Synapse Bootcamp - Module 13

More Fun with Power-Ups - Answer Key

More Fun with Power-Ups - Answer Key **1**

Answer Key **2**

Power-Up Command Options 2

Exercise 1 Answer 2

Power-Ups: FileParser 6

Exercise 2 Answer 6

Power-Ups: synapse-mitre-attack 9

Exercise 3 Answer 9

Answer Key

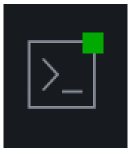
Power-Up Command Options

Exercise 1 Answer

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

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

- The Console Tool has a blinking green square to show there are status messages:



- The Console Tool displays the following output (text wraps):

```
VirusTotal: querying url
https://www.virustotal.com/api/v3/domains/goest.mrbonus.com/res
olutions with params {'limit': 40}
virustotal._relationship: Retrieving resolutions (6 total).
```

The `--debug` output includes:
- The API URL queried.
- The parameters passed with the query (in this example, **`'limit': '40'`**).
- The VirusTotal endpoint queried.
- The number of results returned.

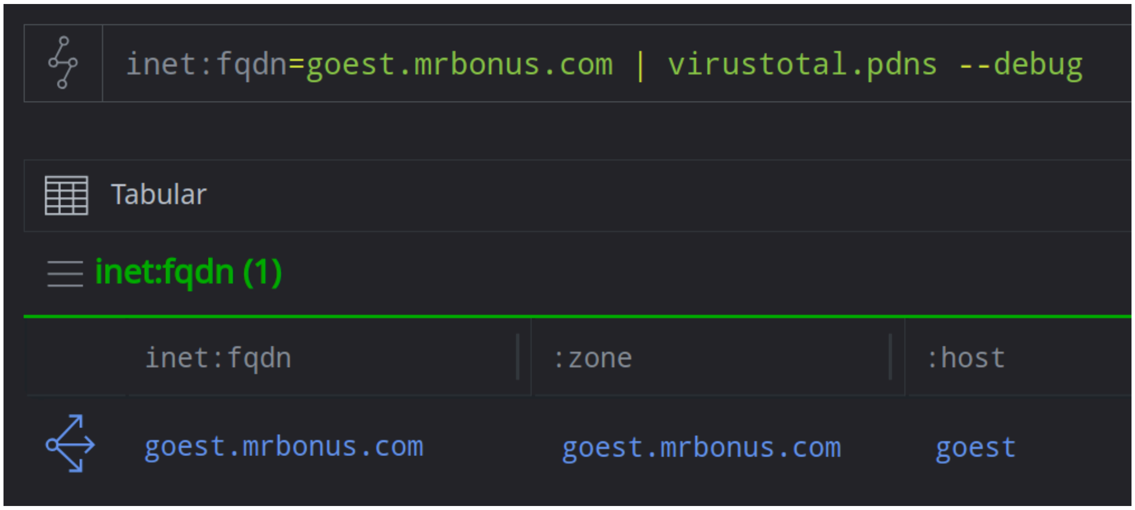
Note that the debug information shows that the **virustotal.pdns** command uses a default **limit** of **40** results. This can be overridden with the **`--size`** parameter if needed. For example:

```
inet:fqdn=goest.mrbonus.com | virustotal.pdns --size 5
```

```
inet:fqdn=goest.mrbonus.com | virustotal.pdns --size 100
```

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

- The Results Panel displays your original node:



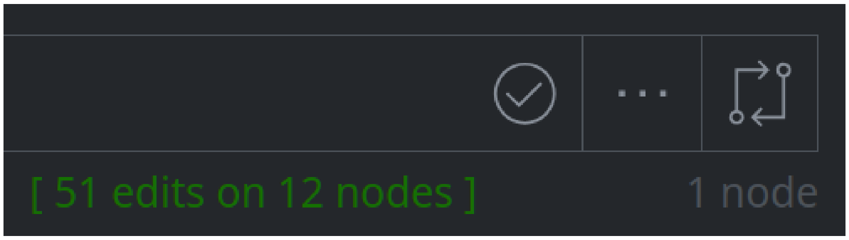
```
inet:fqdn=goest.mrbonus.com | virustotal.pdns --debug
```

inet:fqdn (1)

inet:fqdn	:zone	:host
goest.mrbonus.com	goest.mrbonus.com	goest

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

- Yes, the command returned data. Synapse indicates that there were edits made:



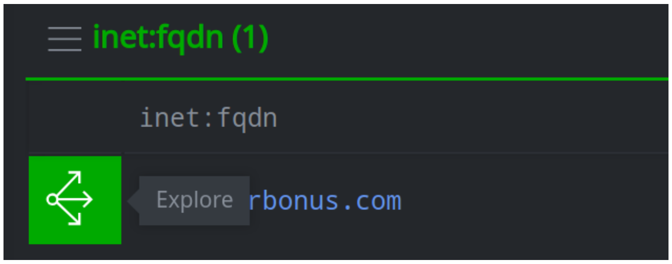
[51 edits on 12 nodes]

1 node

In addition, the **--debug** output (above) indicates there were results ('6 total') returned.

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

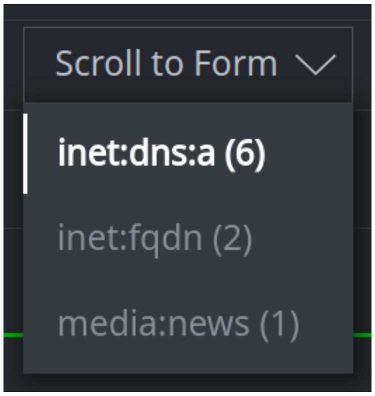
- Use the **Explore** button next to the FQDN to view adjacent nodes:


inet:fqdn (1)

inet:fqdn

Explore rbonus.com

The new results include the DNS A (**inet:dns:a**) nodes created by the **virustotal.pdns** Storm command:

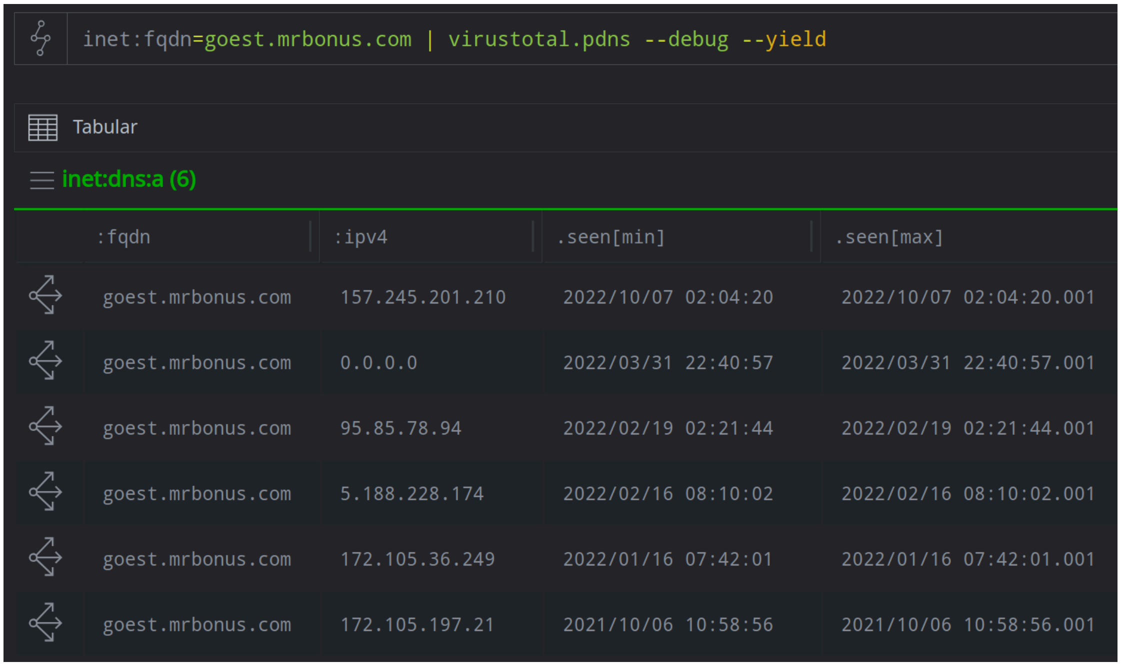


- You can also use Storm to **pivot** from the FQDN to the **inet:dns:a** nodes:

```
inet:fqdn=goest.mrbonus.com -> inet:dns:a
```

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

- The Results Panel displays the DNS A records (**`inet:dns:a`** nodes) returned by VirusTotal:



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

inet:dns:a (6)

	:fqdn	:ipv4	.seen[min]	.seen[max]
	goest.mrbonus.com	157.245.201.210	2022/10/07 02:04:20	2022/10/07 02:04:20.001
	goest.mrbonus.com	0.0.0.0	2022/03/31 22:40:57	2022/03/31 22:40:57.001
	goest.mrbonus.com	95.85.78.94	2022/02/19 02:21:44	2022/02/19 02:21:44.001
	goest.mrbonus.com	5.188.228.174	2022/02/16 08:10:02	2022/02/16 08:10:02.001
	goest.mrbonus.com	172.105.36.249	2022/01/16 07:42:01	2022/01/16 07:42:01.001
	goest.mrbonus.com	172.105.197.21	2021/10/06 10:58:56	2021/10/06 10:58:56.001

Note: By default, Power-Up commands return your **original** node(s) so that commands can be chained together. For example, you can send a set of nodes through a "pipeline" of several Power-Up commands, where each command enriches the data in some way. (We'll see an example of this later in the course when we discuss Automation!)

The **`--yield`** option displays the "main" node or nodes returned by the command in cases where you want to easily view the primary **results** from the command, instead of your original node(s).

Keep in mind that the **`--yield`** option **only** displays the nodes returned by the command you run (in this case, **`virustotal.pdns`**).

If there are additional DNS A records in Synapse for the FQDN (i.e., from a different source), they would **not** be displayed by **`--yield`**. You would need to pivot (or Explore) from the original FQDN to see all of the associated records.

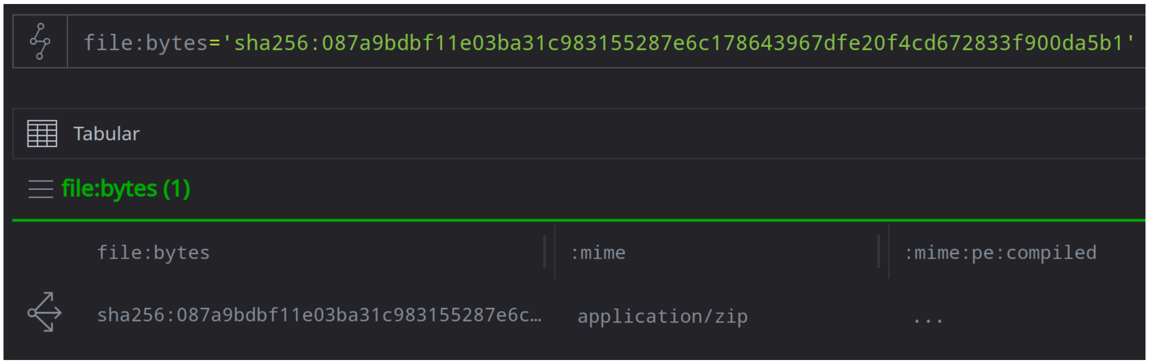
Power-Ups: FileParser

Exercise 2 Answer

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

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

- Synapse displays the **`file:bytes`** node that was downloaded:



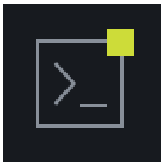
```
file:bytes='sha256:087a9bdbf11e03ba31c983155287e6c178643967dfe20f4cd672833f900da5b1'
```

file:bytes (1)

file:bytes	:mime	:mime:pe:compiled
sha256:087a9bdbf11e03ba31c983155287e6c…	application/zip	...

