Synapse Bootcamp - Module 8

Intro to Storm - Exercises

Objectives

In these exercises you will:

- Use Storm to perform simple lift operations
- Use Storm to lift using mathematical operators
- Use Storm to lift using extended operators

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.

The **Storm Quick Reference** guides on **Lifts** and **Basic Operations** (included with the supplemental materials provided for this course) may be helpful for this (and future) exercises.

The online **lift** reference includes detailed documentation and examples for all lift operations. It is part of the Storm Reference included with the Synapse User Guide.

Basic Lifts

Exercise 1

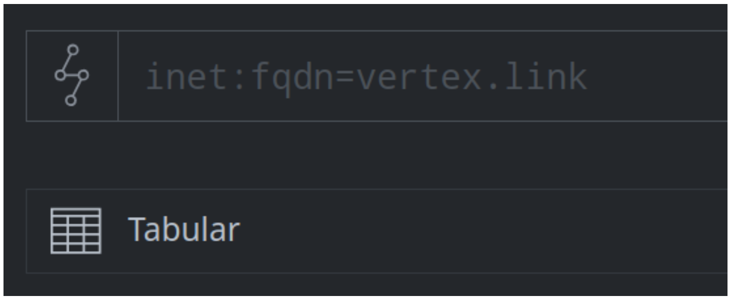
Objective:
- **Use Storm to perform basic lift operations.**

Part 1

In Module 2 (Exploring Data in Synapse), we practiced **lifting** nodes by entering common indicators into the **Storm Query Bar** using **Lookup mode.**

Here we will learn how to lift those same nodes in **Storm mode** using Storm.

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



- Below are some of the indicators we worked with in Module 2 using Lookup mode:

```
50.2.160.146
```

```
d41d8cd98f00b204e9800998ecf8427e
```

```
mfa.cdep[@]mfa.gov.lv
```

```
hxxps://45.154.14[.]235/2023/PotPlayer.exe
```

The values represent an IP address, an MD5 hash, an email address, and a URL.

Question 1: How would you **lift** each of these nodes using **Storm?**

Part 2

You are investigating a suspicious IP address and want to know what domains have resolved to the IP:

```
46.37.164.184
```

In Lookup mode, you could enter the IPv4 and use the **Explore** button to navigate to the DNS A records (`inet:dns:a` nodes).

Instead you want to use Storm to lift the `inet:dns:a` records for this IPv4 address **directly.**

Question 2: Using Storm, how can you lift the `inet:dns:a` nodes for IPv4 `46.37.164.184`?

Part 3

The Synapse NetTools Power-Up retrieves IP netblock whois data (netblock registration data) and records it using an `inet:whois:iprec` form. You want to browse the network registration data in Synapse. You aren't looking for any network in particular - you just want to see the current data.

Question 3: How can you use Storm to lift **all** of the network whois data (**`inet:whois:iprec`** nodes) in Synapse?

Part 4

You are investigating the threat group Brass Typhoon and want to see all the nodes in Synapse that Microsoft says are related to this group.

(We use the tag **`rep.microsoft.brass_typhoon`** to indicate nodes Microsoft associates with this group.)

Question 4: How can you use Storm to lift all of the nodes that Microsoft says are associated with Brass Typhoon?

Question 5: How can you **modify** your Storm query to only lift the **domains** Microsoft says are associated with Brass Typhoon?

Lifts with Mathematical Operators

Exercise 2

Objective:

- **Use mathematical operators to perform lifts with Storm.**

You are searching for potentially malicious files and are looking for unusually large files (**`file:bytes`** nodes), which may be ignored by some antivirus / antimalware products.

Question 1: How can you use Storm to lift all of the files (**`file:bytes`** nodes) whose size is larger than 5 MB? (**Note:** use **5000000** bytes as an approximation for 5 MB.)

Question 2: How many files are there?

Lifts with Extended Operators

Exercise 3

Objective:

- **Use Storm's extended operators to perform custom lifts.**

Part 1

You want to see all of the IPv4 addresses in Synapse that are located in South Korea.

The geolocation information stored in the `:loc` property for IPv4 nodes is a dotted string, and the values may vary depending on the data source. Some may simply read '**kr**', but others may have values like '**kr.gyeonggi.goyang-si**'

Question 1: How can you use Storm to lift all of the IPv4 nodes whose **`:loc`** property **starts with** 'kr'?

Question 2: How many IPv4 addresses are there?

Part 2

You are investigating an incident that occurred in March 2020. You are hunting for malware samples that were compiled during that time period (March 1, 2020 through March 31, 2020) that may be related to the incident.

Question 3: How can you use Storm to lift all of the files (**`file:bytes`**) nodes whose compile time (**`:mime:pe:compiled`**) is between **2020/03/01** and **2020/03/31**?

Question 4: How many files are there?