27
Last change	2018-11-13 16:10:27
Modification map	
Sightings	0 (0)

Galaxies

Intrusion Set

+ Tropic Trooper

Attack Pattern

+ Valid Accounts
+ Rundll32 - T108
+ Web Shell - T11
+ Registry Run K
+ Accessibility F
+ DLL Side-Load
+ Deobfuscate/D
+ Application Wi
+ File and Direct
+ Process Disco
+ Query Registry
+ System Inform
+ System Servic
+ Standard Cryp
+ Remote File C
+ Exfiltration Ov

Galaxies

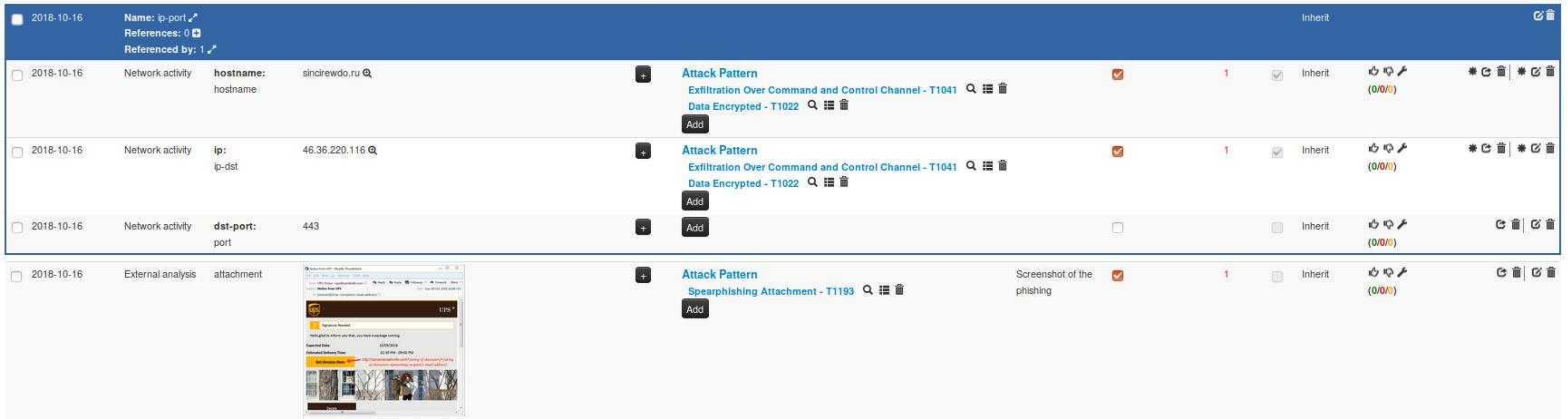
Threat Actor

- Sofacy

Description	The Sofacy Group (also known as APT28, Pawn Storm, Fancy Bear and Sednit) is a cyber espionage group believed to have ties to the Russian government. Likely operating since 2007, the group is known to target government, military, and security organizations. It has been characterized as an advanced persistent threat.
Synonyms	APT 28 APT28 Pawn Storm Fancy Bear Sednit TsarTeam TG-4127 Group-4127 STRONTIUM Grey-Cloud
Source	MISP Project
Authors	Alexandre Dulaunoy Florian Roth Thomas Schreck Timo Steffens Various
Country	RU
Refs	https://en.wikipedia.org/wiki/Sofacy_Group

MISP Threat Sharing

Storing and Displaying ATT&CK Mapped Data



☐	2018-10-16	**Name:** ip-port **References:** 0 **Referenced by:** 1								Inherit	
☐	2018-10-16	Network activity	**hostname:** hostname	sincirewdo.ru	+	Attack Pattern Exfiltration Over Command and Control Channel - T1041 Data Encrypted - T1022 Add		☑	1	☑	Inherit	(0/0/0)
☐	2018-10-16	Network activity	**ip:** ip-dst	46.36.220.116	+	Attack Pattern Exfiltration Over Command and Control Channel - T1041 Data Encrypted - T1022 Add		☑	1	☑	Inherit	(0/0/0)
☐	2018-10-16	Network activity	**dst-port:** port	443	+	Add		☐		☐	Inherit	(0/0/0)
☐	2018-10-16	External analysis	attachment		+	Attack Pattern Spearphishing Attachment - T1193 Add	Screenshot of the phishing	☑	1	☐	Inherit	(0/0/0)

Courtesy of Alexandre Dulaunoy

Ability to link to indicators and files

MISP
Threat Sharing

Lesson 3.1 Summary

1. Considered how the ATT&CK mapped data would be consumed, linked, contextualized, and imported/exported

2. Reviewed internal and external storage platform options for your environment and requirements

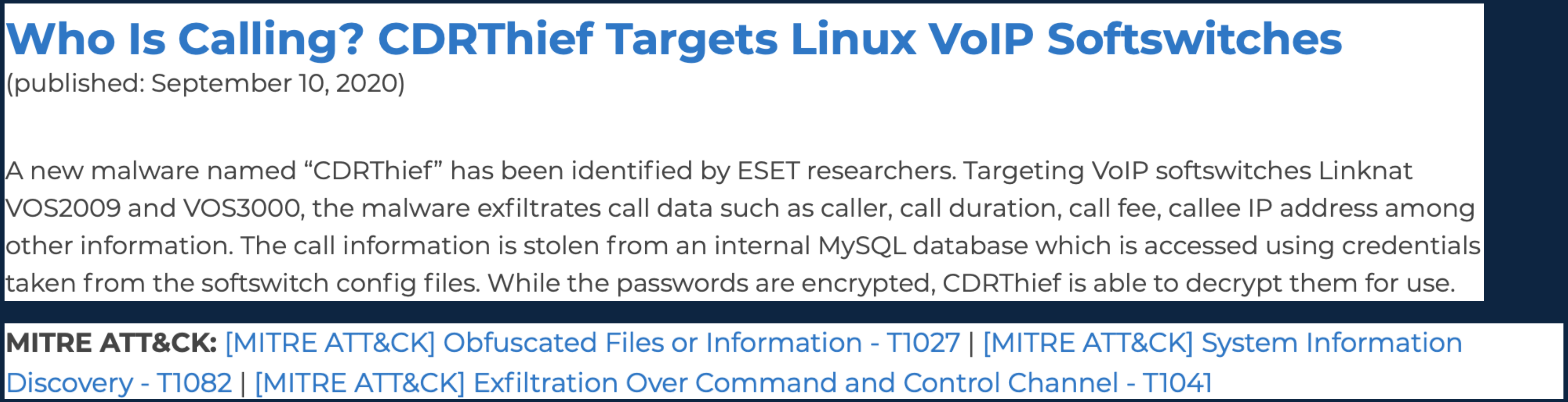
Lesson 3.2 Expressing and Storing ATT&CK® Mapped Data

Lesson 3.2 Objectives

1 Review methods for expressing and storing mapped-data

2 Identify the most effective approach for your environment and requirements

Expressing and Storing ATT&CK Mapped Data



Who Is Calling? CDRThief Targets Linux VoIP Softswitches

(published: September 10, 2020)

A new malware named “CDRThief” has been identified by ESET researchers. Targeting VoIP softswitches Linknat VOS2009 and VOS3000, the malware exfiltrates call data such as caller, call duration, call fee, callee IP address among other information. The call information is stolen from an internal MySQL database which is accessed using credentials taken from the softswitch config files. While the passwords are encrypted, CDRThief is able to decrypt them for use.

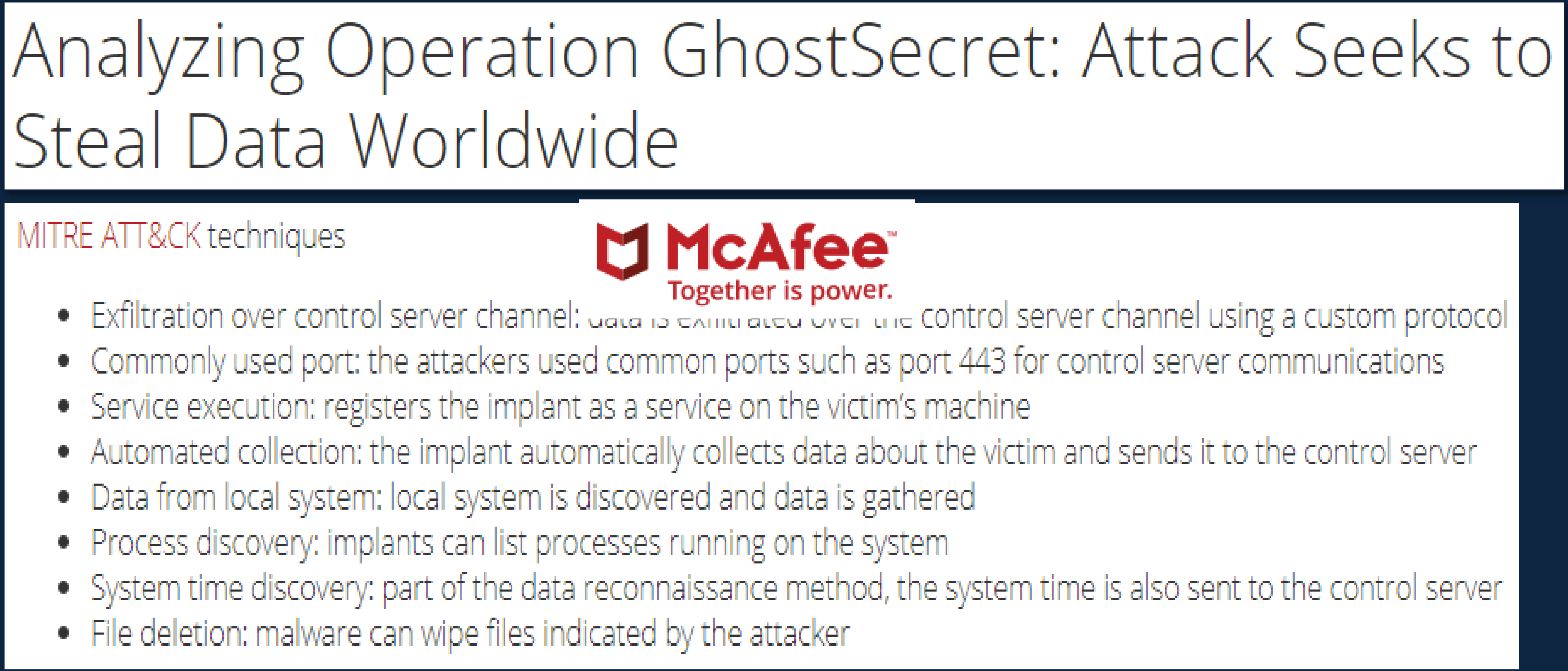
MITRE ATT&CK: [MITRE ATT&CK] Obfuscated Files or Information - T1027 | [MITRE ATT&CK] System Information Discovery - T1082 | [MITRE ATT&CK] Exfiltration Over Command and Control Channel - T1041

Techniques at the end of a report

ANOMALI

Expressing and Storing ATT&CK Mapped Data

Techniques at the end of a report



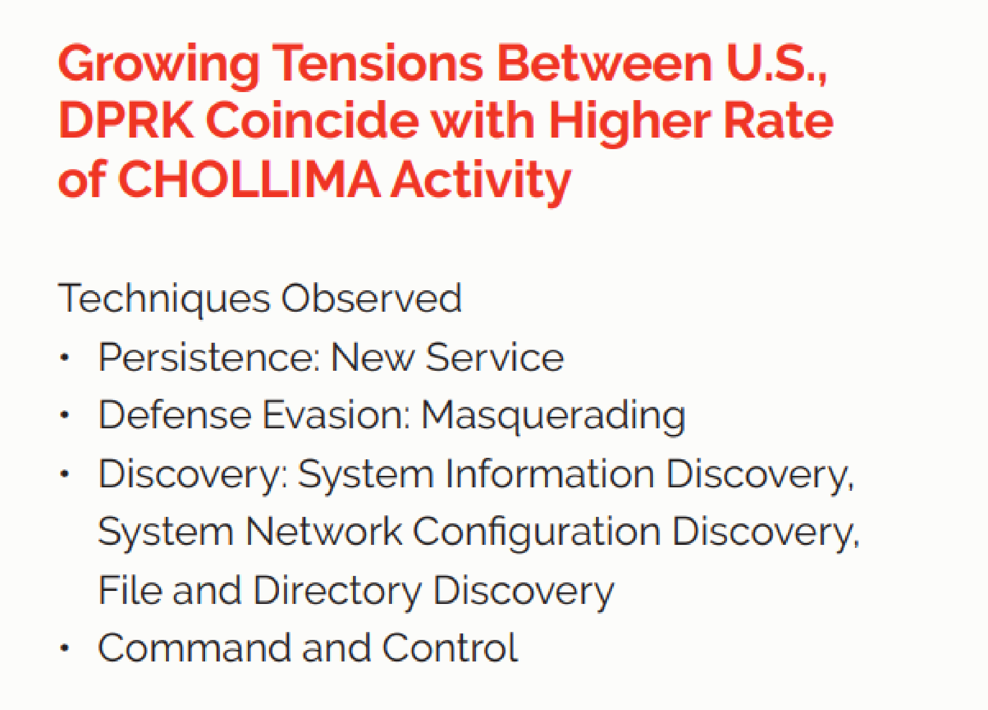
Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide

McAfee
Together is power.

