Vertex

Synapse Bootcamp - Module 13

More Fun with Power-Ups - Exercises

Objectives

In these exercises you will:

- Run Power-Up Storm commands using the Storm Query Bar
- Use command options to change the default behavior of Power-Ups
- Use the FileParser Power-Up to parse indicators from a file
- Use the synapse-mitre-attack Power-Up

> **Note:** We are constantly updating Synapse and its Power-Ups! We do our best to make sure our course documents (slides, exercises, and answer keys) are up-to-date. However, you may notice small differences (such as between a screen capture in the documents and the appearance of your current instance of Synapse).
>
> If something is unclear or if you identify an error, please reach out to us so we can assist!

Exercises

- All exercises use the **Research Tool** with the **Storm Mode Selector** set to **Storm mode.**
- Some example queries may wrap due to length.

- In the **Console Tool,** click the **Storm Query Bar Menu** and select **Clear console:**

Power-Up Command Options

Exercise 1

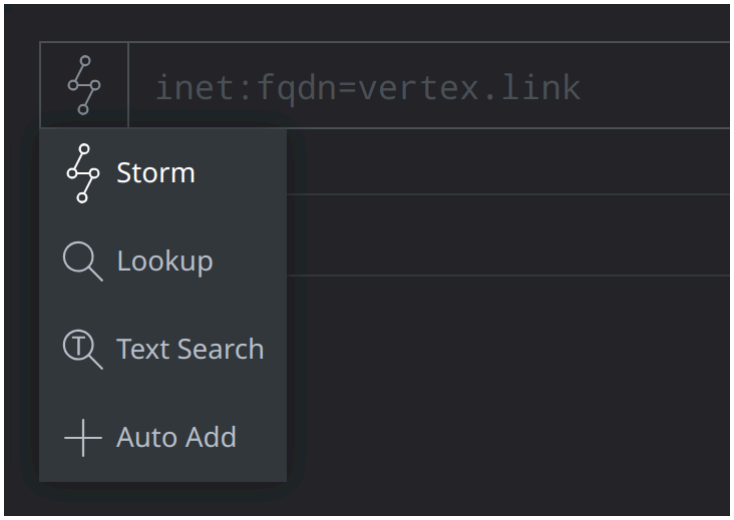
Objective:

- **Run Power-Up Storm commands using the Storm Query Bar.**
- **Understand how the use of different options affects command behavior.**

You are researching an FQDN associated with the ShadowPad malware family and want to retrieve passive DNS data for the domain.

Part 1 - View the FQDN and existing connections

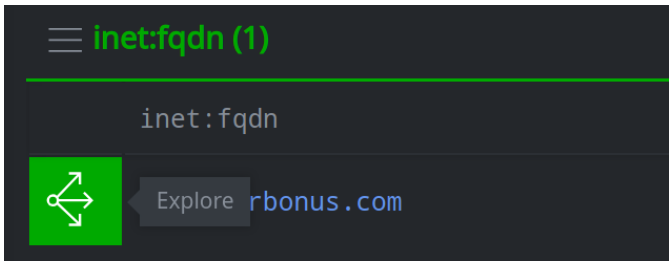
- In the **Research Tool,** ensure your **Storm Query Bar** is in **Storm mode:**



- Enter the following in the **Storm Query Bar** and press **Enter** to lift the FQDN:

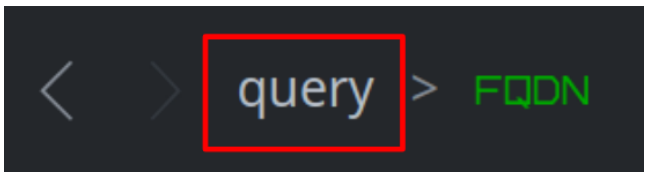
```
inet:fqdn=goest.mrbonus.com
```

- Click the **Explore** button next to the FQDN to view adjacent nodes:



Note that there are very few nodes currently "connected" to the FQDN.

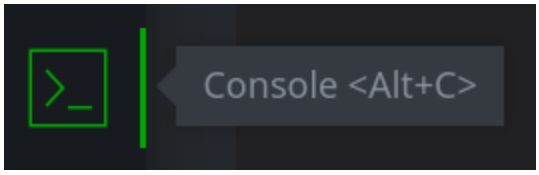
- In your **breadcrumbs,** click **query** to return to your original query:



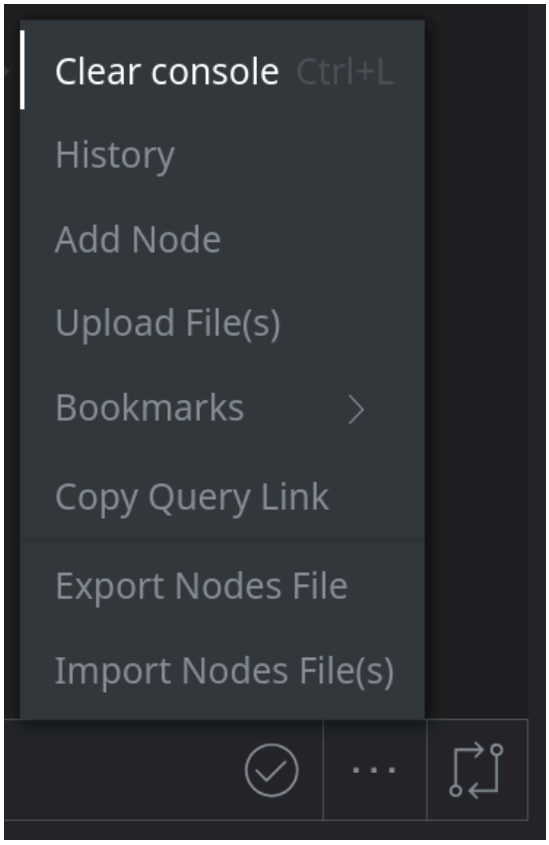
Part 2 - Clear the Console Tool

You want to use the **--debug** option with the Power-Up command to view status information. To more easily view the debug information, you want to clear the **Console Tool** of any existing output.

- From your **Toolbar,** select the **Console Tool:**

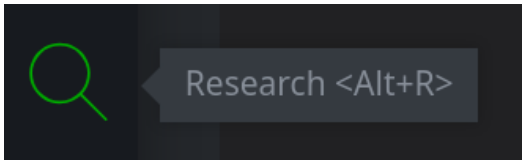


- Click the **Storm Query Bar menu** (the three dots (. . .) or "meatball menu") and select **Clear Console**:



Part 3 - Use Power-Up Storm commands to enrich the FQDN

- From your **Toolbar,** select the **Research Tool:**

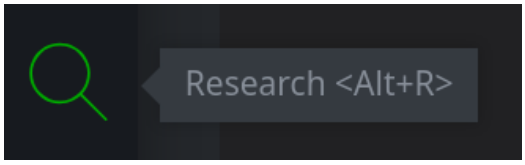


- In the **Query Bar,** enter the following and press **Enter** to run the **virustotal.pdns** Storm command on your FQDN:

```
inet:fqdn=goest.mrbonus.com | virustotal.pdns --debug
```

Question 1: What output is displayed in the Console Tool?

- Return to the **Research Tool:**



Question 2: What node (or nodes) are displayed in the Results Panel after running the query?

Question 3: Did the command return any data? How can you tell?

Question 4: How can you view the data that was returned?

You want to run the same command again, but this time with the `--yield` option in addition to `--debug`.

- In the **Research Tool,** in the **Query Bar,** enter the following and press **Enter** to run the modified query:

```
inet:fqdn=goest.mrbonus.com | virustotal.pdns --debug --yield
```

Question 5: What node (or nodes) are displayed in your Results Panel after running the query?

Power-Ups: FileParser

Exercise 2

Objective:
- **Use the FileParser Power-Up to extract data from a ZIP archive.**

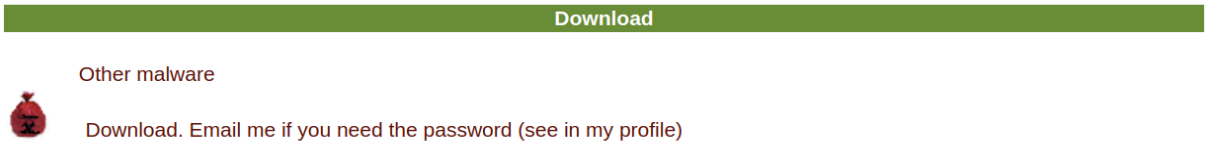
Mila Parkour's **Contagio** blog historically reported on threats and provided samples of related malware for download.

You want to retrieve and parse a set of malware samples using the FileParser Power-Up.

