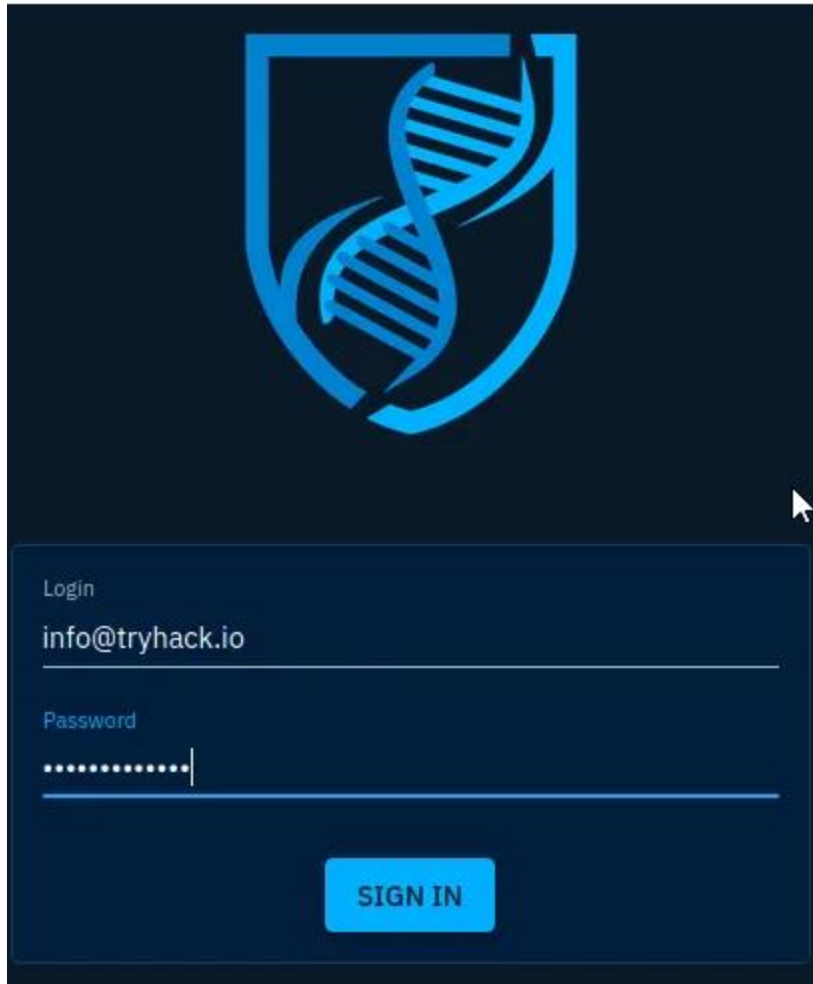


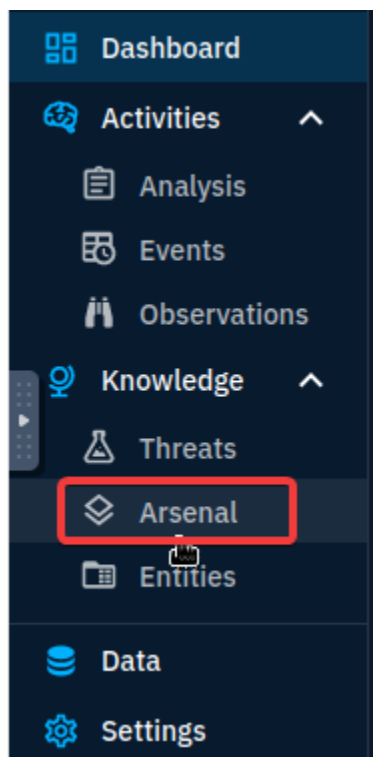
Task 4: OpenCTI Dashboard 1

To open this, you will have to start the machine by clicking on the button, and surfing to the ip within an attackbox that you can start in the room also.

