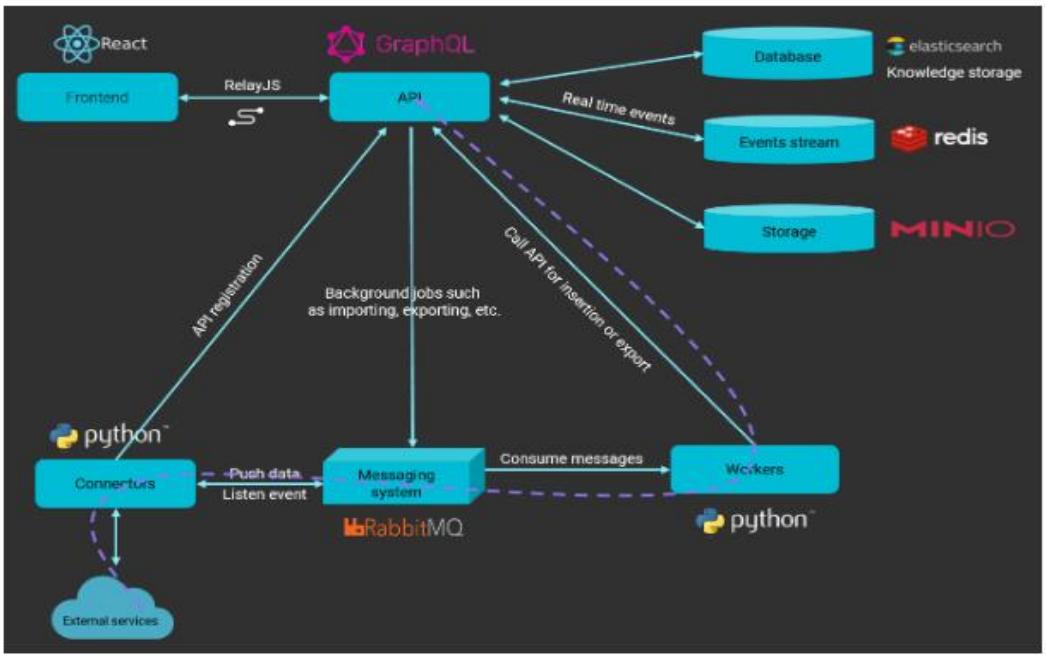
TRY HACK ME: OpenCTI Write-Up

Task 3 OpenCTI Data Model-

OpenCTI Data Model

OpenCTI uses a variety of knowledge schemas in structuring data, the main one being the Structured Threat Information Expression (STIX2) standards. STIX is a serialised and standardised language format used in threat intelligence exchange. It allows for the data to be implemented as entities and relationships, effectively tracing the origin of the provided information.

This data model is supported by how the platform's architecture has been laid out. The image below gives an architectural structure for your know-how.



The highlight services include:

GraphQL API: The API connects clients to the database and the messaging system.

Write workers: Python processes utilised to write queries asynchronously from the RabbitMQ messaging system.

Connectors: Another set of python processes used to ingest, enrich or export data on the platform. These connectors provide the application with a robust network of integrated systems and frameworks to create threat intelligence relations and allow users to improve their defence tactics.

According to OpenCTI, connectors fall under the following classes:

Class	Description	Examples
External Input Connector	Ingests information from external sources	CVE, MISP, TheHive, MITRE
Stream Connector	Consumes platform data stream	History, Tanium
Internal Enrichment Connector	Takes in new OpenCTI entities from user requests	Observables enrichment
Internal Import File Connector	Extracts information from uploaded reports	PDFs, STIX2 Import
Internal Export File Connector	Exports information from OpenCTI into different file formats	CSV, STIX2 export, PDF

Refer to the connectors and data model documentation for more details on configuring connectors and the data schema.

Answer to the questions of this section-

No Answer needed

Task 4 OpenCTI Dashboard 1-

OpenCTI Dashboard

Once connected to the platform, the opening dashboard showcases various visual widgets summarising the threat data ingested into OpenCTI. Widgets on the dashboard showcase the current state of entities ingested on the platform via the total number of entities, relationships, reports and observables ingested, and changes to these properties noted within 24 hours.