MITRE ATT&CK techniques

- Exfiltration over control server channel: data is exfiltrated over the control server channel using a custom protocol
- Commonly used port: the attackers used common ports such as port 443 for control server communications
- Service execution: registers the implant as a service on the victim's machine
- Automated collection: the implant automatically collects data about the victim and sends it to the control server
- Data from local system: local system is discovered and data is gathered
- Process discovery: implants can list processes running on the system
- System time discovery: part of the data reconnaissance method, the system time is also sent to the control server
- File deletion: malware can wipe files indicated by the attacker

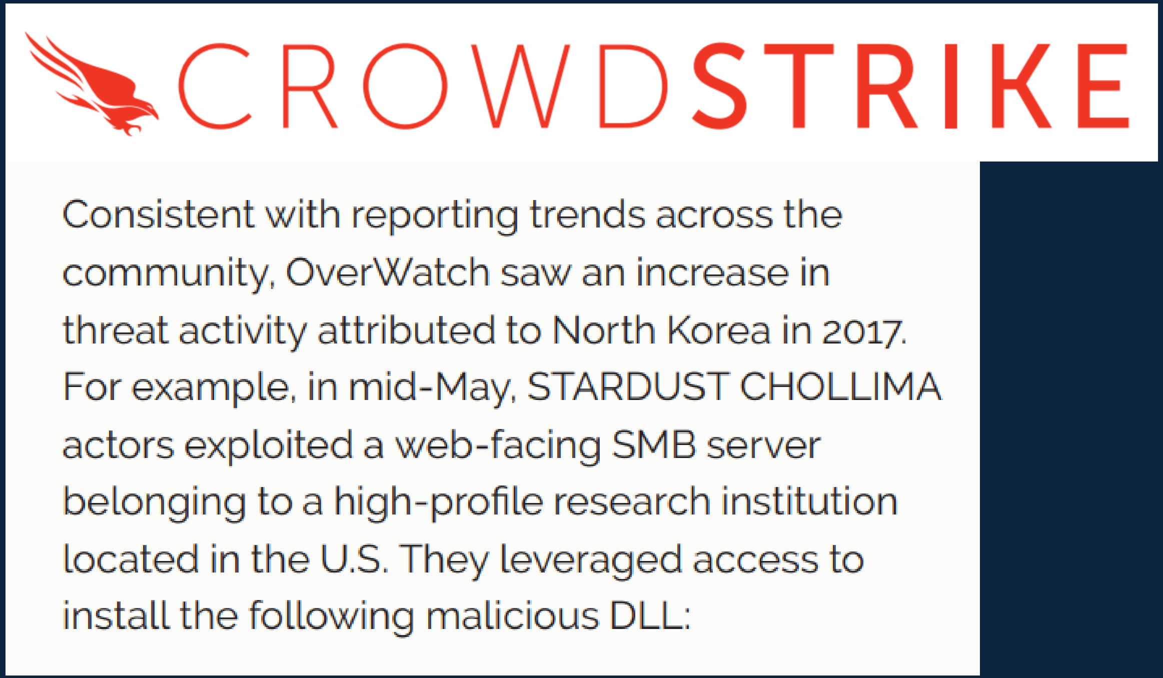
Expressing and Storing ATT&CK Mapped Data



Growing Tensions Between U.S., DPRK Coincide with Higher Rate of CHOLLIMA Activity

Techniques Observed

- Persistence: New Service
- Defense Evasion: Masquerading
- Discovery: System Information Discovery, System Network Configuration Discovery, File and Directory Discovery
- Command and Control



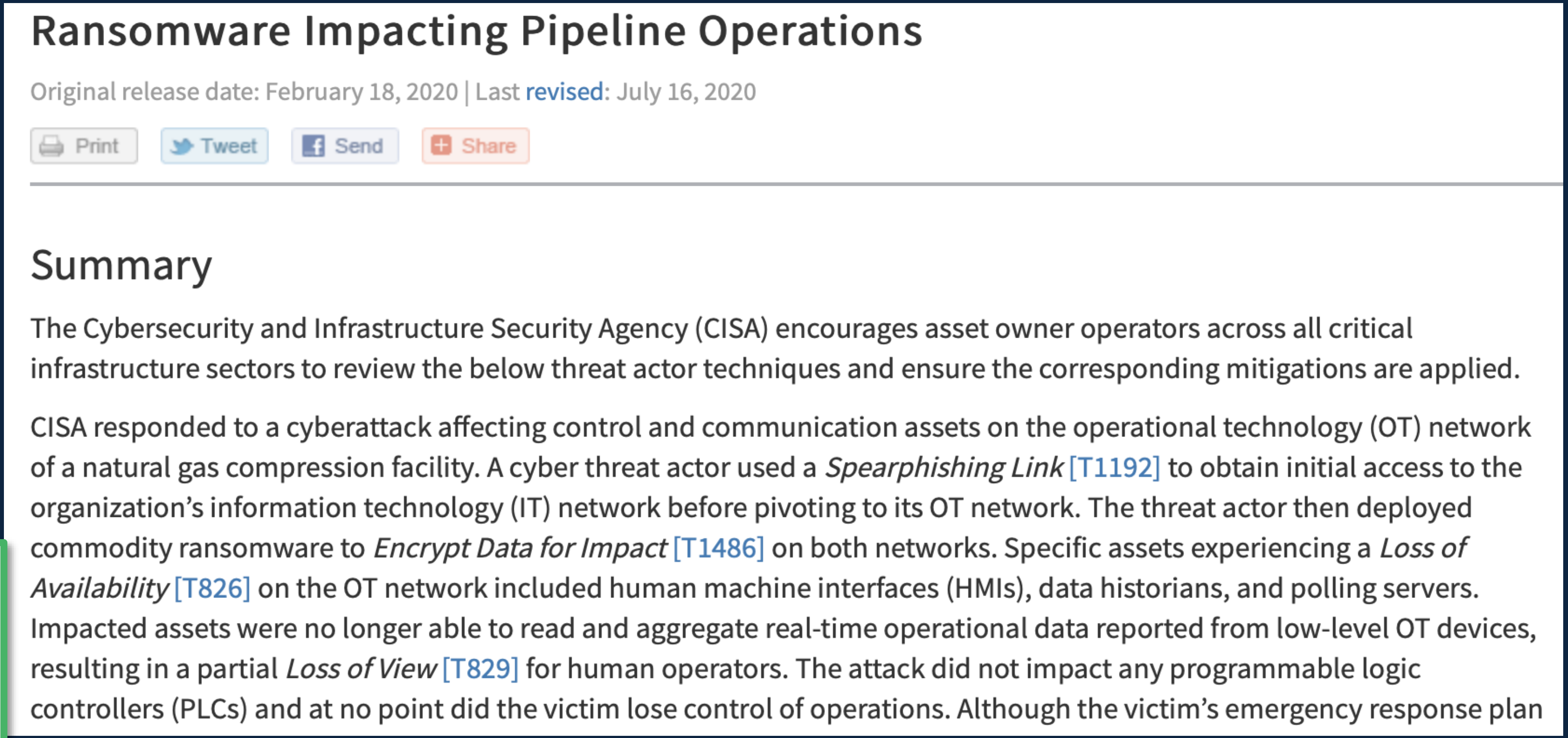
CROWDSTRIKE

Consistent with reporting trends across the community, OverWatch saw an increase in threat activity attributed to North Korea in 2017. For example, in mid-May, STARDUST CHOLLIMA actors exploited a web-facing SMB server belonging to a high-profile research institution located in the U.S. They leveraged access to install the following malicious DLL:

Techniques at the beginning of a report

https://www.crowdstrike.com/resources/reports/2018-crowdstrike-global-threat-report-blurring-the-lines-between-statecraft-and-tradecraft/

Expressing and Storing ATT&CK Mapped Data



Ransomware Impacting Pipeline Operations

Original release date: February 18, 2020 | Last revised: July 16, 2020

Summary

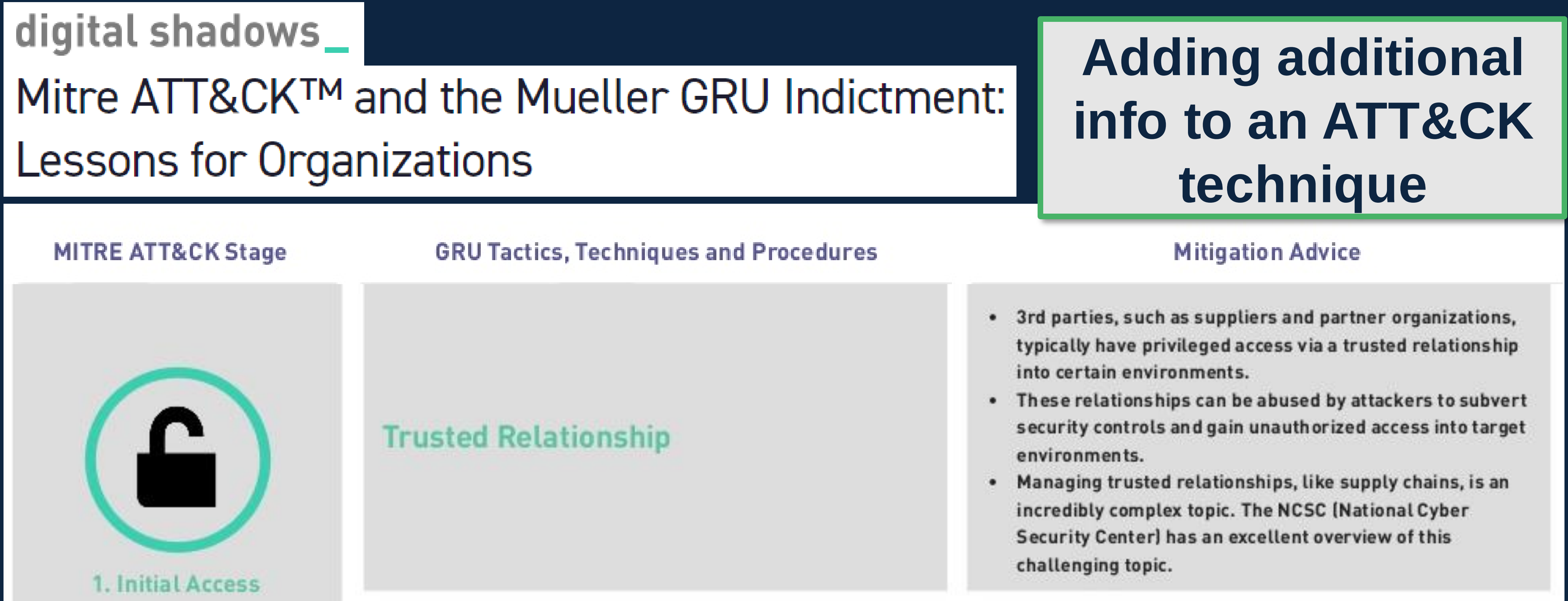
The Cybersecurity and Infrastructure Security Agency (CISA) encourages asset owner operators across all critical infrastructure sectors to review the below threat actor techniques and ensure the corresponding mitigations are applied.

CISA responded to a cyberattack affecting control and communication assets on the operational technology (OT) network of a natural gas compression facility. A cyber threat actor used a *Spearphishing Link* [T1192] to obtain initial access to the organization's information technology (IT) network before pivoting to its OT network. The threat actor then deployed commodity ransomware to *Encrypt Data for Impact* [T1486] on both networks. Specific assets experiencing a *Loss of Availability* [T826] on the OT network included human machine interfaces (HMIs), data historians, and polling servers. Impacted assets were no longer able to read and aggregate real-time operational data reported from low-level OT devices, resulting in a partial *Loss of View* [T829] for human operators. The attack did not impact any programmable logic controllers (PLCs) and at no point did the victim lose control of operations. Although the victim's emergency response plan

In-text Techniques in a report

https://us-cert.cisa.gov/ncas/alerts/aa20-049a

Expressing and Storing ATT&CK Mapped Data



digital shadows_

Mitre ATT&CK™ and the Mueller GRU Indictment: Lessons for Organizations

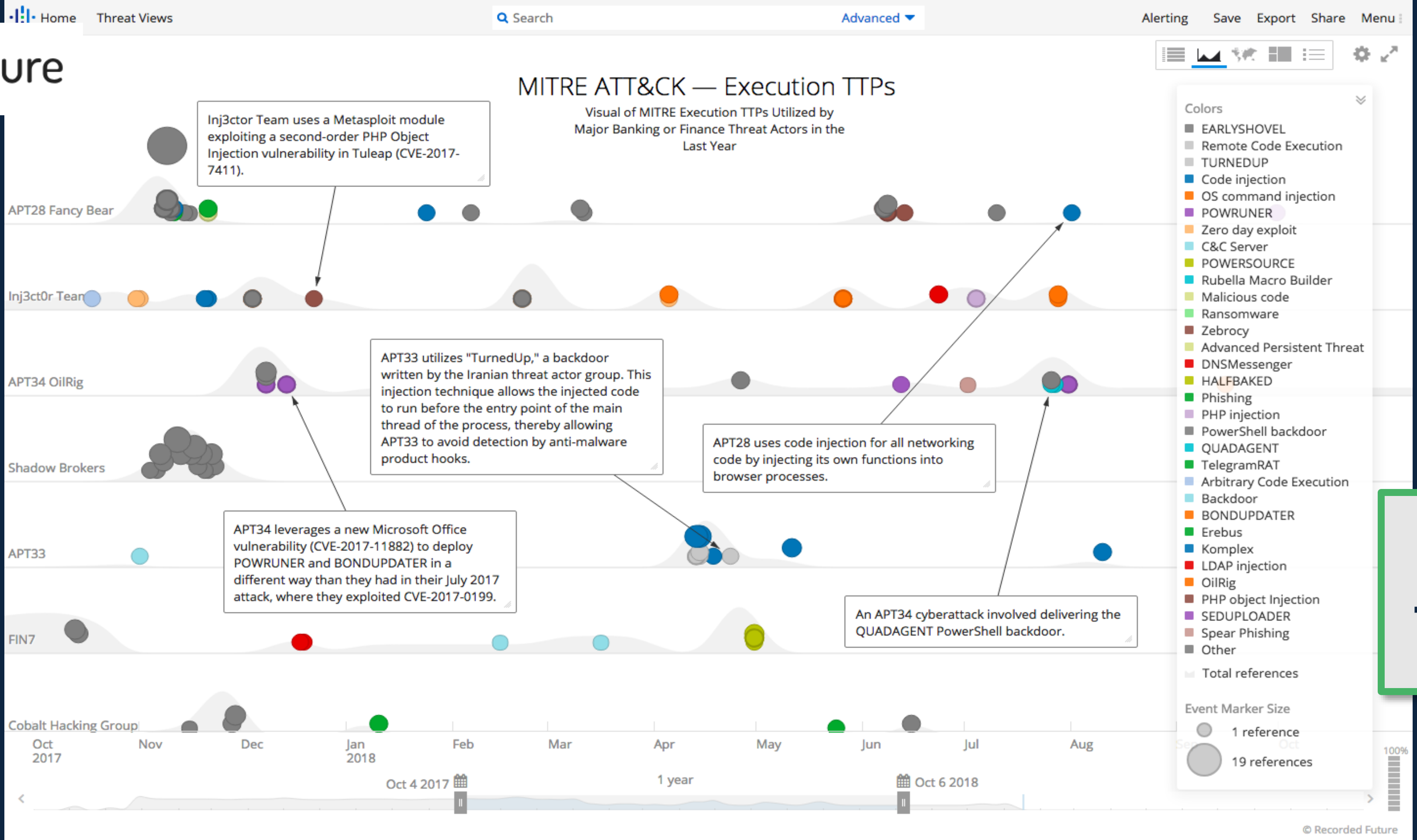
MITRE ATT&CK Stage	GRU Tactics, Techniques and Procedures	Mitigation Advice
1. Initial Access	Trusted Relationship	• 3rd parties, such as suppliers and partner organizations, typically have privileged access via a trusted relationship into certain environments. • These relationships can be abused by attackers to subvert security controls and gain unauthorized access into target environments. • Managing trusted relationships, like supply chains, is an incredibly complex topic. The NCSC (National Cyber Security Center) has an excellent overview of this challenging topic.