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

- **Yes.** The Console Tool has a blinking yellow square to indicate a warning message is present:

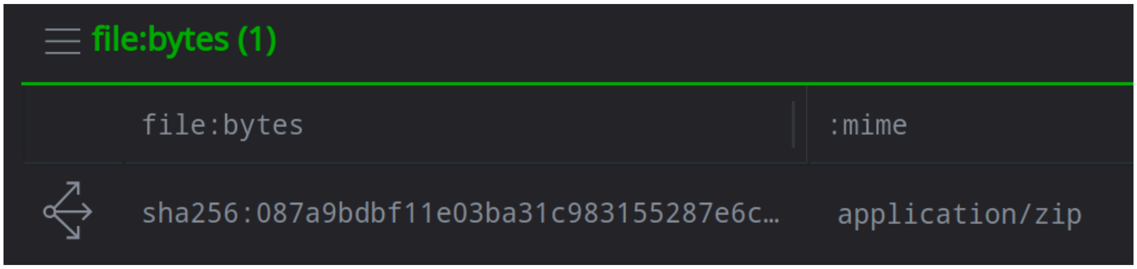


The warning message states that FileParser needs a password to extract the contents:

```
fileparser parsing sha256:
087a9bdbf11e03ba31c983155287e6c178643967dfe20f4cd672833f900da5b1
WARNING: Parse error: Bad password for file
'CalypsoAPT_win_samp/0031c7b63c1e1cd36d55f585d97e2b21a13a19858d5
a1aa5455e5cc64b41e6e9'
```

Question 3: What is displayed in your Results Panel?

- Your original `file:bytes` node is still displayed in the Results Panel:

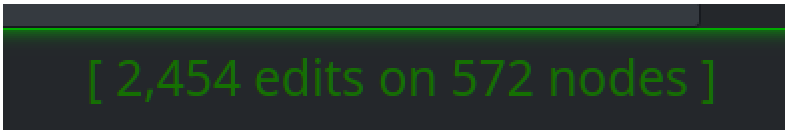


file:bytes (1)

file:bytes	:mime
sha256:087a9bdbf11e03ba31c983155287e6c…	application/zip

Question 4: Was FileParser able to extract the files?

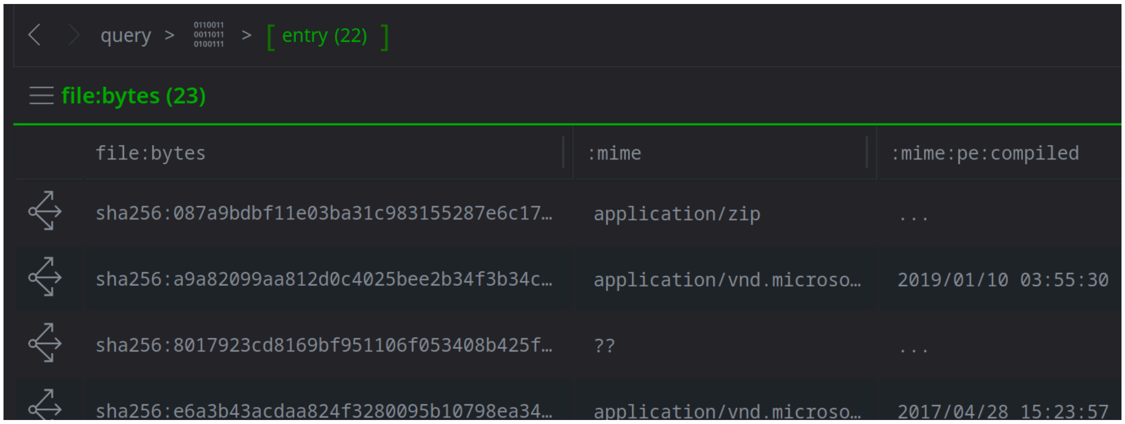
- **Yes.** Synapse's query status shows that several edits were made (the exact number of edits made on your system may vary):



[2,454 edits on 572 nodes]

Question 5: How many files were extracted?

- FileParser extracted **22 files** from the ZIP archive:



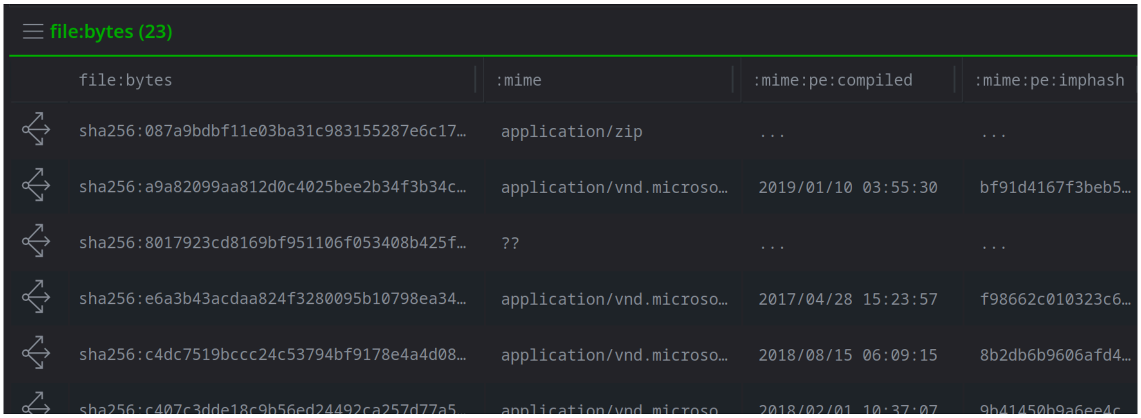
file:bytes (23)

file:bytes	:mime	:mime:pe:compiled
sha256:087a9bdbf11e03ba31c983155287e6c17…	application/zip	...
sha256:a9a82099aa812d0c4025bee2b34f3b34c…	application/vnd.microso…	2019/01/10 03:55:30
sha256:8017923cd8169bf951106f053408b425f…	??	...
sha256:e6a3b43acdaa824f3280095b10798ea34…	application/vnd.microso…	2017/04/28 15:23:57

Note: When you **Explore** from the `file:archive:entry` nodes, Synapse displays a total of 23 files. This includes the "parent" file - the ZIP archive - and the 22 archive "entry" files that were extracted.