Activities & Knowledge

The OpenCTI categorises and presents entities under the Activities and Knowledge groups on the left-side panel. The activities section covers security incidents ingested onto the platform in the form of reports. It makes it easy for analysts to investigate these incidents. In contrast, the Knowledge

section provides linked data related to the tools adversaries use, targeted victims and the type of threat actors and campaigns used.

Analysis

The Analysis tab contains the input entities in reports analysed and associated external references. Reports are central to OpenCTI as knowledge on threats and events are extracted and processed. They allow for easier identification of the source of information by analysts. Additionally, analysts can add their investigation notes and other external resources for knowledge enrichment. As displayed below, we can look at the Triton Software report published by MITRE ATT&CK and observe or add to the details provided.

Events

Security analysts investigate and hunt for events involving suspicious and malicious activities across their organisational network. Within the Events tab, analysts can record their findings and enrich their threat intel by creating associations for their incidents.

Observations

Technical elements, detection rules and artefacts identified during a cyber attack are listed under this tab: one or several identifiable makeup indicators. These elements assist analysts in mapping out threat events during a hunt and perform correlations between what they observe in their environments against the intel feeds.

Threats

All information classified as threatening to an organisation or information would be classified under threats. These will include:

Threat Actors: An individual or group of attackers seeking to propagate malicious actions against a target.

Intrusion Sets: An array of TTPs, tools, malware and infrastructure used by a threat actor against targets who share some attributes. APTs and threat groups are listed under this category on the platform due to their known pattern of actions.

Campaigns: Series of attacks taking place within a given period and against specific victims initiated by advanced persistent threat actors who employ various TTPs. Campaigns usually have specified objectives and are orchestrated by threat actors from a nation state, crime syndicate or other disreputable organisation.

Arsenal

This tab lists all items related to an attack and any legitimate tools identified from the entities.

Malware: Known and active malware and trojan are listed with details of their identification and mapping based on the knowledge ingested into the platform. In our example, we analyse the 4H RAT malware and we can extract information and associations made about the malware.

Attack Patterns: Adversaries implement and use different TTPs to target, compromise, and achieve their objectives. Here, we can look at the details of the Command-Line Interface and make decisions based on the relationships established on the platform and navigate through an investigation associated with the technique.

Courses of Action: MITRE maps out concepts and technologies that can be used to prevent an attack technique from being employed successfully. These are represented as Courses of Action (CoA) against the TTPs.

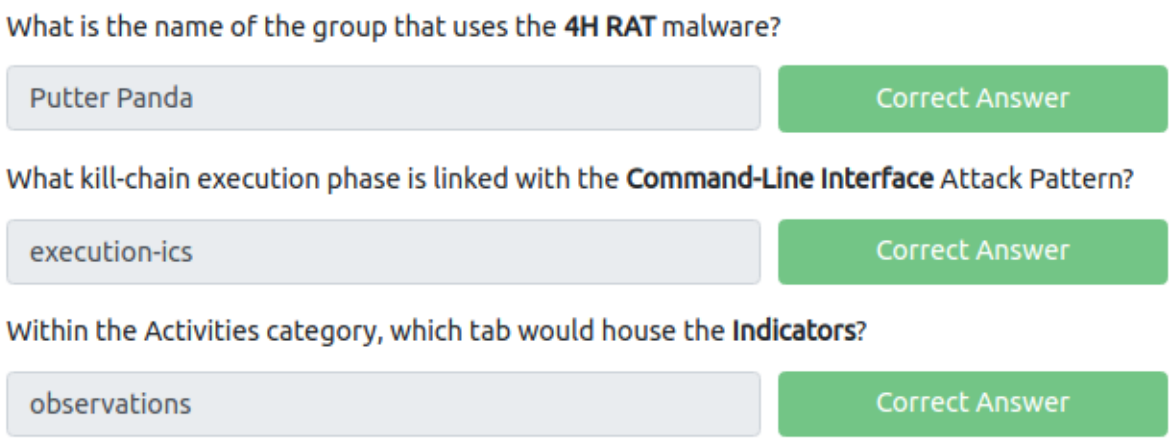
Tools: Lists all legitimate tools and services developed for network maintenance, monitoring and management. Adversaries may also use these tools to achieve their objectives. For example, for the Command-Line Interface attack pattern, it is possible to narrow down that CMD would be used as an execution tool. As an analyst, one can investigate reports and instances associated with the use of the tool.