Adding additional info to an ATT&CK technique

https://www.digitalshadows.com/blog-and-research/mitre-attck-and-the-mueller-gru-indictment-lessons-for-organizations/

Expressing and Storing ATT&CK Mapped Data

Recorded Future



MITRE ATT&CK — Execution TTPs

Visual of MITRE Execution TTPs Utilized by Major Banking or Finance Threat Actors in the Last Year

Inj3ctor Team uses a Metasploit module exploiting a second-order PHP Object Injection vulnerability in Tuleap (CVE-2017-7411).

APT33 utilizes "TurnedUp," a backdoor written by the Iranian threat actor group. This injection technique allows the injected code to run before the entry point of the main thread of the process, thereby allowing APT33 to avoid detection by anti-malware product hooks.

APT28 uses code injection for all networking code by injecting its own functions into browser processes.

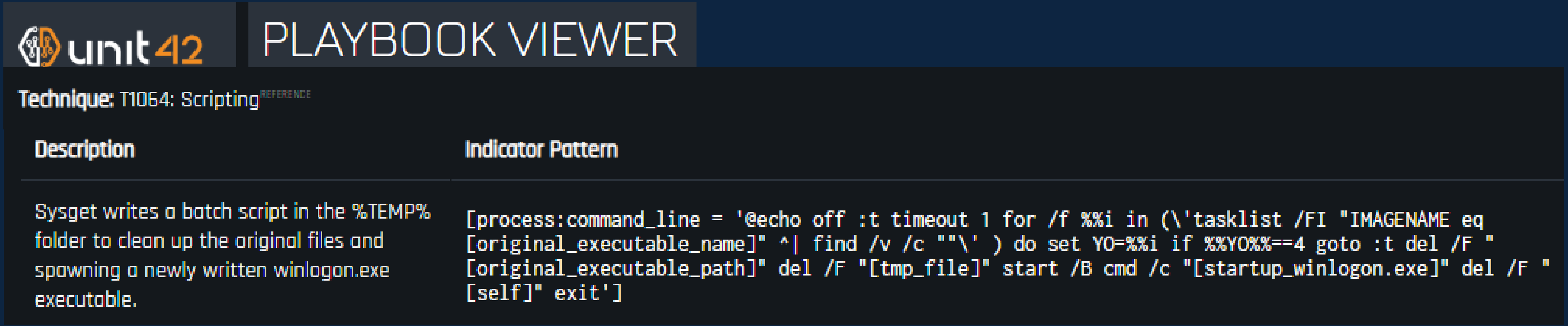
APT34 leverages a new Microsoft Office vulnerability (CVE-2017-11882) to deploy POWRUNER and BONDUPDATER in a different way than they had in their July 2017 attack, where they exploited CVE-2017-0199.

An APT34 cyberattack involved delivering the QUADAGENT PowerShell backdoor.

With timestamps

https://www.recordedfuture.com/mitre-attack-framework/

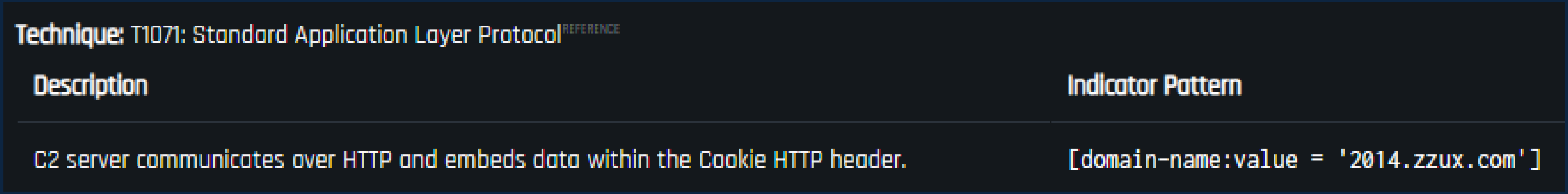
Expressing and Storing ATT&CK Mapped Data



unit42 PLAYBOOK VIEWER

Technique: T1064: Scripting^REFERENCE

Description	Indicator Pattern
Sysget writes a batch script in the %TEMP% folder to clean up the original files and spawning a newly written winlogon.exe executable.	`[process:command_line = '@echo off :t timeout 1 for /f %%i in (\'tasklist /FI "IMAGENAME eq [original_executable_name]" ^| find /v /c ""\' ) do set YO=%%i if %%YO%%==4 goto :t del /F "[original_executable_path]" del /F "[tmp_file]" start /B cmd /c "[startup_winlogon.exe]" del /F "[self]" exit']`

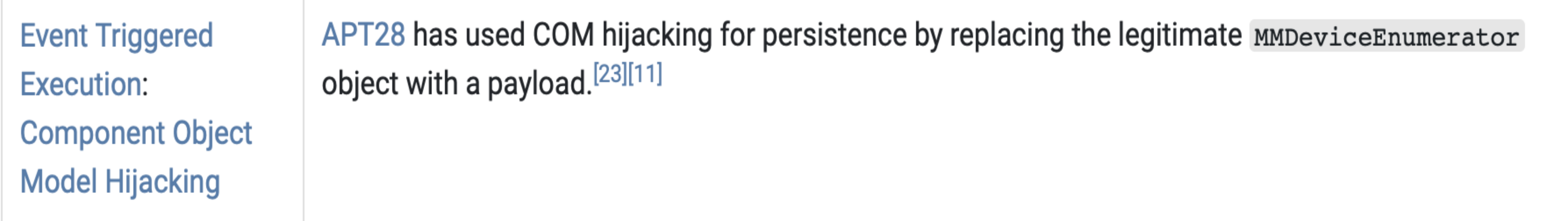


Technique: T1071: Standard Application Layer Protocol^REFERENCE

Description	Indicator Pattern
C2 server communicates over HTTP and embeds data within the Cookie HTTP header.	`[domain-name:value = '2014.zzux.com']`

https://pan-unit42.github.io/playbook_viewer/

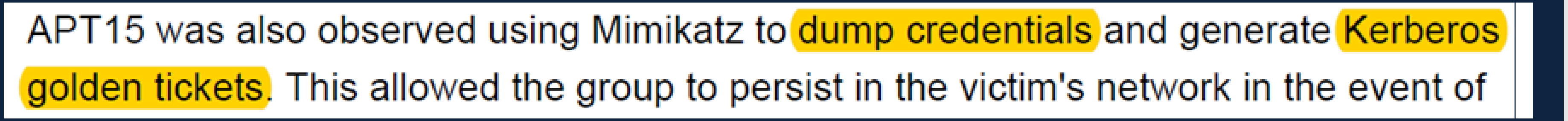
Expressing and Storing ATT&CK Mapped Data



Event Triggered Execution: Component Object Model Hijacking	APT28 has used COM hijacking for persistence by replacing the legitimate `MMDeviceEnumerator` object with a payload.[23][11]

https://attack.mitre.org/groups/G0007/

Full-Text Report



APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets. This allowed the group to persist in the victim's network in the event of

https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

ATT&CK Technique

OS Credential Dumping (T1003)

Lesson 3.2 Summary

1 Reviewed various methods and levels of detail for expressing and storing mapped-data

2 Examined how to identify the most effective approach for your environment and requirements

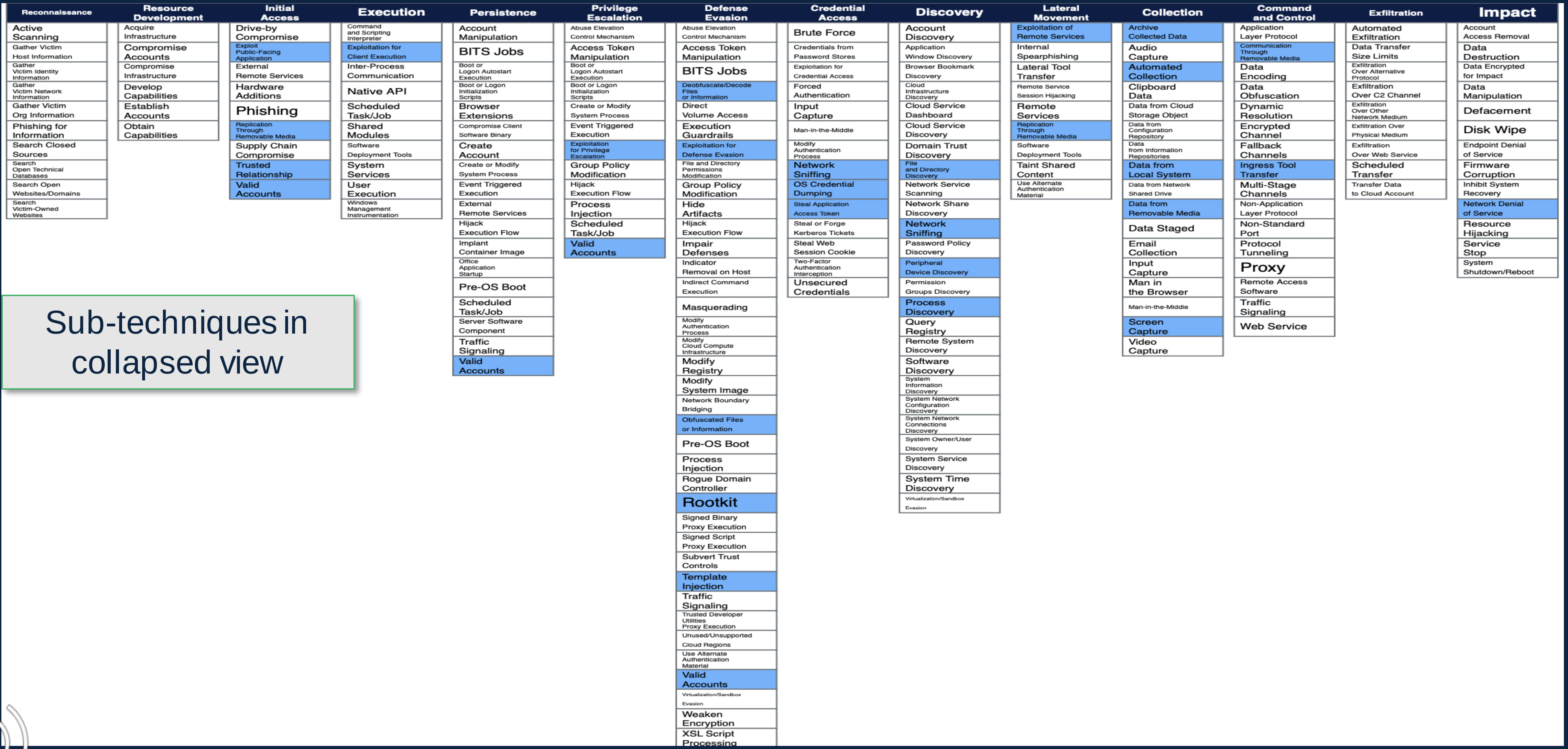
Lesson 3.3
Analyzing ATT&CK®
Mapped Data

Lesson 3.3 Objectives

1. Review the ATT&CK Navigator process for storing, analyzing, visualizing and exporting data in ATT&CK Navigator

2. Learn how to prioritize techniques and sub-techniques to inform actionable intelligence

APT28 Techniques

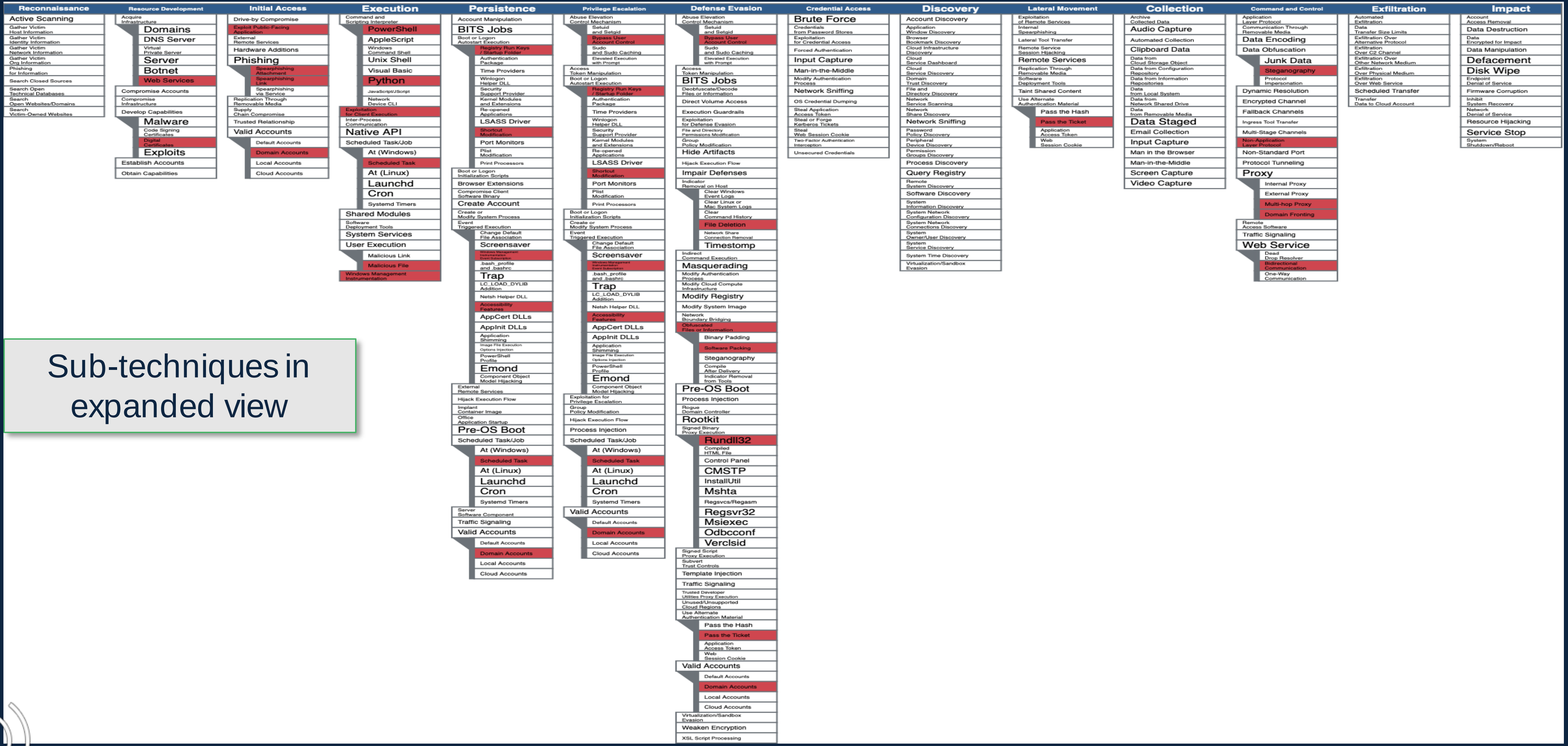


Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts
Gather Victim Org Information	Establish Accounts	Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System Process
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution
Search Closed Sources		Supply Chain Compromise	Software Deployment Tools	Create Account	Exploitation for Privilege Escalation
Search Open Technical Databases		Trusted Relationship	System Services	Create or Modify System Process	Group Policy Modification
Search Open Websites/Domains		Valid Accounts	User Execution	Event Triggered Execution	Hijack Execution Flow
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection
				Hijack Execution Flow	Scheduled Task/Job
				Implant Container Image	Valid Accounts
				Office Application Startup	
				Pre-OS Boot	
				Scheduled Task/Job	
				Server Software Component	
				Traffic Signaling	
				Valid Accounts	

Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Direct Volume Access	Input Capture	Cloud Service Dashboard	Remote Services	Data from Cloud Storage Object	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Execution Guardrails	Man-in-the-Middle	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Exploitation for Defense Evasion	Modify Authentication Process	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
File and Directory Permissions Modification	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Group Policy Modification	OS Credential Dumping	Network Service Scanning	Use Alternate Authentication Material	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Hide Artifacts	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service
Hijack Execution Flow	Steal or Forge Kerberos Tickets	Network Sniffing		Data Staged	Non-Standard Port		Resource Hijacking
Impair Defenses	Steal Web Session Cookie	Password Policy Discovery		Email Collection	Protocol Tunneling		Service Stop
Indicator Removal on Host	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture	Proxy		System Shutdown/Reboot
Indirect Command Execution	Unsecured Credentials	Permission Groups Discovery		Man in the Browser	Remote Access Software		
Masquerading		Process Discovery		Man-in-the-Middle	Traffic Signaling		
Modify Authentication Process		Query Registry		Screen Capture	Web Service		
Modify Cloud Compute Infrastructure		Remote System Discovery		Video Capture			
Modify Registry		Software Discovery					
Modify System Image		System Information Discovery					
Network Boundary Bridging		System Network Configuration Discovery					
Obfuscated Files or Information		System Network Connections Discovery					
Pre-OS Boot		System Owner/User Discovery					
Process Injection		System Service Discovery					
Rogue Domain Controller		System Time Discovery					
Rootkit		Virtualization/Sandbox Evasion					
Signed Binary Proxy Execution							
Signed Script Proxy Execution							
Subvert Trust Controls							
Template Injection							
Traffic Signaling							
Trusted Developer Utilities Proxy Execution							
Unused/Unsupported Cloud Regions							
Use Alternate Authentication Material							
Valid Accounts							
Virtualization/Sandbox Evasion							
Weaken Encryption							
XSL Script Processing							

Sub-techniques in collapsed view

APT29 Techniques & Sub-techniques



Reconnaissance
- Active Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites

Resource Development
- Acquire Infrastructure
  - Domains
  - DNS Server
  - Virtual Private Server
  - Server
  - Botnet
  - Web Services
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
  - Malware
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
- Establish Accounts
- Obtain Capabilities

Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts

Execution
- Command and Scripting Interpreter
  - PowerShell
  - AppleScript
  - Windows Command Shell
  - Unix Shell
  - Visual Basic
  - Python
  - JavaScript/JScript
  - Network Device CLI
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/Job
  - At (Windows)
  - Scheduled Task
  - At (Linux)
  - Launchd
  - Cron
  - Systemd Timers
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
  - Malicious Link
  - Malicious File
- Windows Management Instrumentation

Persistence
- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
  - Registry Run Keys / Startup Folder
  - Authentication Package
  - Time Providers
  - Winlogon Helper DLL
  - Security Support Provider
  - Kernel Modules and Extensions
  - Re-opened Applications
  - LSASS Driver
  - Shortcut Modification
  - Port Monitors
  - Plist Modification
  - Print Processors
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
  - Change Default File Association
  - Screensaver
  - Windows Management Instrumentation Event Subscription
  - .bash_profile and .bashrc
  - Trap
  - LC_LOAD_DYLIB Addition
  - Netsh Helper DLL
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs
  - Application Shimming
  - Image File Execution Options Injection
  - PowerShell Profile
  - Emond
  - Component Object Model Hijacking
- External Remote Services
- Hijack Execution Flow
- Implant Container Image
- Office Application Startup
- Pre-OS Boot
- Scheduled Task/Job
  - At (Windows)
  - Scheduled Task
  - At (Linux)
  - Launchd
  - Cron
  - Systemd Timers
- Server Software Component
- Traffic Signaling
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts

Privilege Escalation
- Abuse Elevation Control Mechanism
  - Setuid and Setgid
  - Bypass User Account Control
  - Sudo and Sudo Caching
  - Elevated Execution with Prompt
- Access Token Manipulation
- Boot or Logon Autostart Execution
  - Registry Run Keys / Startup Folder
  - Authentication Package
  - Time Providers
  - Winlogon Helper DLL
  - Security Support Provider
  - Kernel Modules and Extensions
  - Re-opened Applications
  - LSASS Driver
  - Shortcut Modification
  - Port Monitors
  - Plist Modification
  - Print Processors
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Event Triggered Execution
  - Change Default File Association
  - Screensaver
  - Windows Management Instrumentation Event Subscription
  - .bash_profile and .bashrc
  - Trap
  - LC_LOAD_DYLIB Addition
  - Netsh Helper DLL
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs
  - Application Shimming
  - Image File Execution Options Injection
  - PowerShell Profile
  - Emond
  - Component Object Model Hijacking
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution Flow
- Process Injection
- Scheduled Task/Job
  - At (Windows)
  - Scheduled Task
  - At (Linux)
  - Launchd
  - Cron
  - Systemd Timers
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts

Defense Evasion
- Abuse Elevation Control Mechanism
  - Setuid and Setgid
  - Bypass User Account Control
  - Sudo and Sudo Caching
  - Elevated Execution with Prompt
- Access Token Manipulation
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Group Policy Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses
- Indicator Removal on Host
  - Clear Windows Event Logs
  - Clear Linux or Mac System Logs
  - Clear Command History
  - File Deletion
  - Network Share Connection Removal
  - Timestomp
- Indirect Command Execution
- Masquerading
- Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Modify Registry
- Modify System Image
- Network Boundary Bridging
- Obfuscated Files or Information
  - Binary Padding
  - Software Packing
  - Steganography
  - Compile After Delivery
  - Indicator Removal from Tools
- Pre-OS Boot
- Process Injection
- Rogue Domain Controller
- Rootkit
- Signed Binary Proxy Execution
  - Rundll32
  - Compiled HTML File
  - Control Panel
  - CMSTP
  - InstallUtil
  - Mshta
  - Regsvcs/Regasm
  - Regsvr32
  - Msiexec
  - Odbcconf
  - Verclsid
- Signed Script Proxy Execution
- Subvert Trust Controls
- Template Injection
- Traffic Signaling
- Trusted Developer Utilities Proxy Execution
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
  - Pass the Hash
  - Pass the Ticket
  - Application Access Token
  - Web Session Cookie
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- Virtualization/Sandbox Evasion
- Weaken Encryption
- XSL Script Processing

Credential Access
- Brute Force
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Input Capture
- Man-in-the-Middle
- Modify Authentication Process
- Network Sniffing
- OS Credential Dumping
- Steal Application Access Token
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials

Discovery
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material
  - Pass the Hash
  - Pass the Ticket
  - Application Access Token
  - Web Session Cookie

Collection
- Archive Collected Data
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Man-in-the-Middle
- Screen Capture
- Video Capture

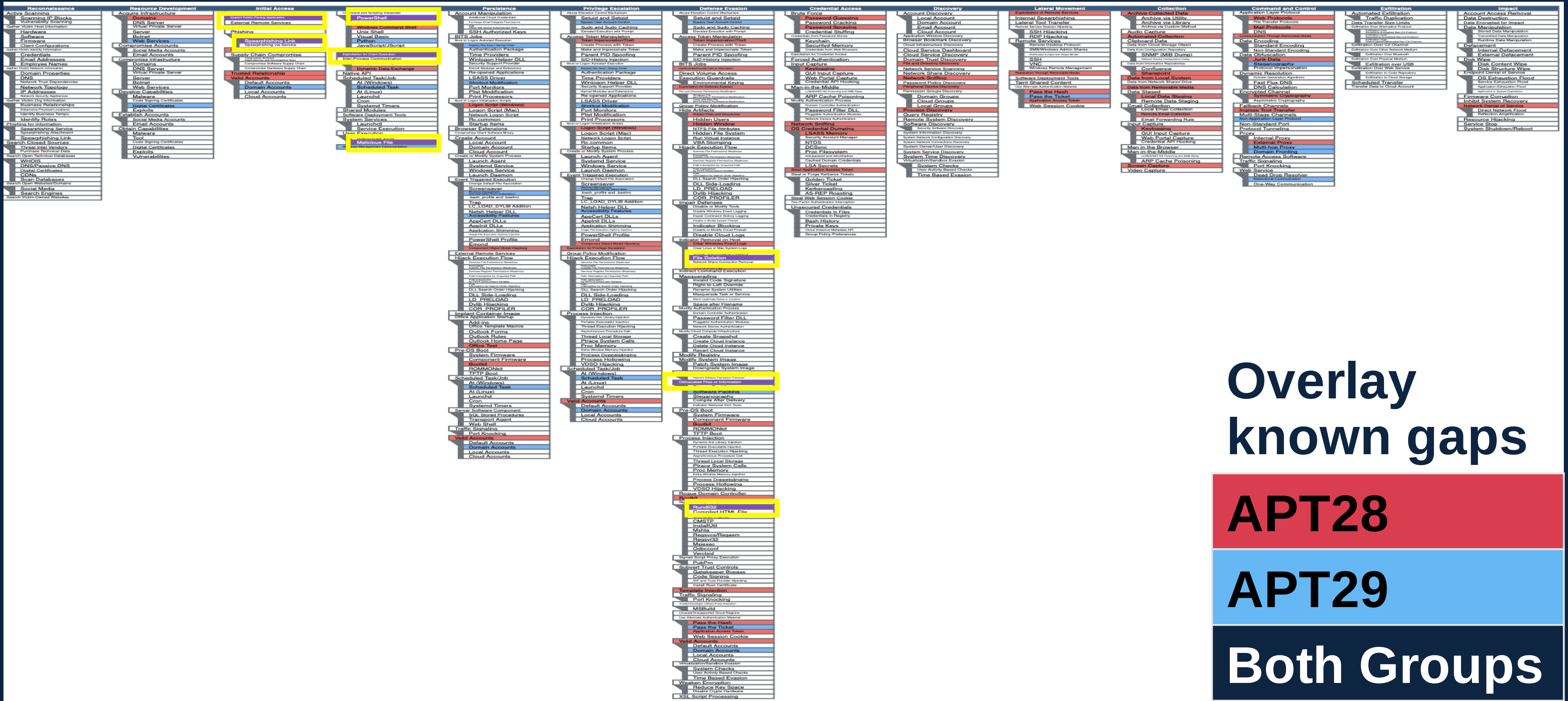
Command and Control
- Application Layer Protocol
- Communication Through Removable Media
- Data Encoding
- Data Obfuscation
  - Junk Data
  - Steganography
  - Protocol Impersonation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
  - Internal Proxy
  - External Proxy
  - Multi-hop Proxy
  - Domain Fronting
- Remote Access Software
- Traffic Signaling
- Web Service
  - Dead Drop Resolver
  - Bidirectional Communication
  - One-Way Communication

Exfiltration
- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- Disk Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Sub-techniques in expanded view

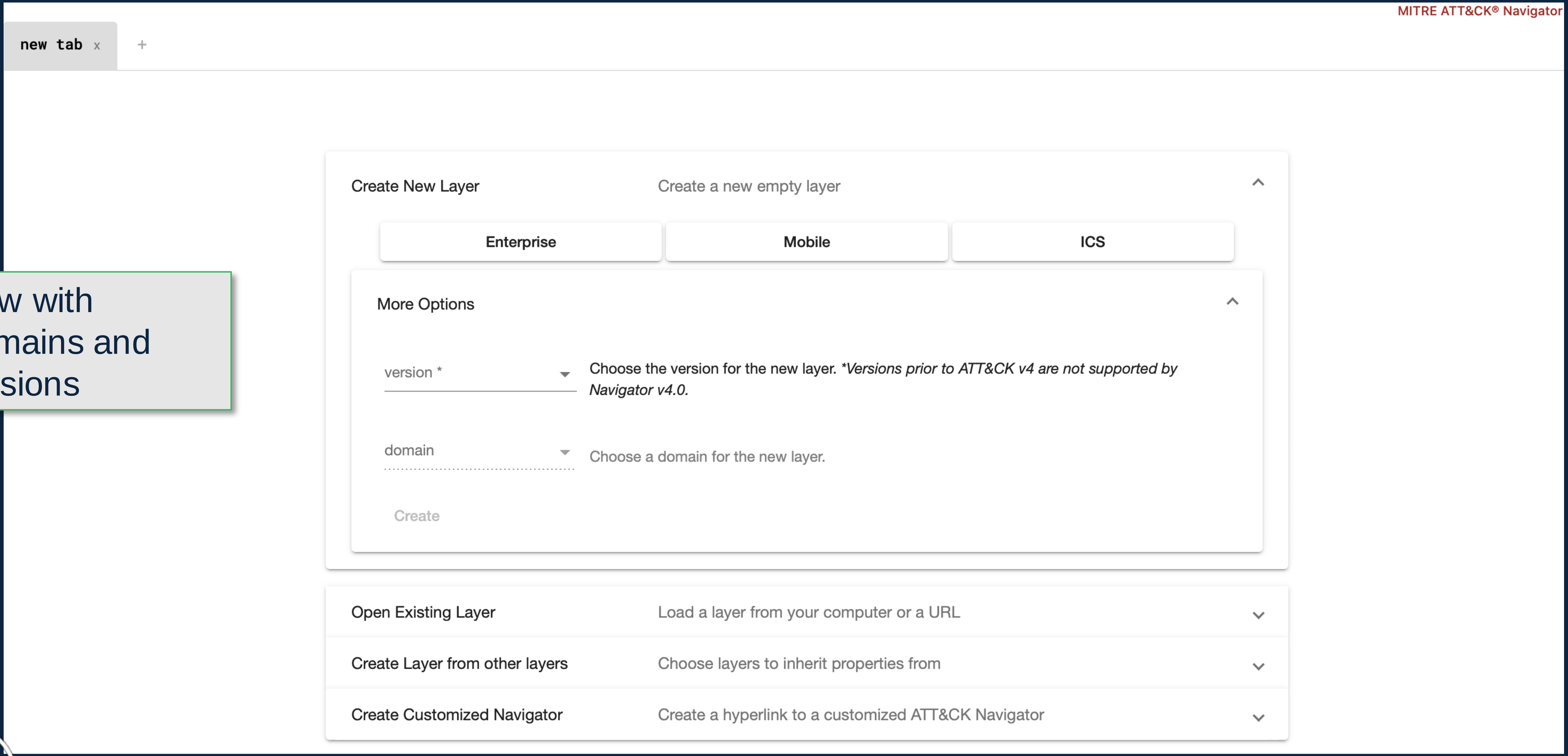
Comparing APT28 and APT29


Reconnaissance
Resource Development
Initial Access
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact

Overlay known gaps

🟥 APT28
🟦 APT29
⬛ Both Groups

Choose Your Layer in Navigator



MITRE ATT&CK® Navigator

new tab x +

Create New Layer — Create a new empty layer

Enterprise | Mobile | ICS

More Options

version * — Choose the version for the new layer. **Versions prior to ATT&CK v4 are not supported by Navigator v4.0.*

domain — Choose a domain for the new layer.

