Vertex

Synapse Bootcamp - Module 19

Introduction to Threat Intelligence in Synapse - Exercises

Objectives

In these exercises you will:

- Use the Threat Intel Workflow to view threat data.
- Use the Threat Intel Workflow to add and link threat data.

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

View Threat Information

Exercise 1

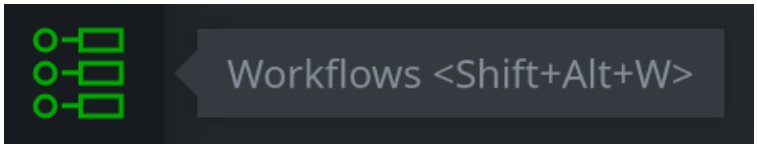
Objective:

- **Use the Threat Intel Workflow to view information about threats, vulnerabilities, and targeting.**

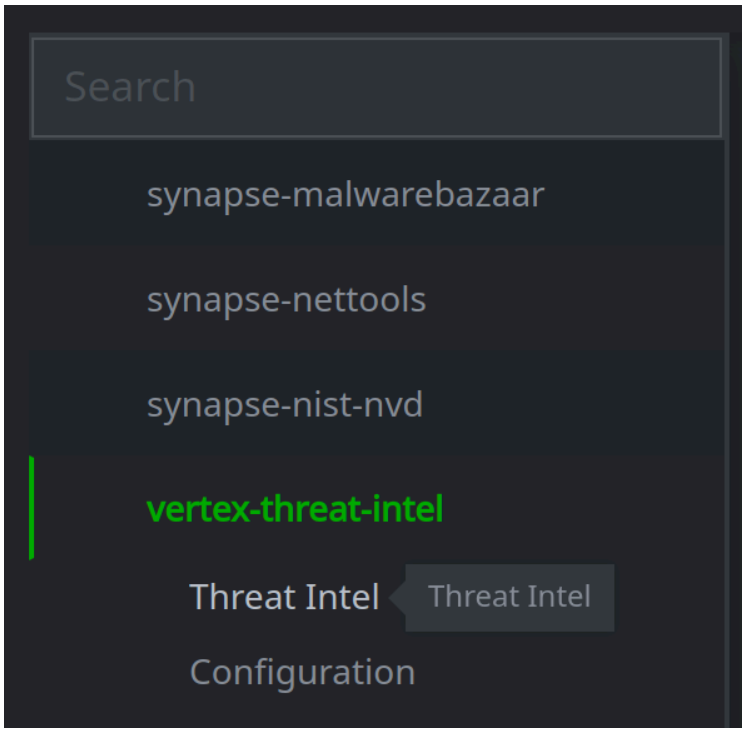
Part 1 - View information about a threat

You want to view information about a threat group called "Armageddon". The group was reported by the Security Service of Ukraine (SSU).

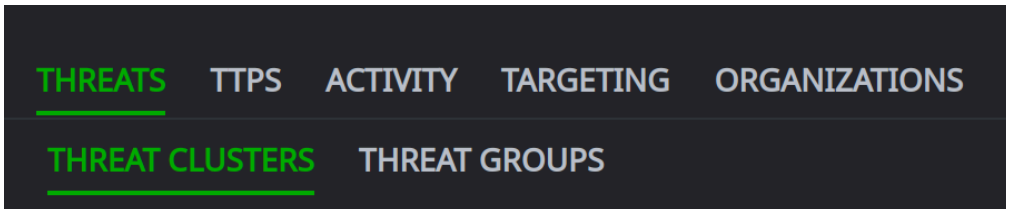
- From your **Toolbar,** select the **Workflows Tool:**



- In the list view, locate the **vertex-threat-intel** entry and select **Threat Intel:**

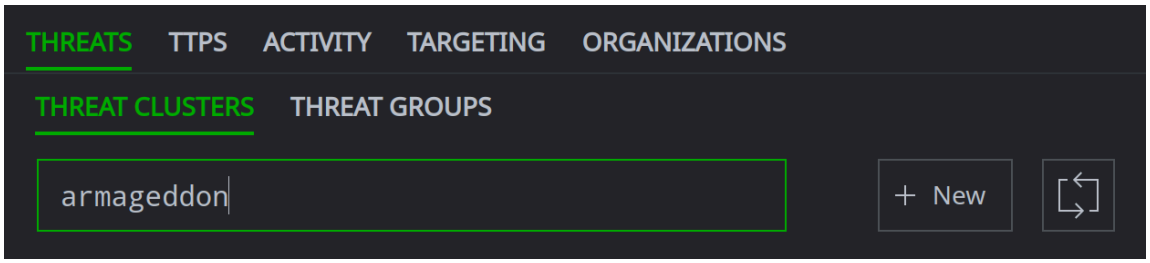


- In the **Selection Panel,** make sure that the **THREATS** tab and **THREAT CLUSTERS** subtab are selected:



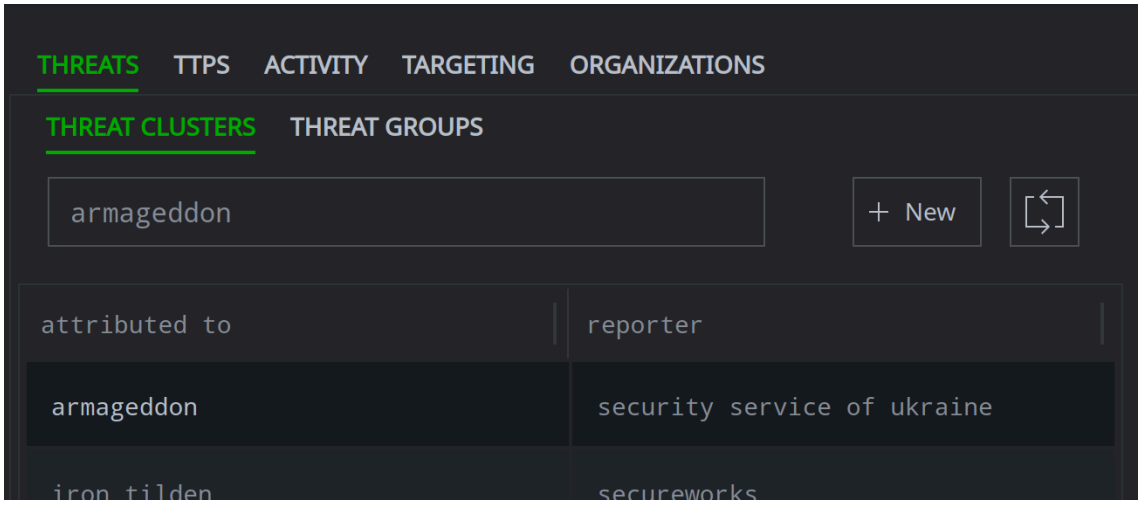
- In the **Search** field, begin typing the following:

```
armageddon
```

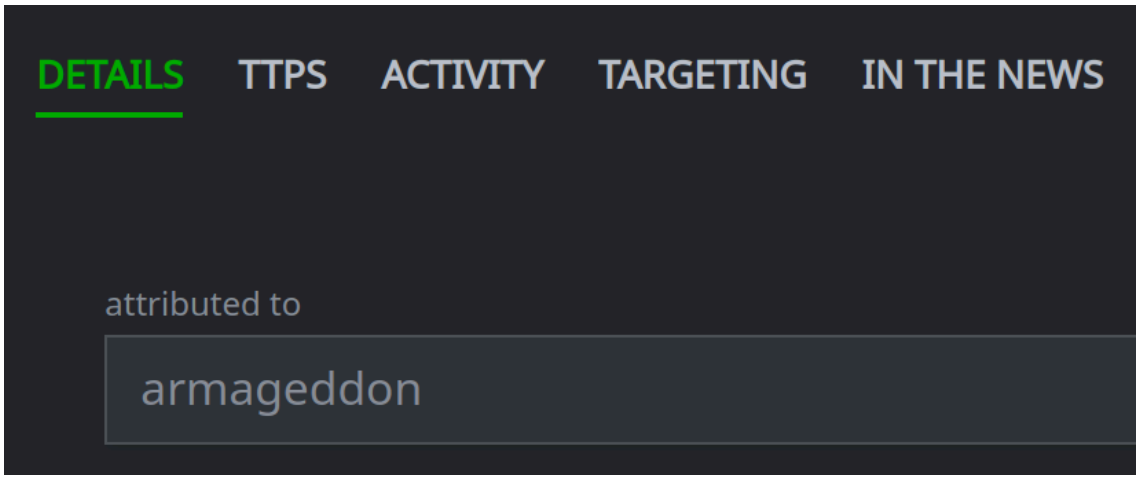


Question 1: How many **threat clusters** are in your results?