Vulnerabilities: Known software bugs, system weaknesses and exposures are listed to provide enrichment for what attackers may use to exploit and gain access to systems. The Common Vulnerabilities and Exposures (CVE) list maintained by MITRE is used and imported via a connector.

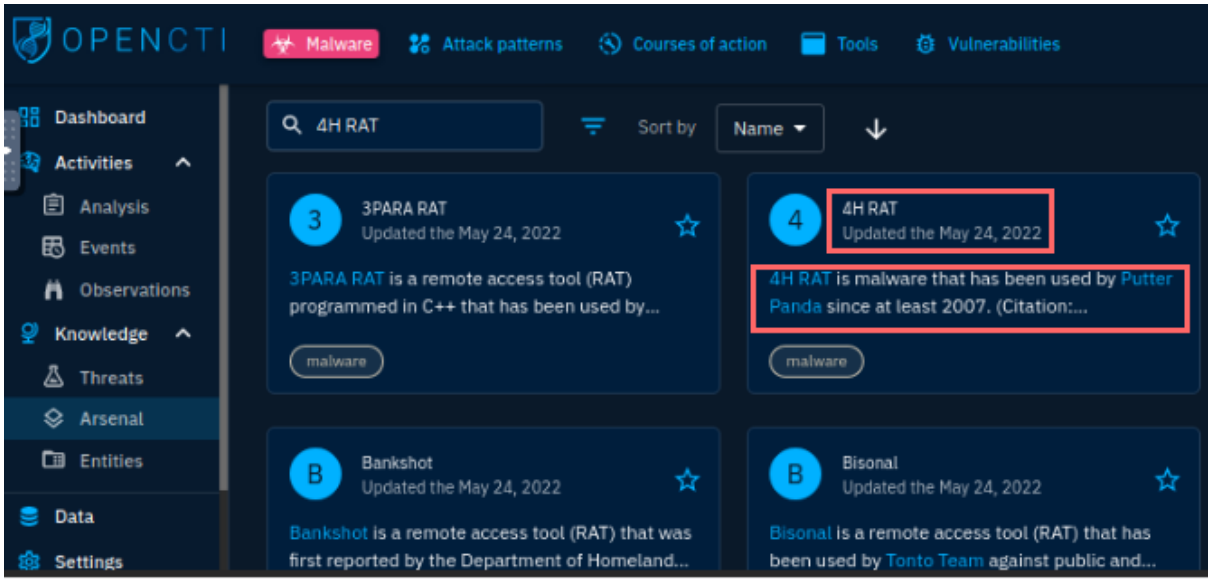
Entities

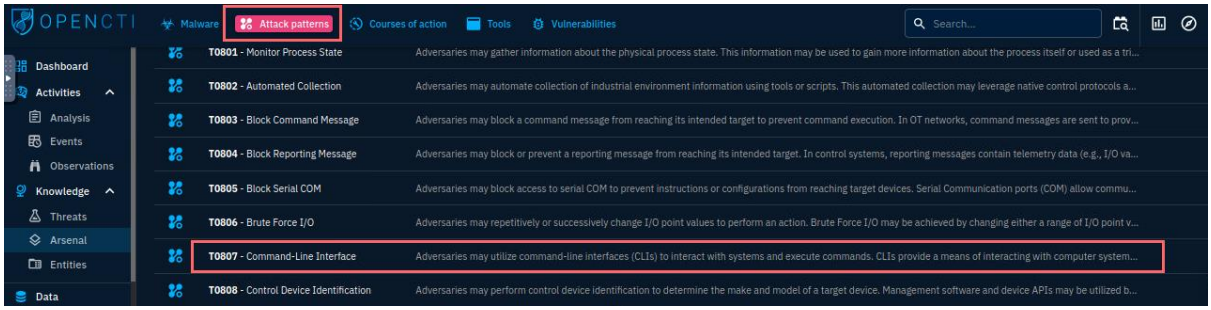
This tab categorises all entities based on operational sectors, countries, organisations and individuals. This information allows for knowledge enrichment on attacks, organisations or intrusion sets.

