Comparing Layers in ATT&CK Navigator

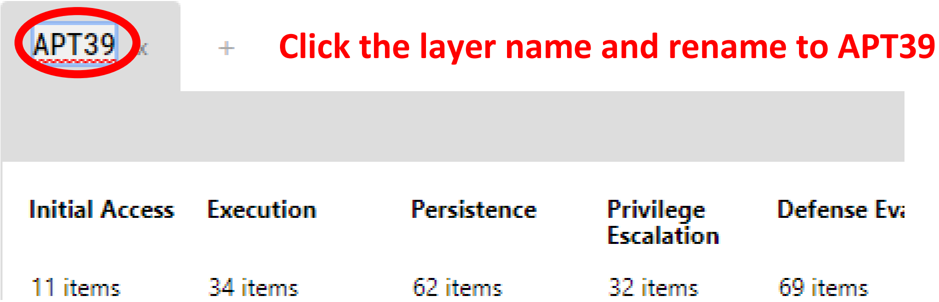
This document provides a walkthrough of how to use the ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/enterprise/) to compare two different layers. (Navigator source code is available at https://github.com/mitre-attack/attack-navigator). This comparison method is useful if you want to compare techniques used by two different groups, but could be applied in many ways – to compare a group to your defensive coverage, your defensive coverage from one week to the next…whatever you want to do!

For this Exercise, you'll compare APT39 techniques to OceanLotus techniques to build upon the previous exercises in the ATT&CK for CTI training. (OceanLotus is the group identified as being behind the Cobalt Kitty campaign according to Cybereason.) To do this, you will:

1. Create a layer and assign a score to techniques used by APT39 in one layer
2. Create a second layer and assign a different score to techniques used by OceanLotus
3. Combine the two using "Create Layer from other layers" using the expression "a + b"
4. Export the layer in the format of your choice

1. Create an APT39 layer and assign a score to techniques used by APT39

Go to the ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/enterprise/). By default, Navigator will start with a new layer called "layer," so you'll work with that. To help keep yourself organized, you will rename the layer to "APT39" by clicking on the name at the top.

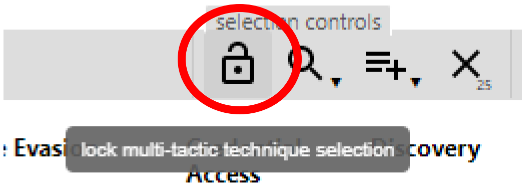


First, you will manually select the 17 techniques used by APT39 from this list (you may find it helpful to print this list or bring it up on a second screen as you select the techniques):

1. Initial Access – Spearphishing Attachment (T1193)
2. Initial Access – Spearphishing Link (T1192)
3. Initial Access – Valid Accounts (T1078)
4. Execution – Scripting (T1064)
5. Execution – User Execution (T1204)
6. Persistence – Scheduled Task (T1053)

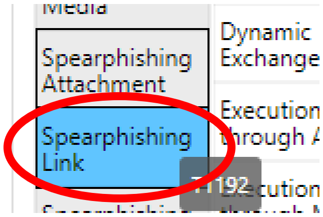
7. Persistence – Shortcut Modification (T1023)
8. Persistence – Registry Run Keys / Startup Folder (T1060)
9. Persistence – Web Shell (T1100)
10. Defense Evasion – Software Packing (T1045)
11. Credential Access – Credential Dumping (T1003)
12. Discovery – Network Service Scanning (T1046)
13. Discovery – System Network Configuration Discovery (T1016)
14. Lateral Movement – Remote Desktop Protocol (T1076)
15. Lateral Movement – Remote Services (T1021)
16. Command and Control – Connection Proxy (T1090)
17. Exfiltration – Data Compressed (T1002)

NOTE: By default, Navigator will select all instances of the same technique if it falls under multiple tactics. For example, Scheduled Task falls under the Execution, Persistence, and Privilege Escalation tactics, so it will be selected under all of the tactics. To turn this functionality off and only select a single tactic for a technique, click on the "lock multi-tactic technique selection" button until it appears in the unlocked position as shown below. (Alternately, you can leave it on and proceed with the exercise in a similar way.)



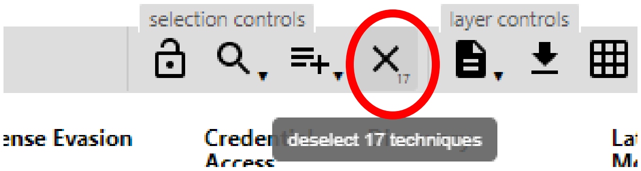
Click to allow you to select a technique under a single tactic only

Click on the first technique to select it. To select multiple techniques, hold down the "Ctrl" key as you select additional techniques. Proceed through the matrix until all 17 of the above techniques are selected.



