

Comparing Layers in ATT&CK Navigator

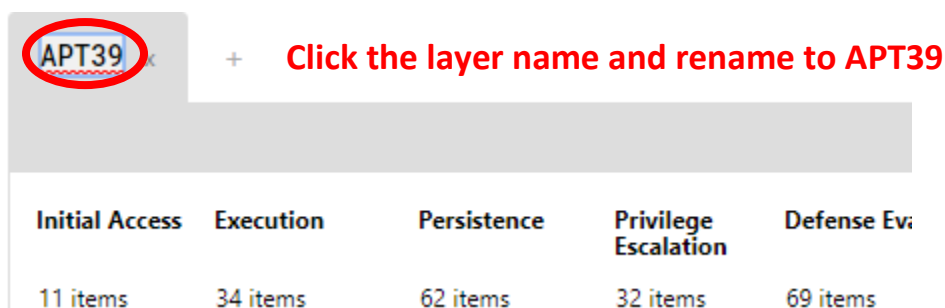
This document provides a walkthrough of how to use the ATT&CK Navigator (<https://mitre-attack.github.io/attack-navigator/enterprise/>) to compare two different layers. (Navigator source code is available at <https://github.com/mitre-attack/attack-navigator>). This comparison method is useful if you 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.

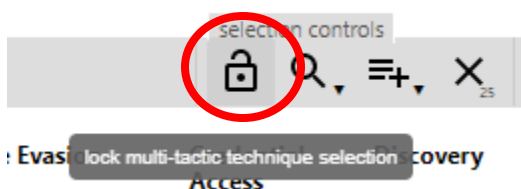


First, you will manually select the 17 techniques used by APT39 from this list (you may find it helpful to print this list or bring it up on a second screen as you select the techniques):

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)

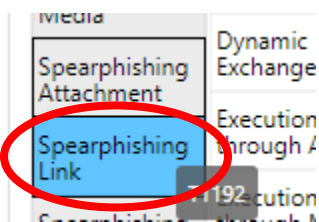
7. Persistence – Shortcut Modification (T1023)
8. Persistence – Registry Run Keys / Startup Folder (T1060)
9. Persistence – Web Shell (T1100)
10. Defense Evasion – Software Packing (T1045)
11. Credential Access – Credential Dumping (T1003)
12. Discovery – Network Service Scanning (T1046)
13. Discovery – 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.)



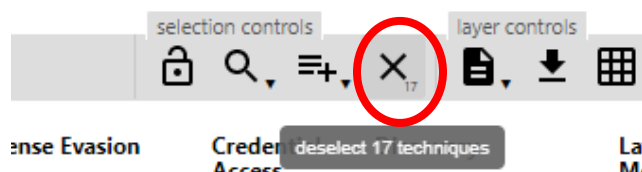
Click to allow you to select a technique under a single tactic only

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.

MITRE ATT&CK™ Navigator

Click Scoring button and enter score of choice (1)

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Communication	Scoring	Technique Controls
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	1	9 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	Accessability 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	Data Encrypted	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	Exfiltration Over Alternative Protocol	Defacement
Replication Through Removable Media	Control Panel Items	Authentication Package	Application Shim	Code Signing	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Disk Content Wipe
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	Authentication Package	Compile After Delivery	Credentials in Registry	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Other Network Medium	Disk Structure Wipe
Spearphishing Link	Execution through API	Bootkit	DLL Search Order Hijacking	Component Firmware	Exploitation for Credential Access	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 Module Load	Browser Extensions	Elevated Execution with Prompt	Component Object Model Hijacking	Forced Authentication	Peripheral Device Discovery	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Other Network Medium	Firmware Corruption
Supply Chain Compromise	Exploitation for Client Execution	Change Default File Association	Emond	Connection Proxy	Hooking	Permission Groups Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithm	Exfiltration Over Other Network Medium	Inhibit System Recovery
		Component	DCShadow	Control Panel Items	Input Capture		Remote File	Input			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