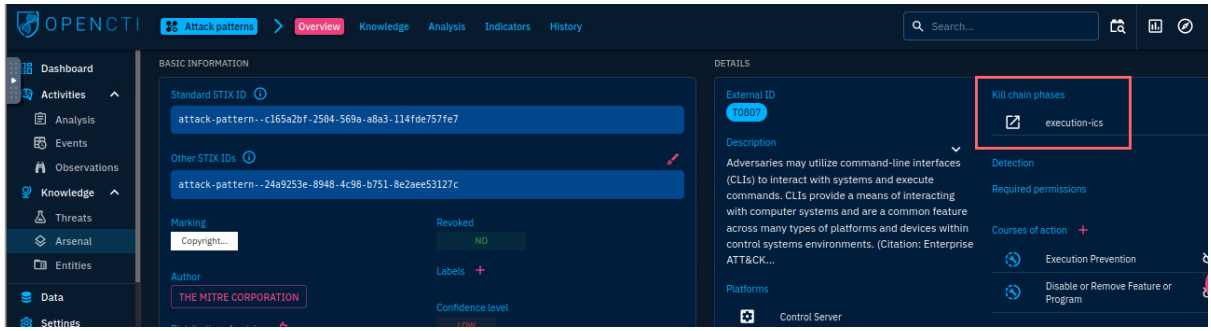
Answer to the questions of this section-

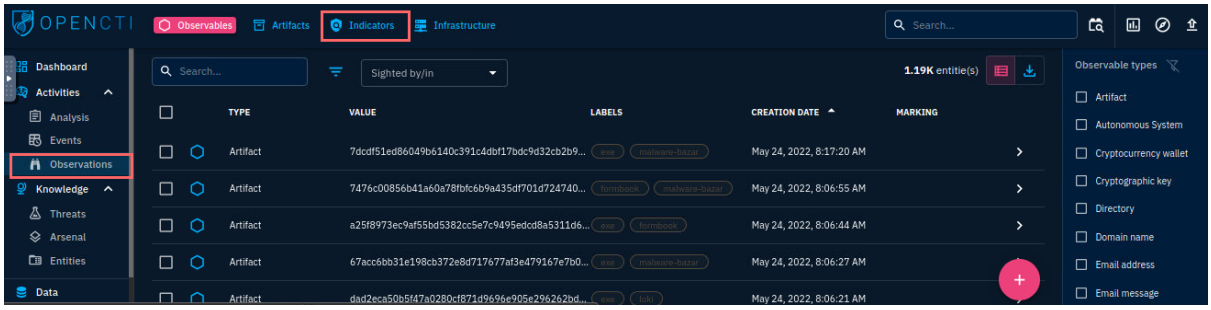


Follow the below steps to answer-









Task 5 OpenCTI Dashboard 2-

General Tabs Navigation

The day-to-day usage of OpenCTI would involve navigating through different entities within the platform to understand and utilise the information for any threat analysis. We will be looking at the

Cobalt Strike malware entity for our walkthrough, mainly found under the Arsenal tab we've covered previously. When you select an intelligence entity, the details are presented to the user through:

Overview Tab: Provides the general information about an entity being analysed and investigated. In our case, the dashboard will present you with the entity ID, confidence level, description, relations created based on threats, intrusion sets and attack patterns, reports mentioning the entity and any external references.

Knowledge Tab: Presents linked information associated with the entity selected. This tab will include the reports associated, indicators, relations and attack pattern timeline of the entity. Additionally, an analyst can view fine-tuned details from the tabs on the right-hand pane, where information about the threats, attack vectors, events and observables used within the entity are presented.

Analysis Tab: Provides the reports where the identified entry has been seen. The analysis provides usable information about a threat and guides investigation tasks.

Indicators Tab: Provides information on IOC identified for all the threats and entities.

Data Tab: Contains the files uploaded or generated for export that are related to the entity. These assist in communicating information about threats being investigated in either technical or non-technical formats.

History Tab: Changes made to the element, attributes, and relations are tracked by the platform worker and this tab will outline the changes.

