TryHackMe: Trooper

The following writeup is for Trooper, a room hosted on TryHackMe. This room involves using OpenCTI and the Mitre ATT&CK navigator to investigate a threat actor. If you are familiar with OpenCTI and Mitre ATT&CK, this room will be super easy for you, otherwise it is a great learning experience.

Scenario: A multinational technology company has been the target of several cyber attacks in the past few months. The attackers have been successful in stealing sensitive intellectual property and causing disruptions to the company's operations. As a CTI analyst, your task is to identify the Tactics, Techniques, and Procedures (TTPs) being used by the Threat group and gather as much information as possible about their identity and motive. For this task, you will utilise the OpenCTI platform as well as the MITRE ATT&CK navigator.

What kind of phishing campaign does APT X use as part of their TTPs?

If you read the provided threat report, you can determine that APT X uses spear-phishing emails:

> APT X, a threat actor group that targets government, military, healthcare, transportation, and high-tech industries in Taiwan, the Philippines, and Hong Kong, has been active since 2011. The group was reportedly using spear-phishing emails with weaponized attachments to exploit known vulnerabilities.

What is the name of the malware used by APT X?

Once again, if you read the report, you can determine that the malware used is called USBferry:

> We found that APT X's latest activities center on targeting Taiwanese and the Philippine military's physically isolated networks through a USBferry attack (the name derived from a sample found in a related research). We also observed targets among military/navy agencies, government institutions, military hospitals, and even a national bank. The group employs USBferry, a USB malware that performs different commands on specific targets, maintains stealth in environments, and steals critical data through USB storage. We started tracking this particular campaign in 2018, and our analysis shows that it uses a fake executable decoy and a USB trojan strategy to steal information.

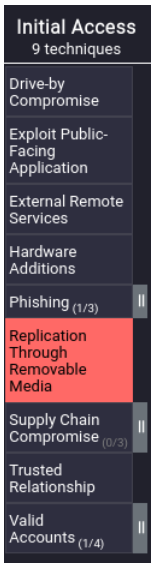
What is the malware's STIX ID?

This is where you need to start using OpenCTI. To find the STIX ID, simply search for "USBferry" in the search bar like as follows:

This should produce one result labelled as malware. Click this result to find the Standard STIX ID:

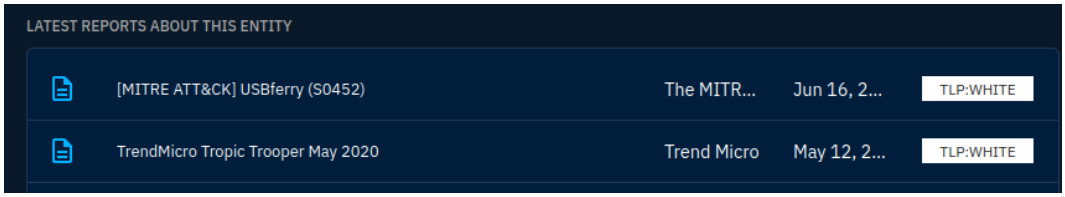
With the use of a USB, what technique did APT X use for initial access?

There are multiple ways to find the answer for this question, you can explore all the techniques listed under the initial access tactic, or you can navigate to the ATT&CK navigator provided by the room to find the answer:



What is the identity of APT X?

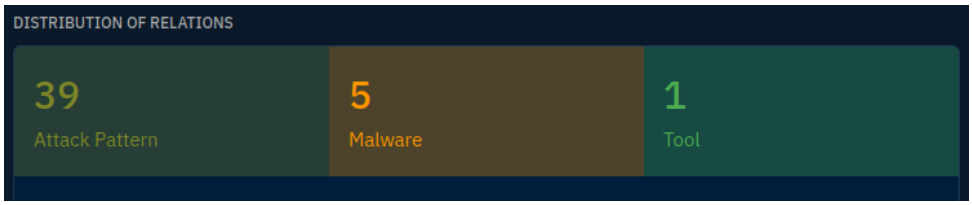
Going back to OpenCTI, if you check out the Analysis tab or the latest reports about this entity section, you can determine that Tropic Trooper is the name of the threat group:



On OpenCTI, how many Attack Pattern techniques are associated with the APT?

Start by searching for the threat group Tropic Trooper:

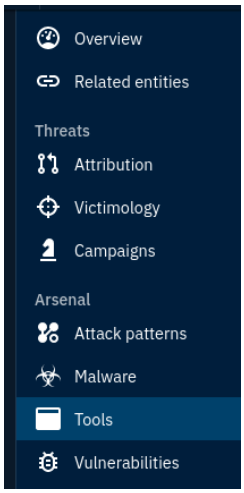
After you select the Tropic Trooper enetity, navigate to the Knowledge tab:



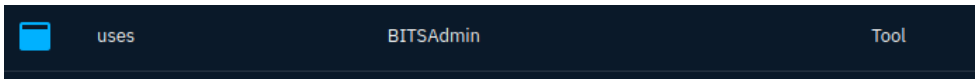
As you can see, Tropic Trooper is associated with 39 attack patterns.

What is the name of the tool linked to the APT?

Using the navigation bar on the right-hand side of the screen. Navigate to the tool section:

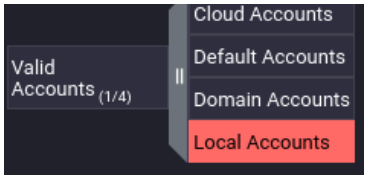


As you can see, Tropic Trooper is only linked to one tool called BITSAdmin:



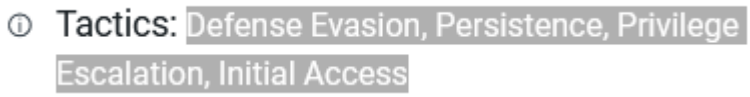
Load up the Navigator. What is the sub-technique used by the APT under Valid Accounts?

If you expand the Valid Accounts technique, you can determine that Tropic Trooper uses Local Accounts:



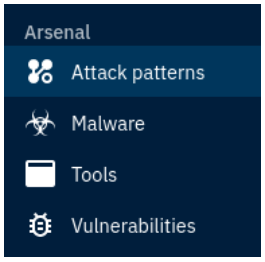
Under what Tactics does the technique above fall?

To answer this question, simply navigate to the Local Accounts sub-technique on Mitre ATT&CK:



What technique is the group known for using under the tactic Collection?

There are multiple ways to find the answer, you can simply navigator to the ATT&CK navigator and find it there, or you can visit the Attack patterns section for Tropic Trooper on OpenCTI:



As you can see, they use Automated Collection:

This was a really fun and interesting room. If you are new to CTI and Mitre ATT&CK, this is a great way to learn. If you get stuck with anything while doing this room, feel free to contact me or check out the plethora of writeups posted.