- In your web browser, view the following Contagio blog post:

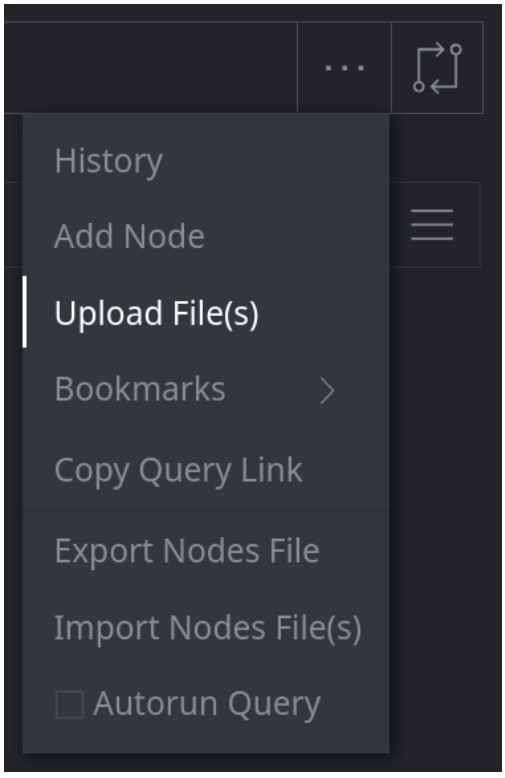
http://contagiodump.blogspot.com/2019/12/apt-calypso-rat-flying-dutchman-samples.html

The blog post contains a link to download the associated samples:



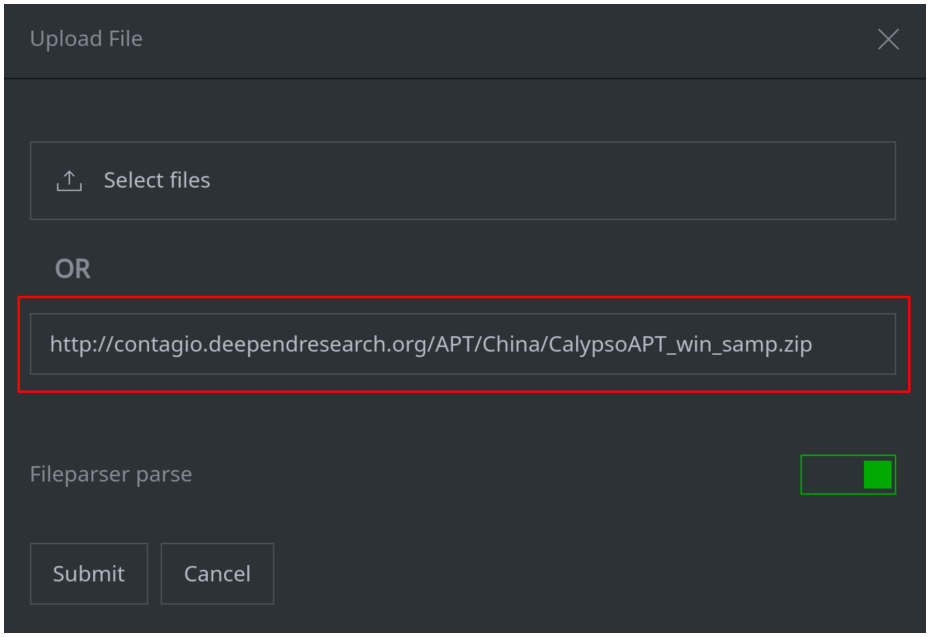
We'll use Synapse's **File Upload** feature to retrieve the file.

- From the **Storm Query Bar meatball menu,** select **Upload File(s):**

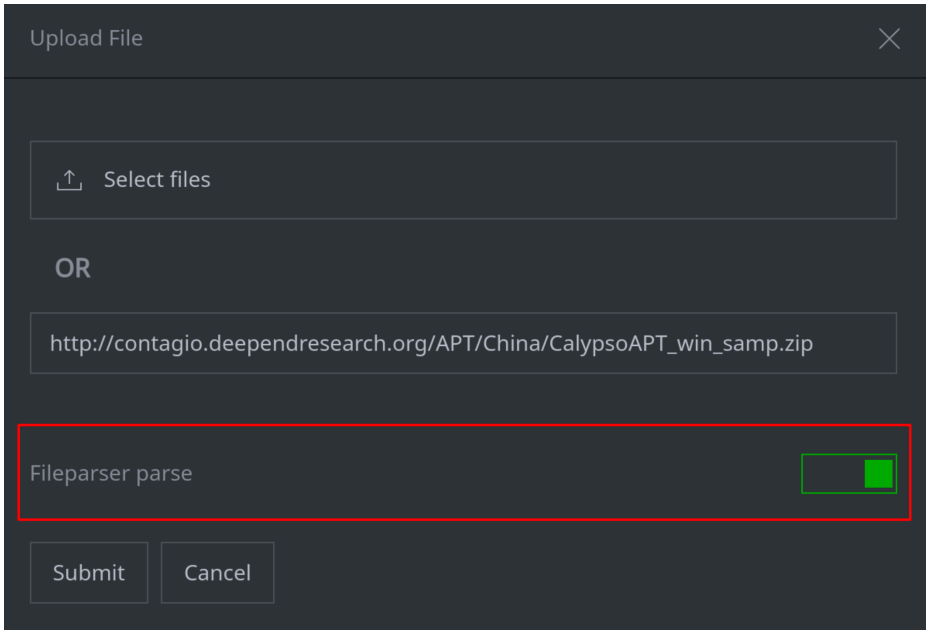


- In the **Upload file** dialog, enter the URL for the zip archive to download:

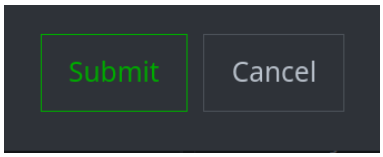
```
http://contagio.deependresearch.org/APT/China/CalypsoAPT_win_samp.zip
```



- Make sure the **FileParser parse** toggle is **ON:**



- Click **Submit** to retrieve the file:



Question 1: What is displayed in your Results Panel after retrieving the file?

Question 2: Are any notifications available from the Console Tool?

FileParser could not parse the encrypted zip file. You can run the **`fileparser.parse`** command manually to extract the contents.

Contagio uses **`infected666`** plus the **last character of the zip file name** (in this case, "**p**" from "CalypsoAPT_win_sam**p**.zip") as their password convention.

- Your **Storm Query Bar** should already contain a lift command that references the **`file:bytes`** node:

```
file:bytes='sha256:087a9bdbf11e03ba31c983155287e6c178643967dfe20f4cd672833f900da5b1'
```

- **Add** the highlighted text to your query and press **Enter** to run FileParser with the specified password:

```
file:bytes=sha256:087a9bdbf11e03ba31c983155287e6c178643967dfe20
f4cd672833f900da5b1 | fileparser.parse --passwd infected666p
```

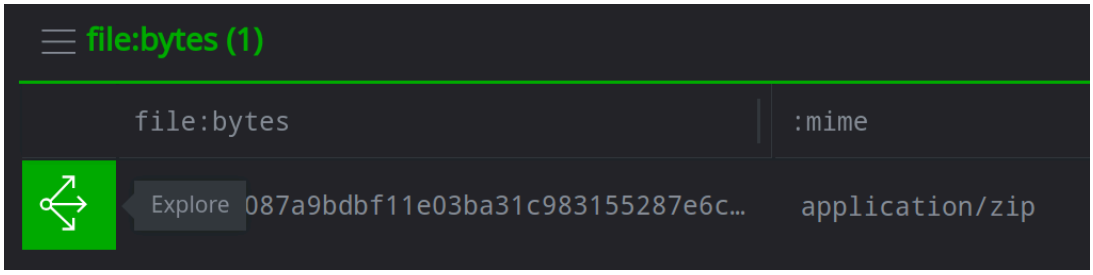
Note: The exercise PDFs may insert line breaks or spaces where values (such as the file above) are forced to wrap. If you copy the above into your Storm query bar and the query fails to run, you may need to manually remove the space / break.

Question 3: What is displayed in your Results Panel?

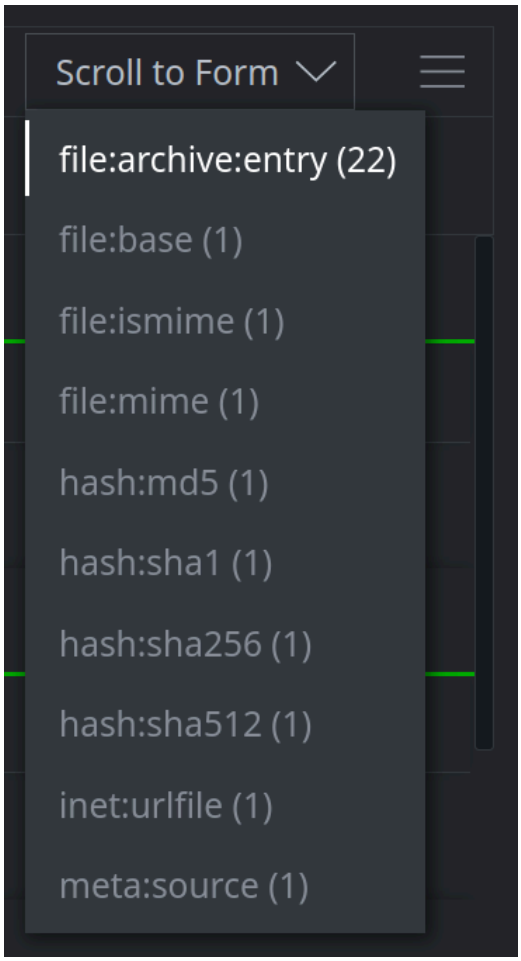
Question 4: Was FileParser able to extract the files?