- In the **Selection Panel, select** the "Armageddon" threat cluster:

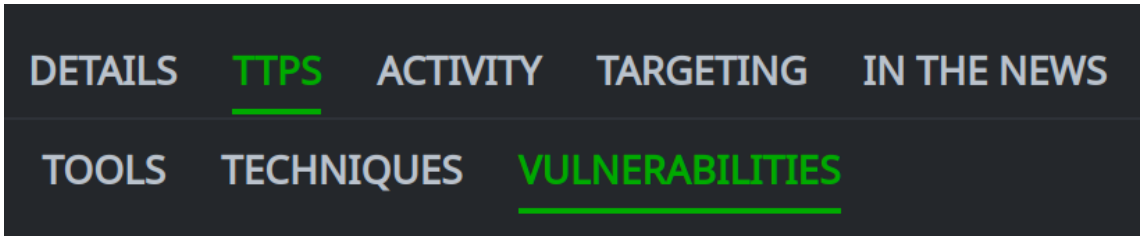


- In the **Profile Panel,** view the information on the **DETAILS** tab:



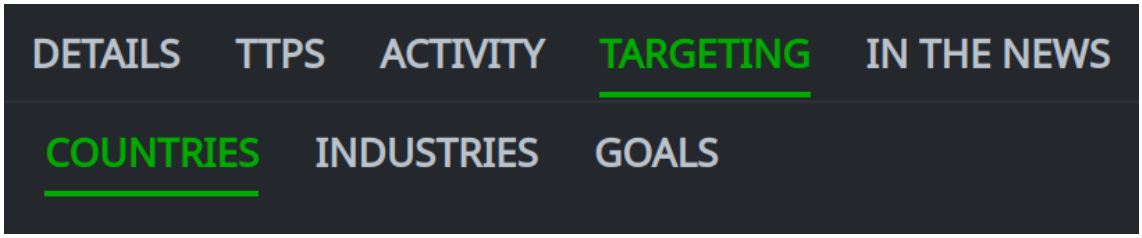
Question 2: How many **alternate names** are used to report on "Armageddon", according to the Security Service of Ukraine (SSU)?

- In the **Profile Panel,** select the **TTPS** tab and the **VULNERABILITIES** subtab:



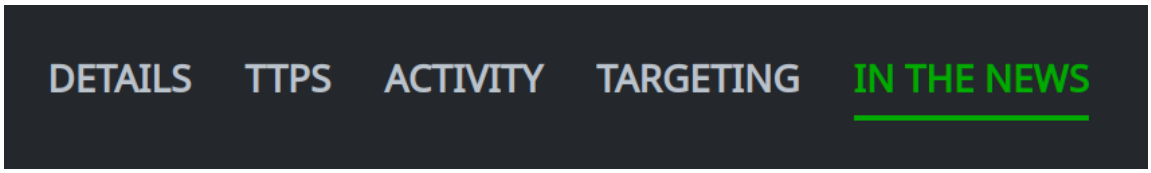
Question 3: Which **vulnerabilities** has Armageddon exploited, according to the SSU?

- In the **Profile Panel,** select the **TARGETING** tab and the **COUNTRIES** subtab:



Question 4: What **countries** has Armageddon targeted, according to the SSU?

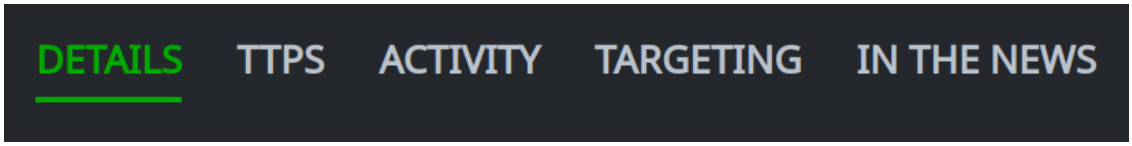
- In the **Profile Panel,** select the **IN THE NEWS** tab:



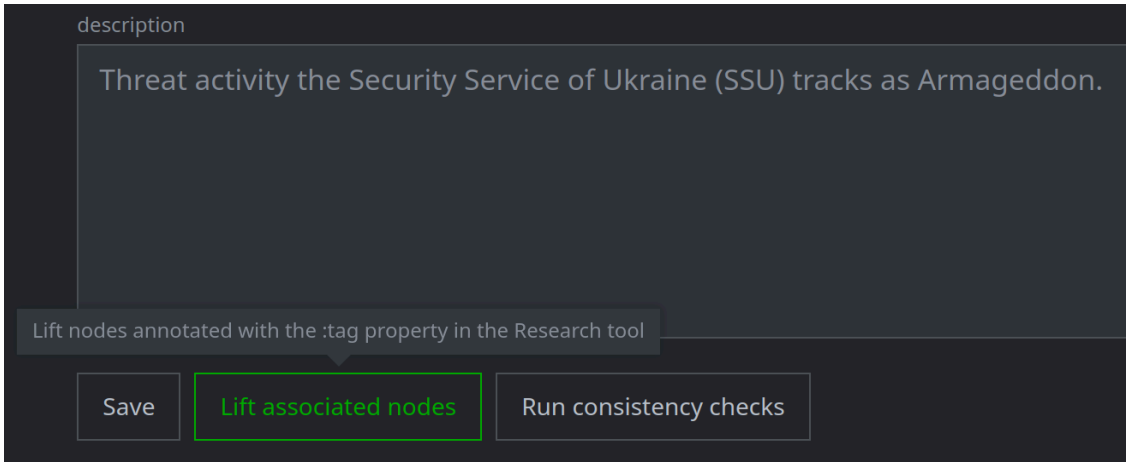
Question 5: How many **reports** in Synapse reference the SSU's Armageddon group?

You want to view any indicators associated with the SSU's "Armageddon" group.

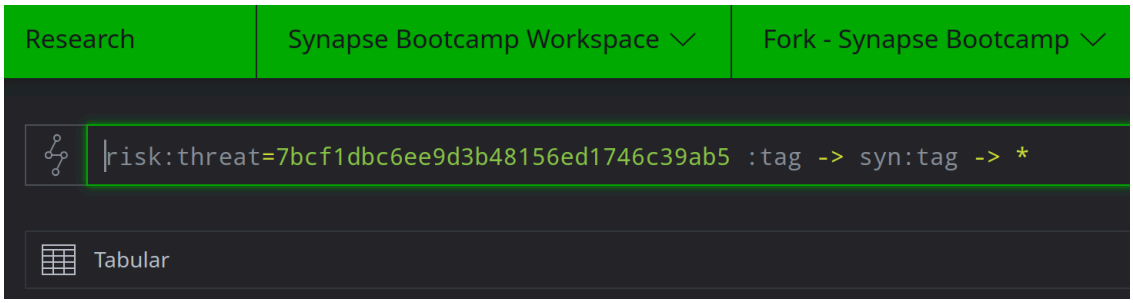
- In the **Profile Panel,** select the **DETAILS** tab:



- Click the **Lift associated nodes** button:



- Synapse takes you to the **Research Tool:**



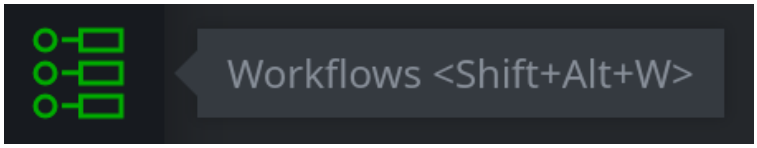
Question 6: What kinds of indicators (nodes) are associated with Armageddon? Are there any unusual objects?

Part 2 - View additional threat data

View vulnerability data

You want to know which threat groups have exploited the Microsoft Exchange "ProxyShell" vulnerability.

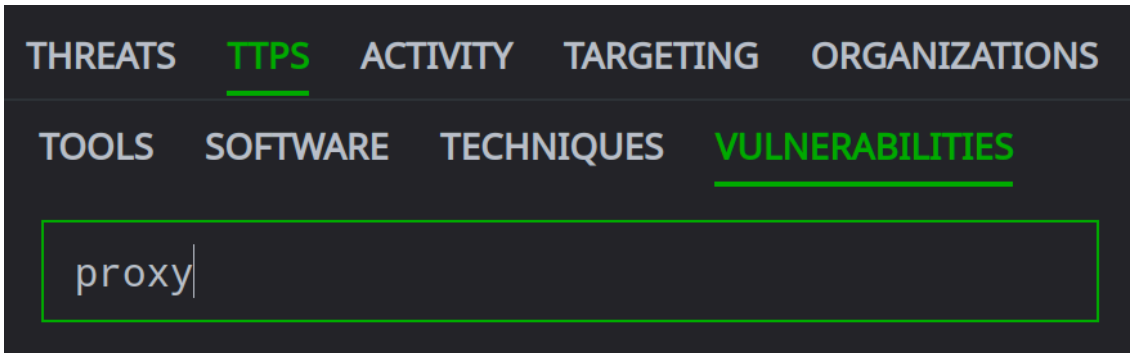
- From your **Toolbar,** select the **Workflows Tool:**