Color Setup Dialog:

Tactic Row Background: ☐ show #dddddd

Scoring Gradient: Low value: 0

remove #66b1ff

remove #66b1ff

add and

Hi

Hex: #66b1ff

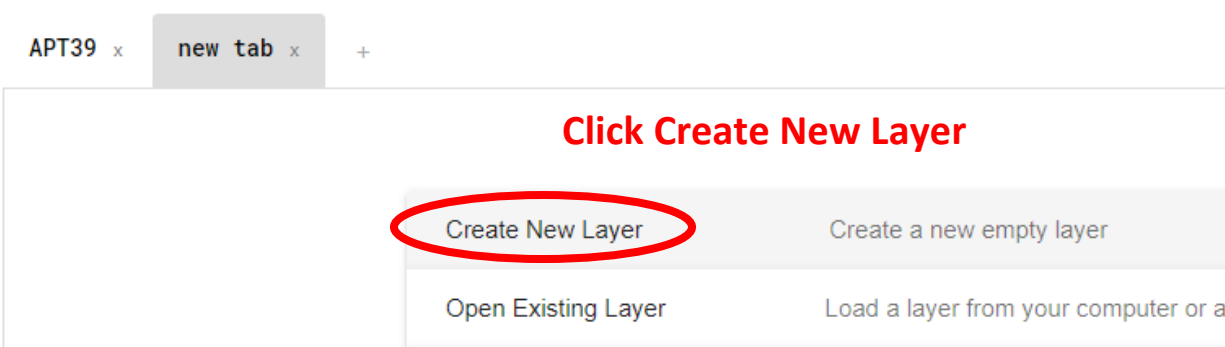
Preset colors: ☐ ☐ ☐ ☐ ☐ ☐ ☒ ☐

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.



You will select the “Create New Layer” option.



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

MITRE ATT&CK™ Navigator

APT39 x OceanLotus x +

selection controls layer controls technique controls

Initial Access Execution Persistence Privilege Escalation Defense Evasion Credential Access Discovery Lateral Movement Collection 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 Compiled HTML File Account Manipulation AppCert DLLs AppCert DLLs Bypass User Account Control Credential Dumping Browser Bookmark Discovery Component Object Model and Distributed COM Clipboard Data Connection Proxy Data Encrypted Data Enc for Impac

Hardware Additions Component Object Model and Distributed COM AppInit DLLs Application Shimming Bypass User Account Control CMSTP File and Directory Discovery Exploitation of Remote Services Custom Command and Control Protocol Data Transfer Size Limits Disk Con Wipe

Replication Through Removable Media Control Panel Items Authentication Package DLL Search Order Hijacking Compiled HTML File Credentials in Registry Network Share Discovery Internal Spearphishing Data from Network Shared Drive Exfiltration Over Alternative Protocol Endpoint of Service

Spearphishing Attachment Dynamic Data Exchange BITS Jobs Component Firmware Exploitation for Credential Access Network Sniffing Logon Scripts Pass the Hash Data from Removable Media Data Encoding Exfiltration Over Command and Control Channel Firmware Corruptic

Spearphishing Link Execution through API Bootkit Dll Hijacking Component Object Model Hijacking Forced Authentication Password Policy Discovery Pass the Ticket Data from Removable Media Data Obfuscation Exfiltration Over Other Network Inhibit Sy Recovery

Spearphishing via Service Execution through Module Load Change Default File Association Elevated Execution with Prompt Connection Proxy Hooking Peripheral Device Discovery Remote Desktop Protocol Data Staged Domain Fronting Exfiltration Over Other Network Network Service