Now you want to view the extracted files.

- In the **Results Panel,** select the **`file:bytes`** node and click the **Explore** button to display adjacent nodes:

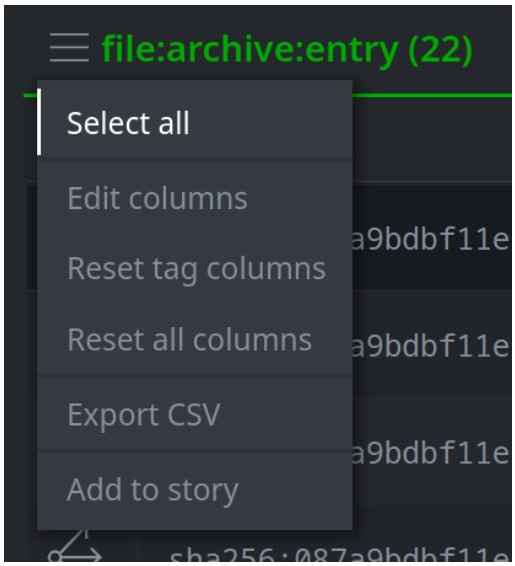


- Use **Scroll to Form** to navigate to the **`file:archive:entry`** nodes:



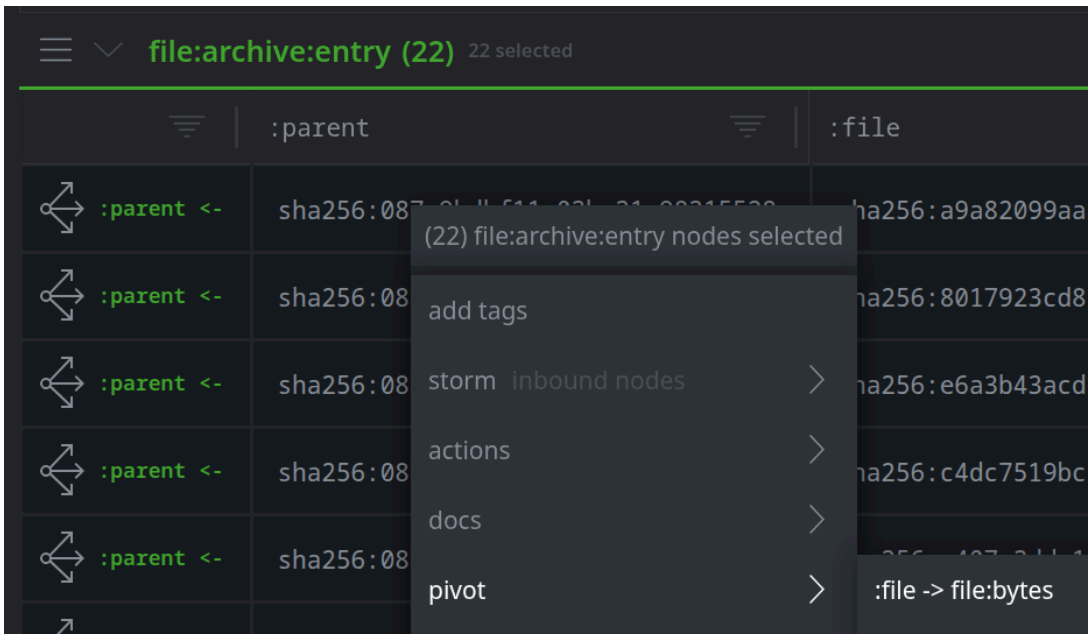
The **`file:archive:entry`** form is used to represent a file and associated metadata contained within an archive (such as a ZIP archive).

- Click the **hamburger menu** next to the **file:archive:entry** header and choose **Select all:**



- We're only interested in the **extracted** files so we'll use the **pivot** menu option.

  Right-click any selected node and choose **pivot > :file -> file:bytes:**



Question 5: How many files were extracted?

Question 6: Did FileParser **also** parse those files? How can you tell?