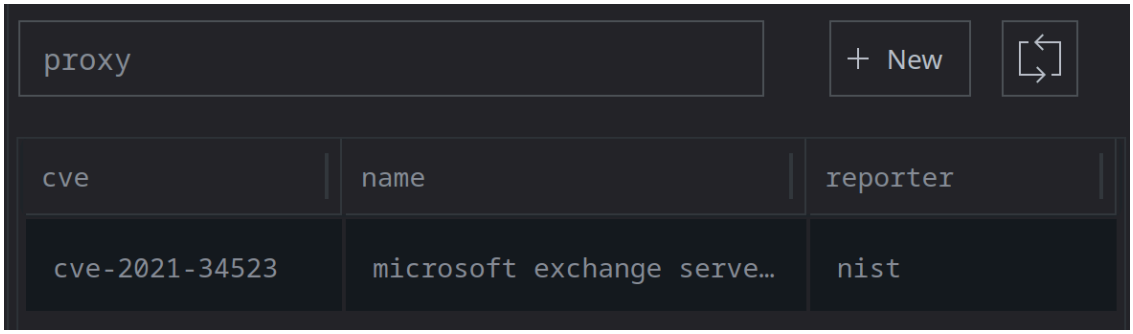
- In the **Selection Panel,** select the **TTPS** tab and the **VULNERABILITIES** subtab:

- In the **Search** field, begin typing the following to search for the "ProxyShell" vulnerabilities[1]:

```
proxy
```



- In the **Results, select** vulnerability **cve-2021-34523**:



[1] "ProxyShell" refers to CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207 affecting Microsoft Exchange Server. https://www.cisa.gov/news-events/alerts/2021/08/21/urgent-protect-against-active-exploitation-proxyshell-vulnerabilities

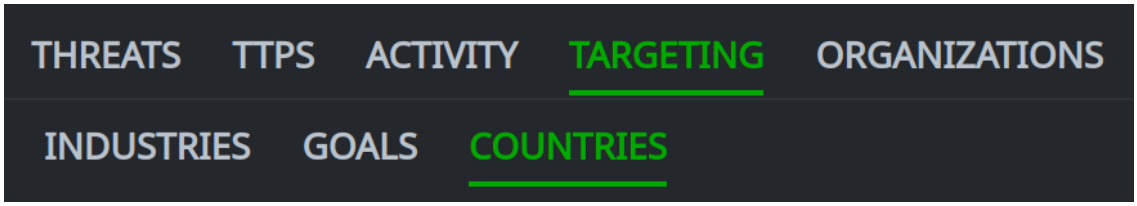
- In the **Profile Panel,** select the **THREAT CLUSTERS** tab:

Question 7: Which **threat clusters** have exploited CVE-2021-34523? Who reported on the threats?

View targeting data for a country

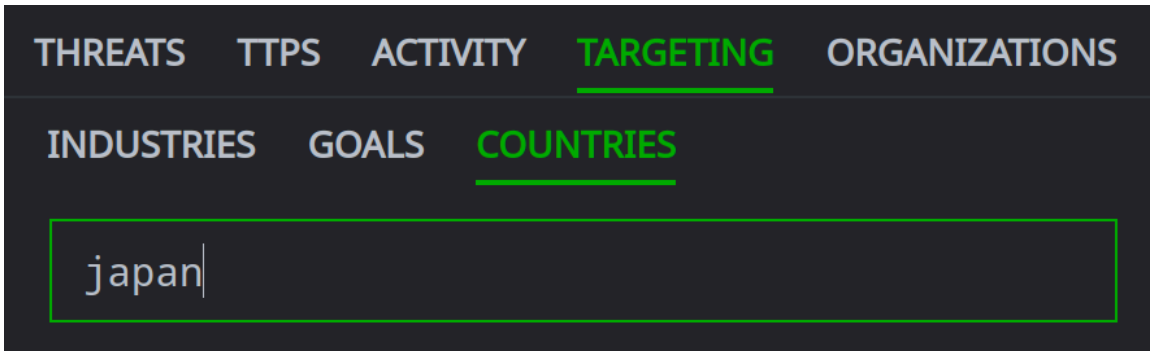
You want to know which threat groups target Japan.

- In the **Selection Panel,** select the **TARGETING** tab and the **COUNTRIES** subtab:



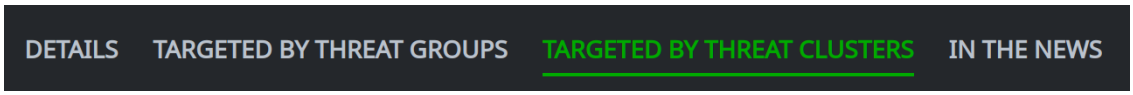
- In the **Search** field, begin typing **japan**

```
japan
```



- In the **Results, select** Japan:

- In the **Profile Panel,** select the **TARGETED BY THREAT CLUSTERS** tab:



Question 8: Which **threat clusters** have targeted Japan? Who reported on the threats?

Add Threat Intel Data Using the Workflow

Exercise 2

Objectives:
- **Use the Threat Intel Workflow to create a threat cluster.**
- **Use the Workflow to link information to the threat cluster.**

You want to create a threat cluster (`risk:threat`) for the activity Dell Secureworks calls BRONZE CANAL.

The profile is included below; you can also view it online.

CHINA

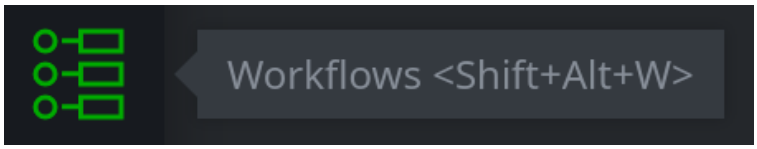
BRONZE CANAL

Objectives	Targeted Espionage
Aliases	BlackTech, Circuit Panda (CrowdStrike), CTG-6177 (SCWX CTU), Palmerworm (Symantec), Shrouded Crossbow (Trend Micro)
Tools	Bifrose, DRIGO, Flagpro, Gh0stTimes, PLEAD, Waterbear

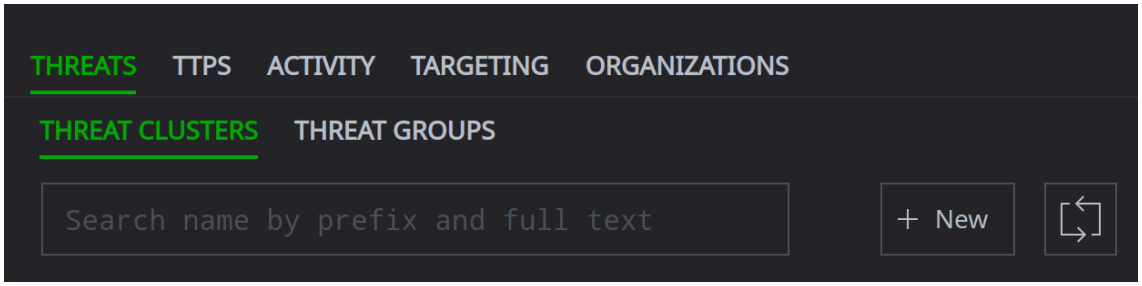
BRONZE CANAL (also known as BlackTech, PLEAD, Shrouded Crossbow, Circuit Panda and Palmerworm) is a cyber espionage threat group assessed with moderate confidence to operate on behalf of China. The group has been active in the Asia region since 2010, and is noted for a targeting focus on Taiwan, Japan and Hong Kong. Third-party security vendors also report some targeting of U.S. organisations. BRONZE CANAL has been observed to deploy malware including Bifrose, PLEAD (TSCookie), Waterbear and, in 2021, GhostTimes and Flagpro. The group is also adept at using and adapting open source exploit tools for common internet facing systems, which may gain them a foothold into target networks. They also employ malware attachments with targeted phishing emails. Targets have included government, media, finance, defence, telecommunications, technology, foreign affairs and construction.

Part 1 - Create the threat cluster (risk:threat)

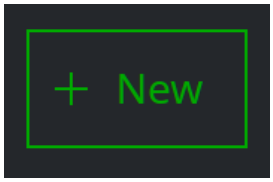
- From your **Toolbar,** select the **Workflows Tool:**



- In the **Selection Panel,** make sure that the **THREATS** tab and **THREAT CLUSTERS** sub-tab are selected:

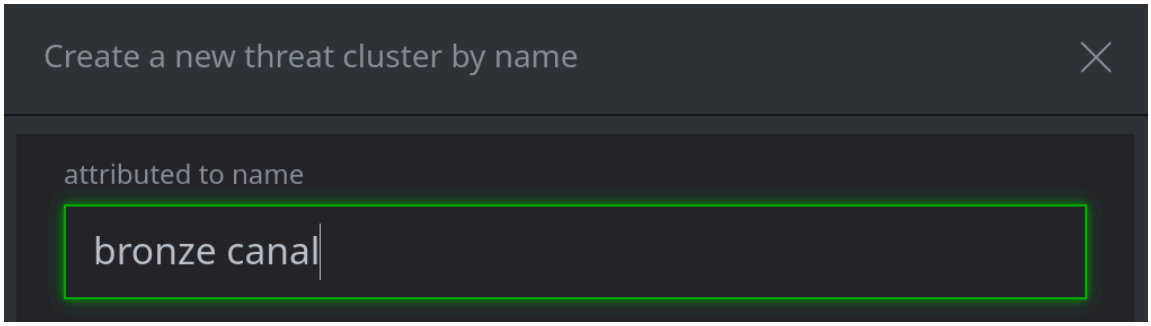


- Click the **+ New** button to create a new threat cluster:



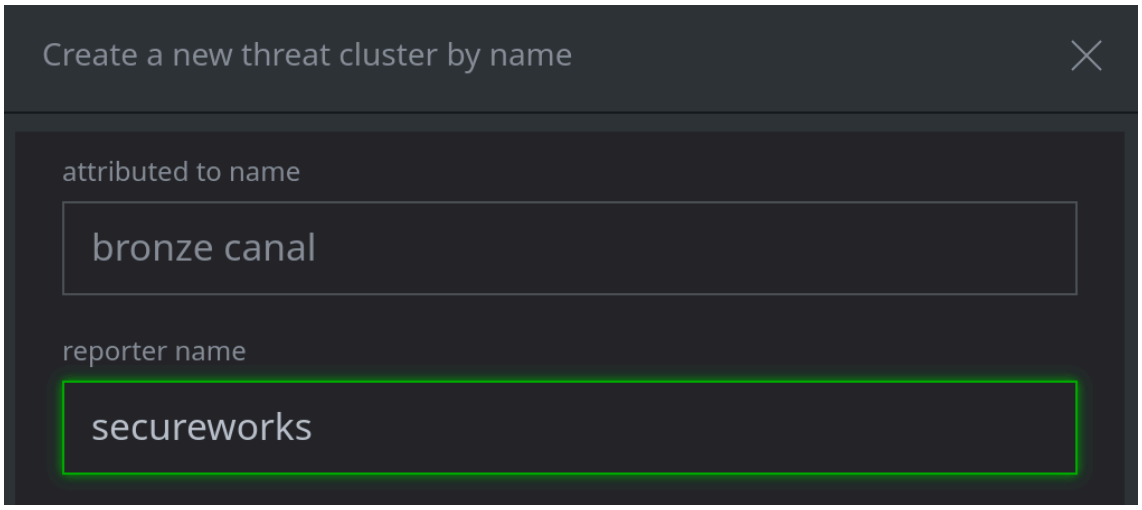
- In the **Create a new threat cluster by name** dialog, in the **attributed to name** field, enter the following:

```
bronze canal
```

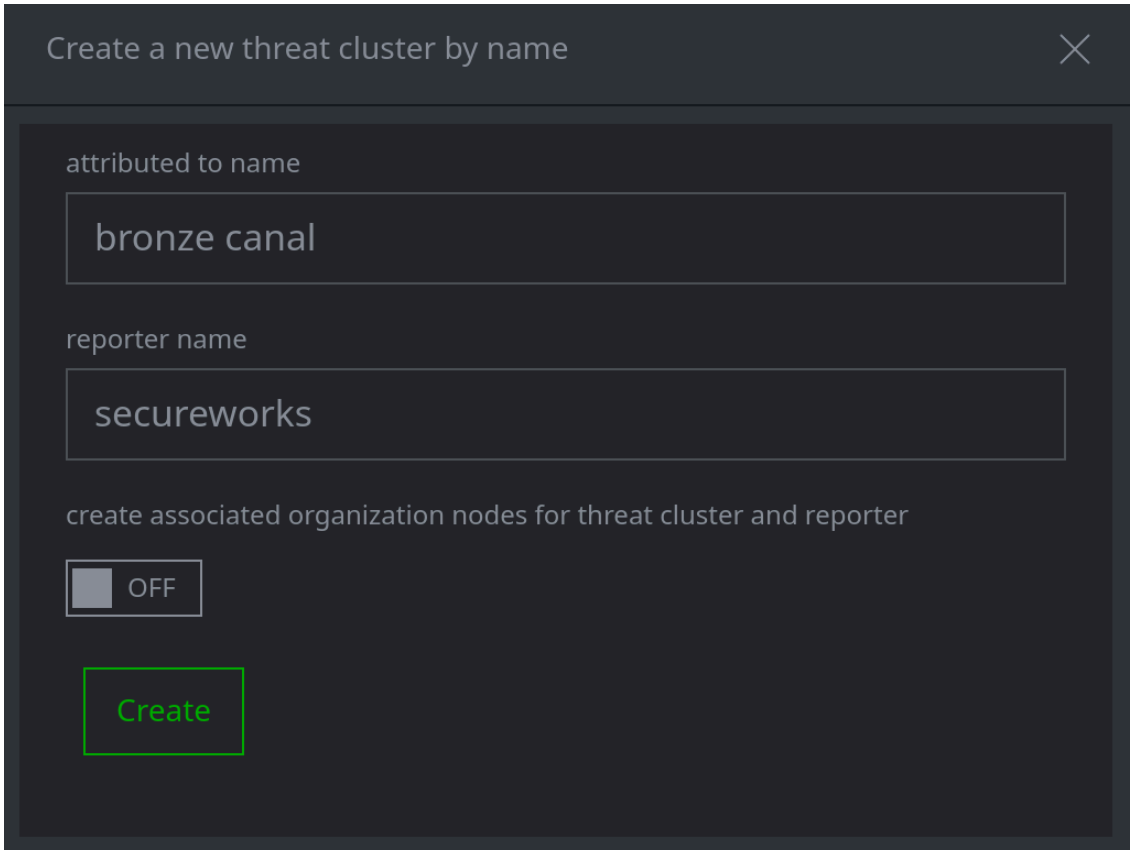


- In the **reporter name** field, enter the following:

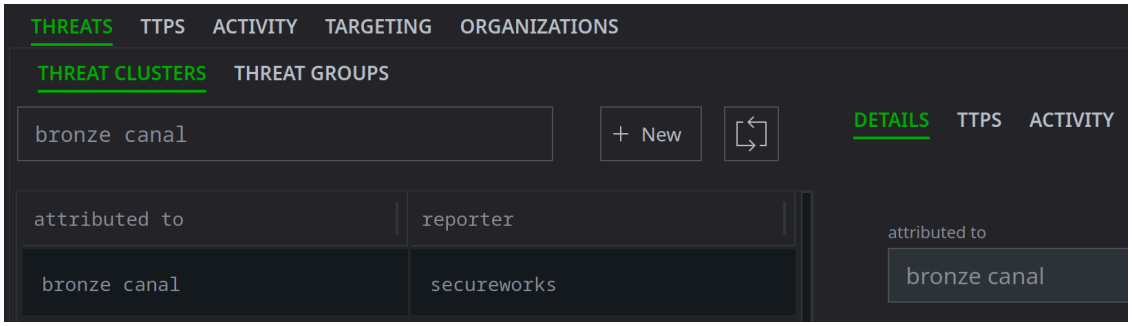
```
secureworks
```



- Click the **Create** button to create the threat cluster:

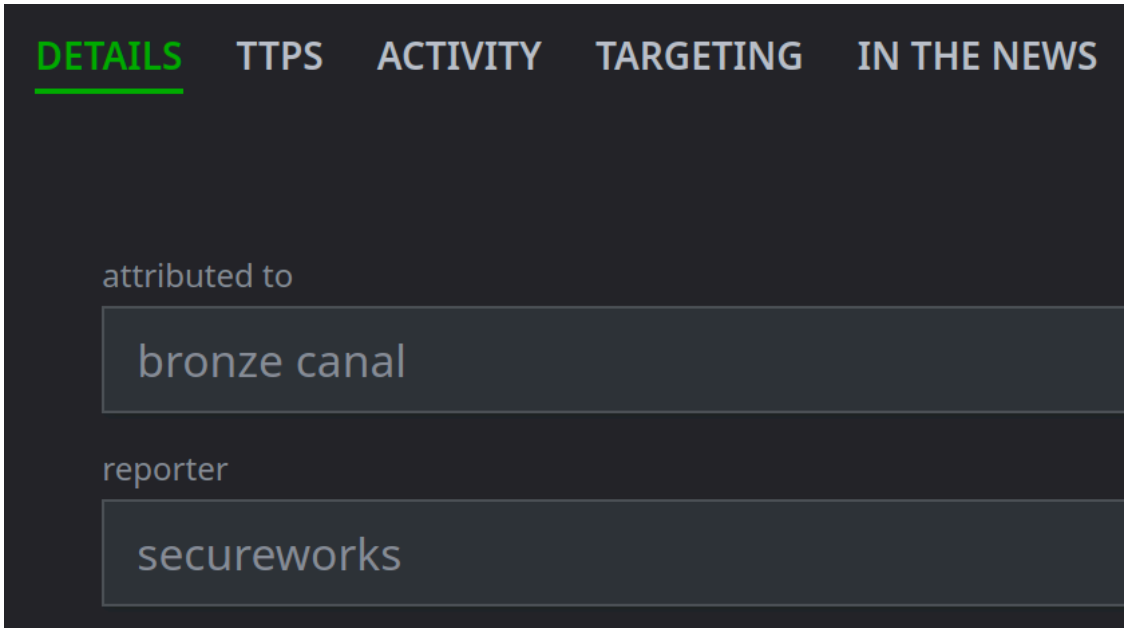


- Synapse creates the threat cluster (`risk:threat`) and automatically **selects** it:



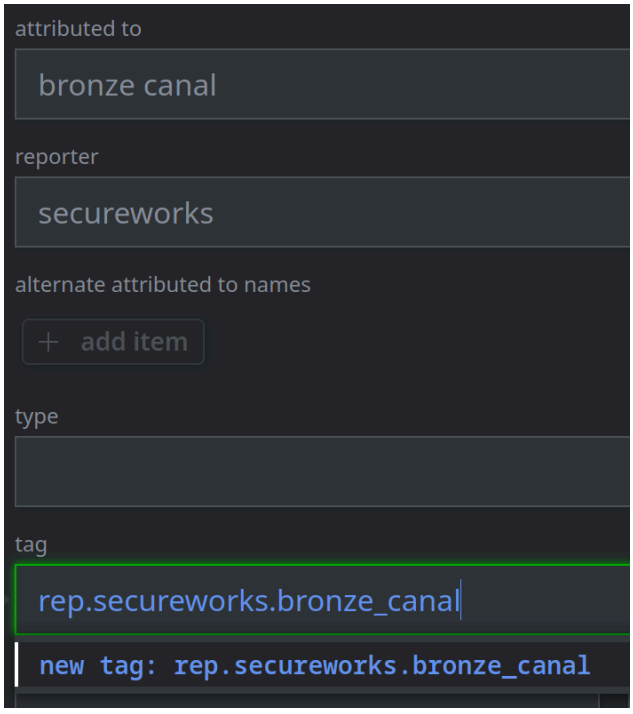
Part 2 - Add properties in the Profile Panel

- In the **Profile Panel,** view the information on the **DETAILS** tab:



- In the **DETAILS** tab, in the **tag** field, enter the following:

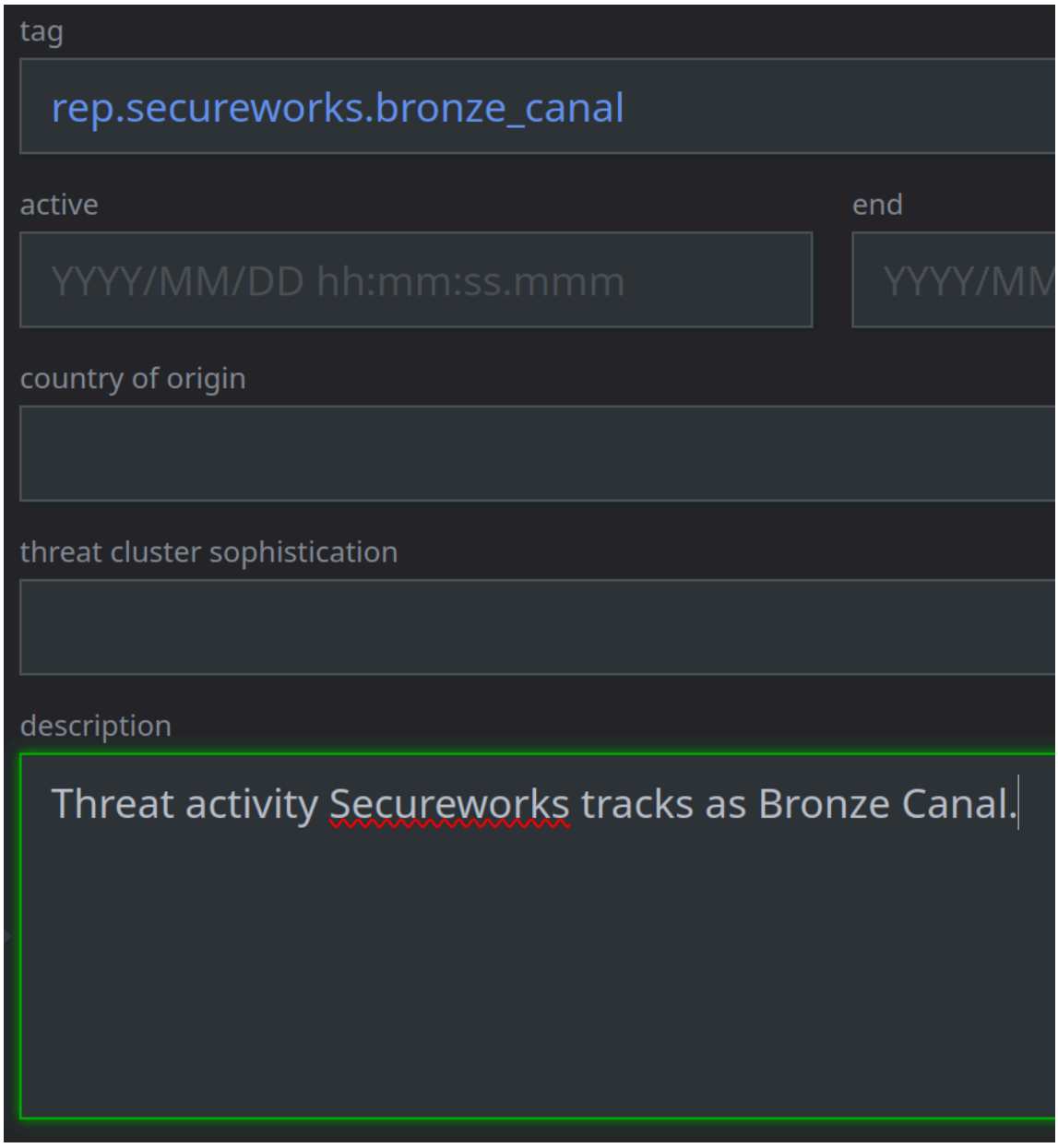
```
rep.secureworks.bronze_canal
```



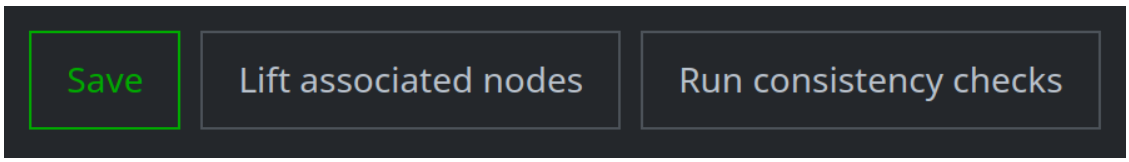
Add the new tag.

- In the **description** field, enter the following:

```
Threat activity Secureworks tracks as Bronze Canal.
```

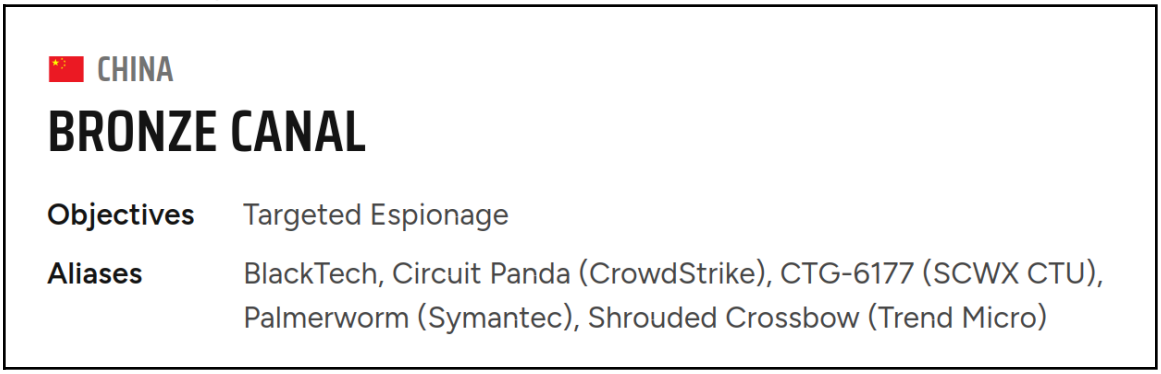


- Click the **Save** button to save your changes:

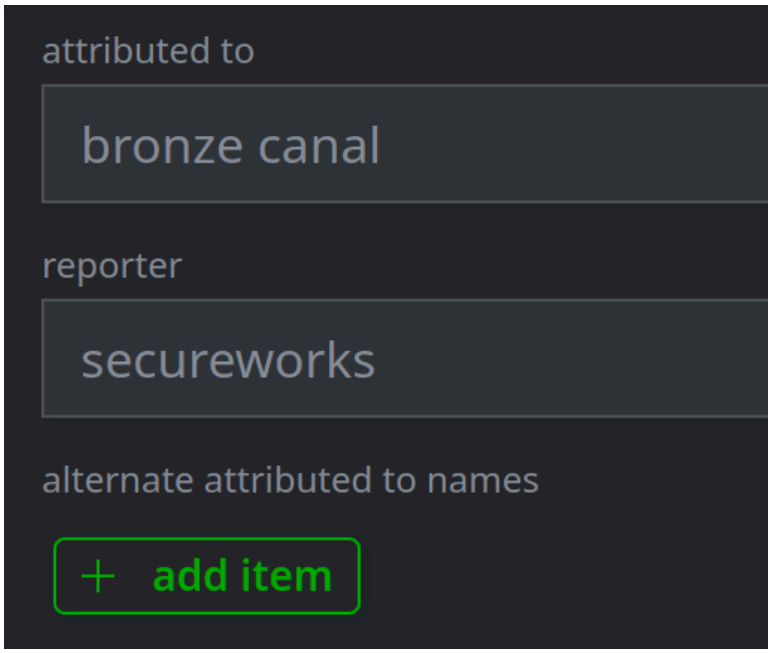


Part 3 - Add alternate names in the Profile Panel

- Secureworks reported several **alternate names** (aliases) for this threat:



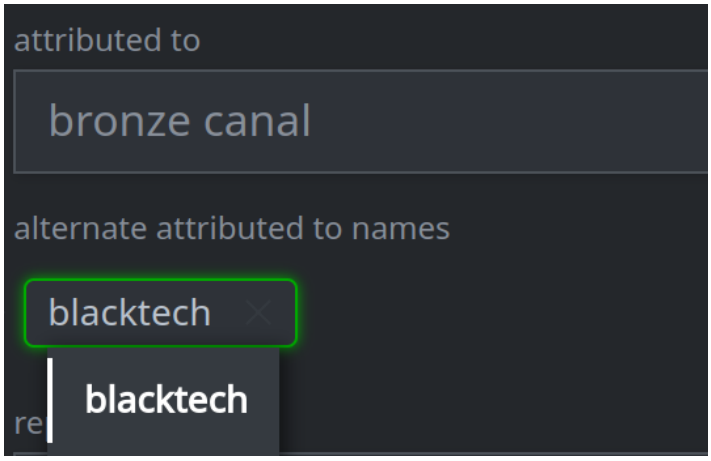
- In the **DETAILS** tab, under **alternate attributed to names,** click the **+ add item** button:



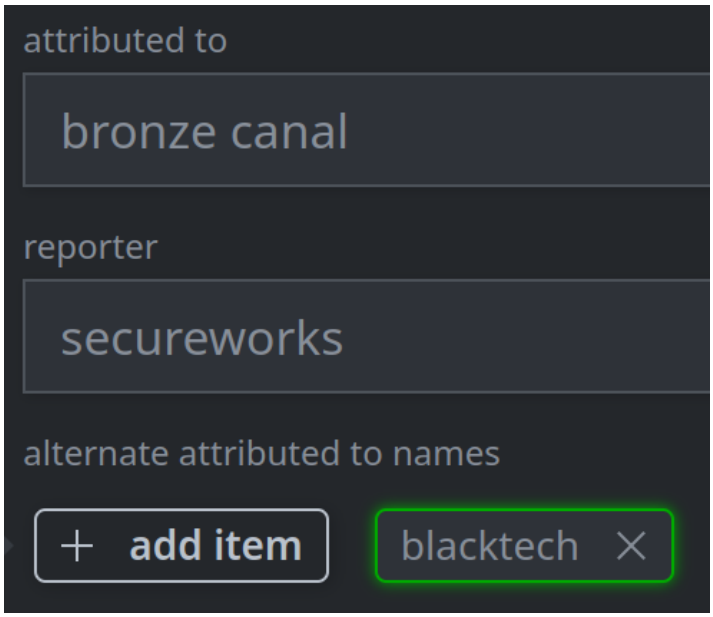
- In the input box, begin typing the following:

```
blacktech
```

Select the name from the list to add it:



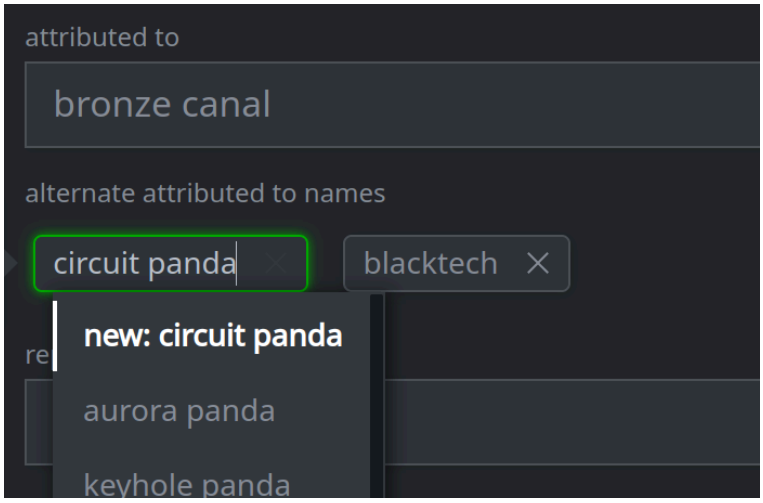
- The name should appear:



- In the input box, type the following:

```
circuit panda
```

Select the **new** option to create and add this name:



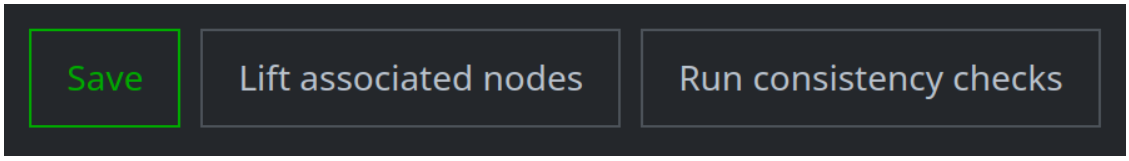
- **Repeat** these steps to add the other aliases:

  ctg-6177

  palmerworm

  shrouded crossbow

- Click the **Save** button to save your changes:

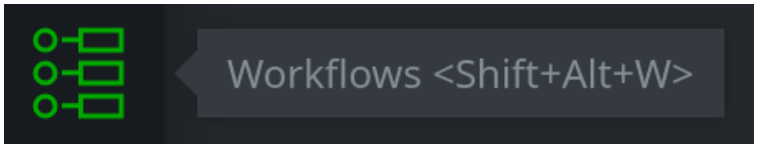


Question 1: What does the **DETAILS** tab look like?

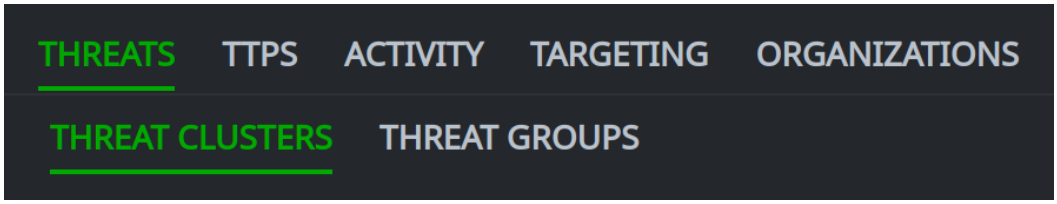
Part 4 - Link information to the threat

Secureworks reported on BRONZE CANAL's goals, targeting, and tools. You can add this information using the Threat Intel Workflow.

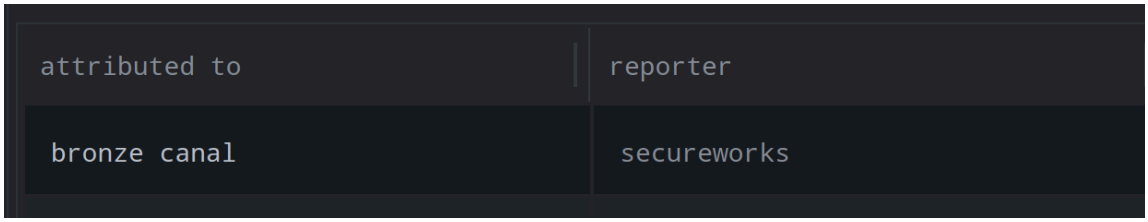
- From your **Toolbar,** select the **Workflows Tool:**



- In the **Selection Panel,** select the **THREATS** tab and **THREAT CLUSTERS** subtab:



- In the **Selection Panel, select** the threat cluster for **bronze canal:**

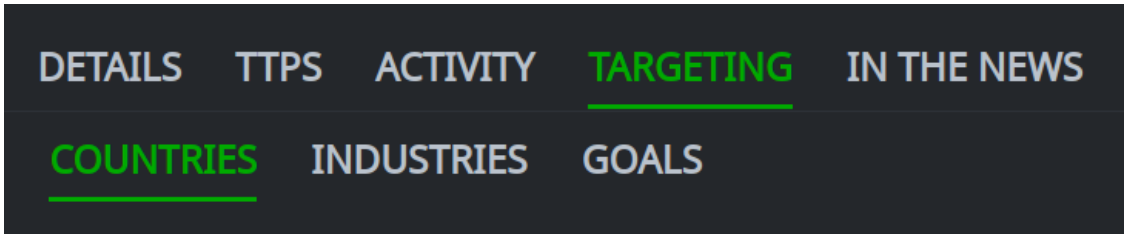


Add targeted countries

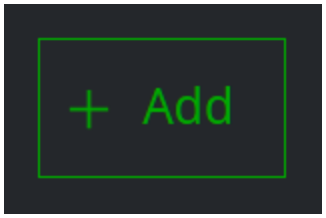
Secureworks reported that Bronze Canal targets **Taiwan, Japan,** and **Hong Kong.**

BRONZE CANAL (also known as BlackTech, PLEAD, Shrouded Crossbow, Circuit Panda and Palmerworm) is a cyber espionage threat group assessed with moderate confidence to operate on behalf of China. The group has been active in the Asia region since 2010, and is noted for a targeting focus on Taiwan, Japan and Hong Kong. Third-party security vendors also report some