Answer to the questions of this section-

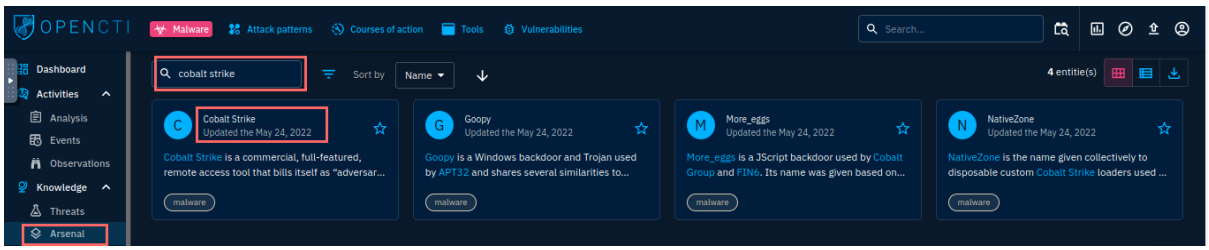
What Intrusion sets are associated with the Cobalt Strike malware with a Good confidence level? (Intrusion1, Intrusion2)

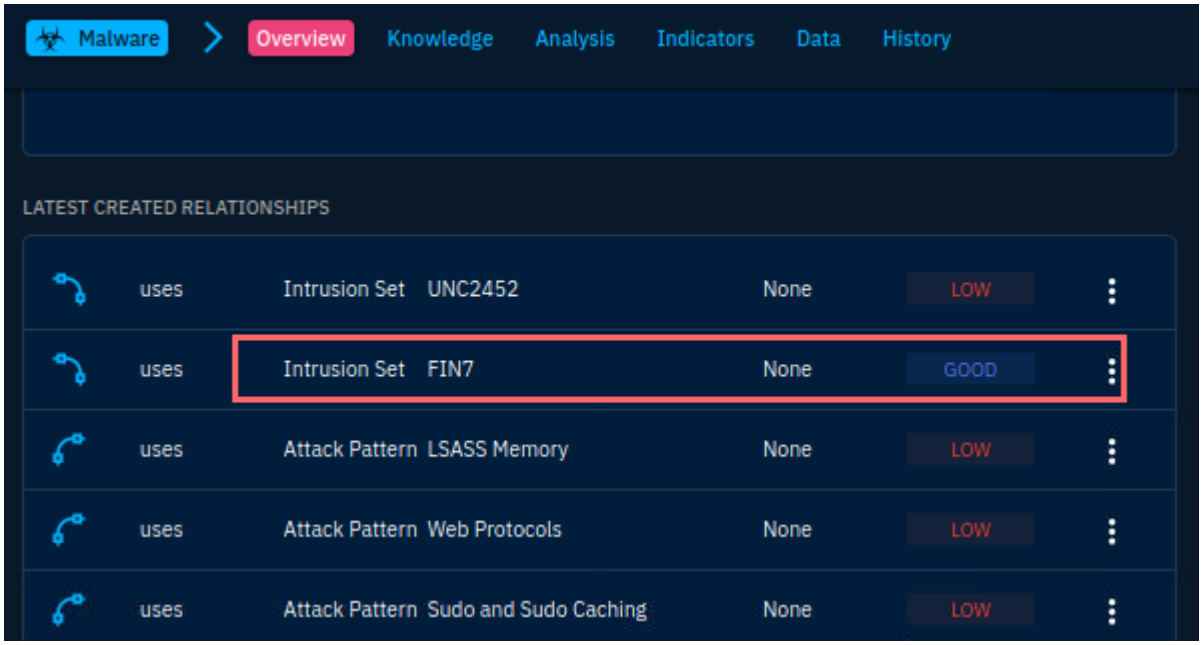
copykittens,fin7 — Correct Answer

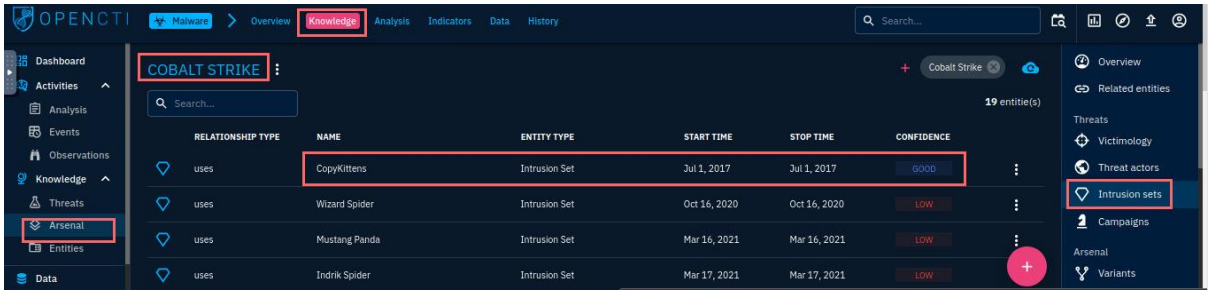
Who is the author of the entity?

the MITRE corporation — Correct Answer

Follow the below steps to answer-







Task 6 Investigative Scenario-

As a SOC analyst, you have been tasked with investigations on malware and APT groups rampaging through the world. Your assignment is to look into