Create

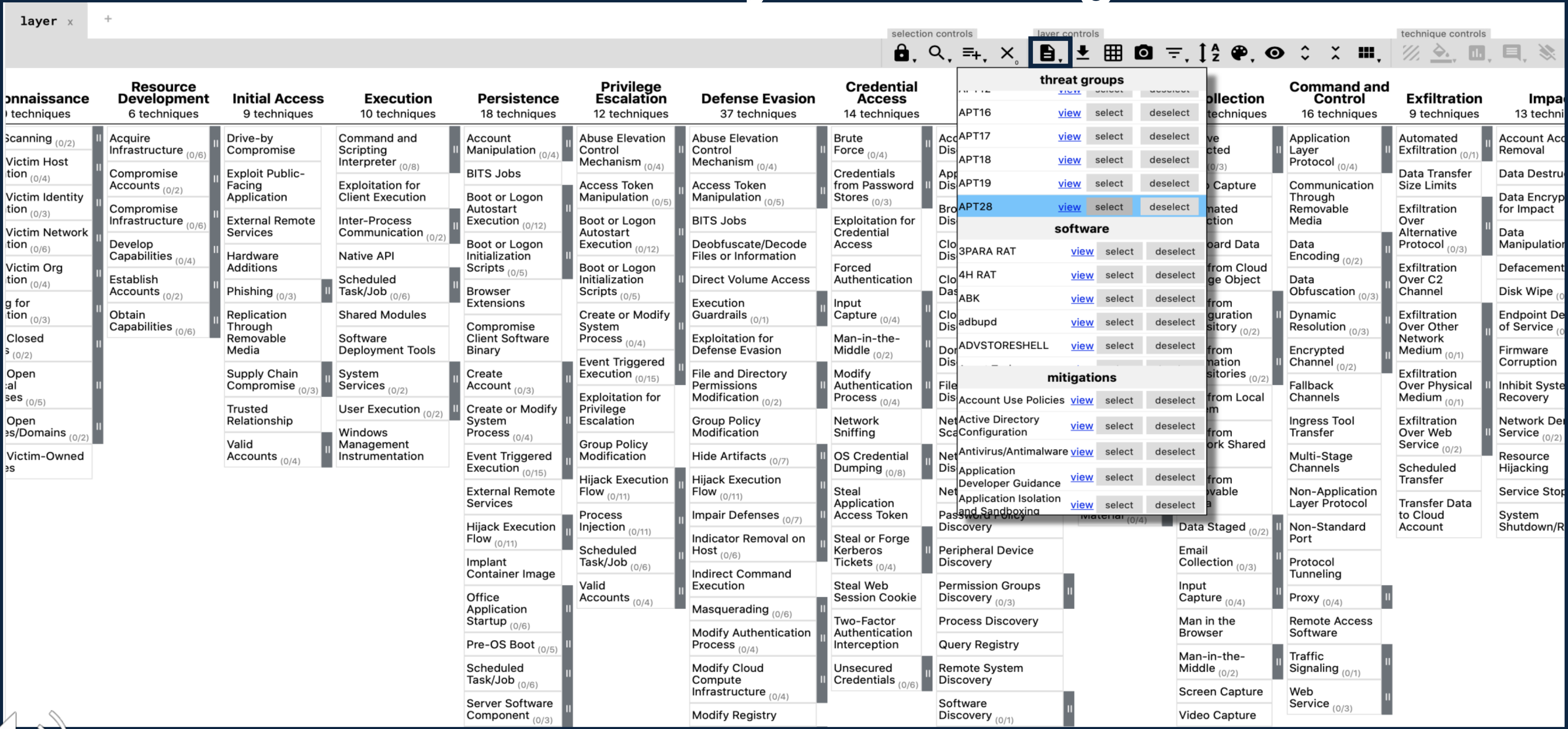
Open Existing Layer — Load a layer from your computer or a URL

Create Layer from other layers — Choose layers to inherit properties from

Create Customized Navigator — Create a hyperlink to a customized ATT&CK Navigator

Now with domains and versions

1. Create an APT28 Layer in Navigator


layer x
+
selection controls
layer controls
technique controls
threat groups
APT16 view select deselect
APT17 view select deselect
APT18 view select deselect
APT19 view select deselect
APT28 view select deselect
software
3PARA RAT view select deselect
4H RAT view select deselect
ABK view select deselect
adbupd view select deselect
ADVSTORESHELL view select deselect
mitigations
Account Use Policies view select deselect
Active Directory Configuration view select deselect
Antivirus/Antimalware view select deselect
Application Developer Guidance view select deselect
Application Isolation and Sandboxing view select deselect

onnaissance
techniques

- Scanning (0/2)
- Victim Host tion (0/4)
- Victim Identity tion (0/3)
- Victim Network tion (0/6)
- Victim Org tion (0/4)
- g for tion (0/3)
- Closed s (0/2)
- Open al ses (0/5)
- Open es/Domains (0/2)
- Victim-Owned es

Resource Development
6 techniques

- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution
10 techniques

- Command and Scripting Interpreter (0/8)
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (0/6)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/2)
- Windows Management Instrumentation

Persistence
18 techniques

- Account Manipulation (0/4)
- BITS Jobs
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- External Remote Services
- Hijack Execution Flow (0/11)
- Implant Container Image
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (0/6)
- Server Software Component (0/3)

Privilege Escalation
12 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution Flow (0/11)
- Process Injection (0/11)
- Scheduled Task/Job (0/6)
- Valid Accounts (0/4)

Defense Evasion
37 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Group Policy Modification
- Hide Artifacts (0/7)
- Hijack Execution Flow (0/11)
- Impair Defenses (0/7)
- Indicator Removal on Host (0/6)
- Indirect Command Execution
- Masquerading (0/6)
- Modify Authentication Process (0/4)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry

Credential Access
14 techniques

- Brute Force (0/4)
- Credentials from Password Stores (0/3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (0/4)
- Man-in-the-Middle (0/2)
- Modify Authentication Process (0/4)
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (0/6)

- Acc Dis
- App Dis
- Bro Dis
- Clo Dis
- Clo Das
- Clo Dis
- Dor Dis
- File Dis
- Net Sca
- Net Dis
- Net
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)

- Material (0/4)

llection
techniques

- ve cted (0/3)
- Capture
- mated ction
- oard Data
- from Cloud ge Object
- from guration sitory (0/2)
- from mation sitories (0/2)
- from Local m
- from ork Shared
- from vable a
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Man in the Browser
- Man-in-the-Middle (0/2)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/1)
- Web Service (0/3)

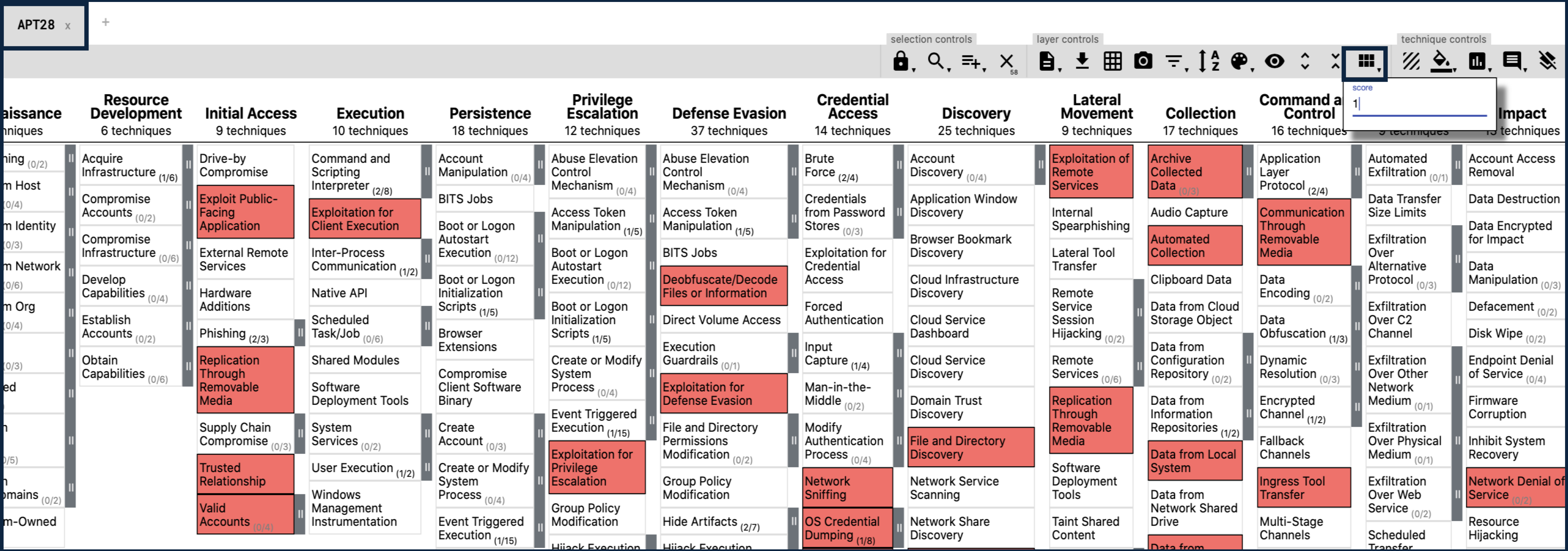
Exfiltration
9 techniques

- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impa
13 techni

- Account Acc Removal
- Data Destru
- Data Encryp for Impact
- Data Manipulation
- Defacement
- Disk Wipe (
- Endpoint De of Service (
- Firmware Corruption
- Inhibit Syste Recovery
- Network De Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/R

2. Assign a Score and Rename the Layer



…aissance
…nniques

- …hing (0/2)
- …m Host (0/4)
- …m Identity (0/3)
- …m Network (0/6)
- …m Org (0/4)
- …(0/3)
- …ed
- …n (0/5)
- …n
- …omains (0/2)
- …m-Owned

Resource Development
6 techniques

- Acquire Infrastructure (1/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution
10 techniques

- Command and Scripting Interpreter (2/8)
- Exploitation for Client Execution
- Inter-Process Communication (1/2)
- Native API
- Scheduled Task/Job (0/6)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (1/2)
- Windows Management Instrumentation

Persistence
18 techniques

- Account Manipulation (0/4)
- BITS Jobs
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (1/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (1/15)

Privilege Escalation
12 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (1/5)
- Create or Modify System Process (0/4)
- Event Triggered Execution (1/15)
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution

Defense Evasion
37 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Group Policy Modification
- Hide Artifacts (2/7)
- Hijack Execution

Credential Access
14 techniques

- Brute Force (2/4)
- Credentials from Password Stores (0/3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (1/4)
- Man-in-the-Middle (0/2)
- Modify Authentication Process (0/4)
- Network Sniffing
- OS Credential Dumping (1/8)

Discovery
25 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content

Collection
17 techniques

- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (1/2)
- Data from Local System
- Data from Network Shared Drive
- Data from

Command a… Control
16 techniques

- Application Layer Protocol (2/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (1/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (1/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels

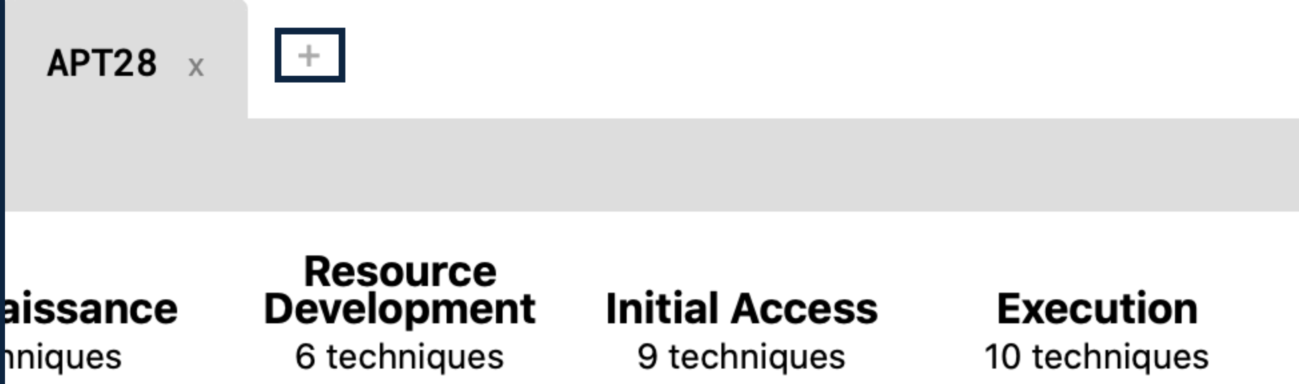
9 techniques

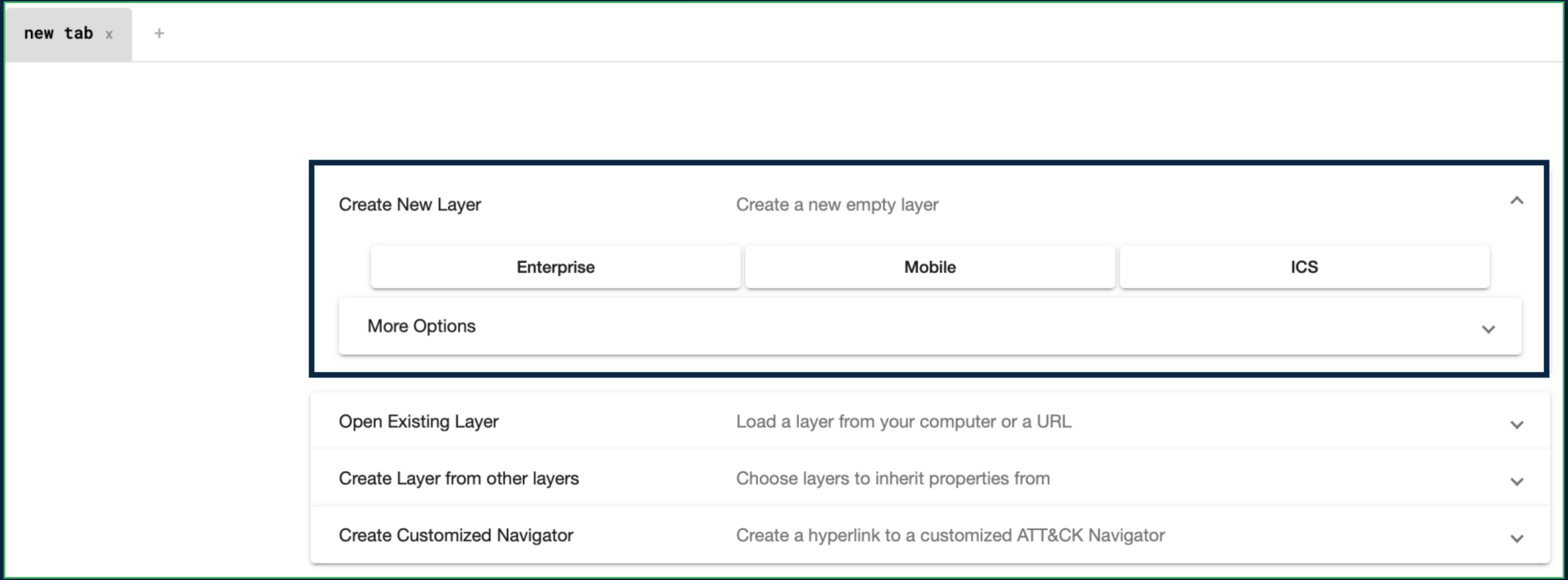
- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking

3. Create a New Layer





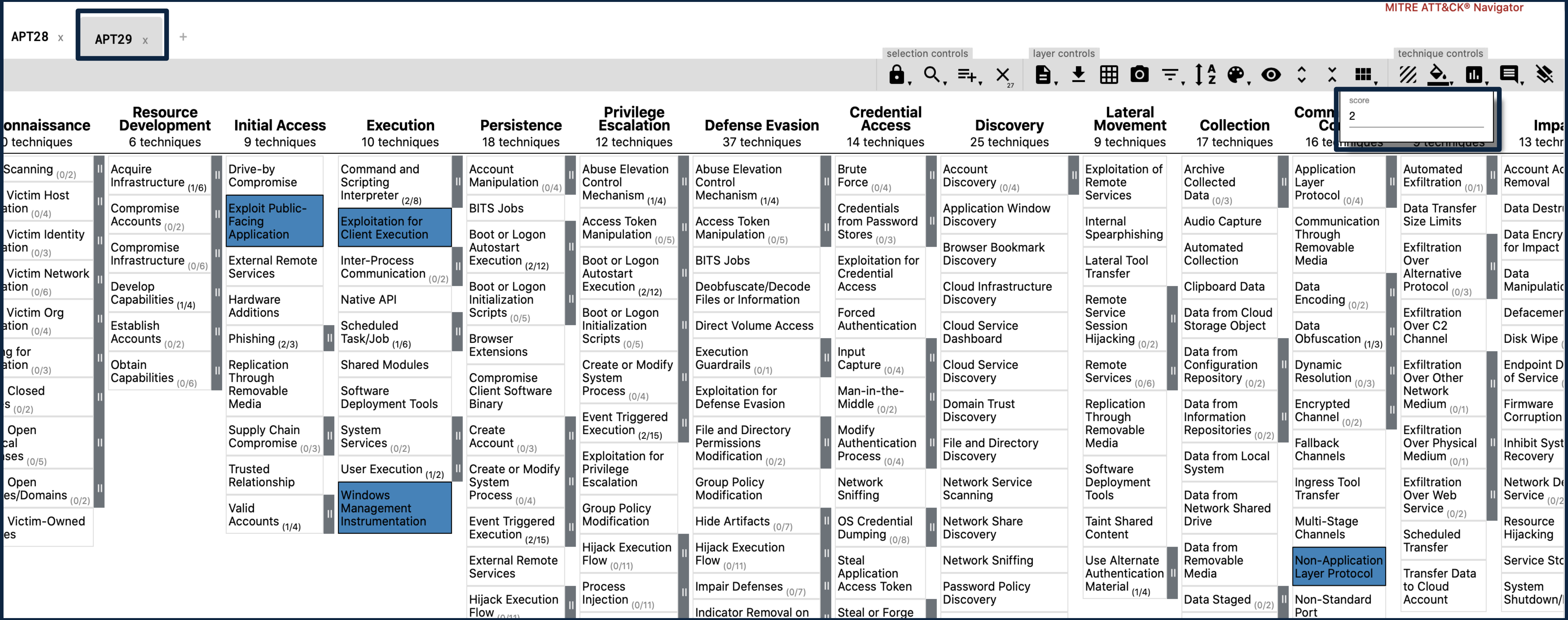
Create New Layer — Create a new empty layer

Open Existing Layer — Load a layer from your computer or a URL

Create Layer from other layers — Choose layers to inherit properties from

Create Customized Navigator — Create a hyperlink to a customized ATT&CK Navigator

4. Repeat the Process but Assign New Score



score
2

onnaissance
0 techniques

- Scanning (0/2)
- Victim Host ation (0/4)
- Victim Identity ation (0/3)
- Victim Network ation (0/6)
- Victim Org ation (0/4)
- g for ation (0/3)
- Closed s (0/2)
- Open cal ses (0/5)
- Open es/Domains (0/2)
- Victim-Owned es

Resource Development
6 techniques

- Acquire Infrastructure (1/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (1/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (1/4)

Execution
10 techniques

- Command and Scripting Interpreter (2/8)
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (1/6)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (1/2)
- Windows Management Instrumentation

Persistence
18 techniques

- Account Manipulation (0/4)
- BITS Jobs
- Boot or Logon Autostart Execution (2/12)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (2/15)
- External Remote Services
- Hijack Execution Flow (0/11)

Privilege Escalation
12 techniques

- Abuse Elevation Control Mechanism (1/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (2/12)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Event Triggered Execution (2/15)
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution Flow (0/11)
- Process Injection (0/11)

Defense Evasion
37 techniques

- Abuse Elevation Control Mechanism (1/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Group Policy Modification
- Hide Artifacts (0/7)
- Hijack Execution Flow (0/11)
- Impair Defenses (0/7)
- Indicator Removal on

Credential Access
14 techniques

- Brute Force (0/4)
- Credentials from Password Stores (0/3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (0/4)
- Man-in-the-Middle (0/2)
- Modify Authentication Process (0/4)
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge

Discovery
25 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (1/4)

Collection
17 techniques

- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/2)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)

Comm Co
16 te

- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (1/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port

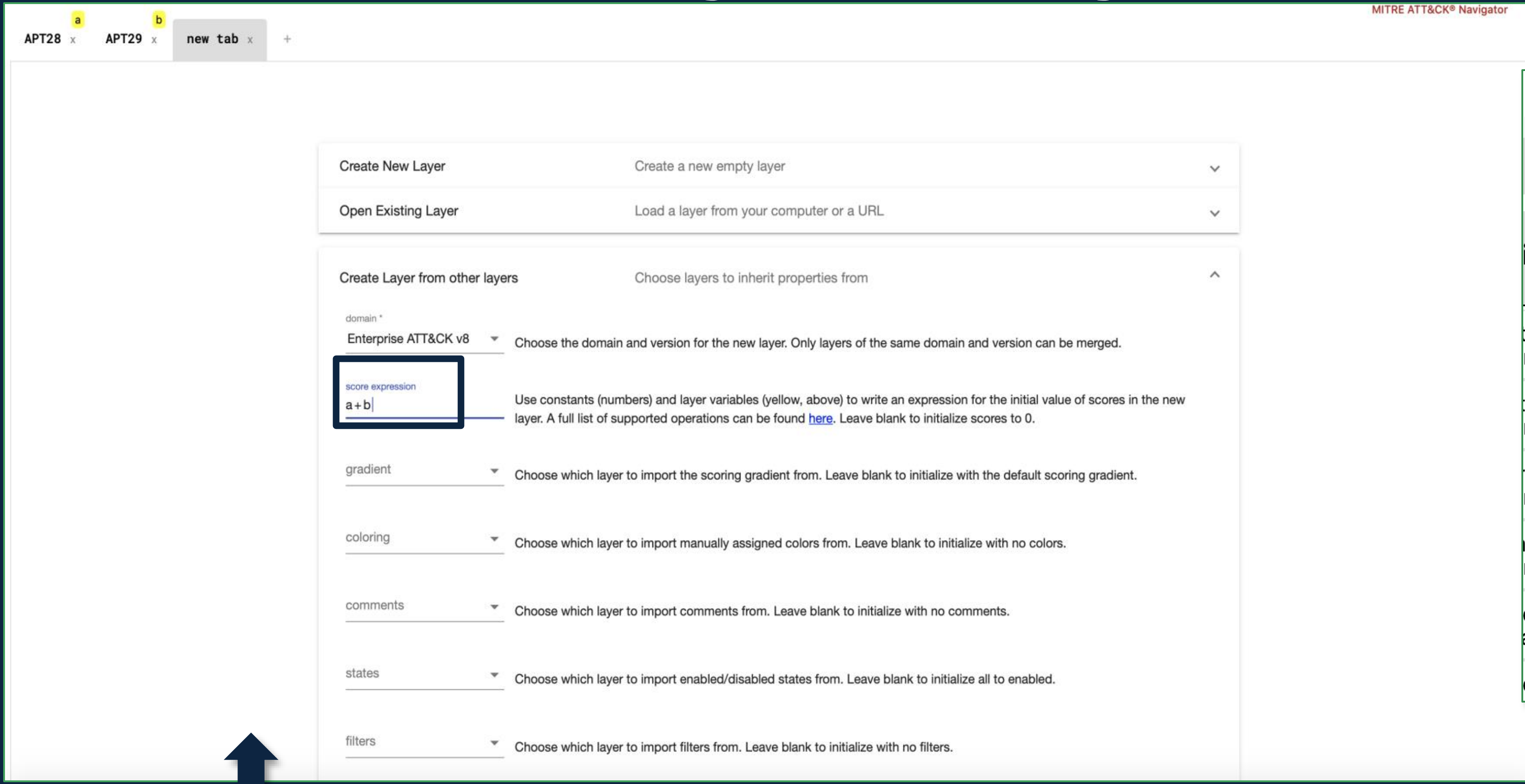
9 techniques

- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impa
13 techn

- Account Ac Removal
- Data Destr
- Data Encry for Impact
- Data Manipulatic
- Defacemer
- Disk Wipe
- Endpoint D of Service
- Firmware Corruption
- Inhibit Syst Recovery
- Network De Service (0/2
- Resource Hijacking
- Service Sto
- System Shutdown/I

5. Combine Layers & Adjust Score Colors



MITRE ATT&CK® Navigator

Create New Layer	Create a new empty layer
Open Existing Layer	Load a layer from your computer or a URL
Create Layer from other layers	Choose layers to inherit properties from

domain * Enterprise ATT&CK v8 — Choose the domain and version for the new layer. Only layers of the same domain and version can be merged.

score expression a+b — Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found here. Leave blank to initialize scores to 0.

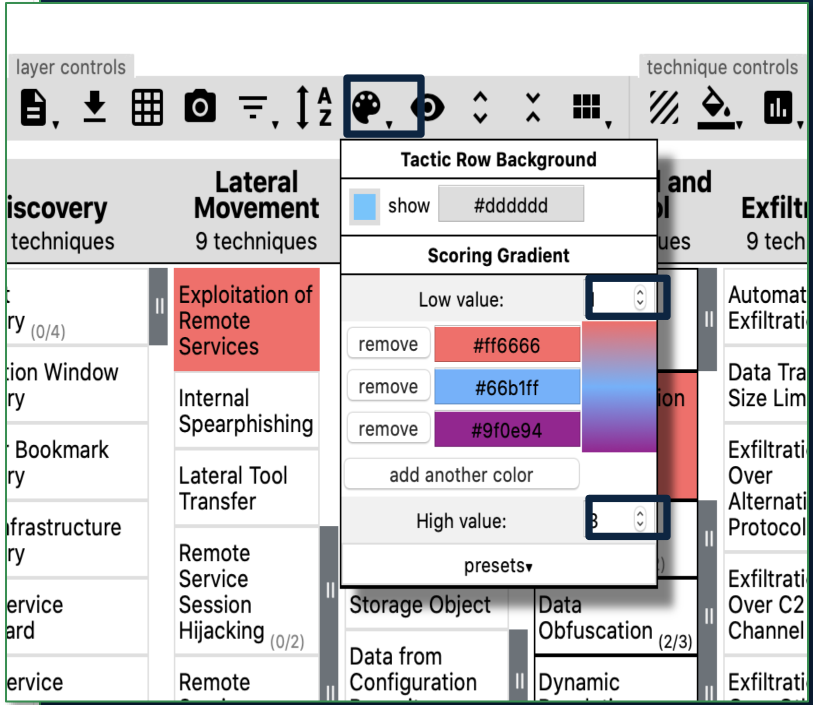
gradient — Choose which layer to import the scoring gradient from. Leave blank to initialize with the default scoring gradient.

coloring — Choose which layer to import manually assigned colors from. Leave blank to initialize with no colors.

comments — Choose which layer to import comments from. Leave blank to initialize with no comments.

states — Choose which layer to import enabled/disabled states from. Leave blank to initialize all to enabled.

filters — Choose which layer to import filters from. Leave blank to initialize with no filters.



