Comparing Layers in ATT&CK Navigator

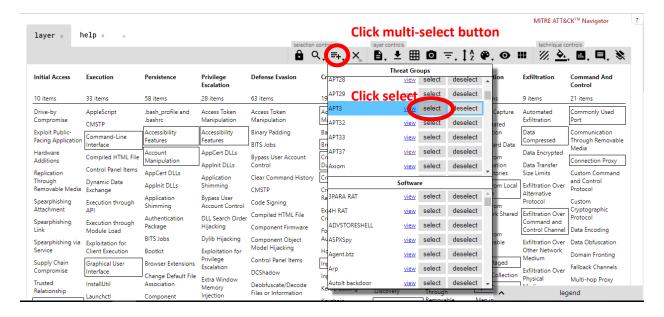
This document provides a walkthrough of how to use the ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/enterprise/) to compare two different layers. (Navigator is also available at https://github.com/mitre-attack/attack-navigator). This walkthrough would be useful if you want to compare 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:

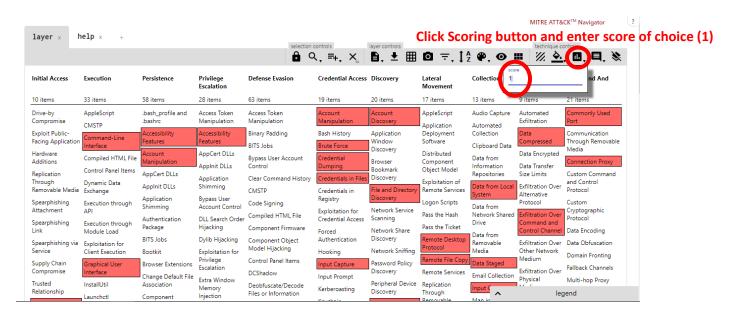
- 1. Create an APT3 layer and assign a score to techniques used by APT3 in one layer
- 2. Create a second layer and assign a score to techniques used by APT29
- 3. Combine the two using "Create Layer from other layers" using the expression "a + b"
- 4. Export the layer in the format of your choice

1. Create an APT3 layer and assign a score to techniques used by APT3

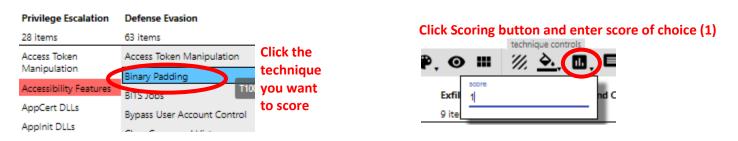
By default, Navigator has a new layer created for you, so you'll work with that. First, you will select the techniques used by APT3. You can use the techniques already mapped to APT3 in ATT&CK by clicking the "Multi-select" button and selecting "APT3." This will highlight all techniques that are in the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



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.



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.



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

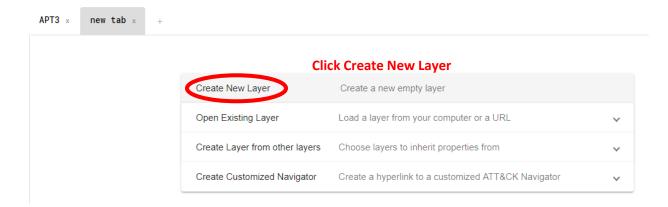


2. Create an APT29 layer and assign a score to techniques used by APT29

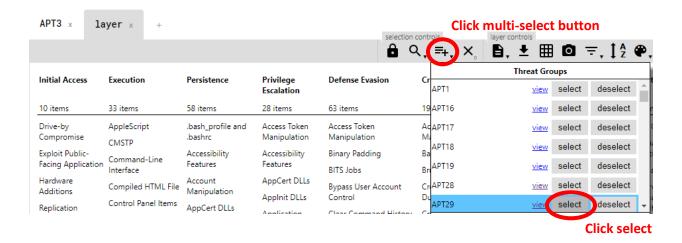
Now, you will create a new layer and repeat this process with APT29 techniques. You will click the plus sign at the top of the Navigator to create a new layer.



