# Comparing Layers in ATT&CK Navigator

This document provides a walkthrough of how to use the ATT&CK Navigator (<u>https://mitre-attack.github.io/attack-navigator/enterprise/</u>) to compare two different layers. (Navigator is also available at <u>https://github.com/mitre-attack/attack-navigator</u>). This walkthrough would be 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 walkthrough, you'll compare APT3 techniques to APT29 techniques. To do this, you will:

- 1. Create an APT3 layer and assign a score to techniques used by APT3 in one layer
- 2. Create a second layer and assign a score to techniques used by APT29
- 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 APT3 layer and assign a score to techniques used by APT3

By default, Navigator has a new layer created for you, so you'll work with that. First, you will select the techniques used by APT3. You can use the techniques already mapped to APT3 in ATT&CK by clicking the "Multi-select" button and selecting "APT3." This will highlight all techniques that are in the ATT&CK Groups page for APT3.

layer × h	elp × +				Clic	k multi-	sele	t but	ton		MITRE ATT&	CK <sup>™</sup> Navigator
				selection		iayer controis		₹, <u>†</u>	<b>e</b> , (	•	technique co	, 🛄 , 🗐 , 🗞
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Cr <sub>APT28</sub>	Threat Gro view	select	deselect	▲ tion		Exfiltration	Command And Control
10 items	33 items	58 items	28 items	63 items		k select	select	deselect	ns		9 items	21 items
Drive-by Compromise	AppleScript CMSTP	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Ac MiAPT32	v w view	select select	leselect deselect	Cap		Automated Exfiltration	Commonly Used Port
Exploit Public- Facing Application	Command-Line Interface	Accessibility Features	Accessibility Features	Binary Padding BITS Jobs	Ba APT33 Bri	view	select	deselect	tion ard	Data	Data Compressed	Communication Through Removable Media
Hardware Additions	Compiled HTML File	Account Manipulation	AppCert DLLs AppInit DLLs	Bypass User Account Control	Cn DuAxiom	<u>view</u> view	select select	deselect deselect	rom atio		Data Encrypted Data Transfer	Connection Proxy
Replication Through Removable Media	Control Panel Items Dynamic Data Exchange	AppCert DLLs AppInit DLLs	Application Shimming	Clear Command History	Cr	Softwar	e		torie rom		Size Limits Exfiltration Over	Custom Command and Control Protocol
Spearphishing Attachment	Execution through	Application Shimming	Bypass User Account Control	Code Signing	Re 3PARA RAT	<u>view</u>	select	deselect	rom		Alternative Protocol	Custom Cryptographic
Spearphishing Link	Execution through	Authentication Package	DLL Search Order Hijacking	Compiled HTML File Component Firmware	Exi4H RAT Cr ADVSTORESHELL	<u>view</u>	select select	deselect deselect	rk S	nared	Exfiltration Over Command and Control Channel	Protocol
	Exploitation for	BITS Jobs	Dylib Hijacking	Component Object Model Hijacking	AuASPXSpy	view	select	deselect	rom (able		Exfiltration Over	
Service Supply Chain	Client Execution Graphical User	Bootkit Browser Extensions	Exploitation for Privilege	Control Panel Items	Hc <sub>Agent.btz</sub>	view	select	deselect	tage		Other Network Medium	Domain Fronting
Compromise	Interface	Change Default File	Escalation Extra Window	DCShadow	Arp	view	select	deselect	Colle	ction	Exfiltration Over Physical	Fallback Channels Multi-hop Proxy
Trusted Relationship	InstallUtil Launchctl	Association Component	Memory Injection	Deobfuscate/Decode Files or Information	Autolt backdoor	view Discovery	select Throug	deselect			uí e	gend

Next, you will assign a score to these highlighted techniques. You do this by clicking the "Scoring" button and choosing a score. You choose 1 in this example.