Supply Chain Exploitation for Control Panel Items Permission Groups

2

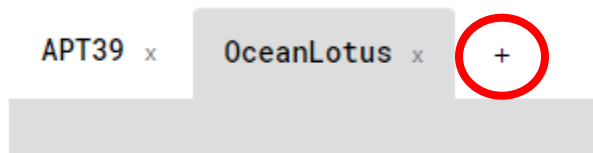
scoring

legend

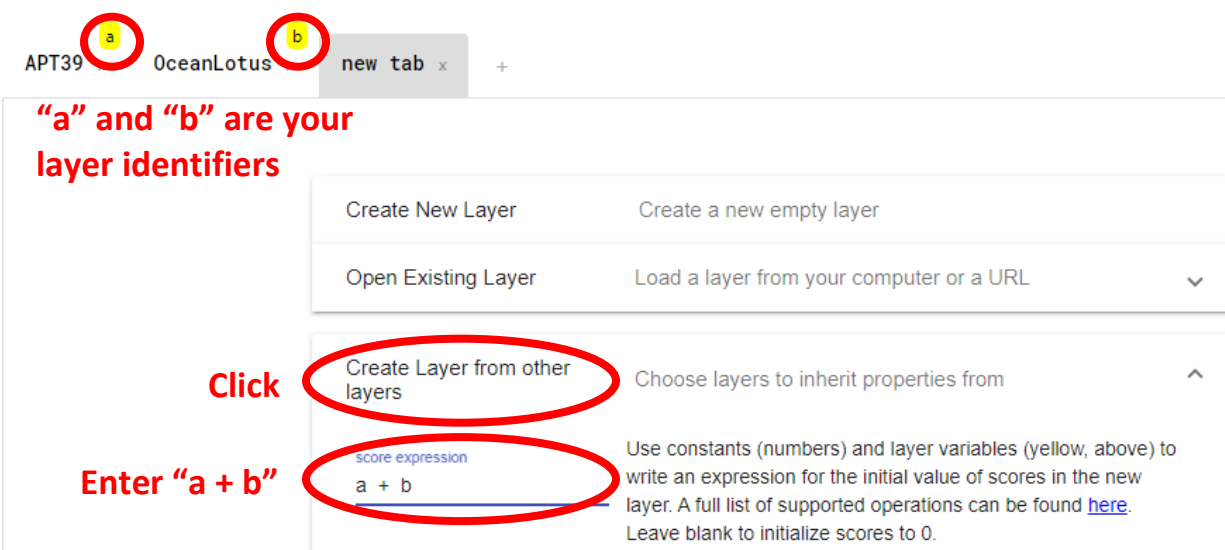
(Tip: To deselect any menu you're in, just click on that button again.)

3. Combine the existing APT39 and OceanLotus layers

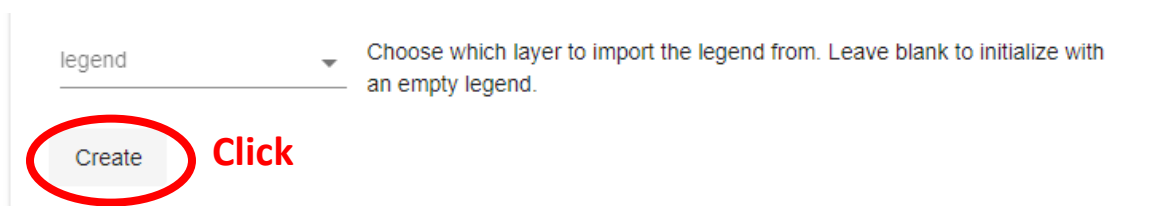
Now that you have two layers, you want to combine them. You will again click the plus sign to create a new layer



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.



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

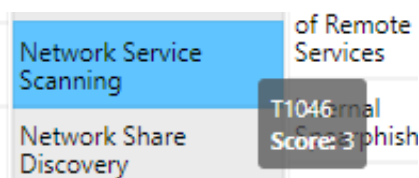


Now you have your combined layer. Initially, all the techniques may appear as various colors depending on the color setup.