Tactic Row Background

show #dddddd

Scoring Gradient

Low value:

remove #ff6666

remove #66b1ff

remove #9f0e94

add another color

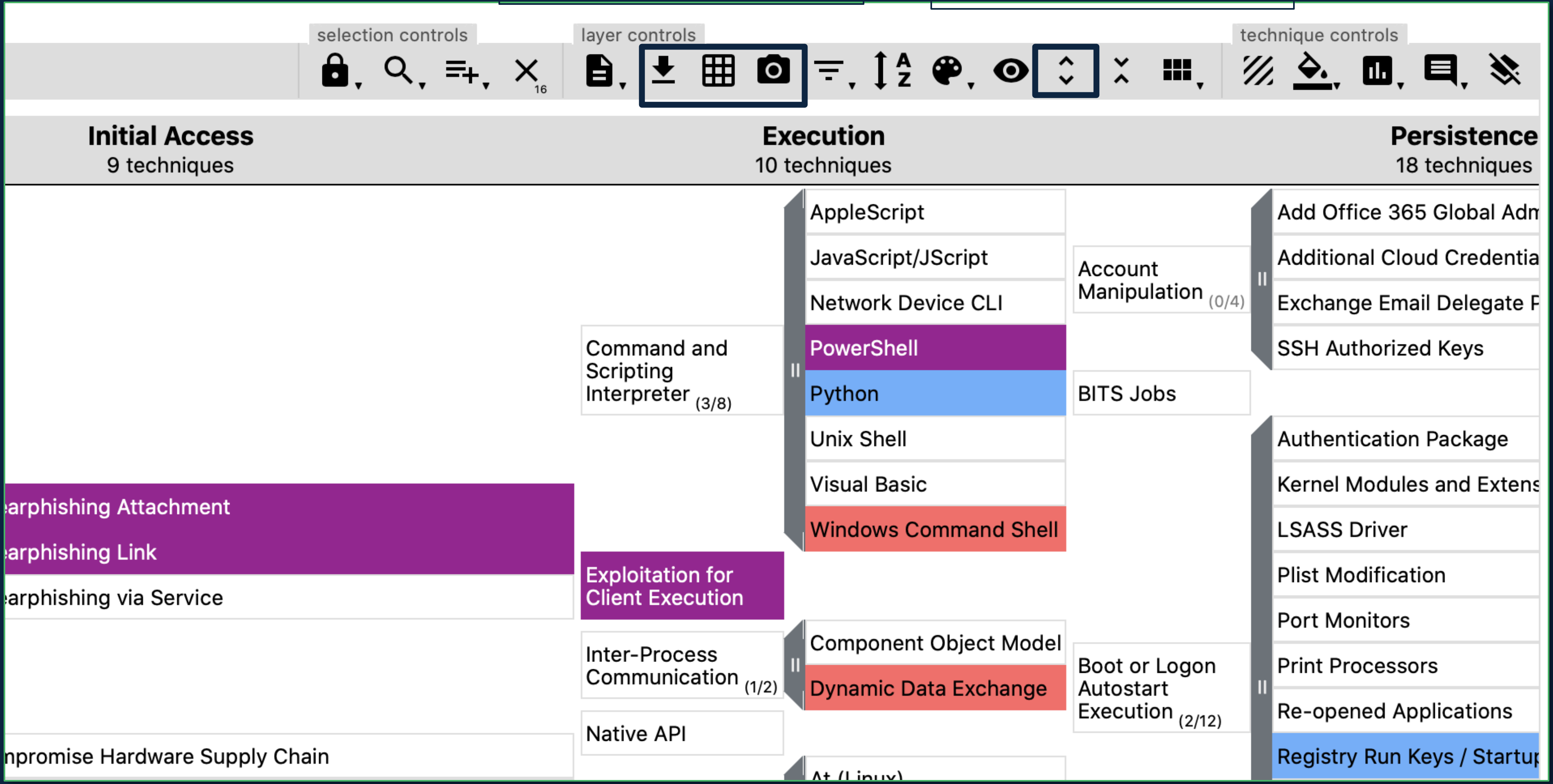
High value: 3

presets▾

“Create Layer from other layers”, combine the scores you have in your two layers (a,b,), and enter the expression “a + b” into the score expression field.

Set low value for 1 and high value (combined techniques) for 3

6. Expand Sub-Techniques & Export/Visualize



Initial Access
9 techniques

Execution
10 techniques

Persistence
18 techniques

earphishing Attachment
earphishing Link
earphishing via Service
npromise Hardware Supply Chain

Command and Scripting Interpreter (3/8)
- AppleScript
- JavaScript/JScript
- Network Device CLI
- PowerShell
- Python
- Unix Shell
- Visual Basic
- Windows Command Shell

Exploitation for Client Execution

Inter-Process Communication (1/2)
- Component Object Model
- Dynamic Data Exchange

Native API

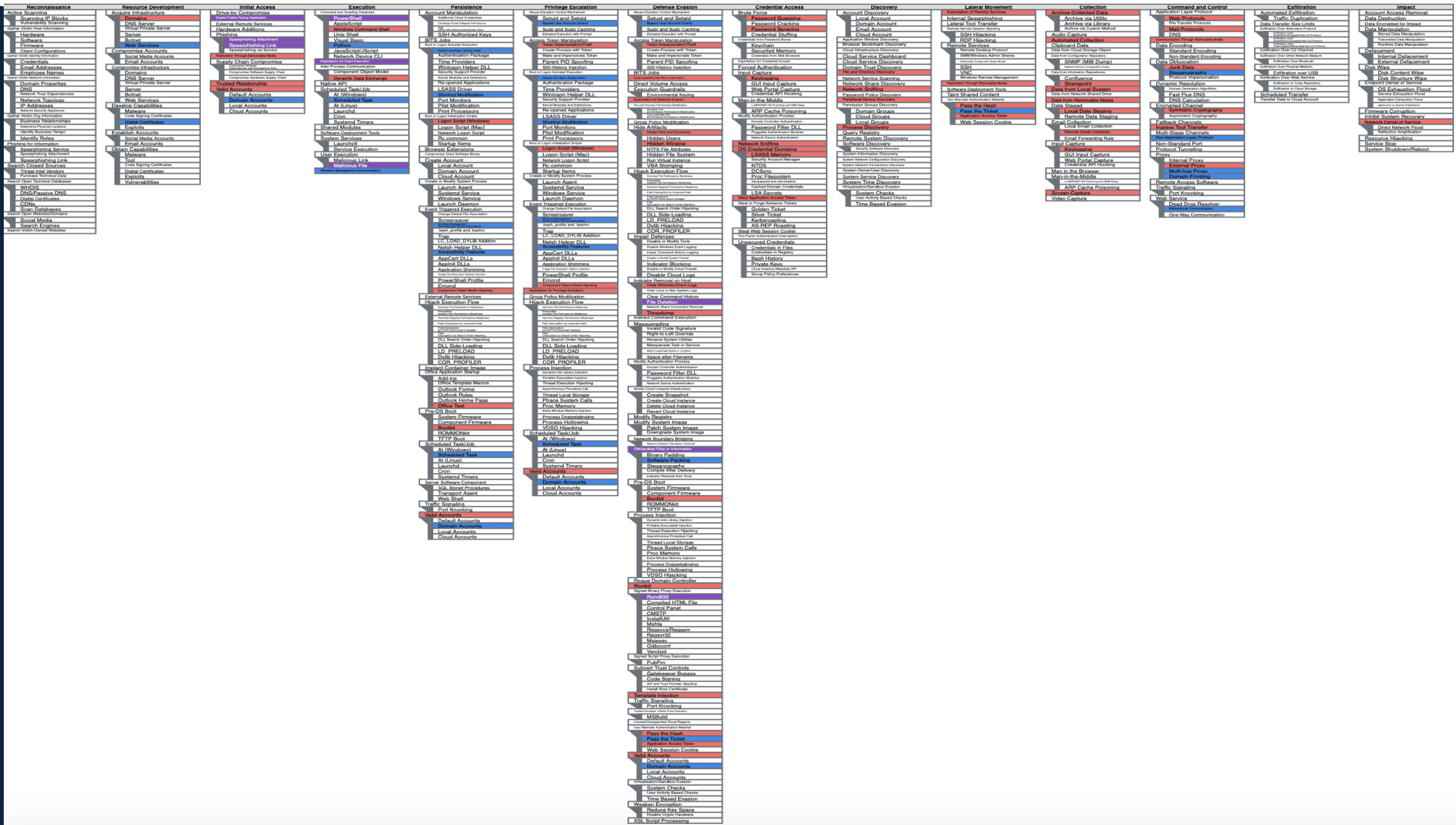
At (Linux)

Account Manipulation (0/4)
- Add Office 365 Global Adm
- Additional Cloud Credentia
- Exchange Email Delegate P
- SSH Authorized Keys

BITS Jobs

Boot or Logon Autostart Execution (2/12)
- Authentication Package
- Kernel Modules and Extens
- LSASS Driver
- Plist Modification
- Port Monitors
- Print Processors
- Re-opened Applications
- Registry Run Keys / Startup

7. Combined Layers Visualized in SVG



Reconnaissance

- Active Scanning
  - Scanning IP Blocks
  - Vulnerability Scanning
- Gather Victim Host Information
  - Hardware
  - Software
  - Firmware
  - Client Configurations
- Gather Victim Identity Information
  - Credentials
  - Email Addresses
  - Employee Names
- Gather Victim Network Information
  - Domain Properties
  - DNS
  - Network Trust Dependencies
  - Network Topology
  - IP Addresses
  - Network Security Appliances
- Gather Victim Org Information
  - Business Relationships
  - Determine Physical Locations
  - Identify Business Tempo
  - Identify Roles
- Phishing for Information
  - Spearphishing Service
  - Spearphishing Attachment
  - Spearphishing Link
- Search Closed Sources
  - Threat Intel Vendors
  - Purchase Technical Data
- Search Open Technical Databases
  - WHOIS
  - DNS/Passive DNS
  - Digital Certificates
  - CDNs
  - Scan Databases
- Search Open Websites/Domains
  - Social Media
  - Search Engines
- Search Victim-Owned Websites

Resource Development

- Acquire Infrastructure
  - Domains
  - DNS Server
  - Virtual Private Server
  - Server
  - Botnet
  - Web Services
- Compromise Accounts
  - Social Media Accounts
  - Email Accounts
- Compromise Infrastructure
  - Domains
  - DNS Server
  - Virtual Private Server
  - Server
  - Botnet
  - Web Services
- Develop Capabilities
  - Malware
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
- Establish Accounts
  - Social Media Accounts
  - Email Accounts
- Obtain Capabilities
  - Malware
  - Tool
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Vulnerabilities

Initial Access

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise
  - Compromise Software Dependencies and Development Tools
  - Compromise Software Supply Chain
  - Compromise Hardware Supply Chain
- Trusted Relationship
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts

Execution

- Command and Scripting Interpreter
  - PowerShell
  - AppleScript
  - Windows Command Shell
  - Unix Shell
  - Visual Basic
  - Python
  - JavaScript/JScript
  - Network Device CLI
- Exploitation for Client Execution
- Inter-Process Communication
  - Component Object Model
  - Dynamic Data Exchange
- Native API
- Scheduled Task/Job
  - At (Windows)
  - Scheduled Task
  - At (Linux)
  - Launchd
  - Cron
  - Systemd Timers
- Shared Modules
- Software Deployment Tools
- System Services
  - Launchctl
  - Service Execution
- User Execution
  - Malicious Link
  - Malicious File
- Windows Management Instrumentation

Persistence

- Account Manipulation
  - Additional Cloud Credentials
  - Exchange Email Delegate Permissions
  - Add Office 365 Global Administrator Role
  - SSH Authorized Keys
- BITS Jobs
- Boot or Logon Autostart Execution
  - Registry Run Keys / Startup Folder
  - Authentication Package
  - Time Providers
  - Winlogon Helper DLL
  - Security Support Provider
  - Kernel Modules and Extensions
  - Re-opened Applications
  - LSASS Driver
  - Shortcut Modification
  - Port Monitors
  - Plist Modification
  - Print Processors
- Boot or Logon Initialization Scripts
  - Logon Script (Windows)
  - Logon Script (Mac)
  - Network Logon Script
  - Rc.common
  - Startup Items
- Browser Extensions
- Compromise Client Software Binary
- Create Account
  - Local Account
  - Domain Account
  - Cloud Account
- Create or Modify System Process
  - Launch Agent
  - Systemd Service
  - Windows Service
  - Launch Daemon
- Event Triggered Execution
  - Change Default File Association
  - Screensaver
  - Windows Management Instrumentation Event Subscription
  - .bash_profile and .bashrc
  - Trap
  - LC_LOAD_DYLIB Addition
  - Netsh Helper DLL
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs
  - Application Shimming
  - Image File Execution Options Injection
  - PowerShell Profile
  - Emond
  - Component Object Model Hijacking
- External Remote Services
- Hijack Execution Flow
  - Services File Permissions Weakness
  - Executable Installer File Permissions Weakness
  - Services Registry Permissions Weakness
  - Path Interception by Unquoted Path
  - Path Interception by PATH Environment Variable
  - Path Interception by Search Order Hijacking
  - DLL Search Order Hijacking
  - DLL Side-Loading
  - LD_PRELOAD
  - Dylib Hijacking
  - COR_PROFILER
- Implant Container Image
- Office Application Startup
  - Add-ins
  - Office Template Macros
  - Outlook Forms
  - Outlook Rules
  - Outlook Home Page
  - Office Test
- Pre-OS Boot
  - System Firmware
  - Component Firmware
  - Bootkit
  - ROMMONkit
  - TFTP Boot
- Scheduled Task/Job
  - At (Windows)
  - Scheduled Task
  - At (Linux)
  - Launchd
  - Cron
  - Systemd Timers
- Server Software Component
  - SQL Stored Procedures
  - Transport Agent
  - Web Shell
- Traffic Signaling
  - Port Knocking
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts

Privilege Escalation

- Abuse Elevation Control Mechanism
  - Setuid and Setgid
  - Bypass User Account Control
  - Sudo and Sudo Caching
  - Elevated Execution with Prompt
- Access Token Manipulation
  - Token Impersonation/Theft
  - Create Process with Token
  - Make and Impersonate Token
  - Parent PID Spoofing
  - SID-History Injection
- Boot or Logon Autostart Execution
  - Registry Run Keys / Startup Folder
  - Authentication Package
  - Time Providers
  - Winlogon Helper DLL
  - Security Support Provider
  - Kernel Modules and Extensions
  - Re-opened Applications
  - LSASS Driver
  - Shortcut Modification
  - Port Monitors
  - Plist Modification
  - Print Processors
- Boot or Logon Initialization Scripts
  - Logon Script (Windows)
  - Logon Script (Mac)
  - Network Logon Script
  - Rc.common
  - Startup Items
- Create or Modify System Process
  - Launch Agent
  - Systemd Service
  - Windows Service
  - Launch Daemon
- Event Triggered Execution
  - Change Default File Association
  - Screensaver
  - Windows Management Instrumentation Event Subscription
  - .bash_profile and .bashrc
  - Trap
  - LC_LOAD_DYLIB Addition
  - Netsh Helper DLL
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs
  - Application Shimming
  - Image File Execution Options Injection
  - PowerShell Profile
  - Emond
  - Component Object Model Hijacking
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution Flow
  - Services File Permissions Weakness
  - Executable Installer File Permissions Weakness
  - Services Registry Permissions Weakness
  - Path Interception by Unquoted Path
  - Path Interception by PATH Environment Variable
  - Path Interception by Search Order Hijacking
  - DLL Search Order Hijacking
  - DLL Side-Loading
  - LD_PRELOAD
  - Dylib Hijacking
  - COR_PROFILER
- Process Injection
  - Dynamic-link Library Injection
  - Portable Executable Injection
  - Thread Execution Hijacking
  - Asynchronous Procedure Call
  - Thread Local Storage
  - Ptrace System Calls
  - Proc Memory
  - Extra Window Memory Injection
  - Process Doppelgänging
  - Process Hollowing
  - VDSO Hijacking
- Scheduled Task/Job
  - At (Windows)
  - Scheduled Task
  - At (Linux)
  - Launchd
  - Cron
  - Systemd Timers
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts

Defense Evasion

- Abuse Elevation Control Mechanism
  - Setuid and Setgid
  - Bypass User Account Control
  - Sudo and Sudo Caching
  - Elevated Execution with Prompt
- Access Token Manipulation
  - Token Impersonation/Theft
  - Create Process with Token
  - Make and Impersonate Token
  - Parent PID Spoofing
  - SID-History Injection
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails
  - Environmental Keying
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
  - Windows File and Directory Permissions Modification
  - Linux and Mac File and Directory Permissions Modification
- Group Policy Modification
- Hide Artifacts
  - Hidden Files and Directories
  - Hidden Users
  - Hidden Window
  - NTFS File Attributes
  - Hidden File System
  - Run Virtual Instance
  - VBA Stomping
- Hijack Execution Flow
  - Services File Permissions Weakness
  - Executable Installer File Permissions Weakness
  - Services Registry Permissions Weakness
  - Path Interception by Unquoted Path
  - Path Interception by PATH Environment Variable
  - Path Interception by Search Order Hijacking
  - DLL Search Order Hijacking
  - DLL Side-Loading
  - LD_PRELOAD
  - Dylib Hijacking
  - COR_PROFILER
- Impair Defenses
  - Disable or Modify Tools
  - Disable Windows Event Logging
  - Impair Command History Logging
  - Disable or Modify System Firewall
  - Indicator Blocking
  - Disable or Modify Cloud Firewall
  - Disable Cloud Logs
- Indicator Removal on Host
  - Clear Windows Event Logs
  - Clear Linux or Mac System Logs
  - Clear Command History
  - File Deletion
  - Network Share Connection Removal
  - Timestomp
- Indirect Command Execution
- Masquerading
  - Invalid Code Signature
  - Right-to-Left Override
  - Rename System Utilities
  - Masquerade Task or Service
  - Match Legitimate Name or Location
  - Space after Filename
- Modify Authentication Process
  - Domain Controller Authentication
  - Password Filter DLL
  - Pluggable Authentication Modules
  - Network Device Authentication
- Modify Cloud Compute Infrastructure
  - Create Snapshot
  - Create Cloud Instance
  - Delete Cloud Instance
  - Revert Cloud Instance
- Modify Registry
- Modify System Image
  - Patch System Image
  - Downgrade System Image
- Network Boundary Bridging
  - Network Address Translation Traversal
- Obfuscated Files or Information
  - Binary Padding
  - Software Packing
  - Steganography
  - Compile After Delivery
  - Indicator Removal from Tools
- Pre-OS Boot
  - System Firmware
  - Component Firmware
  - Bootkit
  - ROMMONkit
  - TFTP Boot
- Process Injection
  - Dynamic-link Library Injection
  - Portable Executable Injection
  - Thread Execution Hijacking
  - Asynchronous Procedure Call
  - Thread Local Storage
  - Ptrace System Calls
  - Proc Memory
  - Extra Window Memory Injection
  - Process Doppelgänging
  - Process Hollowing
  - VDSO Hijacking
- Rogue Domain Controller
- Rootkit
- Signed Binary Proxy Execution
  - Rundll32
  - Compiled HTML File
  - Control Panel
  - CMSTP
  - InstallUtil
  - Mshta
  - Regsvcs/Regasm
  - Regsvr32
  - Msiexec
  - Odbcconf
  - Verclsid
- Signed Script Proxy Execution
  - PubPrn
- Subvert Trust Controls
  - Gatekeeper Bypass
  - Code Signing
  - SIP and Trust Provider Hijacking
  - Install Root Certificate
- Template Injection
- Traffic Signaling
  - Port Knocking
- Trusted Developer Utilities Proxy Execution
  - MSBuild
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
  - Pass the Hash
  - Pass the Ticket
  - Application Access Token
  - Web Session Cookie
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- Virtualization/Sandbox Evasion
  - System Checks
  - User Activity Based Checks
  - Time Based Evasion
- Weaken Encryption
  - Reduce Key Space
  - Disable Crypto Hardware
- XSL Script Processing

Credential Access

- Brute Force
  - Password Guessing
  - Password Cracking
  - Password Spraying
  - Credential Stuffing
- Credentials from Password Stores
  - Keychain
  - Securityd Memory
  - Credentials from Web Browsers
- Exploitation for Credential Access
- Forced Authentication
- Input Capture
  - Keylogging
  - GUI Input Capture
  - Web Portal Capture
  - Credential API Hooking
- Man-in-the-Middle
  - LLMNR/NBT-NS Poisoning and SMB Relay
  - ARP Cache Poisoning
- Modify Authentication Process
  - Domain Controller Authentication
  - Password Filter DLL
  - Pluggable Authentication Modules
  - Network Device Authentication
- Network Sniffing
- OS Credential Dumping
  - LSASS Memory
  - Security Account Manager
  - NTDS
  - DCSync
  - Proc Filesystem
  - /etc/passwd and /etc/shadow
  - Cached Domain Credentials
  - LSA Secrets
- Steal Application Access Token
- Steal or Forge Kerberos Tickets
  - Golden Ticket
  - Silver Ticket
  - Kerberoasting
  - AS-REP Roasting
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials
  - Credentials In Files
  - Credentials in Registry
  - Bash History
  - Private Keys
  - Cloud Instance Metadata API
  - Group Policy Preferences

Discovery

- Account Discovery
  - Local Account
  - Domain Account
  - Email Account
  - Cloud Account
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
  - Domain Groups
  - Cloud Groups
  - Local Groups
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
  - Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion
  - System Checks
  - User Activity Based Checks
  - Time Based Evasion

Lateral Movement

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
  - SSH Hijacking
  - RDP Hijacking
- Remote Services
  - Remote Desktop Protocol
  - SMB/Windows Admin Shares
  - Distributed Component Object Model
  - SSH
  - VNC
  - Windows Remote Management
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material
  - Pass the Hash
  - Pass the Ticket
  - Application Access Token
  - Web Session Cookie

Collection

- Archive Collected Data
  - Archive via Utility
  - Archive via Library
  - Archive via Custom Method
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository
  - SNMP (MIB Dump)
  - Network Device Configuration Dump
- Data from Information Repositories
  - Confluence
  - Sharepoint
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
  - Local Data Staging
  - Remote Data Staging
- Email Collection
  - Local Email Collection
  - Remote Email Collection
  - Email Forwarding Rule
- Input Capture
  - Keylogging
  - GUI Input Capture
  - Web Portal Capture
  - Credential API Hooking
- Man in the Browser
- Man-in-the-Middle
  - LLMNR/NBT-NS Poisoning and SMB Relay
  - ARP Cache Poisoning
- Screen Capture
- Video Capture

Command and Control

- Application Layer Protocol
  - Web Protocols
  - File Transfer Protocols
  - Mail Protocols
  - DNS
- Communication Through Removable Media
- Data Encoding
  - Standard Encoding
  - Non-Standard Encoding
- Data Obfuscation
  - Junk Data
  - Steganography
  - Protocol Impersonation
- Dynamic Resolution
  - Domain Generation Algorithms
  - Fast Flux DNS
  - DNS Calculation
- Encrypted Channel
  - Symmetric Cryptography
  - Asymmetric Cryptography
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
  - Internal Proxy
  - External Proxy
  - Multi-hop Proxy
  - Domain Fronting
- Remote Access Software
- Traffic Signaling
  - Port Knocking
- Web Service
  - Dead Drop Resolver
  - Bidirectional Communication
  - One-Way Communication

Exfiltration

- Automated Exfiltration
  - Traffic Duplication
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
  - Exfiltration Over Symmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium
  - Exfiltration Over Bluetooth
- Exfiltration Over Physical Medium
  - Exfiltration over USB
- Exfiltration Over Web Service
  - Exfiltration to Code Repository
  - Exfiltration to Cloud Storage
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
  - Stored Data Manipulation
  - Transmitted Data Manipulation
  - Runtime Data Manipulation
- Defacement
  - Internal Defacement
  - External Defacement
- Disk Wipe
  - Disk Content Wipe
  - Disk Structure Wipe
- Endpoint Denial of Service
  - OS Exhaustion Flood
  - Service Exhaustion Flood
  - Application Exhaustion Flood
  - Application or System Exploitation
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
  - Direct Network Flood
  - Reflection Amplification
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Lesson 3.3 Summary

1 Learned how to map multiple threat groups in ATT&CK Navigator to enable analysis and identification of overlapping techniques/sub-techniques.

2 Examined how to prioritize techniques and sub-techniques for actionable intelligence

Lesson 3.4
Exercise 3:
Comparing Layers in ATT&CK® Navigator

Lesson 3.4 Objectives

1. Practice defining and comparing layers in Navigator

2. Review the overlapping techniques and sub-techniques

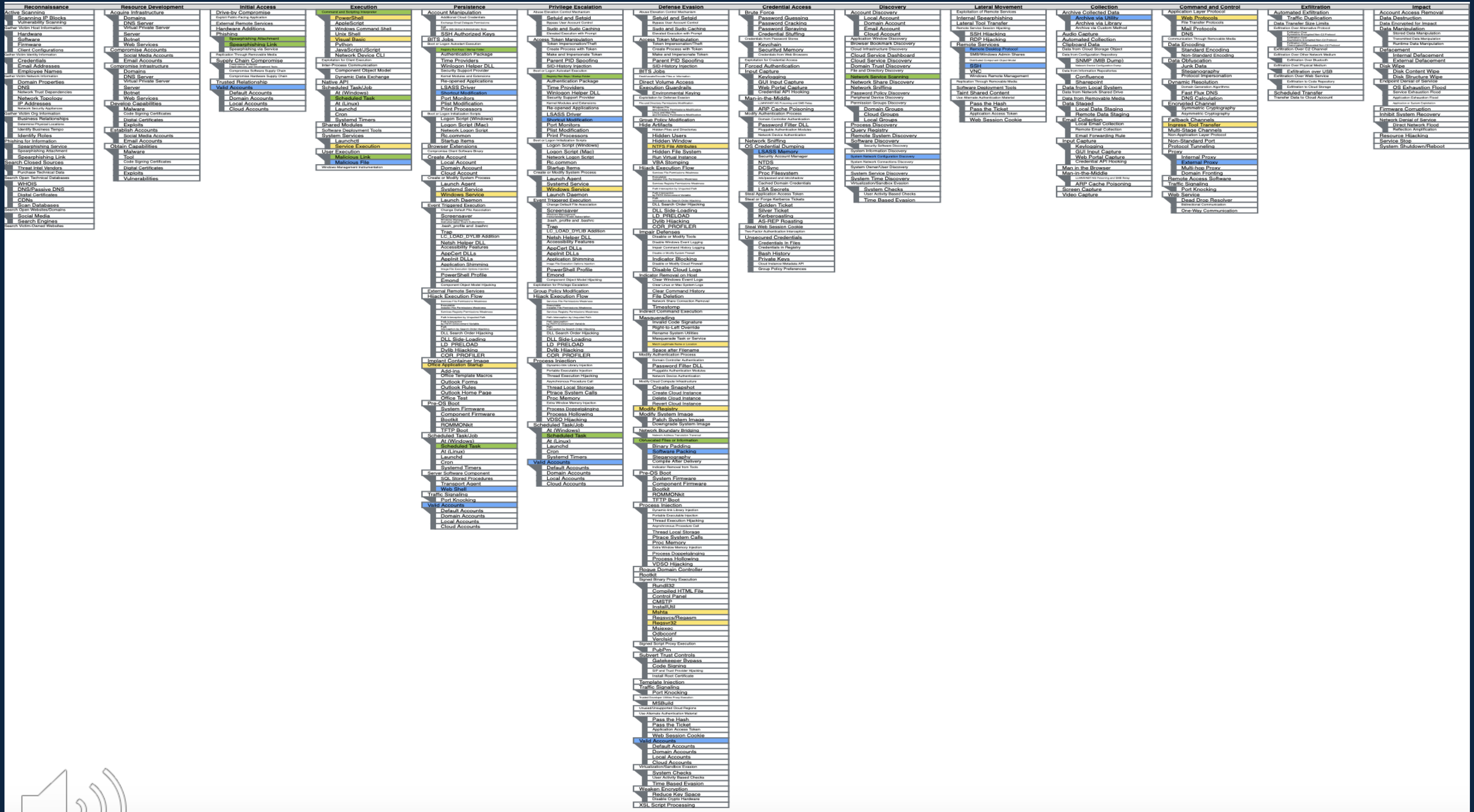
Exercise 3: Comparing Layers in Navigator

- Refer to the Resources section for Exercise 3
  - The techniques and sub-techniques are listed in the “APT39 and Cobalt Kitty Techniques” PDF

1. Open ATT&CK Navigator: http://bit.ly/attacknav
2. Enter the techniques and sub-techniques from APT39 and Cobalt Kitty/OceanLotus into separate Navigator layers with a unique score for each layer.
3. Combine the layers in Navigator to create a third layer
4. Color score your third layer
5. Make a list of the techniques and sub-techniques that overlap between the two groups

- Please pause. We suggest giving yourself 15 minutes for this exercise.

Exercise 3: Comparing Layers in Navigator



APT39 Techniques/Subs

APT32 (OceanLotus) Techniques/Subs

Overlapping Techniques/Subs that both groups employ

Exercise 3: Comparing Layers in Navigator

- What are some of the overlapping techniques and sub-techniques you identified?

Exercise 3: Comparing Layers in ATT&CK Navigator

Here are the overlapping techniques between APT39 and APT32:

- Phishing:Spearphishing Attachment (T1566.001)
- Phishing: Spearphishing Link (T1566.002)
- Command and Scripting Interpreter (T1059)
- Scheduled Task/Job:Scheduled Task (T1053.005)
- User Execution: Malicious Link(T1204.001)
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
- Obfuscated Files or Information (T1027)
- Network Service Scanning (T1046)

Lesson 3.4 Summary

1. Worked through defining and comparing layers in Navigator process and identified the overlapping techniques and sub-techniques

2. Reviewed the APT32 and APT39 intersecting outcomes

Next Up:

Module 4:
Making Defensive Recommendations from ATT&CK® Mapped Data

End of Module 3