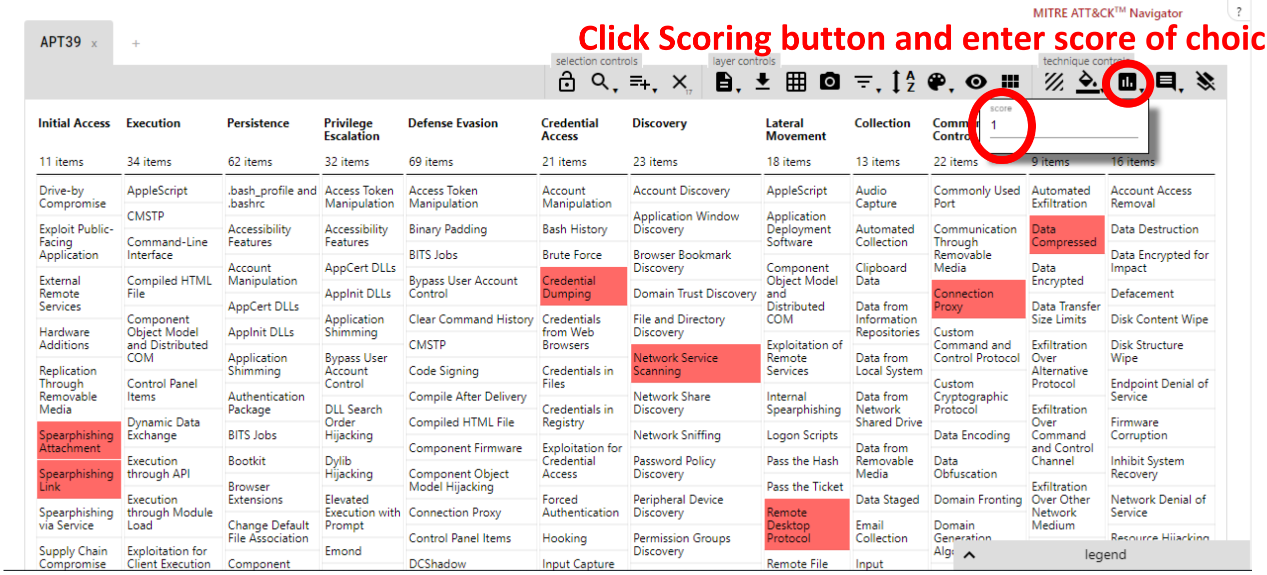
Hold down "Ctrl" key as you select multiple techniques

You can verify you have 17 techniques selected by hovering over the "deselect" option by not clicking it.



Hover over "deselect" button to verify selected number of techniques

Next, you will assign a score to these highlighted techniques. You do this by clicking the “Scoring” button and choosing a score. Make the score 1 for this exercise.



Click Scoring button and enter score of choice (1)

MITRE ATT&CK™ Navigator

APT39

Initial Access (11 items)
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise

Execution (34 items)
- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Component Object Model and Distributed COM
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution

Persistence (62 items)
- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component

Privilege Escalation (32 items)
- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Dylib Hijacking
- Elevated Execution with Prompt
- Emond

Defense Evasion (69 items)
- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Connection Proxy
- Control Panel Items
- DCShadow

Credential Access (21 items)
- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials from Web Browsers
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture

Discovery (23 items)
- Account Discovery
- Application Window Discovery
- Browser Bookmark 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

Lateral Movement (18 items)
- AppleScript
- Application Deployment Software
- Component Object Model and Distributed COM
- Exploitation of Remote Services
- Internal Spearphishing
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File

Collection (13 items)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input

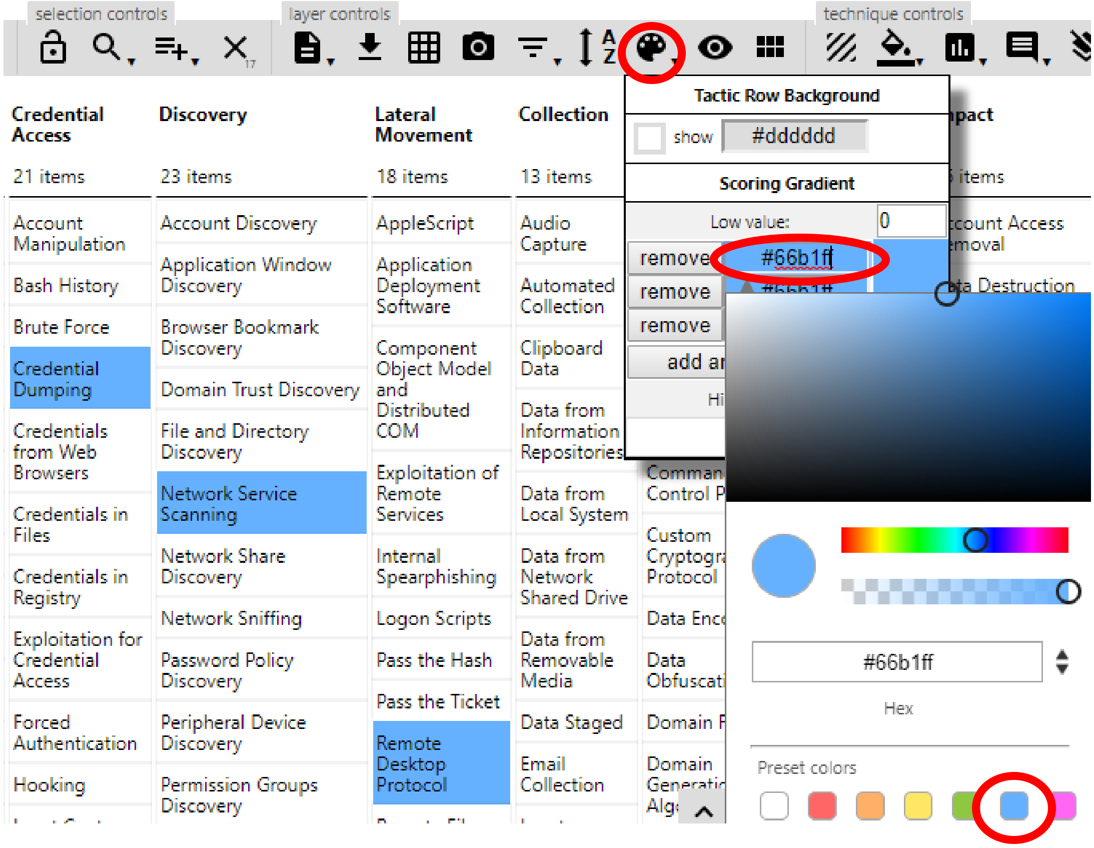
Comm Contro (22 items)
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Alg