laver × h	elp × +						Click Sco	ring hut		CK <sup>™</sup> Navigator ? enter score o	of choico (1
Idyel x	nelp x +			selection o		layer controls			technique c	ontrolo	
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection 1	•	nd And	
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	13 items	9 items	21 items	
Drive-by Compromise	AppleScript CMSTP	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript Application	Audio Capture Automated	Automated Exfiltration	Commonly Used Port	
Exploit Public- Facing Application	Command-Line Interface	Accessibility Features	Accessibility Features	Binary Padding BITS Jobs	Bash History Brute Force	Application Window Discovery	Deployment Software	Collection Clipboard Data	Data Compressed	Communication Through Removable Media	
Hardware Additions	Compiled HTML File	Account Manipulation	AppCert DLLs AppInit DLLs	Bypass User Account Control	Credential Dumping	Browser Bookmark	Distributed Component	Data from Information	Data Encrypted Data Transfer	Connection Proxy	
Replication Through Removable Media	Control Panel Items Dynamic Data Exchange	AppCert DLLs AppInit DLLs	Application Shimming	Clear Command History CMSTP	Credentials in Files Credentials in	Discovery File and Directory	Object Model Exploitation of Remote Services	Repositories Data from Local	Size Limits Exfiltration Over	Custom Command and Control Protocol	
Spearphishing Attachment	Execution through API	Application Shimming	Bypass User Account Control	Code Signing	Registry Exploitation for	Discovery Network Service	Logon Scripts	System Data from	Alternative Protocol	Custom Cryptographic	
Spearphishing Link	Execution through Module Load	Authentication Package	DLL Search Order Hijacking	Compiled HTML File Component Firmware	Credential Access	Scanning Network Share	Pass the Hash Pass the Ticket	Network Shared Drive	Exfiltration Over Command and Control Channel	Protocol Data Encoding	
Spearphishing via Service	Exploitation for Client Execution	BITS Jobs Bootkit	Dylib Hijacking Exploitation for	Component Object Model Hijacking	Authentication Hooking	Discovery Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network		
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Privilege Escalation	Control Panel Items	Input Capture	Password Policy Discovery	Remote File Copy Remote Services	Data Staged	Medium Exfiltration Over	Domain Fronting Fallback Channels	
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory	DCShadow Deobfuscate/Decode	Input Prompt Kerberoasting	Peripheral Device Discovery	Replication	Email Collection	Physical	Multi-hop Proxy	
Relationship	Launchctl	Component	Injection	Files or Information	Kauahain	Discovery	Through Removable	Man in	le	gend	

If you want to add other techniques that you know APT3 has used (e.g. Binary Padding), you can just click on the technique and use the "Scoring" button to assign a score to those techniques too.

Privilege Escalation	Defense Evasion			
28 items	63 items	_		n and enter score of oue controls
Access Token	Access Token Manipulation	Click the	• • • • //	à. m e
Manipulation	Binary Padding	technique	• • • • • • • • • • • • • • • • • • • •	
Accessibility Features	BITS JOOS	you want	Exfil 1	nd C
AppCert DLLs	Bypass User Account Control	to score	9 iter	
AppInit DLLs				

To help keep yourself organized, you will name the layer "APT3" by clicking on the name at the top.

Click	the layer nam	e and rename to A	РТЗ		selection	controls	
					ê (	೩, ≡+,	<b>X</b> <sub>56</sub>
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasio	on	Credentia	l Acce

## 2. Create an APT29 layer and assign a score to techniques used by APT29

Now, you will create a new layer and repeat this process with APT29 techniques. You will click the plus sign at the top of the Navigator to create a new layer.

APT3 x	Click the + t	to create a new lay	er		
				select	ion controls Q, ≡+, :
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential /

You will select the "Create New Layer" option.

APT3 x	new tab ×	+			
			Clic	ck Create 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	~

Now you'll repeat what you did with APT3 (but with APT29 this time) to select techniques.

APT3 × la	yer × +			selection		a multi-select	butto	on	
				ê c		∎, ± ⊞ Threat Gro		<del>,</del> ‡2	<b>e</b> ,
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Cr APT1	view	select	deselect	
10 items	33 items	58 items	28 items	63 items	19APT16	view	select	deselect	
Drive-by Compromise	AppleScript CMSTP	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	AcAPT17 Ma	<u>view</u>	select	deselect	
Exploit Public- Facing Application	Command-Line	Accessibility Features	Accessibility Features	Binary Padding BITS Jobs	APT18 Ba Bn <sup>APT19</sup>	<u>view</u>	select select	deselect deselect	
Hardware Additions	Compiled HTML File	Account Manipulation	AppCert DLLs	Bypass User Account Control	CnAPT28	<u>view</u>	select	deselect	
Replication	Control Panel Items	AppCert DLLs	AppInit DLLs	Close Command History	Di APT29	<u>viev</u>	select	deselect	

Next, you will give the APT29 techniques a different score than what you gave the APT3 techniques in the other layer. You choose 2.