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

- **Yes,** FileParser **also** parsed the files that it extracted from the ZIP archive:



file:bytes (23)

file:bytes	:mime	:mime:pe:compiled	:mime:pe:imphash
sha256:087a9bdbf11e03ba31c983155287e6c17…	application/zip	...	...
sha256:a9a82099aa812d0c4025bee2b34f3b34c…	application/vnd.microso…	2019/01/10 03:55:30	bf91d4167f3beb5…
sha256:8017923cd8169bf951106f053408b425f…	??	...	...
sha256:e6a3b43acdaa824f3280095b10798ea34…	application/vnd.microso…	2017/04/28 15:23:57	f98662c010323c6…
sha256:c4dc7519bccc24c53794bf9178e4a4d08…	application/vnd.microso…	2018/08/15 06:09:15	8b2db6b9606afd4…
sha256:c407c3dde18c9b56ed24492ca257d77a5…	application/vnd.microso…	2018/02/01 10:37:07	9b41450b9a6ee4c…

FileParser set additional properties for the `file:bytes` nodes. This includes the `:mime` property (where FileParser was able to identify the MIME type) and properties such as `:mime:pe:compiled`.

Tip: FileParser parses files **recursively** by default. If FileParser identifies additional files "contained" within a file, it will parse those as well. "Contained" may include:

- A zip archive containing compressed files.
- An executable that is signed with a code-signing certificate.
- An RFC822 email message with a base64-encoded attachment.

This behavior can be disabled with the `--no-recurse` option.

Power-Ups: synapse-mitre-attack

Exercise 3 Answer

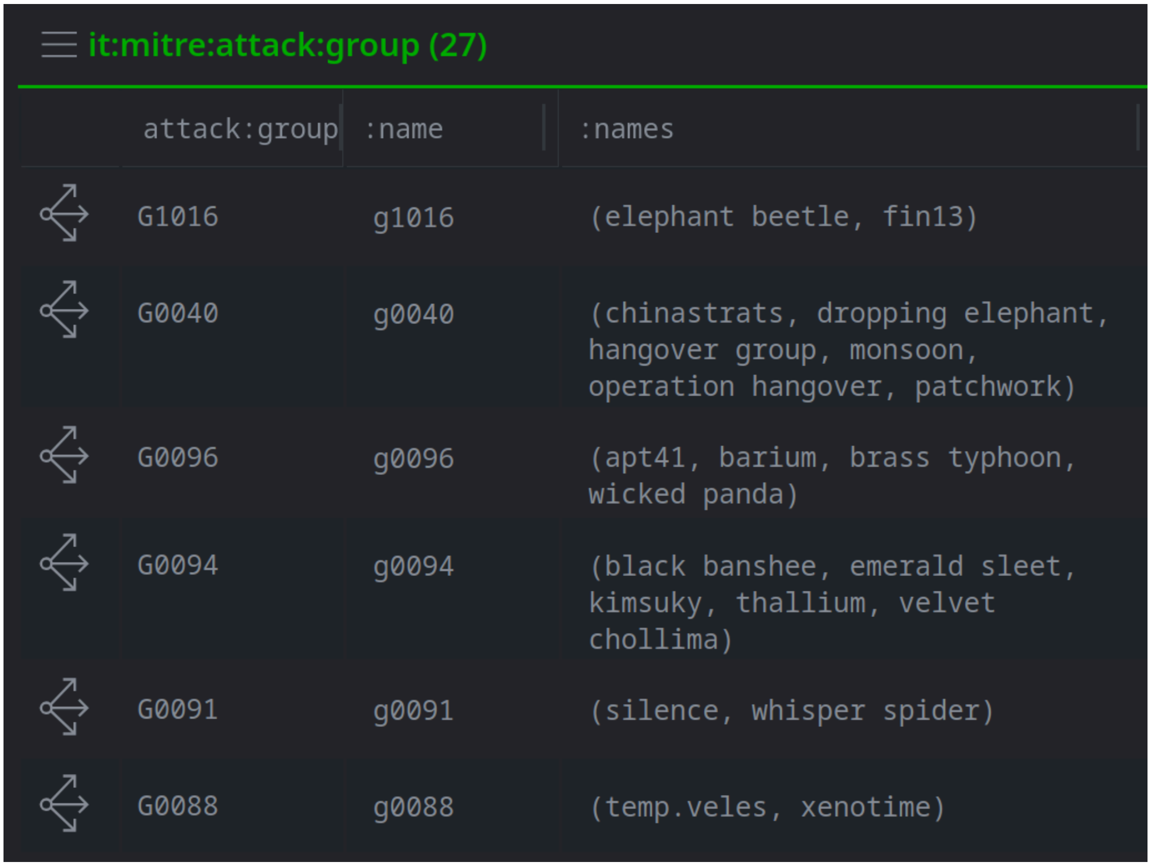
Objective:

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

Part 1

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

- MITRE reports that **27** threat groups (`it:mitre:attack:group`) have used this technique (as of July 2024):