APT39 x OceanLotus x layer by operation x

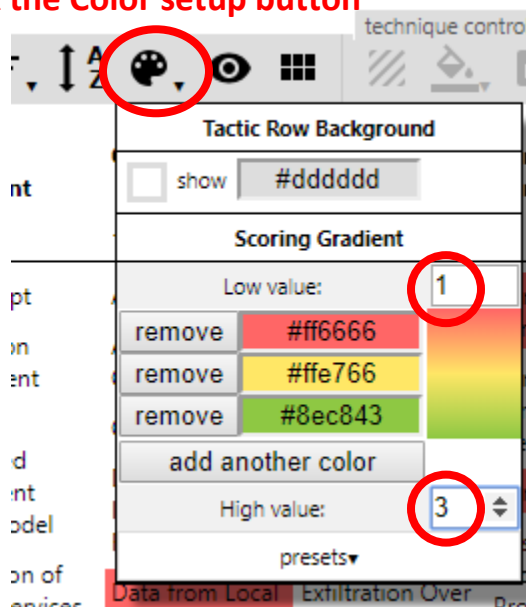
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Later. Move
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 ite
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account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

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).



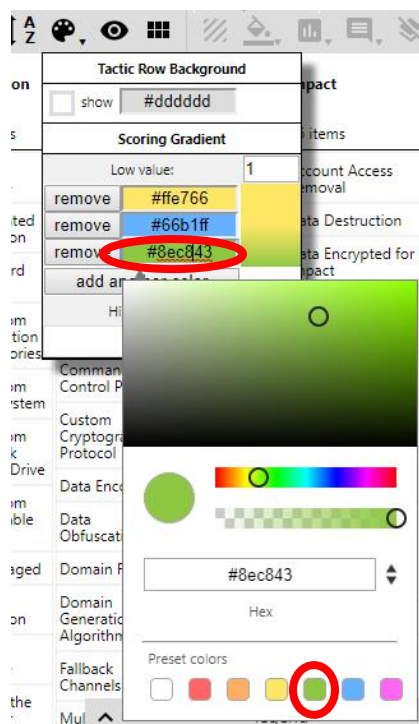
You can change the colors that appear for each score by clicking the "Color setup" button. You know the values are 1, 2, and 3, so make the low value 1 and the high value 3. Navigator knows 2 is halfway between 1 and 3 so will automatically use the middle color for the value of 2.

Click the Color setup button



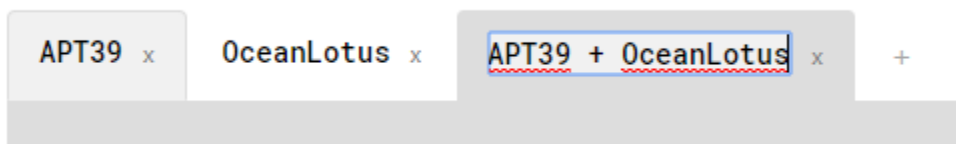
Enter 1 as a low value and 3 as a high value

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.



Click to choose
your color for
each score

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



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

MITRE ATT&CK™ Navigator

APT39 x OceanLotus x APT39 + OceanLotus x

selection controls layer controls technique controls

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	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Exfiltration Over Alternative Protocol	Disk Content Wipe	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Endpoint Denial of Service	Firmware Corruption
Spearphishing Link	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Credentials in Registry	Network Sniffing	Pass the Hash	Data from Removable Media	Data Encoding	Inhibit System Recovery	Network Denial of Service
Spearphishing via Service	Execution through Module Load	Bootkit	Dylib Hijacking	Component Firmware	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data Staged	Domain Fronting	Resource Hijacking	
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Elevated Execution with Prompt	Connection Proxy	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithm		
		Change Default File Association	Control Panel Items	Control Panel Items	Hooking	Permission Groups Discovery	Remote File	Input			
		Component	Emond	DCShadow	Input Capture						