9 items
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium

16 items
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking

You may choose to give your techniques a different color, such as blue in this example, by clicking on the “color setup” button, selecting each value, and making each value blue. This will change all your techniques to the selected color.

Click color setup button and choose your colors by clicking in the value sections and selecting the desired color



Tactic Row Background

□ show #dddddd

Scoring Gradient

Low value: 0

remove #66b1ff

remove #66b1ff

remove

add ar

Hi

#66b1ff

Hex

Preset colors

Credential Access (21 items)
- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials from Web Browsers
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking

Discovery (23 items)
- Account Discovery
- Application Window Discovery
- Browser Bookmark 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

Lateral Movement (18 items)
- AppleScript
- Application Deployment Software
- Component Object Model and Distributed COM
- Exploitation of Remote Services
- Internal Spearphishing
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol

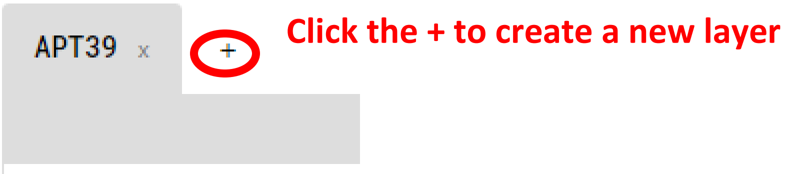
Collection (13 items)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection

- Comman Control P
- Custom Cryptogra Protocol
- Data Enc
- Data Obfuscat
- Domain F
- Domain Generatic Alg

pact (items)
- ccount Access emoval
- ta Destruction

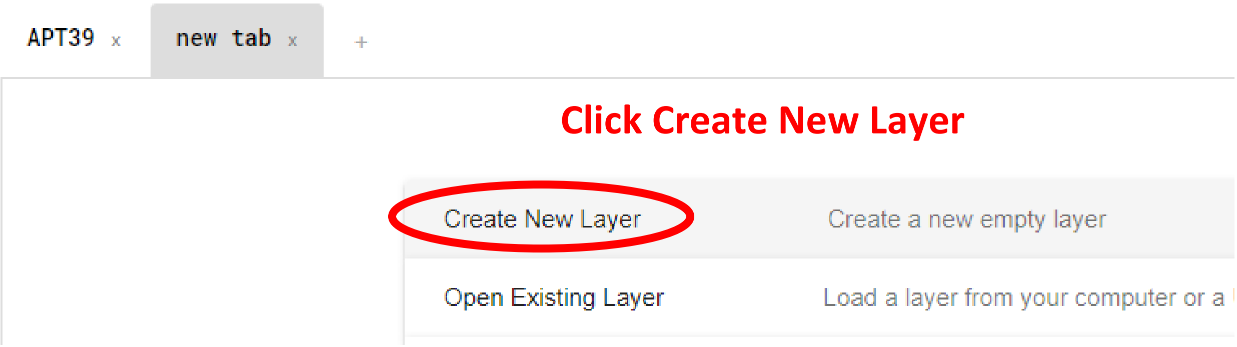
2. Create an OceanLotus layer and assign a score to techniques used by OceanLotus

Now, you will create a new layer and repeat this process with OceanLotus techniques. You will click the plus sign at the top of the Navigator to create a new layer.



Click the + to create a new layer

You will select the "Create New Layer" option.