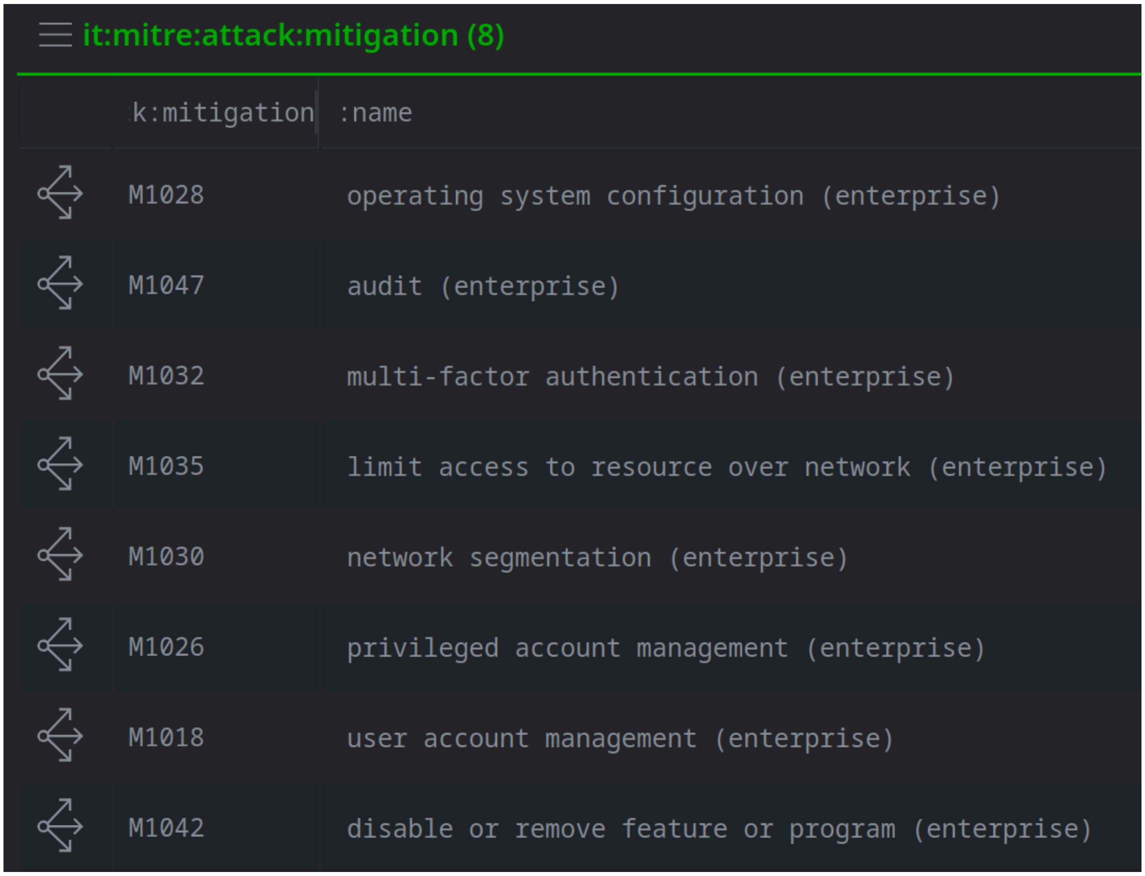


it:mitre:attack:group (27)

attack:group	:name	:names
G1016	g1016	(elephant beetle, fin13)
G0040	g0040	(chinastrats, dropping elephant, hangover group, monsoon, operation hangover, patchwork)
G0096	g0096	(apt41, barium, brass typhoon, wicked panda)
G0094	g0094	(black banshee, emerald sleet, kimsuky, thallium, velvet chollima)
G0091	g0091	(silence, whisper spider)
G0088	g0088	(temp.veles, xenotime)

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

- MITRE lists **8** mitigations (as of July 2024):

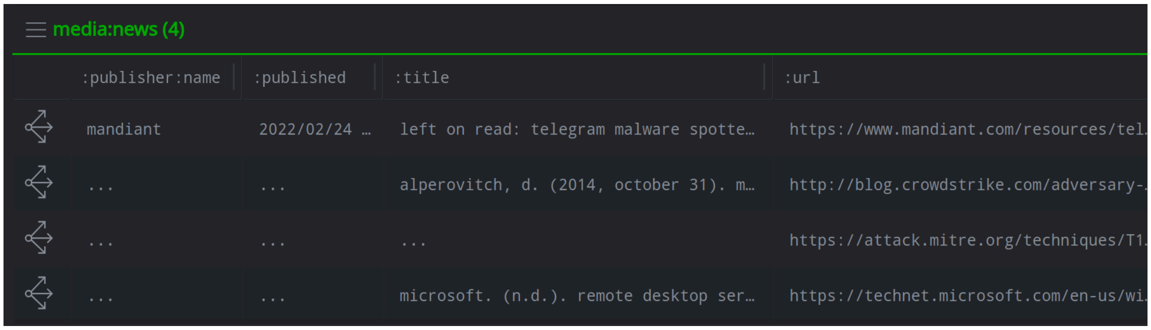


it:mitre:attack:mitigation (8)

k:mitigation	:name
M1028	operating system configuration (enterprise)
M1047	audit (enterprise)
M1032	multi-factor authentication (enterprise)
M1035	limit access to resource over network (enterprise)
M1030	network segmentation (enterprise)
M1026	privileged account management (enterprise)
M1018	user account management (enterprise)
M1042	disable or remove feature or program (enterprise)

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

- **Four** articles reference the technique (as of July 2024):



media:news (4)

:publisher:name	:published	:title	:url
mandiant	2022/02/24 …	left on read: telegram malware spotte…	https://www.mandiant.com/resources/tel…
...	...	alperovitch, d. (2014, october 31). m…	http://blog.crowdstrike.com/adversary-…
...	...	...	https://attack.mitre.org/techniques/T1…
...	...	microsoft. (n.d.). remote desktop ser…	https://technet.microsoft.com/en-us/wi…

The articles include:

  - The MITRE ATT&CK web page for the technique (https://attack.mitre.org/techniques/T1021/001)

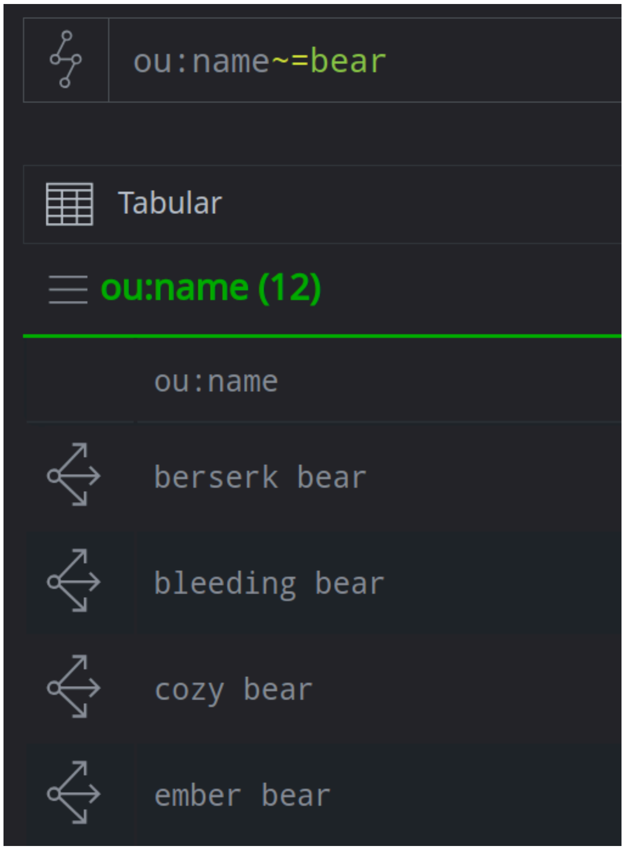
  - Articles **cited** by MITRE in documenting the technique (the Microsoft and CrowdStrike articles).
  - A Mandiant blog that lists ATT&CK Techniques used in the activity described in the report.