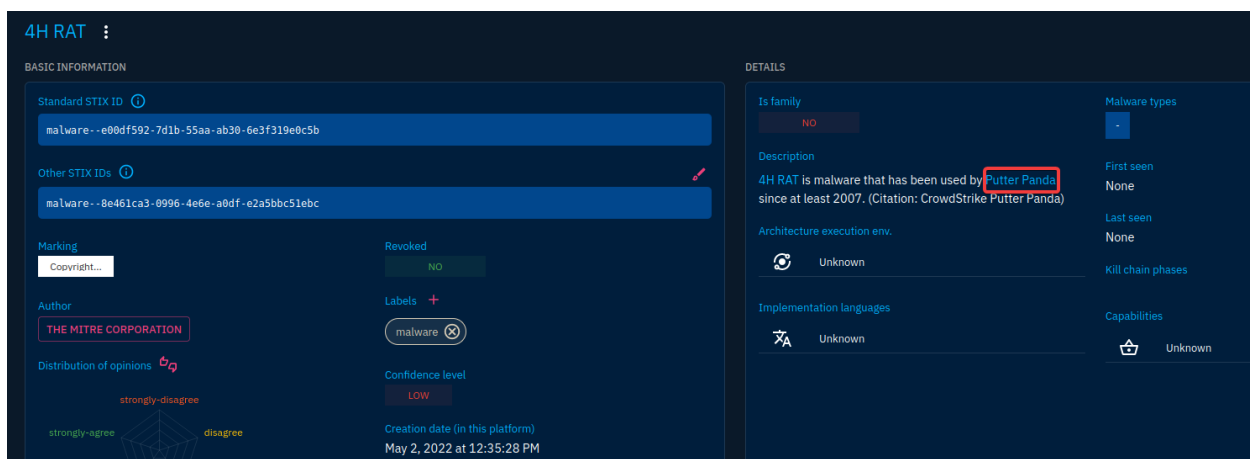


Q: What is the name of the group that uses the **4H RAT** malware?

Under the arsenal tab of the openCTI dashboard



We'll see the 4H RAT malware tab, and when we click on it we can see this:

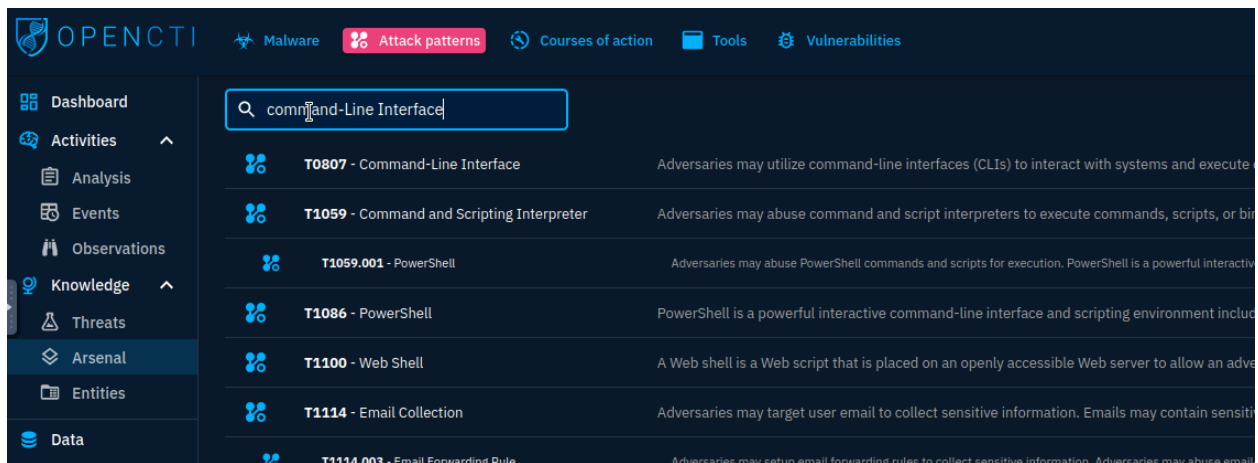


And under the details section, we can see the description.