Power-Ups: synapse-mitre-attack

Exercise 3

Objective:
- **View and navigate MITRE ATT&CK data.**

Part 1

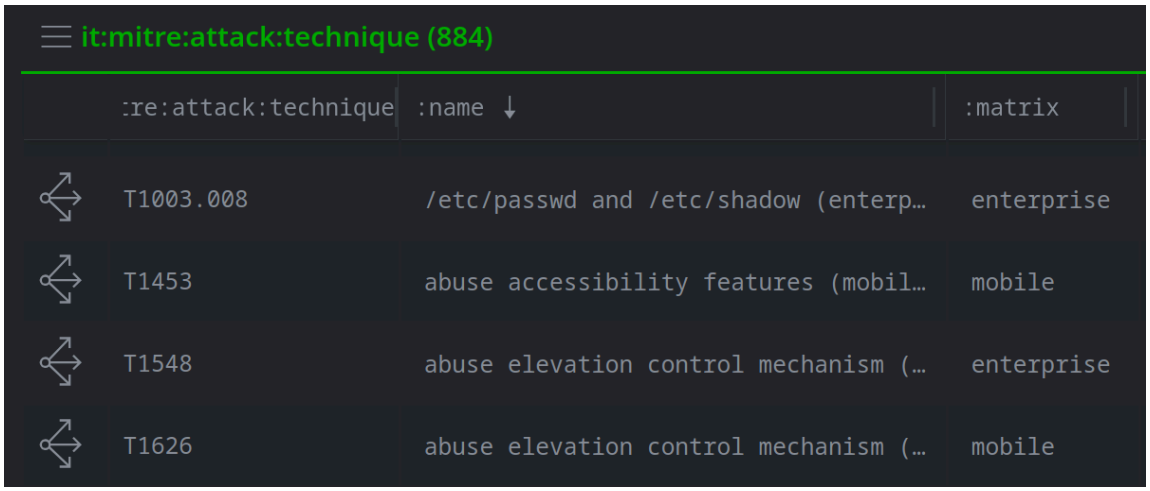
You want to view information related to MITRE ATT&CK Techniques.

- In the **Research Tool,** enter the following in your **Storm Query Bar** and press **Enter** to lift the MITRE ATT&CK Techniques:

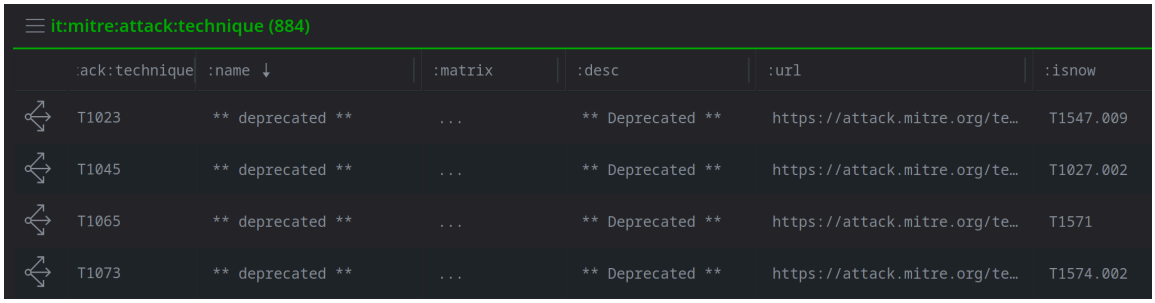
```
it:mitre:attack:technique
```

- **Browse** the available Techniques. Note that:

  Each technique is associated with an ATT&CK Matrix (Enterprise, ICS, Mobile):



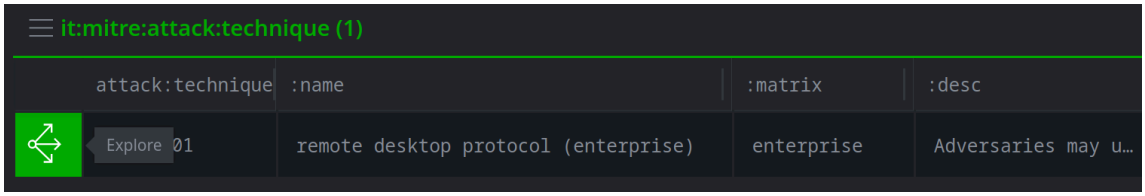
Some Techniques are **deprecated** by MITRE. If the Technique has a one-to-one replacement, the new Technique is listed in the **`:isnow`** property:



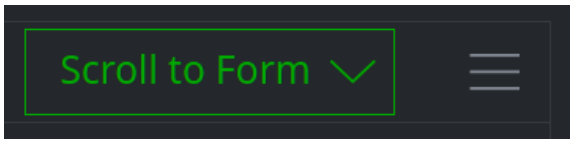
- Enter the following in your **Storm Query Bar** and press **Enter** to run the query:

```
it:mitre:attack:technique=T1021.001
```

- In the **Results Panel,** click the **Explore** button next to the node to display adjacent nodes:

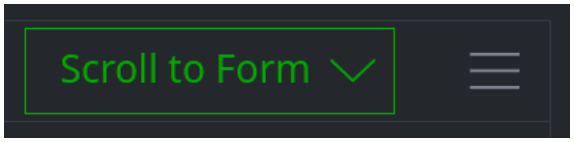


- Click the **Scroll to Form** button and select **it:mitre:attack:group**:



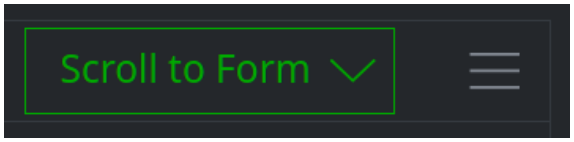
Question 1: According to MITRE, how many threat groups use this technique?