> **Tip:** When the synapse-mitre-attack Power-Up is installed, Synapse is able to automatically recognize and extract or "scrape" references to MITRE ATT&CK components (such as "T1021.001") from text. We'll see this feature when we look at the Spotlight Tool!

Part 2

Question 4: How many names are there?

- There are **12** names that include "bear" (as of July 2024):



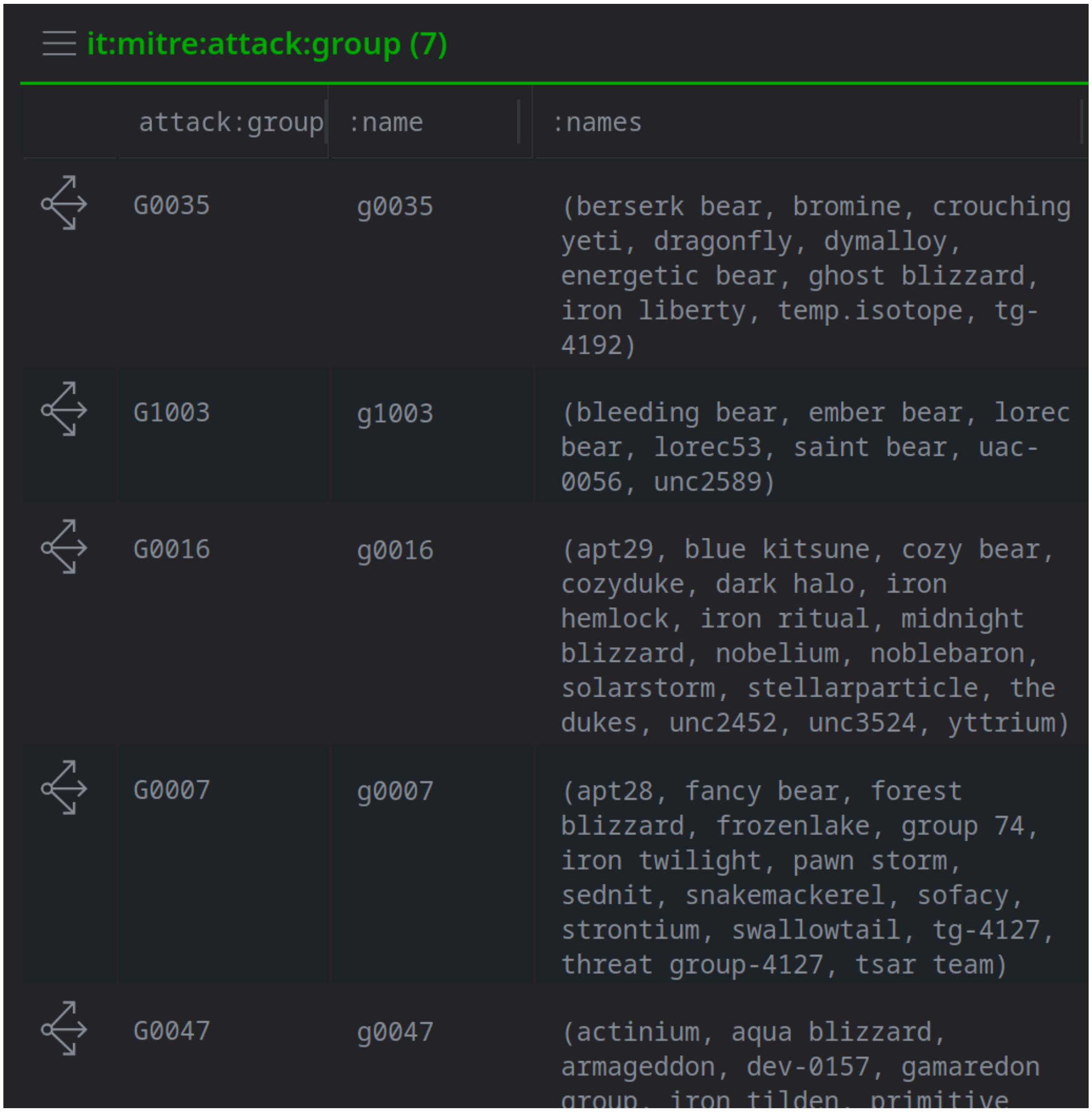
```
ou:name~=bear
```

ou:name (12)

ou:name
berserk bear
bleeding bear
cozy bear
ember bear

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

- There are **7** Groups (as of July 2024):



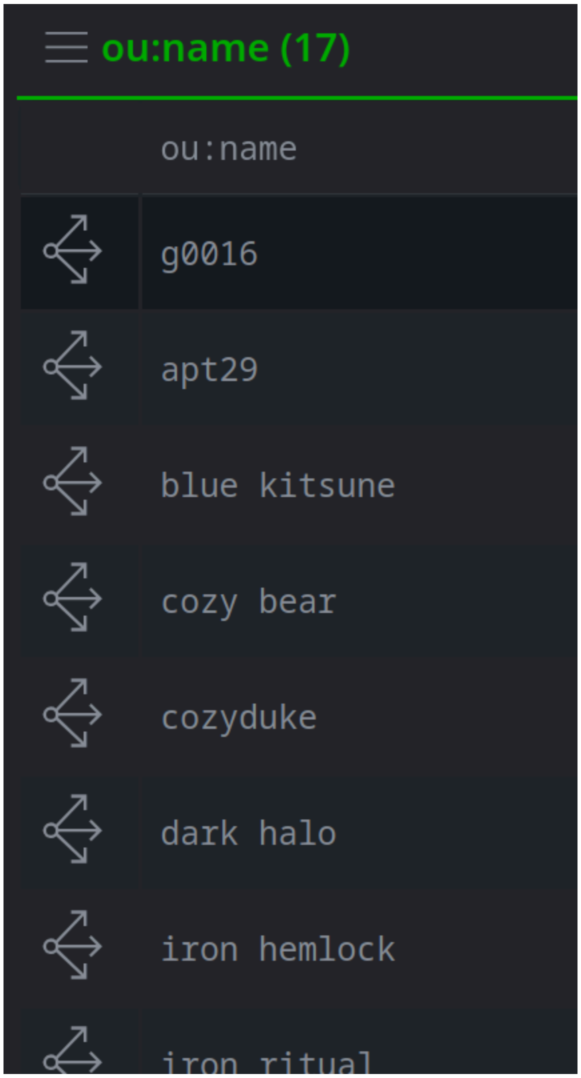
it:mitre:attack:group (7)