_									MITRE ATT&	CK <sup>™</sup> Navigator	
APT3 × la	iyer × +			selection	controls	laver controls	Click Sco	ring but	ton and	enter score	e of choice (2)
				ê a	(,≡+, × <u>_</u>	Ê, ± ⊞	<b>◎</b> <del>,</del> ‡	ê 🖗, 🗿	•• 🥢 <u>&gt;</u>	. 💷 , 🗏 , 🚿	
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collecti n 2	)	nd And	
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	13 items	9 items	21 items	
Drive-by Compromise	AppleScript CMSTP	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript Application	Audio Capture Automated	Automated Exfiltration	Commonly Used Port	
Exploit Public- Facing Application	Command-Line Interface	Accessibility Features	Accessibility Features	Binary Padding BITS Jobs	Bash History Brute Force	Application Window Discovery	Deployment Software	Collection Clipboard Data	Data Compressed	Communication Through Removable Media	

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

You then name your layer "APT29" so you can better keep track of it.



#### 3. Combine the existing APT3 and APT29 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 APT3 layer as "a" and your APT29 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.

APT3 APT29 new tab	• x +		
"a" and "b" are your layer identifiers			
	Create New Layer	Create a new empty layer	
	Open Existing Layer	Load a layer from your computer or a URL	~
Click	Create Layer from other layers	Choose layers to inherit properties from	^
Enter "a + b"	a + b	se constants (numbers) and layer variables (yellow, above) to write an pression for the initial value of scores in the new layer. A full list of apported operations can be found <u>here</u> . Leave blank to initialize scores to	I

## To create the layer, you'll click the "Create" button at the bottom of the section.

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 <u>here</u> . Leave blank to initialize scores to 0.
coloring	<ul> <li>Choose which layer to import manually assigned colors from. Leave blank t</li> <li>initialze with no colors.</li> </ul>
comments	<ul> <li>Choose which layer to import comments from. Leave blank to initialize with no comments.</li> </ul>
states	<ul> <li>Choose which layer to import enabled/disabled states from. Leave blank to initialize all to enabled.</li> </ul>
filters	<ul> <li>Choose which layer to import filters - stages and platforms - from. Leave</li> <li>blank to initialize with no filters.</li> </ul>
legend	<ul> <li>Choose which layer to import the legend from. Leave blank to initialize with an empty legend.</li> </ul>
Create	

APT3 × APT2	9 × layer by	operation x +		
Initial Access	Execution	Persistence	Privilege Escalation	Defense Eva
11 items	33 items	59 items	28 items	67 items
Drive-by Compromise Exploit Public-Facing	AppleScript CMSTP	.bash_profile and .bashrc	Access Token Manipulation	Access Toke Manipulatio
Application	Command-Line	Accessibility Features	Accessibility Features	Binary Padd
External Remote	Interface	Account Manipulation	AppCert DLLs	BITS Jobs
Services Hardware Additions	Compiled HTML File	AppCert DLLs	Applnit DLLs	Bypass User Control

Now you have your combined layer. Initially, all the techniques will appear with the same color:

However, if you scroll over techniques, you'll see that some techniques have a score of 1 (these are the ones used by APT3 only), some have a score of 2 (these are the ones used by APT29 only), and some of have a score of 3 (these are the ones used by APT3 and APT29).

APT3 × AP	T29 x layer	by operation	x +	
Initial Access	Execution	Persistence	Privilege Escalation	Defense E
10 items	33 items	58 items	28 items	63 items
Drive-by Compromise	AppleScript CMSTP	.bash_profile and .bashrc	Access Token Manipulation	Access Tol Manipulat
Exploit Public- Facing Application	Command-Line Interface	Accessibility Features	Accessibility T1015 <sup>res</sup>	Binary Pad BITS Jobs
Hardware Additions	Compiled HTML File	Account Manipulation	AppInit DLLs	Bypass Us Control

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.