- Click the **Scroll to Form** button and select **it:mitre:attack:mitigation**:



Question 2: According to MITRE, what mitigations are available for this technique?

- Click the **Scroll to Form** button and select **media:news**:



Question 3: How many articles in Synapse reference or describe the use of this technique?

Part 2

You know that some researchers use the word "bear" to name threats associated with Russia. You want to know how many threat names in Synapse include the word "bear".

In Synapse, threat names are organization names (**`ou:name`** nodes).

- Enter the following in your **Storm Query Bar** and press **Enter** to view the **`ou:name`** nodes that contain the string "bear":

```
ou:name~=bear
```

Question 4: How many names are there?

You want to view MITRE ATT&CK information related to these groups.

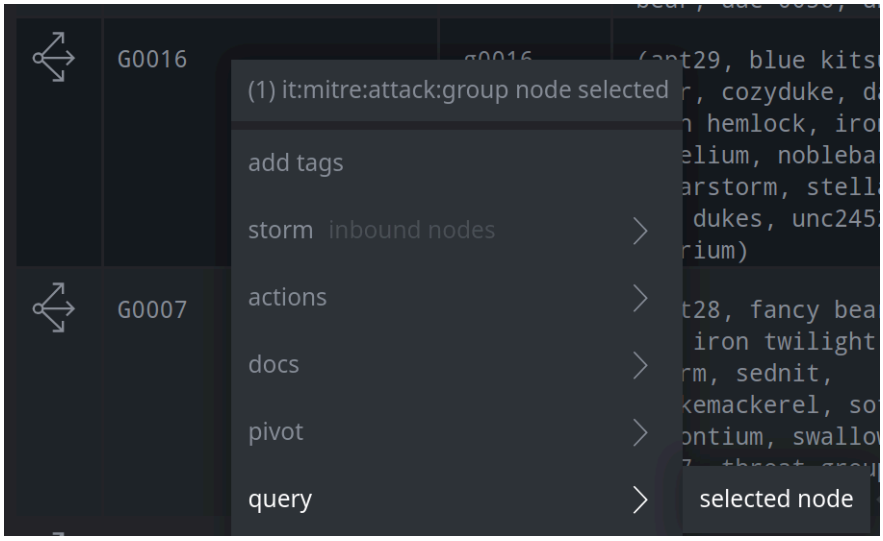
- Enter the following in your **Storm Query Bar** and press **Enter** to **pivot** from the **`ou:name`** nodes to any associated **`it:mitre:attack:group`** nodes:

```
ou:name~=bear -> it:mitre:attack:group | uniq
```

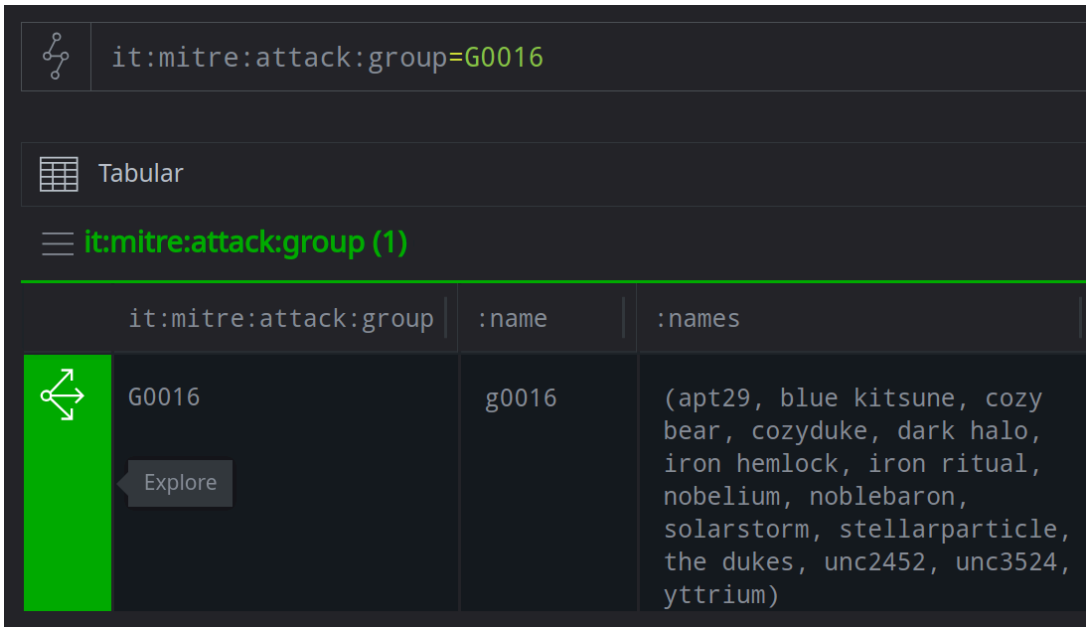
Question 5: How many MITRE ATT&CK Groups are there?