attack:group	:name	:names
G0035	g0035	(berserk bear, bromine, crouching yeti, dragonfly, dymalloy, energetic bear, ghost blizzard, iron liberty, temp.isotope, tg-4192)
G1003	g1003	(bleeding bear, ember bear, lorec bear, lorec53, saint bear, uac-0056, unc2589)
G0016	g0016	(apt29, blue kitsune, cozy bear, cozyduke, dark halo, iron hemlock, iron ritual, midnight blizzard, nobelium, noblebaron, solarstorm, stellarparticle, the dukes, unc2452, unc3524, yttrium)
G0007	g0007	(apt28, fancy bear, forest blizzard, frozenlake, group 74, iron twilight, pawn storm, sednit, snakemackerel, sofacy, strontium, swallowtail, tg-4127, threat group-4127, tsar team)
G0047	g0047	(actinium, aqua blizzard, armageddon, dev-0157, gamaredon group, iron tilden, primitive

Note: Some MITRE Groups have more than one "bear" name. For example, G1003 includes the names "bleeding bear", "ember bear", "lorec bear", and "saint bear".

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

- MITRE associates **17** names with this group (as of July 2024):



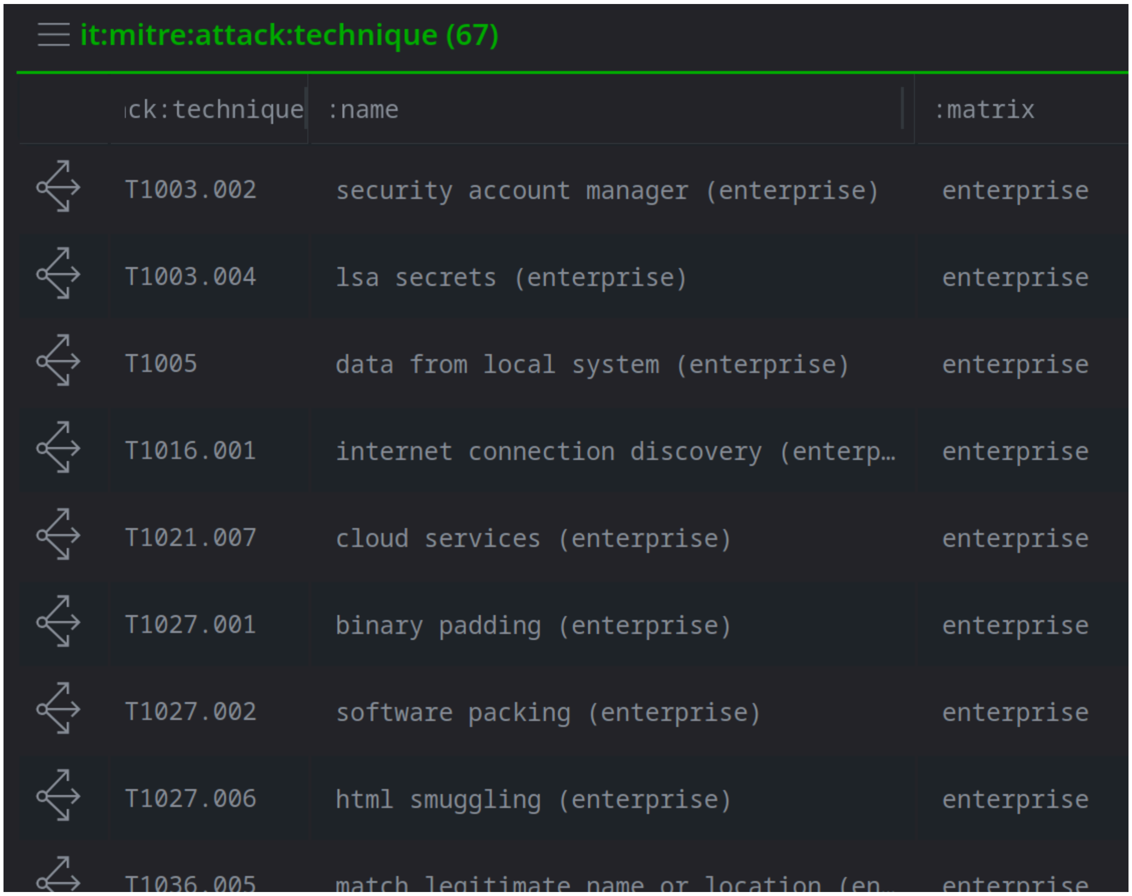
ou:name (17)

ou:name
g0016
apt29
blue kitsune
cozy bear
cozyduke
dark halo
iron hemlock
iron ritual

Note: this includes MITRE's Group designation G0016.