Now you can choose the colors you want for each layer. You choose to make APT3 techniques (score = 1) yellow, APT29 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.



©2019 The MITRE Corporation. ALL RIGHTS RESERVED Approved for public release. Distribution unlimited 18-1528-38.

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

APT3 x	APT29 x	APT3 + APT29 ×

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

APT3 × APT29	× APT3 + APT2	9 x +							MITR	ATT&CK <sup>™</sup> Navigator
					sel	ection controls Q, ≡+, X <sub>0</sub>	layer controls	D <del>,</del> 12 @		ique controls
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated	Commonly Used Port
Exploit Public-Facing	CMSTP	Accessibility Features	Manipulation	Binary Padding	Bash History	Application Window	Application	Automated Collection		Communication Through
Application	Command-Line Interface	Account Manipulation	Accessibility Features	BITS Jobs	Brute Force	Discovery	Deployment Software	Clipboard Data	Data Compressed	Removable Media
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	Browser Bookmark Discovery	Distributed Component Object	Data from	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Clear Command History	Credentials in Files	File and Directory	Model	Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	Discovery	Exploitation of Remote		Exfiltration Over	Custom Cryptographic
	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for	Network Service	Services	System	Alternative Protocol	Protocol
Spearphishing Link	Execution through	BITS Jobs	DLL Search Order	Compiled HTML File	Credential Access	Scanning	Logon Scripts	Data from Network	Exfiltration Over	Data Encoding
Spearphishing via	Module Load	Bootkit	Hijacking	Component Firmware	Forced Authentication	Network Share Discovery	Pass the Hash	Shared Drive	Command and Control Channel	Data Obfuscation
Service	Exploitation for Client Execution	Browser Extensions	Dylib Hijacking	Component Object Model	Hooking	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over	Domain Fronting
Supply Chain Compromise	Graphical User Interface	Change Default File	Exploitation for	Hijacking	Input Capture	Password Policy	Remote Desktop Protocol	Data Staged	Other Network	Fallback Channels
Trusted Relationship	InstallUtil	Association	Privilege Escalation	Control Panel Items	Input Prompt	Discovery	Remote File Copy	Email Collection	Medium	Multi-hop Proxy
Valid Accounts	Launchetl	Component Firmware	Extra Window Memory Injection	DCShadow	Kerberoasting	Peripheral Device	Remote Services	Input Capture	Exfiltration Over Physical Medium	Multi-Stage Channels
Valid Accounts	Launcheti Local Job Scheduling	Component Object Model Hijacking	File System	Deobfuscate/Decode Files or Information	Keychain	Discovery	Replication Through	Man in the Browser	Scheduled Transfer	Multiband
	LSASS Driver	Create Account	Permissions Weakness		LLMNR/NBT-NS	Permission Groups Discovery	Removable Media	Screen Capture		Communication
		DLL Search Order	Hooking Image File Execution Options Injection	Disabling Security Tools	Poisoning Network Sniffing Password Filter DLL	Process Discovery	Shared Webroot Video Capture			Multilayer Encryption
	Mshta PowerShell	DLL Search Order Hijacking		DLL Search Order Hijacking		Query Registry	SSH Hijacking			Port Knocking
		Dylib Hijacking		DLL Side-Loading		Remote System	Taint Shared Content			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Launch Daemon	Exploitation for Defense Evasion	Private Keys	Discovery	Third-party Software			Remote File Copy
	Regsvr32 Rundll32	File System Permissions Weakness	New Service Path Interception	Extra Window Memory Injection	Securityd Memory Two-Factor	Security Software Discovery	Windows Admin Shares			Standard Application Layer Protocol
	Scheduled Task Scripting	Hidden Files and Directories	Plist Modification	File Deletion	Authentication Interception	System Information Discovery	Windows Remote Management			Standard Cryptographic Protocol
	Service Execution	Hooking	Port Monitors Process Injection	File Permissions Modification File System Logical Offsets		System Network Configuration	-		^	legend

### 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.



©2019 The MITRE Corporation. ALL RIGHTS RESERVED Approved for public release. Distribution unlimited 18-1528-38.

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.





©2019 The MITRE Corporation. ALL RIGHTS RESERVED Approved for public release. Distribution unlimited 18-1528-38.

## 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.