the **CaddyWiper malware and APT37 group**. Gather information from OpenCTI to answer the following questions.

Answer to the questions of this section-

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

2022/03/15 Correct Answer Hint

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

native Api Correct Answer Hint

How many malware relations are linked to this Attack technique?

113 Correct Answer Hint

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

bloodhound,empire,shimratreporter Correct Answer Hint

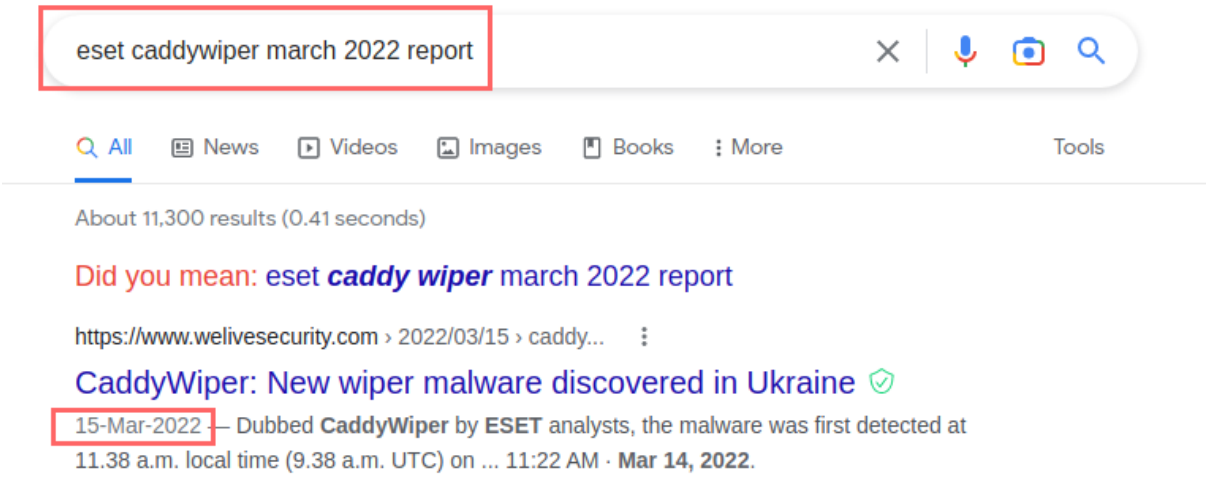
What country is **APT37** associated with?