You want to view more detailed information on MITRE Group G0016 (Cozy Bear / APT29 / etc.)

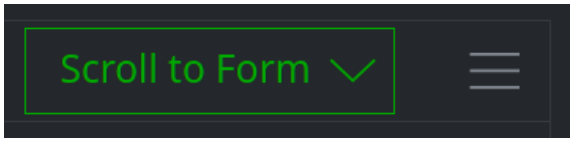
- In the **Results Panel,** locate the **`it:mitre:attack:group`** for group **G0016. Right-click** the node and select **query > selected node** from the menu:



- In the **Results Panel,** click the **Explore** button next to the group to navigate to adjacent nodes:

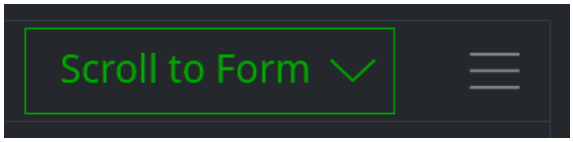


- Use **Scroll to form** to navigate to the **`ou:name`** nodes:



Question 6: According to MITRE, how many different names are associated with this group?

- Use **Scroll to form** to navigate to the `it:mitre:attack:technique` nodes:



Question 7: According to MITRE, how many techniques are used by this group?

Part 3

If time allows, complete the following additional exercise.

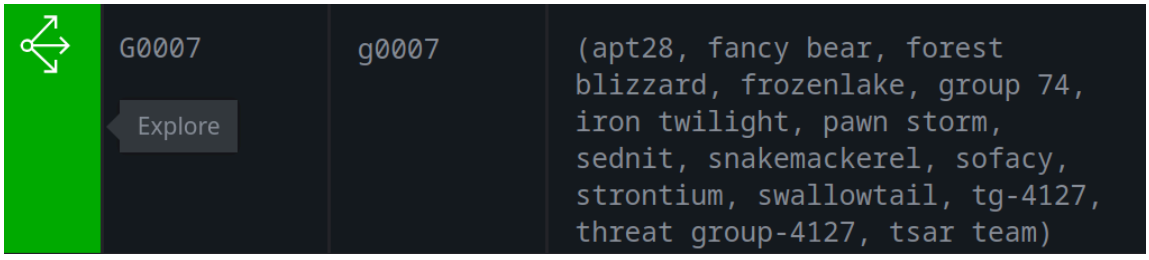
You want to look at the similarities between G0016 (Cozy Bear / APT29) and G0007 (Fancy Bear / APT28).

- In your **Storm Query Bar,** enter the following to **lift** the two groups and press **Enter** to run the query:

```
it:mitre:attack:group=G0016 it:mitre:attack:group=G0007
```

In the previous exercise, viewed the techniques that MITRE associates with Cozy Bear (G0016). You want to see the techniques associated with Fancy Bear (G0007).

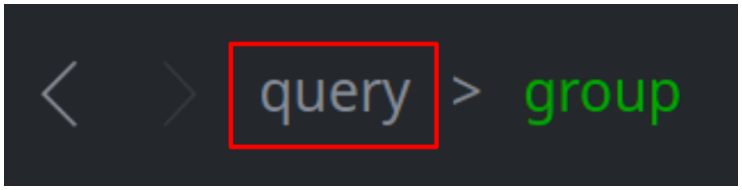
- In the **Results Panel,** locate **G0007.** Click the **Explore** button next to the group to navigate to adjacent nodes:



Question 8: According to MITRE, how many techniques are used by this group?

You want to see the techniques that these groups **share in common.** We can use the Storm **intersect** command to find this information.

- In your **breadcrumbs,** click **query** to return to your original query:



- In the **Query Bar, add** the highlighted text and press **Enter** to run the query:

```
it:mitre:attack:group=G0016 it:mitre:attack:group=G0007
   | intersect { -> it:mitre:attack:technique }
```

Question 9: How many techniques do the groups share in common?