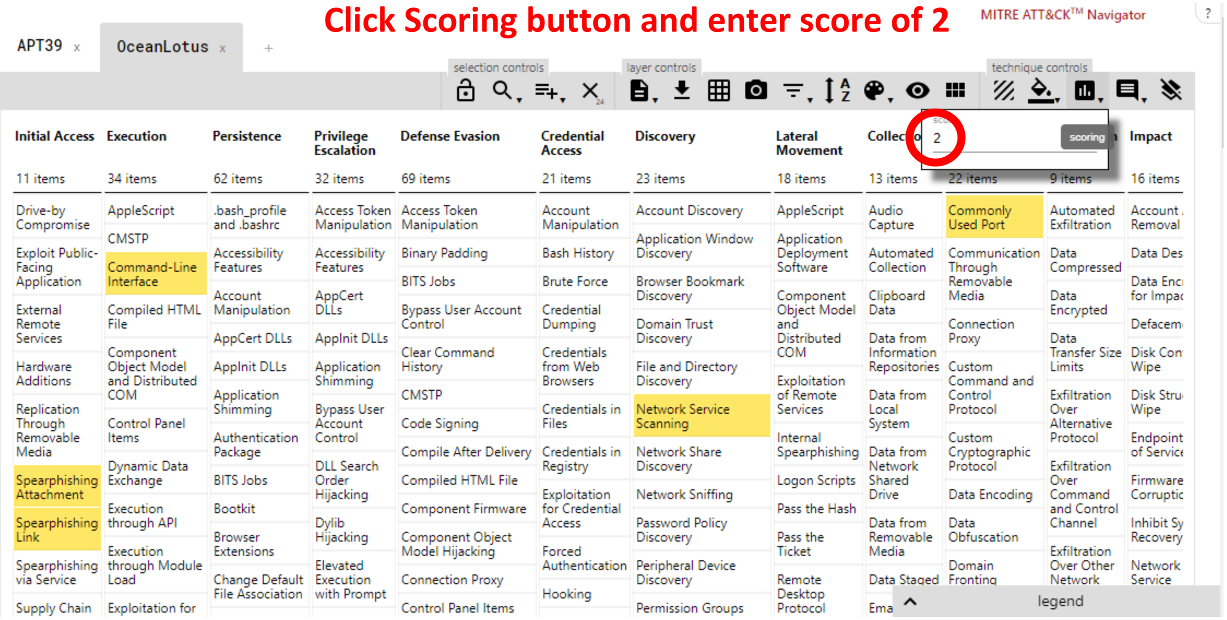
Click Create New Layer

Now you'll repeat what you did with APT39, but with OceanLotus this time. Toggle the "multi-tactic technique" selection, name your layer, and select the following 21 techniques (holding down "Ctrl" as you do this). Give your techniques a **different** score than you did in the APT39 layer (use 2 for this exercise), and then color them as you choose (we chose yellow in the below example):

1. Initial Access – Spearphishing Attachment (T1193)
2. Initial Access – Spearphishing Link (T1192)
3. Execution – Command-Line Interface (T1059)
4. Execution/Defense Evasion – Mshta (T1170)
5. Execution – PowerShell (T1086)
6. Execution – Regsvr32 (T1117)
7. Execution/Persistence – Scheduled Task (T1053)
8. Execution/Defense Evasion – Scripting (T1064)
9. Execution – User Execution (T1204)
10. Persistence – Modify Existing Service (T1031)
11. Persistence – New Service (T1050)
12. Persistence – Office Application Startup (T1137)
13. Persistence – Registry Run Keys / Startup Folder (T1060)
14. Defense Evasion – Masquerading (T1036)

15. Defense Evasion – Modify Registry (T1112)
16. Defense Evasion – NTFS File Attributes (T1096)
17. Defense Evasion – Obfuscated Files or Information (T1027)
18. Discovery – Network Service Scanning (T1046)
19. Command and Control – Commonly Used Port (T1043)
20. Command and Control – Remote File Copy (T1105)
21. Command and Control – Standard Application Layer Protocol (T1071)

If you did this as we described above, you will get a layer that looks like the below.



Click Scoring button and enter score of 2

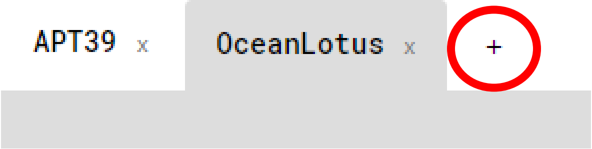
2

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collec			Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Des
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Enc for Impac
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacem
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Con Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Stru Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network	Endpoint of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting		Firmware Corruptic
Supply Chain	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Ema			Inhibit Sy Recovery
	Exploitation for	Browser Extensions		Component Firmware	Hooking	Peripheral Device Discovery					Network Service
		Change Default File Association		Component Object Model Hijacking		Permission Groups					
				Connection Proxy							
				Control Panel Items							

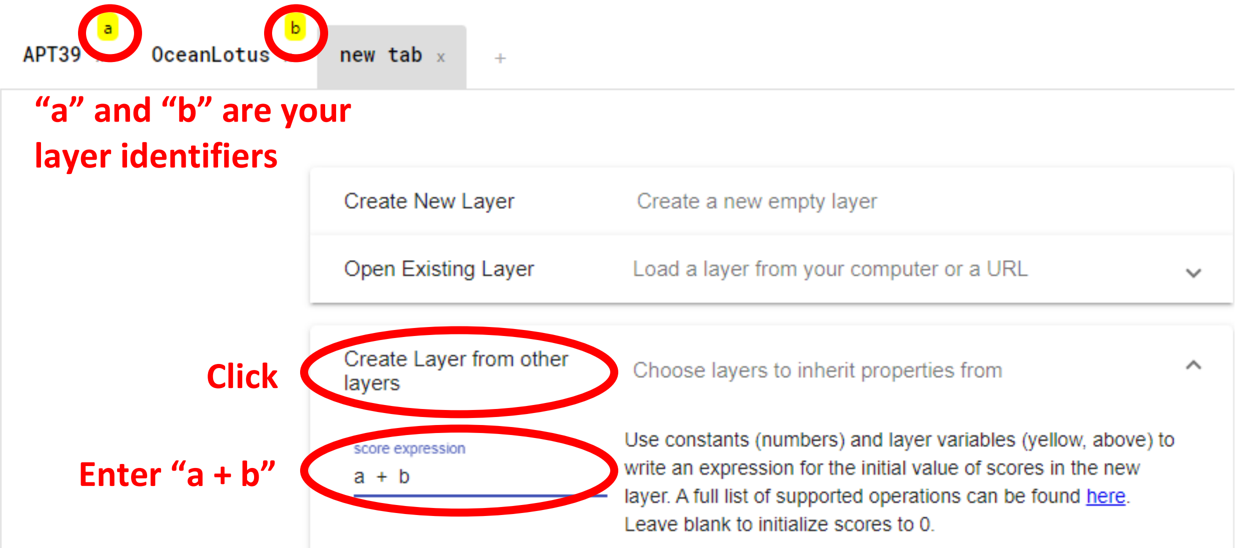
(**Tip**: To deselect any menu you're in, just click on that button again.)