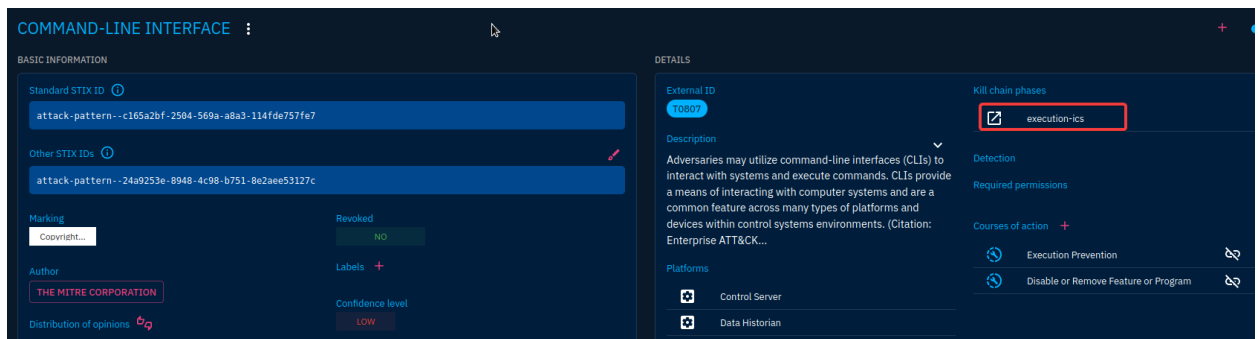
A: Putter Panda

Q: What kill-chain phase is linked with the **Command-Line Interface** Attack Pattern?

Again, under arsenal we can click on the attack patterns page, and look up command-line interface.



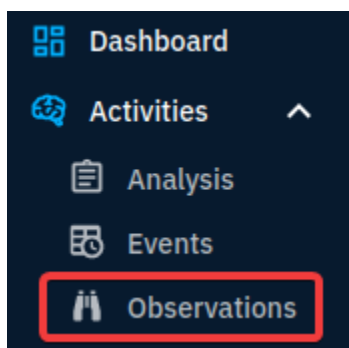
After clicking on the first option, we can see under details the kill chain phase



A: execution-ics

Q: Within the Activities category, which tab would house the **Indicators**?

Under the activities tab, there is a tab observations, which was explained earlier in the room.