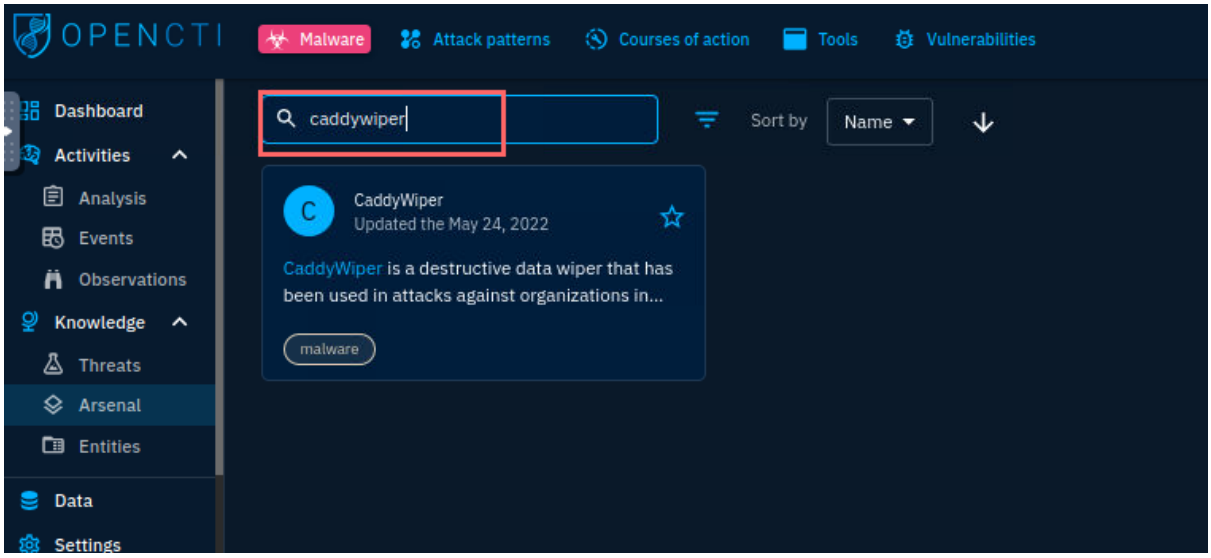
north korea Correct Answer Hint

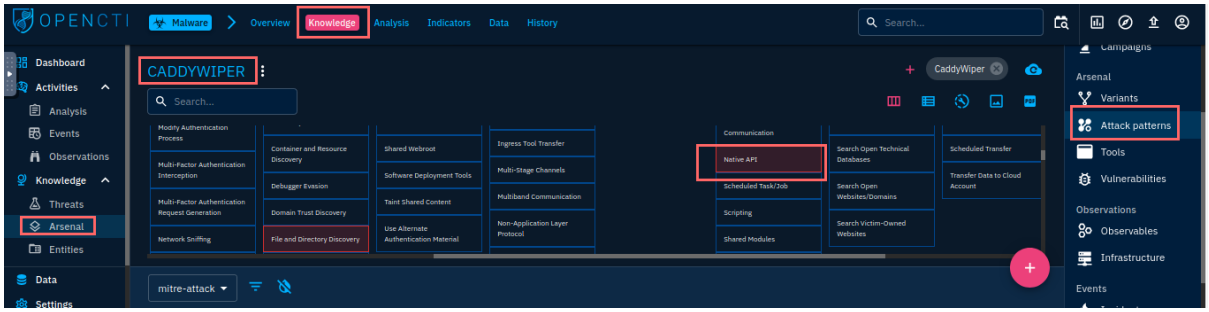
Which Attack techniques are used by the group for initial access? (Ans: Technique1, Technique2)