3. Combine the existing APT39 and OceanLotus layers

Now that you have two layers, you want to combine them. You will again click the plus sign to create a new layer



But this time you will select the option to “Create Layer from other layers” to expand the dropdown. When you expand the dropdown, Navigator helpfully gives letter names for each of your existing layers in yellow. So, you know that Navigator identifies your APT39 layer as “a” and your OceanLotus layer as “b.” You want to combine the scores you have in your two layers, so you choose addition and enter the expression “a + b” into the score expression field.



“a” and “b” are your layer identifiers

Create a new empty layer

Load a layer from your computer or a URL

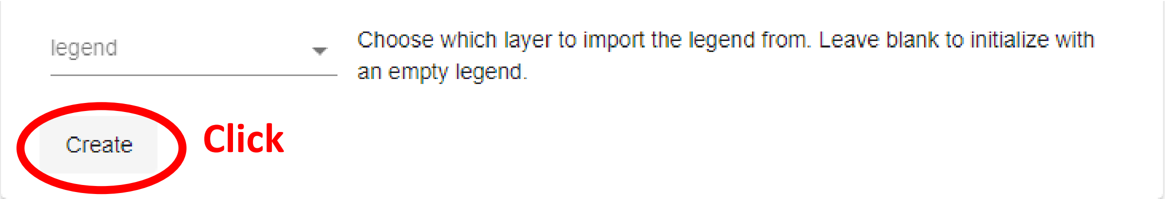
Click

Choose layers to inherit properties from

Enter “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.

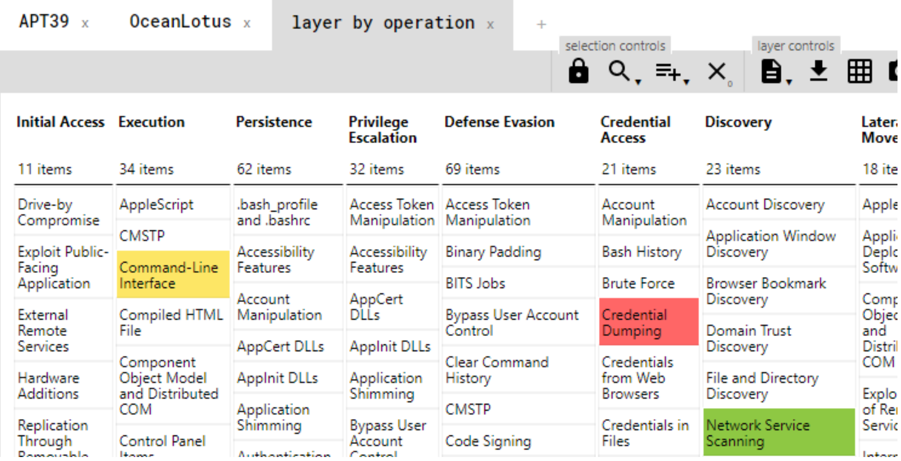
To create the layer, you’ll click the “Create” button at the bottom of the section.



Choose which layer to import the legend from. Leave blank to initialize with an empty legend.

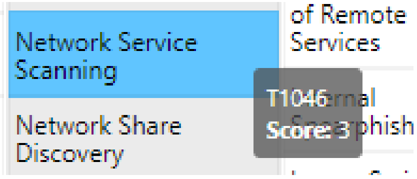
Click

Now you have your combined layer. Initially, all the techniques may appear as various colors depending on the color setup.



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Later Move
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 ite
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Apple
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Appli Deplc Softw
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Comp Objec and Distri COM
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Explo of Rei Servic
Replication Through	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	
	Control Panel	Application Shimming	Bypass User Account	CMSTP	Credentials in Files	Network Service Scanning	
				Code Signing			

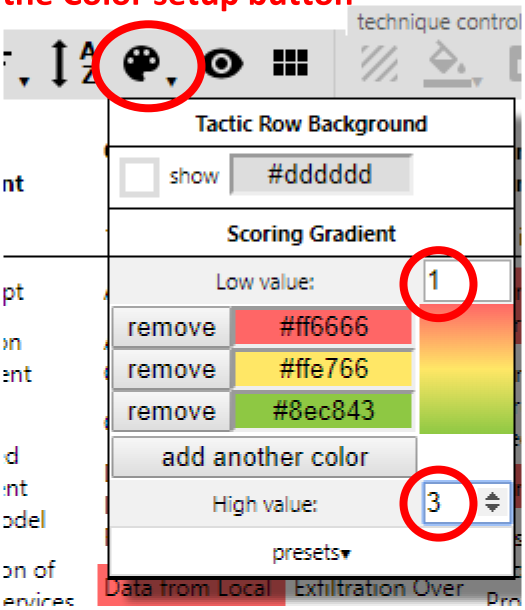
However, if you scroll over techniques, you'll see that some techniques have a score of 1 (these are the ones used by APT39 only), some have a score of 2 (these are the ones used by OceanLotus only), and some of have a score of 3 (these are the ones used by both APT39 and OceanLotus).