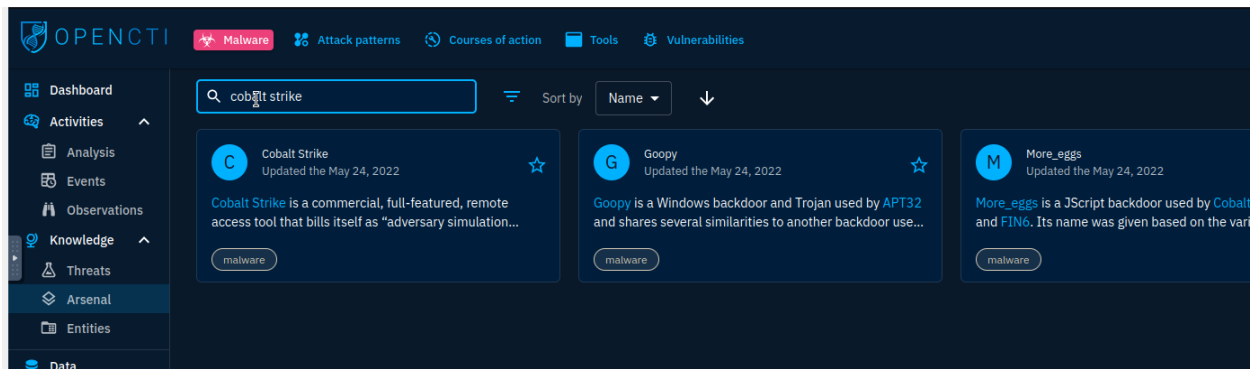


A: Observations

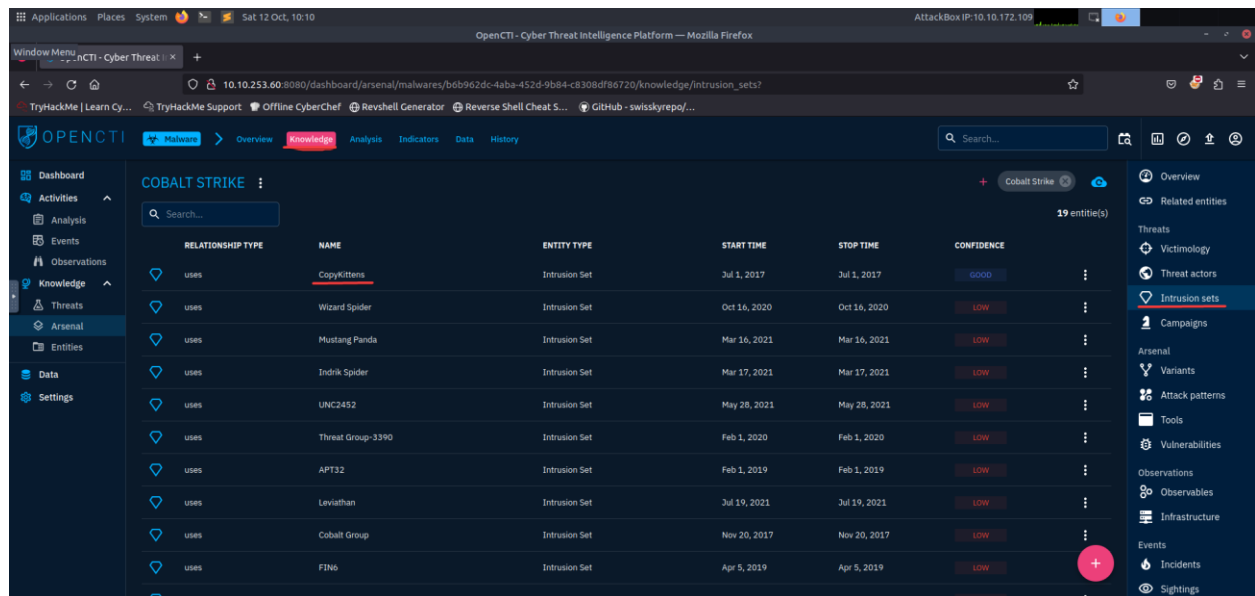
Task 5: OpenCTI Dashboard 2

Q: What Intrusion sets are associated with the Cobalt Strike malware with a Good confidence level? (Intrusion1, Intrusion2)

Under arsenal again, and searching up the cobalt strike malware. We get this.



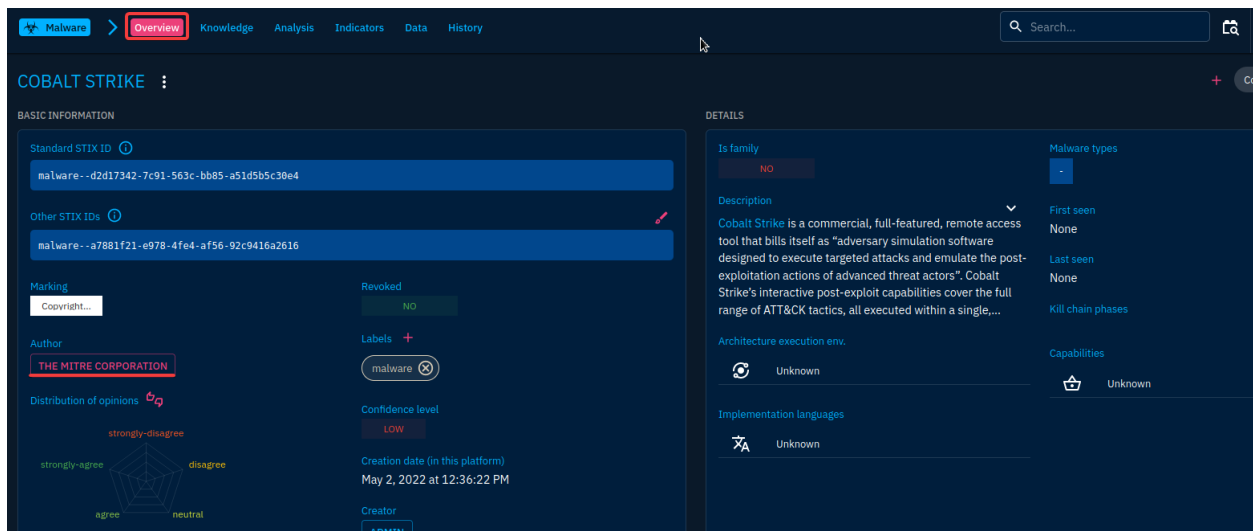
And clicking on the first option. We can go to the knowledge tab, followed by clicking on intrusion sets on the right side. And we get the uses of the app.