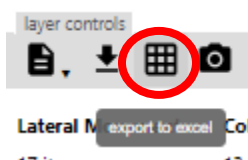
legend

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

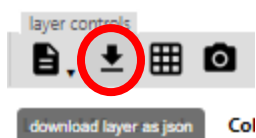
1. Initial Access – Spearphishing Attachment (T1193)
2. Initial Access – Spearphishing Link (T1192)
3. Execution – Scripting (T1064)
4. Execution – User Execution (T1204)
5. Persistence – Registry Run Keys / Startup Folder (T1060)
6. Persistence – Scheduled Task (T1053)
7. Discovery – Network Service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

4. Export the layer

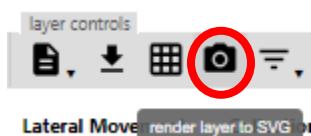
You have a couple options for how you can export the Navigator layer, and which one you choose will depend on how you want to work with it. You can export to Excel (arguably the best analyst tool of all time). This option will just export colors, not scores.



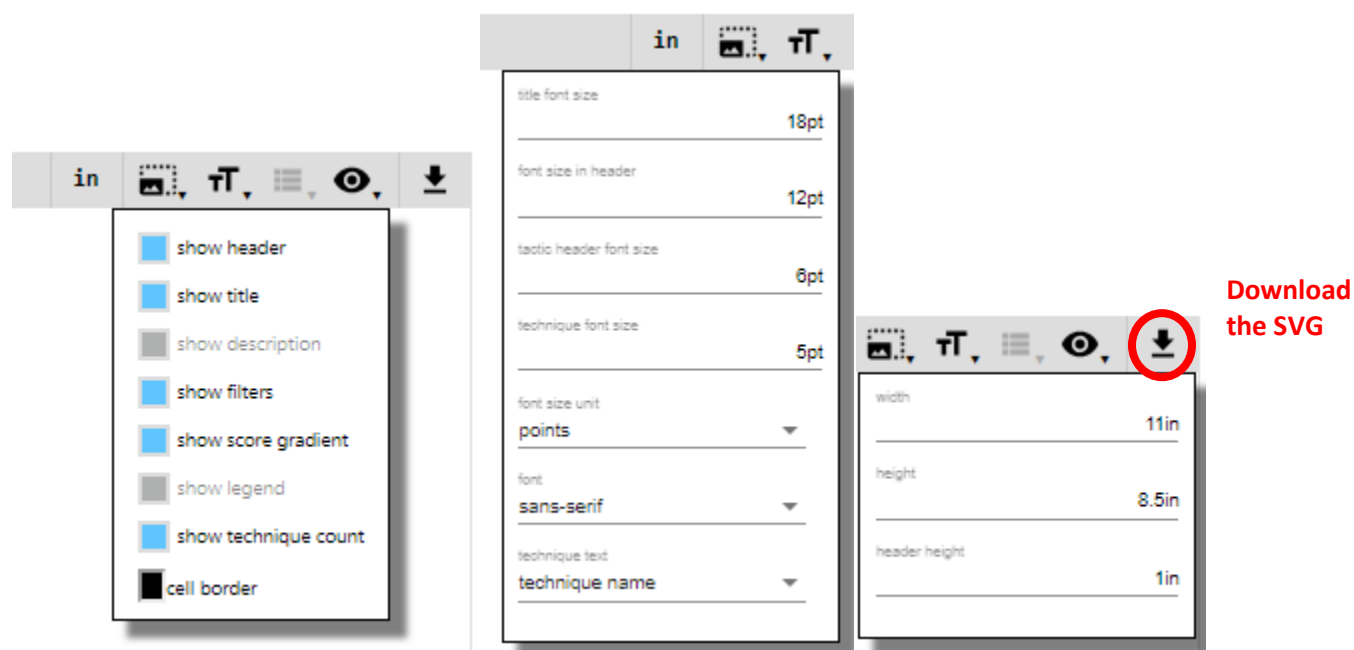
You can also download the layer as JSON, which might be useful if you want to script a layer's ingest into another tool or save it for later manipulation in the Navigator.



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.



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.

Help!