- In the **Profile Panel,** select the **TARGETING** tab and the **COUNTRIES** subtab:

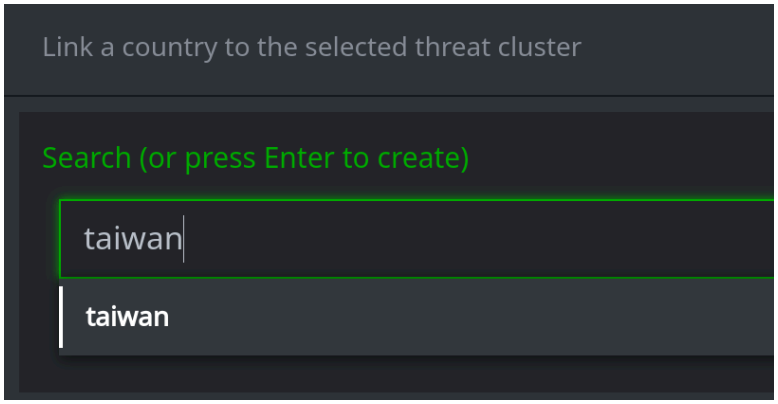


- Click the **+ Add** button:



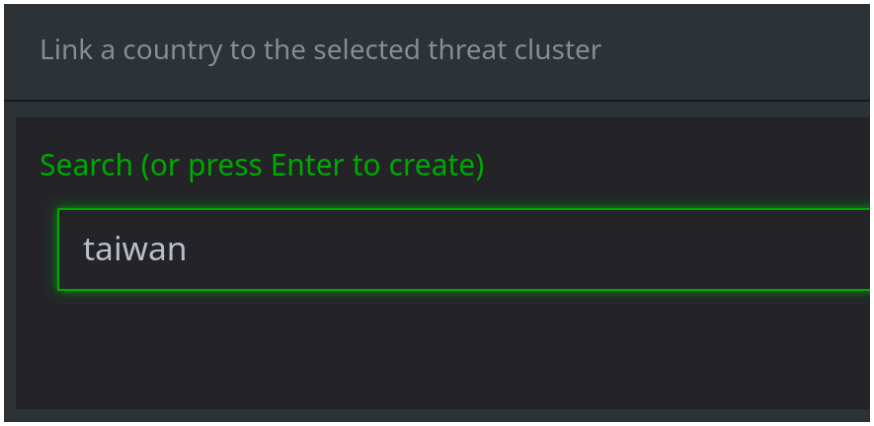
- In the **Search bar,** begin typing to locate the country **taiwan:**

```
taiwan
```



Select the name from the results.

- Make sure your cursor is in the search field. Press **Enter** to add the country:

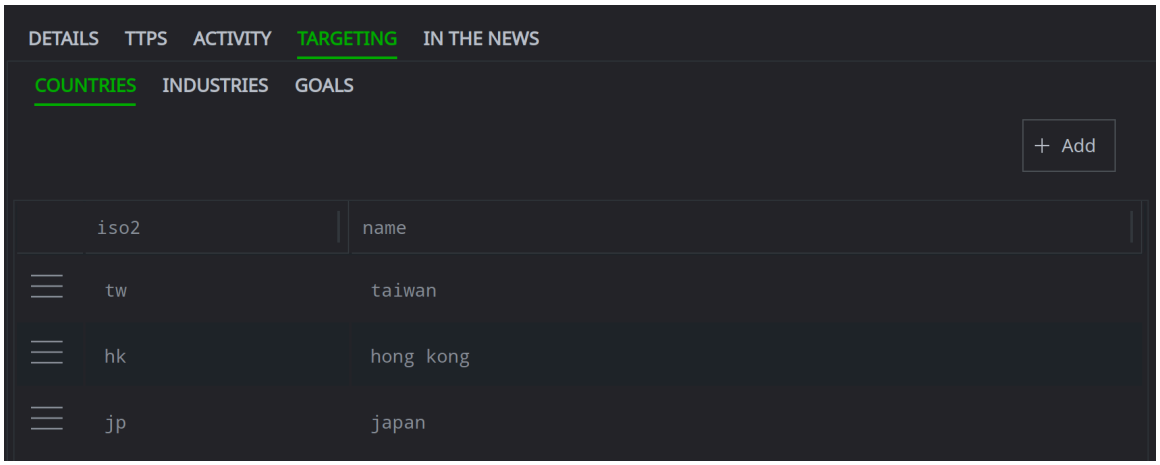


- **Repeat** the steps to add the other countries:

```
japan
```


hong kong

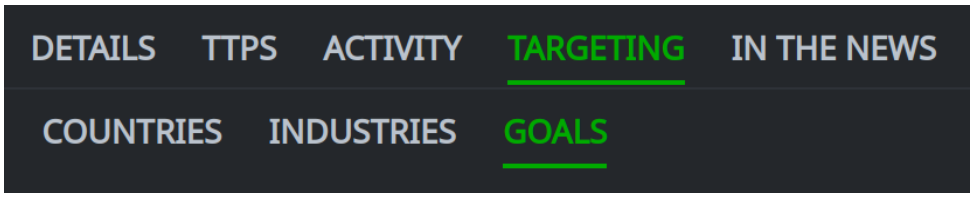
- When you finish, you should see **three** countries listed:



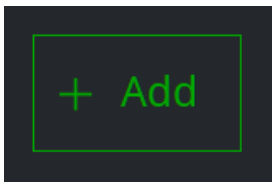
Add goals

Secureworks reported that Bronze Canal is an **espionage** group.

- In the **Profile Panel,** select the**TARGETING** tab and the **GOALS** subtab:



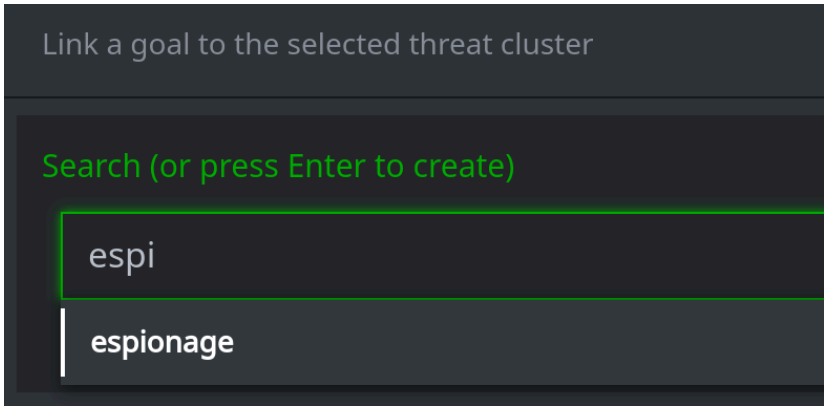
- Click the **+ Add** button:



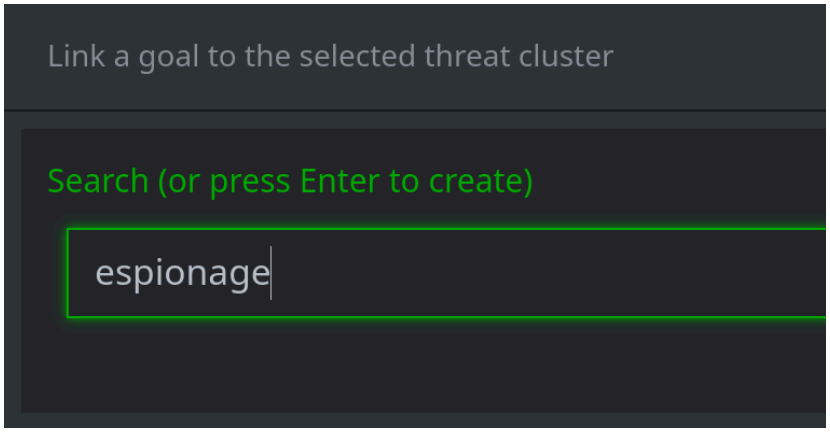
- In the **Search** field, search for **espionage:**

  ```
  espionage
  ```

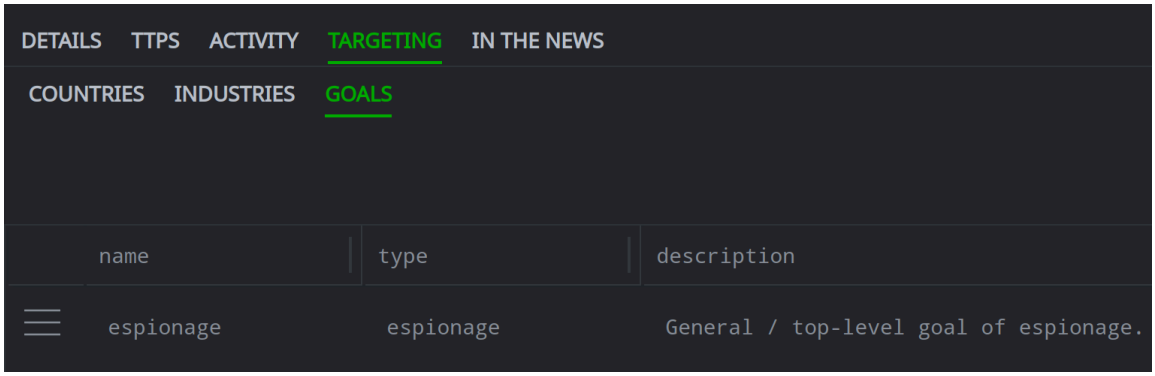
  Select the name from the results:



- Make sure your cursor is in the search field. Press **Enter** to add the goal:



- The goal should be listed:



Add tools

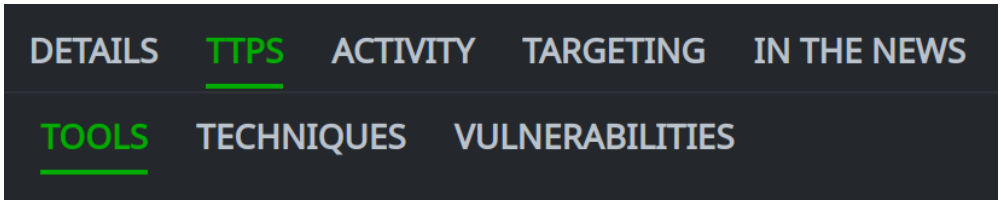
Secureworks reported several **tools** used by Bronze Canal.