A: CopyKittens, FIN7

Q: Who is the author of the entity?

While staying on cobalt strike and going back to overview, we can see an author section under basic information

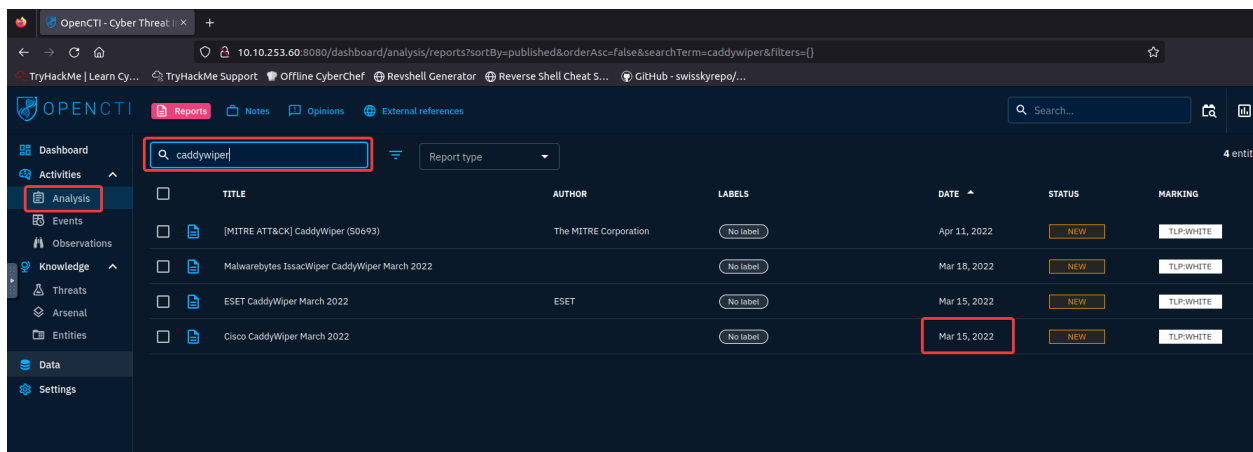


A: The MITRE Corporation

Task 6: Investigative Scenario

Q: What is the earliest date recorded related to CaddyWiper? Format: YYYY/MM/DD

Under activities, click on analysis, and look up caddywiper

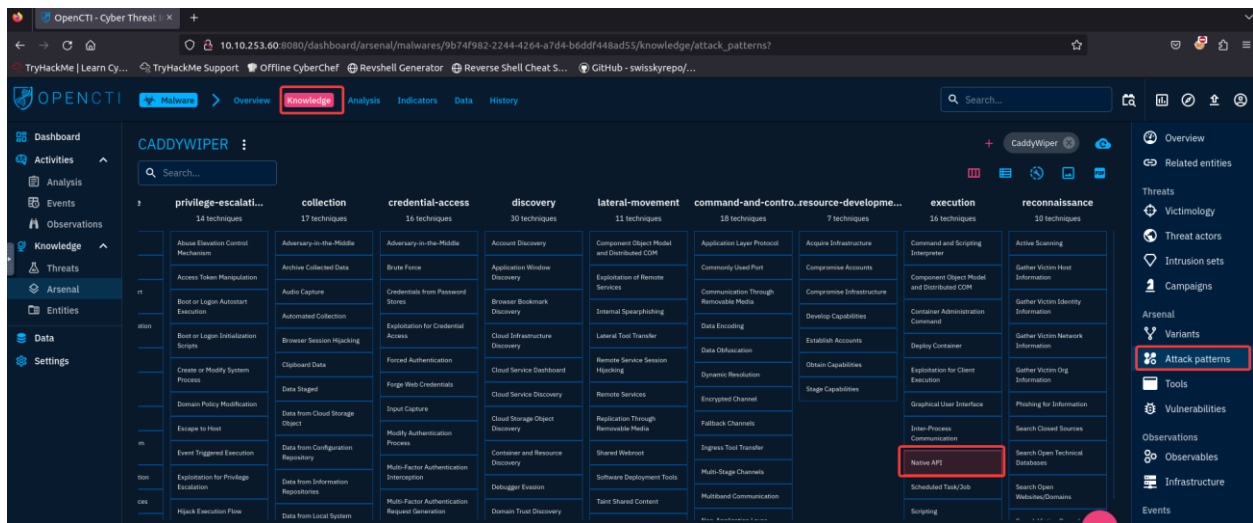