T1046
Score: 3

You can change the colors that appear for each score by clicking the "Color setup" button. You know the values are 1, 2, and 3, so make the low value 1 and the high value 3. Navigator knows 2 is halfway between 1 and 3 so will automatically use the middle color for the value of 2.

Click the Color setup button



Tactic Row Background

□ show #dddddd

Scoring Gradient

Low value: 1

remove #ff6666

remove #ffe766

remove #8ec843

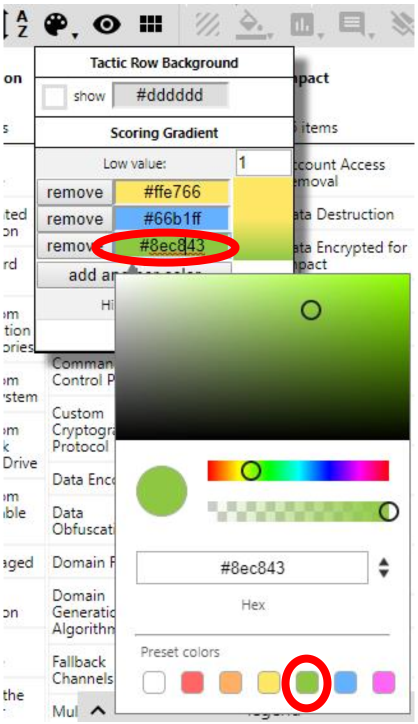
add another color

High value: 3

presets▾

Enter 1 as a low value and 3 as a high value

Now you can choose the colors you want for each layer. You choose to make APT39 techniques (score = 1) yellow, OceanLotus techniques (score = 2) blue, and both groups (score = 3) green in order to convey that yellow plus blue makes green. You can use the default colors in Navigator or specify your own hex values/choose your own custom colors if you'd like.



Tactic Row Background

□ show #dddddd

Scoring Gradient

Low value: 1

remove #ffe766

remove #66b1ff

remove #8ec843

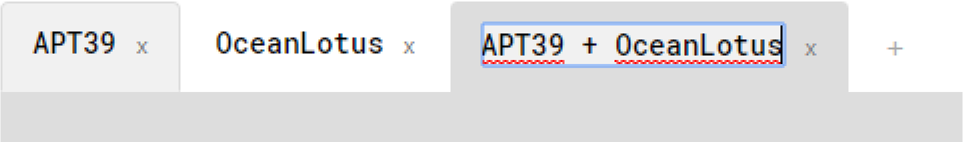
#8ec843

Hex

Preset colors

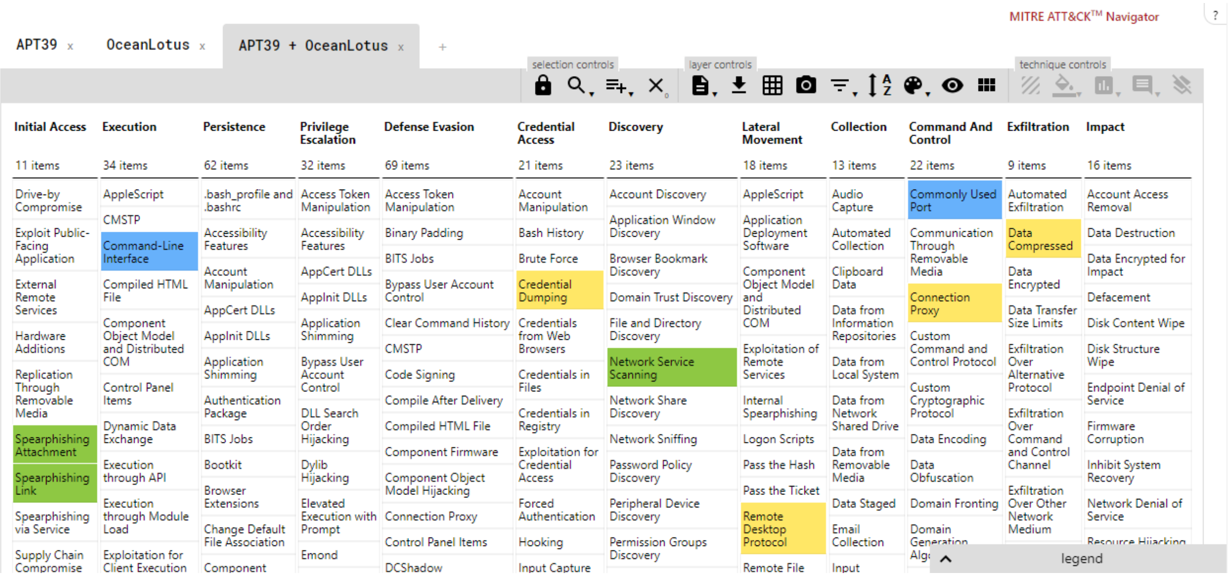
Click to choose your color for each score

Again, you'll want to name your layers so you don't lose track.



APT39 x | OceanLotus x | APT39 + OceanLotus x | +

Now you have a layer showing you the three categories of techniques in different colors, with different scores.