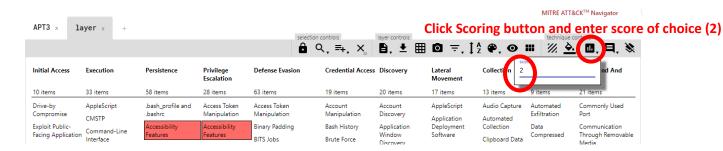
You will select the "Create New Layer" option.



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



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



(**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.

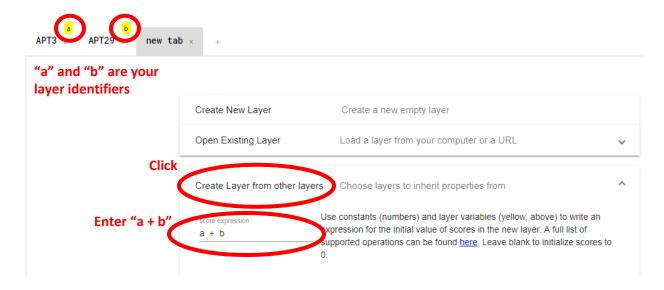


3. Combine the existing APT3 and APT29 layers

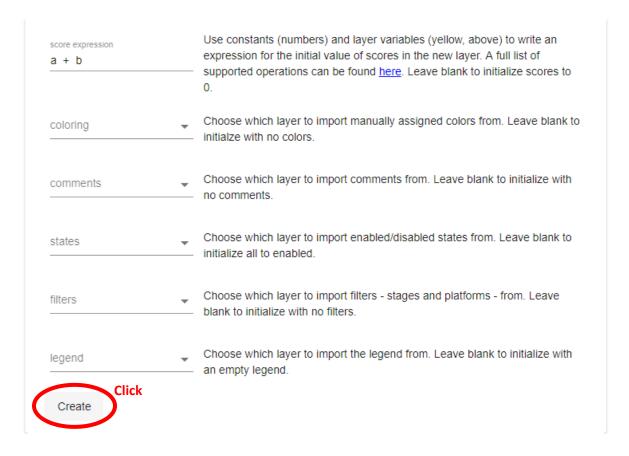
Now that you have two layers, you want to combine them. You will again click the plus sign to create a new layer



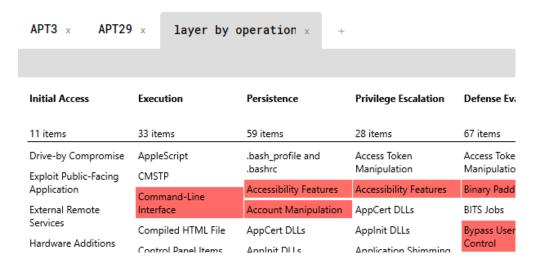
But this time you will select the option to "Create Layer from other layers" to expand the dropdown. When you expand the dropdown, Navigator helpfully gives letter names for each of your existing layers in yellow. So, you know that Navigator identifies your APT3 layer as "a" and your APT29 layer as "b." 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.



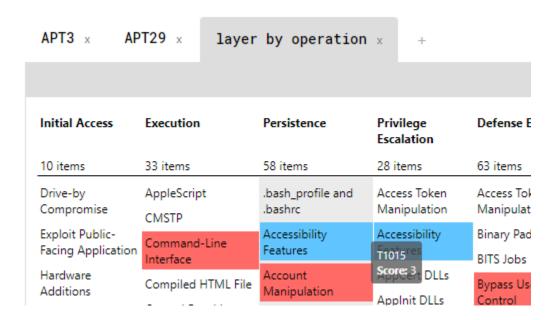
To create the layer, you'll click the "Create" button at the bottom of the section.



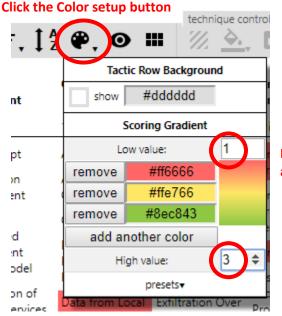
Now you have your combined layer. Initially, all the techniques will appear with the same color:



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).