A: 2022/03/15

Q: Which **Attack technique** is used by the malware for execution?

Looking up the malware under the arsenal tab, we can find the knowledge tab, and on the right side we can select the attack patterns

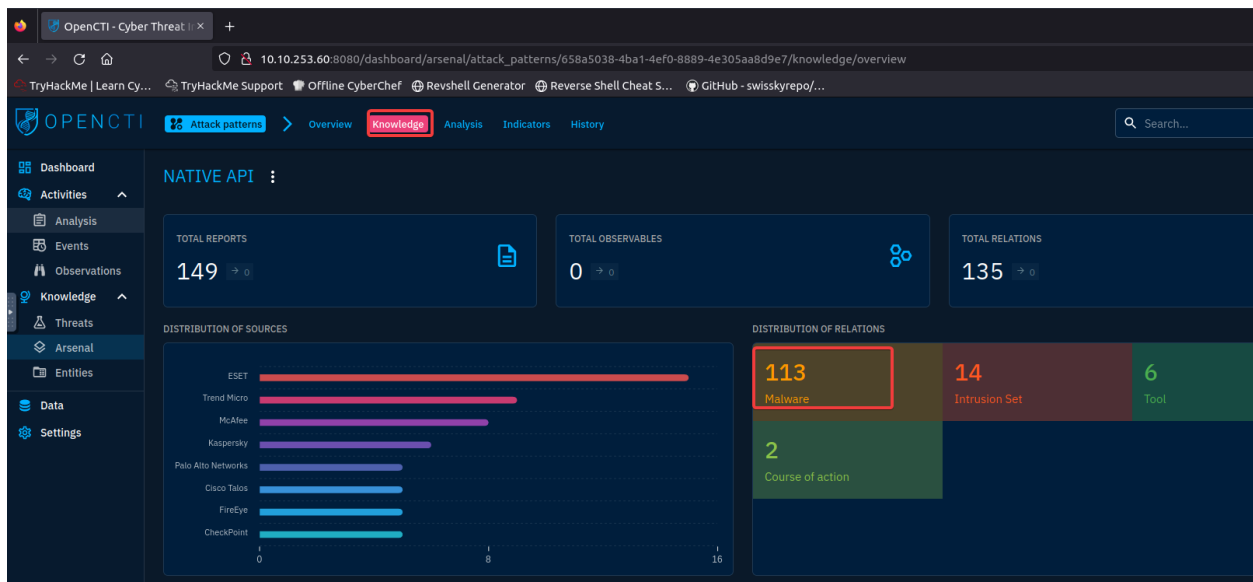
In this matrix, under execution, we can see the red coloured technique, which is Native API



A: Native API

Q: How many malware relations are linked to this Attack technique?