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

- MITRE associates **67** techniques with this group (as of July 2024):



it:mitre:attack:technique (67)

ck:technique	:name	:matrix
T1003.002	security account manager (enterprise)	enterprise
T1003.004	lsa secrets (enterprise)	enterprise
T1005	data from local system (enterprise)	enterprise
T1016.001	internet connection discovery (enterp…	enterprise
T1021.007	cloud services (enterprise)	enterprise
T1027.001	binary padding (enterprise)	enterprise
T1027.002	software packing (enterprise)	enterprise
T1027.006	html smuggling (enterprise)	enterprise
T1036.005	match legitimate name or location (en…	enterprise

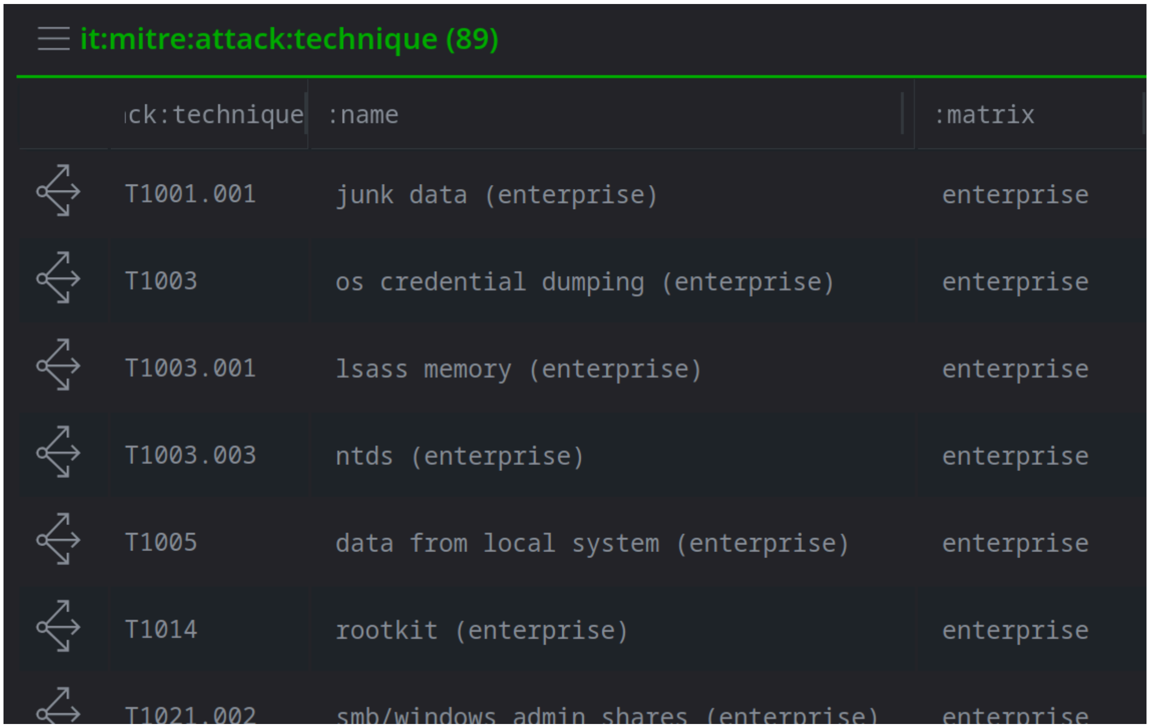
.

Part 3

If time allows, complete the following additional exercise.

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

- MITRE associates **89** techniques with this group (as of July 2024):

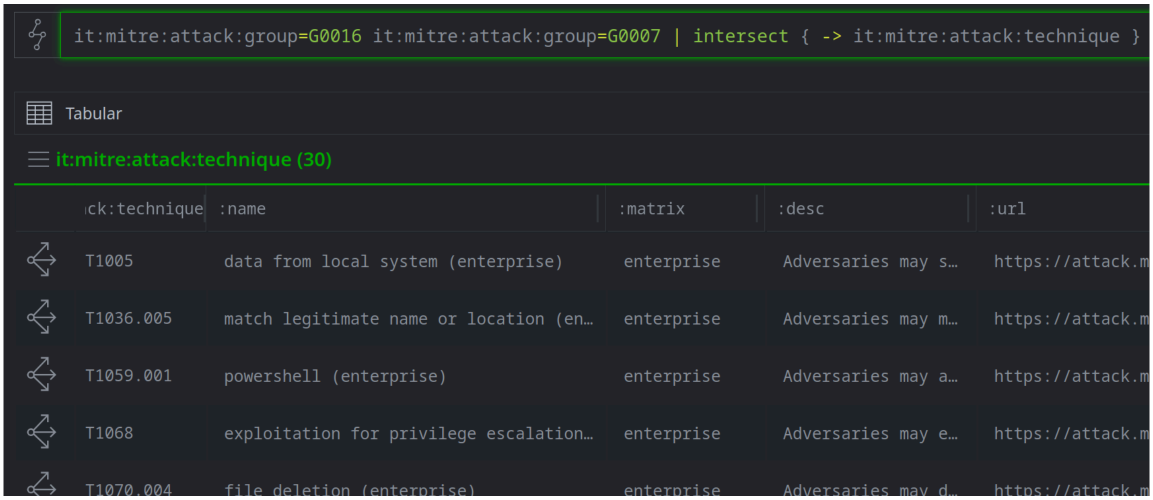


it:mitre:attack:technique (89)

ck:technique	:name	:matrix
T1001.001	junk data (enterprise)	enterprise
T1003	os credential dumping (enterprise)	enterprise
T1003.001	lsass memory (enterprise)	enterprise
T1003.003	ntds (enterprise)	enterprise
T1005	data from local system (enterprise)	enterprise
T1014	rootkit (enterprise)	enterprise
T1021.002	smb/windows admin shares (enterprise)	enterprise

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

- The groups share **30** techniques in common (as of July 2024):



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

it:mitre:attack:technique (30)

ck:technique	:name	:matrix	:desc	:url
T1005	data from local system (enterprise)	enterprise	Adversaries may s…	https://attack.m
T1036.005	match legitimate name or location (en…	enterprise	Adversaries may m…	https://attack.m
T1059.001	powershell (enterprise)	enterprise	Adversaries may a…	https://attack.m
T1068	exploitation for privilege escalation…	enterprise	Adversaries may e…	https://attack.m
T1070.004	file deletion (enterprise)	enterprise	Adversaries may d…	https://attack.m

Tip: The Synapse `intersect` command is useful for displaying **overlapping** sets of results.

`Intersect` takes a set of nodes (in this case, our two groups) and performs the **pivot** (or traversal) operation that you specify (in the curly braces) for each inbound node.

A "normal" pivot would return **all** of the techniques used by **either** group. `Intersect` tells Synapse to **only** return the techniques used by **both** groups - the *intersection* of the results from G0007 and G0016.

More information on `intersect` can be found in the Storm documentation or by viewing the command help in the **Console Tool:**

```
intersect --help
```