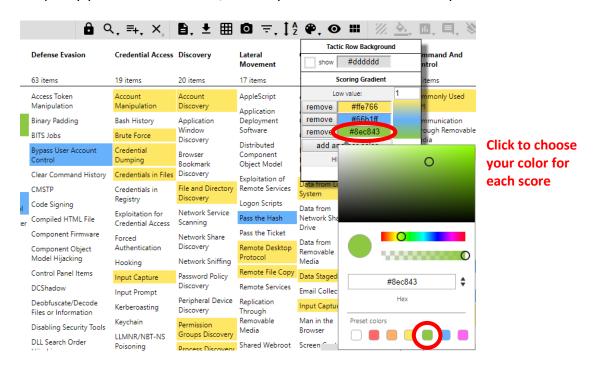


You can change the colors that appear for each score by clicking the "Color setup" button. You know the values are 1, 2, and 3, so make the low value 1 and the high value 3. Navigator knows 2 is halfway between 1 and 3 so will automatically use the middle color for the value of 2.



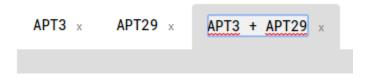
Enter 1 as a low value and 3 as a high value

Now you can choose the colors you want for each layer. You choose to make 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.

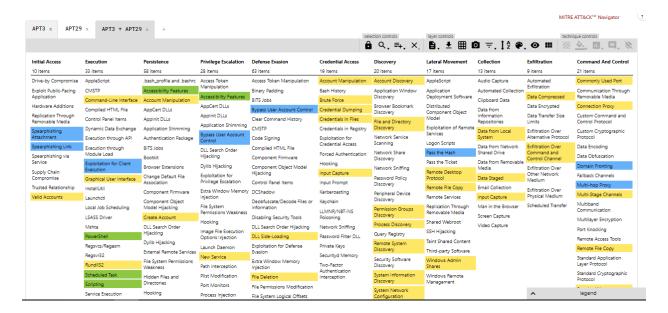


©2019 The MITRE Corporation. ALL RIGHTS RESERVED Approved for public release. Distribution unlimited 18-1528-38.

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



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



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.

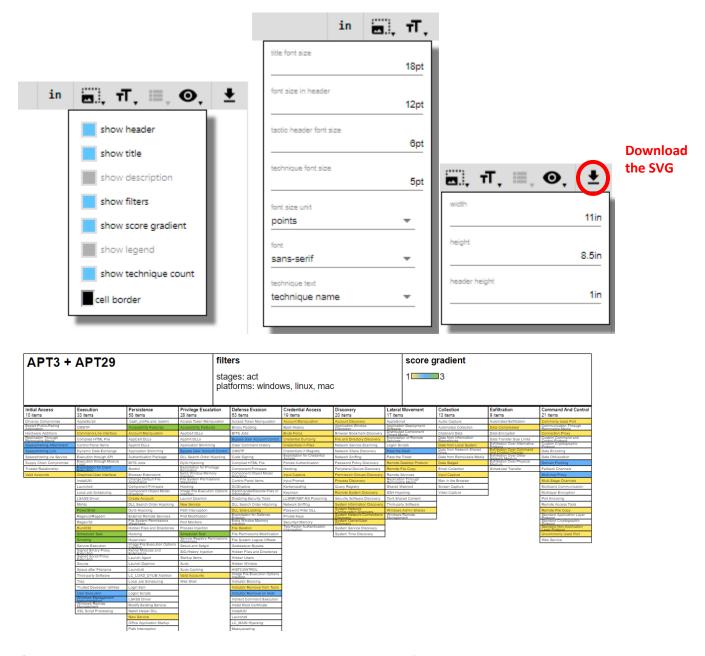


©2019 The MITRE Corporation. ALL RIGHTS RESERVED Approved for public release. Distribution unlimited 18-1528-38.

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.