CHINA

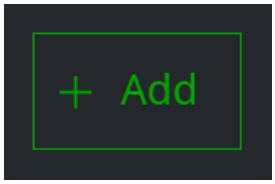
BRONZE CANAL

Objectives	Targeted Espionage
Aliases	BlackTech, Circuit Panda (CrowdStrike), CTG-6177 (SCWX CTU), Palmerworm (Symantec), Shrouded Crossbow (Trend Micro)
Tools	Bifrose, DRIGO, Flagpro, Gh0stTimes, PLEAD, Waterbear

- In the **Profile Panel,** select the **TTPS** tab and the **TOOLS** subtab:

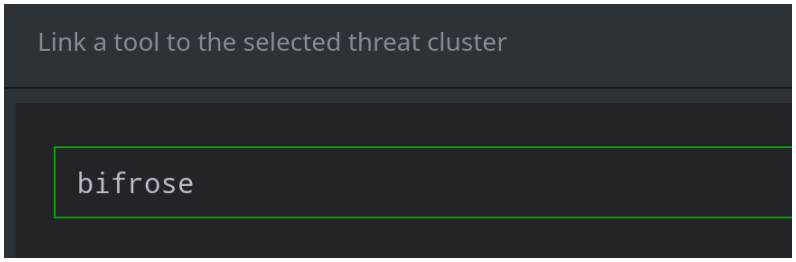


- Click the **+ Add** button:



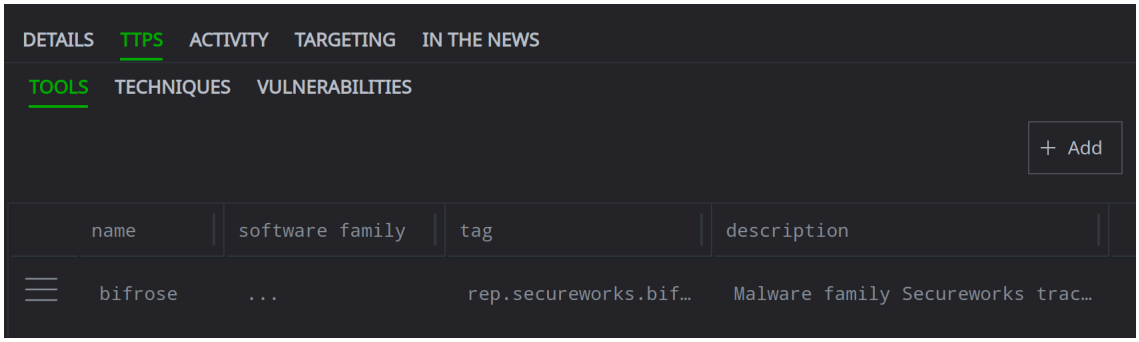
- In the **Search** field, search for **bifrose:**

```
bifrose
```



- In the results, **right-click** the **hamburger menu** next to the **bifrose** entry for **secureworks** and select **Link selected node(s):**

- The tool should be listed:



- **Repeat** the steps to add the other tools:

drigo

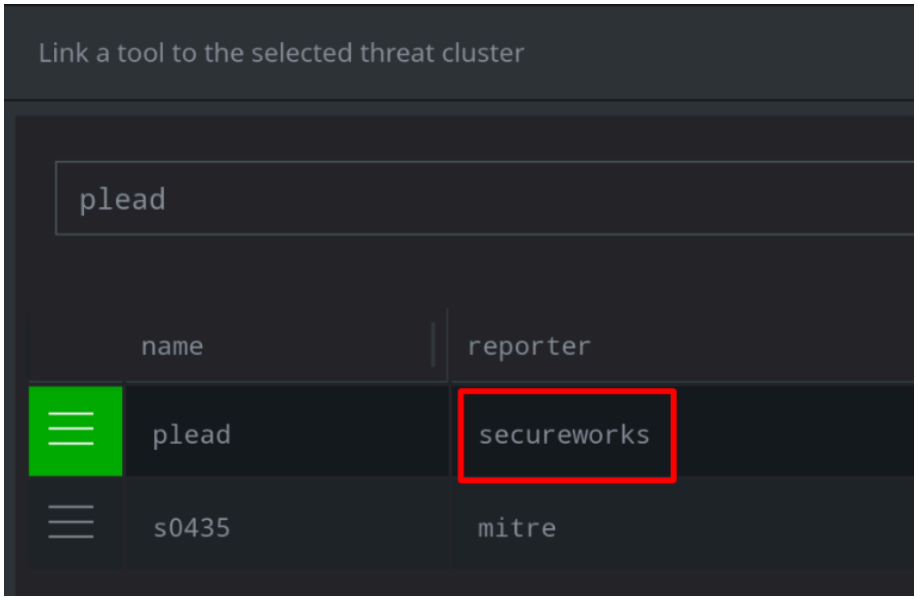
flagpro

gh0sttimes

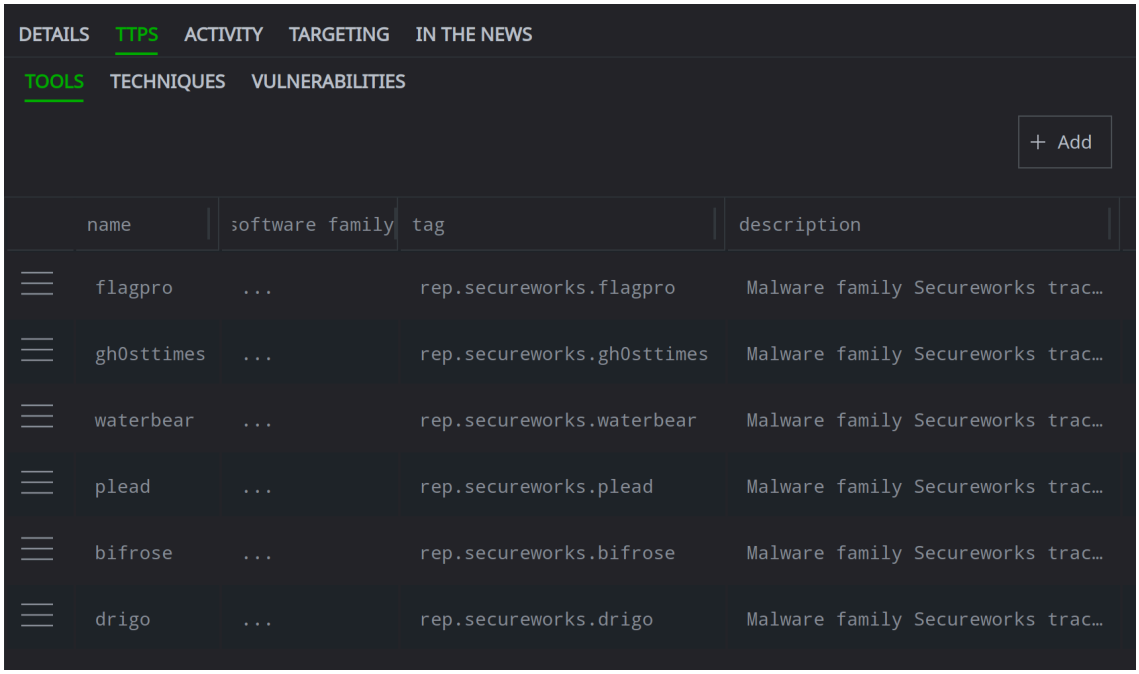
plead

waterbear

Note: if your search finds more than one match, select the result for **secureworks:**



- When you are finished, you should see **six** tools:



Tip: If any of these tools did not exist, you could create them in the **Selection Panel** under the **TTPS** tab, **TOOLS** subtab.

Congratulations! You created a profile for Bronze Canal in the Threat Intel Workflow! You can view information about the threat using the Workflow tabs. Alternatively, you can **query** the new threat cluster node and view or Explore the **`risk:threat`** node in the Research Tool.