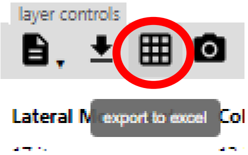
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting		Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Alg		Inhibit System Recovery
	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File	Input			Network Denial of Service
		Change Default File Association		Component Object Model Hijacking	Input Capture	Permission Groups Discovery					Resource Hijacking
		Component		Connection Proxy							
				Control Panel Items							
				DCShadow							

If you followed the above instructions, you should find that the following techniques have been used by both APT39 and OceanLotus:

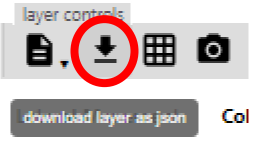
1. Initial Access – Spearphishing Attachment (T1193)
2. Initial Access – Spearphishing Link (T1192)
3. Execution – Scripting (T1064)
4. Execution – User Execution (T1204)
5. Persistence – Registry Run Keys / Startup Folder (T1060)
6. Persistence – Scheduled Task (T1053)
7. Discovery – Network Service Scanning (T1046)

4. Export the layer

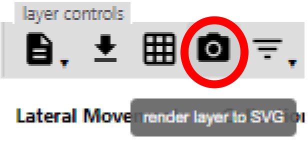
You have a couple options for how you can export the Navigator layer, and which one you choose will depend on how you want to work with it. You can export to Excel (arguably the best analyst tool of all time). This option will just export colors, not scores.



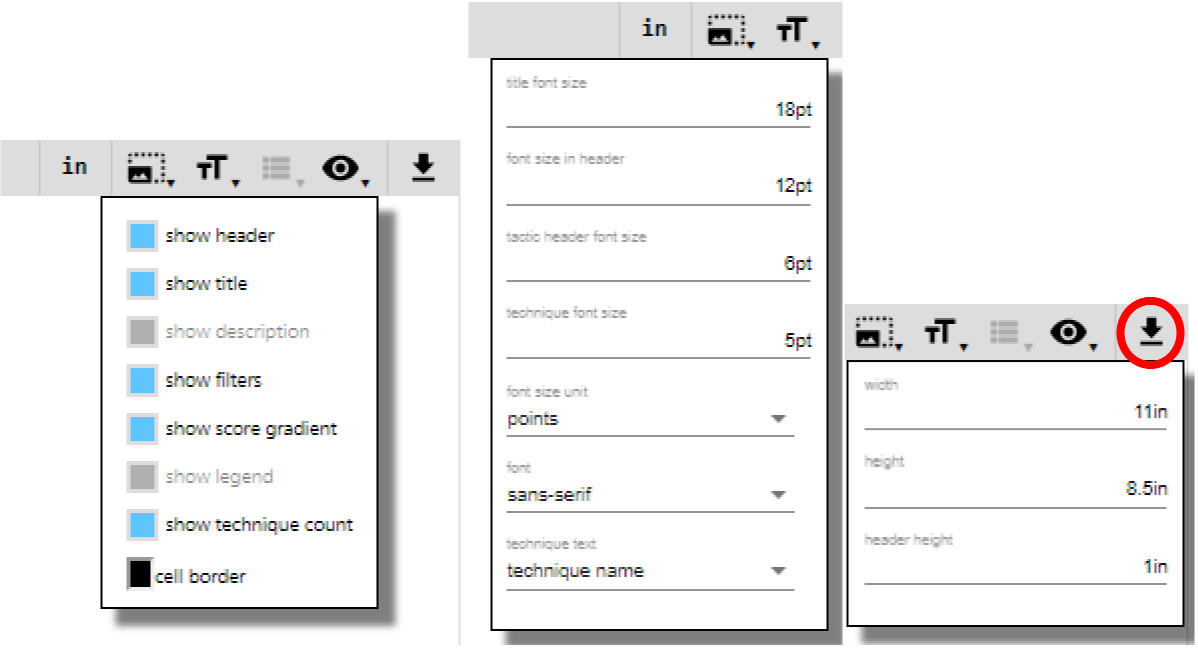
You can also download the layer as JSON, which might be useful if you want to script a layer's ingest into another tool or save it for later manipulation in the Navigator.



Maybe you want to download it as an image for a PowerPoint so you can show off what you know about adversary groups. You can export the layer as an SVG image file.



As you export to SVG, you have lots of options on what you want to include as well as the format, text, size, etc. Click the download button to get a copy of your SVG to use however you see fit.