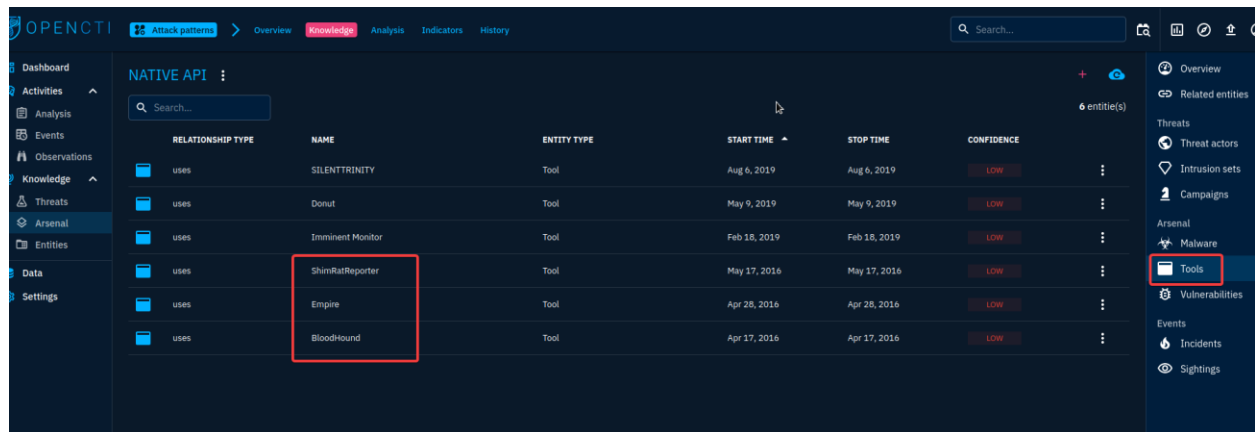
Clicking on Native api, will bring us to the attack patterns page, clicking on knowledge we can see the total relations to malware



A: 113

Q: Which 3 tools were used by the Attack Technique in 2016? (Ans: Tool1, Tool2, Tool3)

Staying on this page, under tools we can find the tools used. And only looking at 2016, we can see there is 3 tools