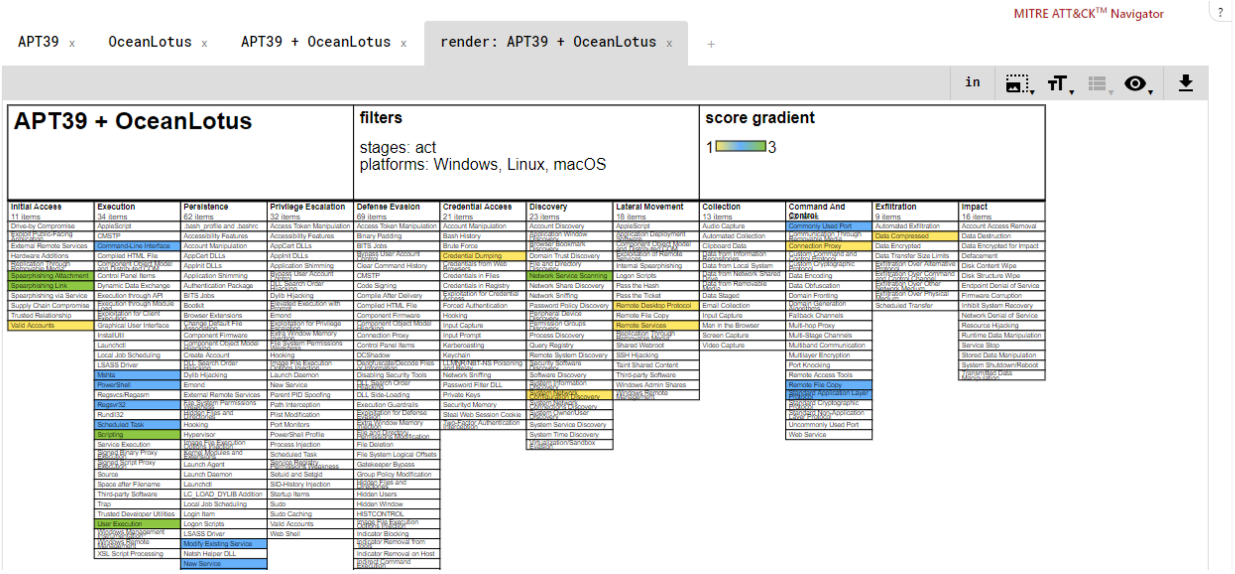


☑ show header
☑ show title
□ show description
☑ show filters
☑ show score gradient
□ show legend
☑ show technique count
■ cell border

title font size: 18pt
font size in header: 12pt
tactic header font size: 6pt
technique font size: 5pt
font size unit: points
font: sans-serif
technique text: technique name

width: 11in
height: 8.5in
header height: 1in

Download the SVG



APT39 + OceanLotus

filters

stages: act
platforms: Windows, Linux, macOS

score gradient

1 3

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory Injection	Two-Factor Authentication Interception	System Service Discovery			Uncommonly Used Port		
	Scripting	Hypervisor	PowerShell Profile	File and Directory Permissions Modification		System Time Discovery			Web Service		
	Service Execution	Image File Execution Options Injection	Process Injection	File Deletion		Virtualization/Sandbox Evasion					
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Scheduled Task	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Service Registry Permissions Weakness	Gatekeeper Bypass							
	Source	Launch Daemon	Setuid and Setgid	Group Policy Modification							
	Space after Filename	Launchctl	SID-History Injection	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Startup Items	Hidden Users							
	Trap	Local Job Scheduling	Sudo	Hidden Window							
	Trusted Developer Utilities	Login Item	Sudo Caching	HISTCONTROL							
	User Execution	Logon Scripts	Valid Accounts	Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver	Web Shell	Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							

Need more help?

Just click the ? in the upper right corner of the Navigator, and it will bring up much more detail on the above controls and more.

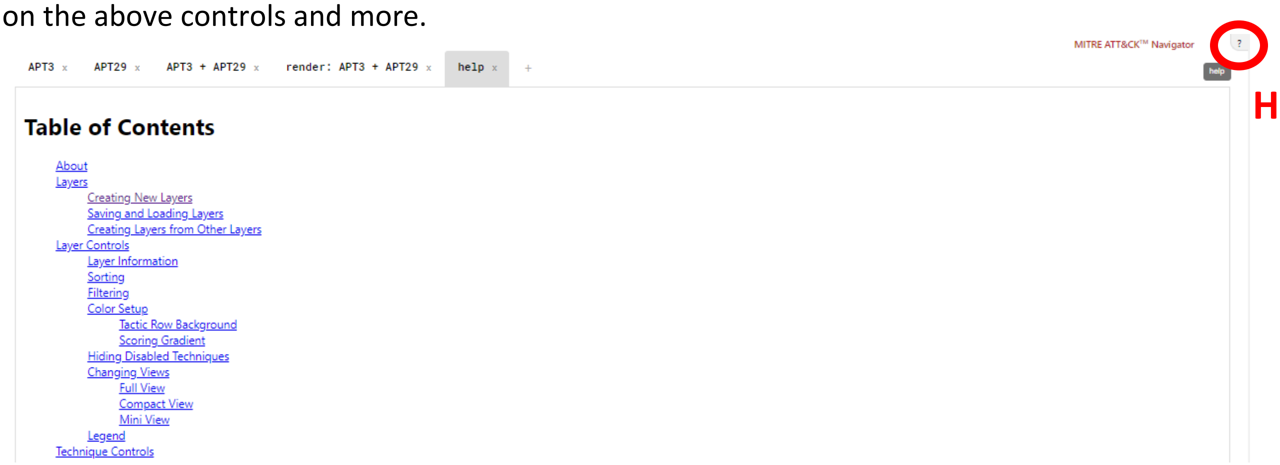


Table of Contents

- About
- Layers
  - Creating New Layers
  - Saving and Loading Layers
  - Creating Layers from Other Layers
- Layer Controls
  - Layer Information
  - Sorting
  - Filtering
  - Color Setup
    - Tactic Row Background
    - Scoring Gradient
  - Hiding Disabled Techniques
  - Changing Views
    - Full View
    - Compact View
    - Mini View
  - Legend
- Technique Controls

Help!