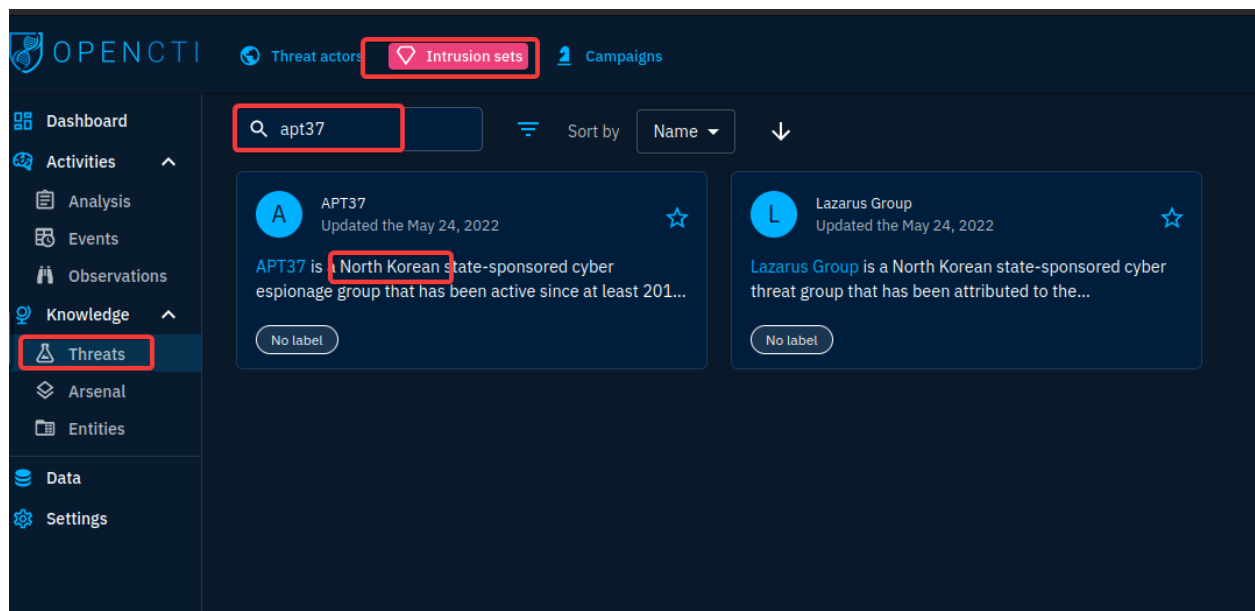


RELATIONSHIP TYPE	NAME	ENTITY TYPE	START TIME	STOP TIME	CONFIDENCE
uses	SILENTRINITY	Tool	Aug 6, 2019	Aug 6, 2019	LOW
uses	Donut	Tool	May 9, 2019	May 9, 2019	LOW
uses	Imminent Monitor	Tool	Feb 18, 2019	Feb 18, 2019	LOW
uses	ShimRatReporter	Tool	May 17, 2016	May 17, 2016	LOW
uses	Empire	Tool	Apr 28, 2016	Apr 28, 2016	LOW
uses	Bloodhound	Tool	Apr 17, 2016	Apr 17, 2016	LOW

A: ShimRatReporter, Empire, Bloodhound

Q: What country is APT37 associated with?

Under the threats tab, looking up the intrusion set apt37 will give us the result without clicking on the intrusion

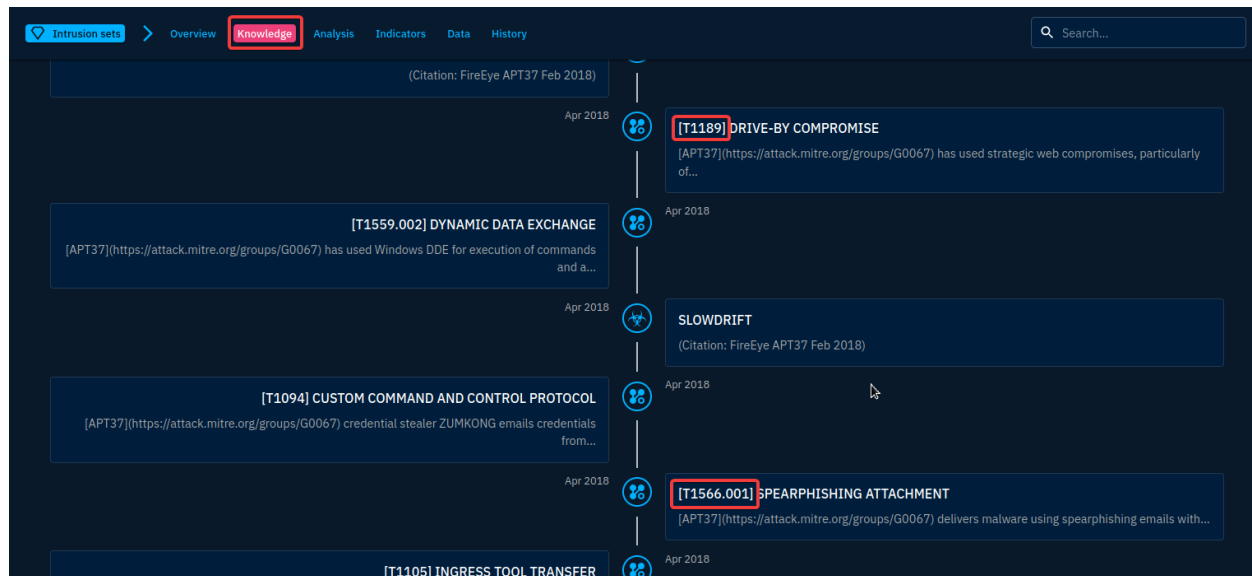


APT37 is a North Korean state-sponsored cyber espionage group that has been active since at least 2011...

A: North Korea

Q: Which Attack techniques are used by the group for initial access? (Ans: Technique1, Technique2)

Clicking on the APT37 tab, we can go to knowledge and scrolling down to the timeline, we can look up the initial access tabs and see the spearphishing and drive-by compromise.



A: T1189, T1566