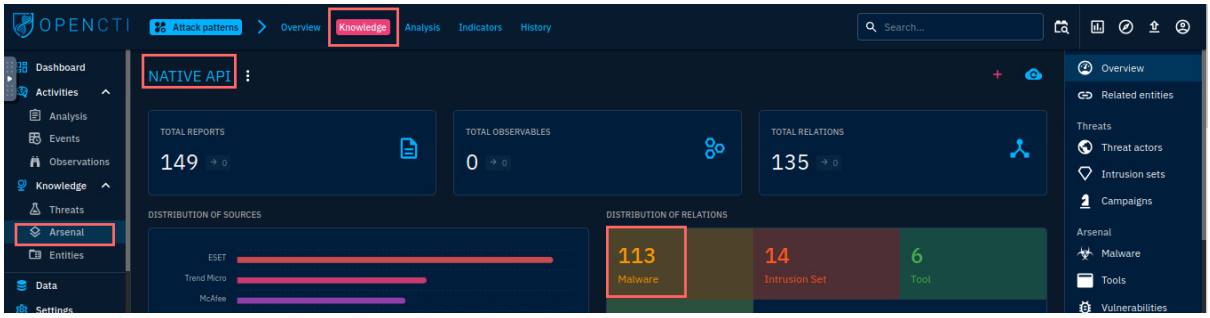
t1189,t1566 Correct Answer Hint

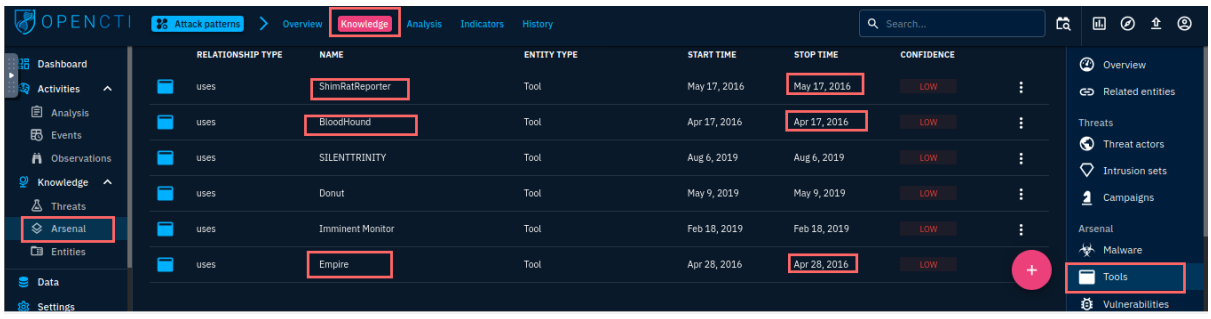
Follow the below steps to answer-

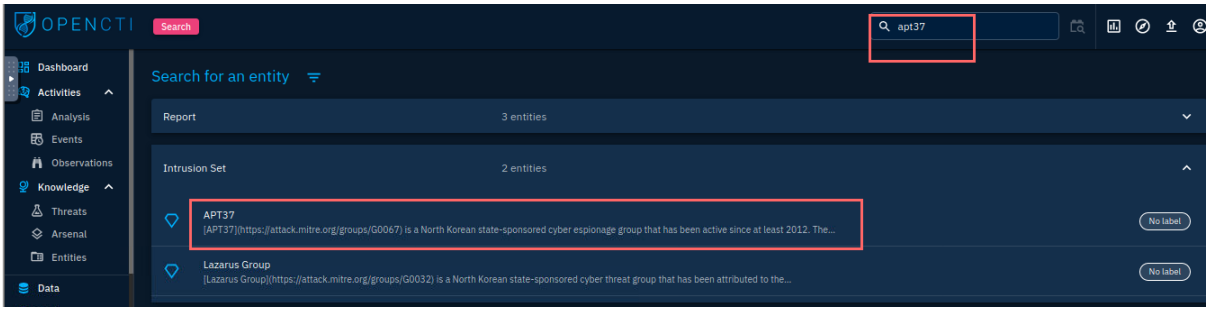


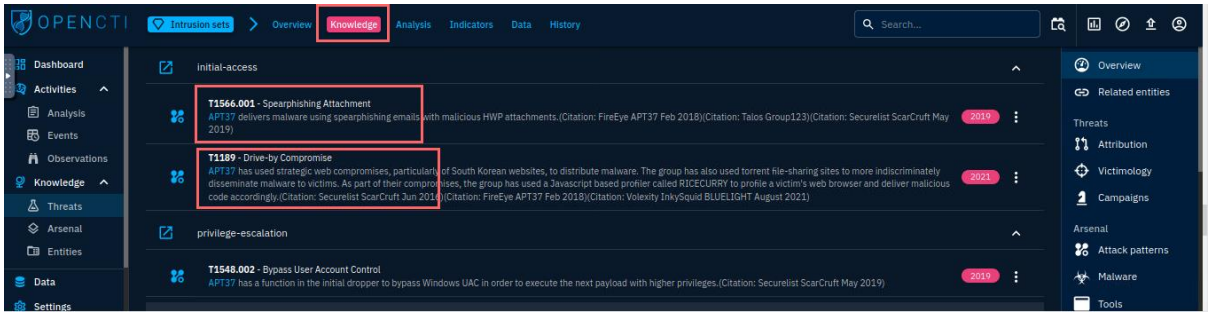

OPENCTI
Malware
Attack patterns
Courses of action
Tools
Vulnerabilities
Dashboard
Activities
Analysis
Events
Observations
Knowledge
Threats
Arsenal
Entities
Data
Settings
caddywiper
Sort by
Name
CaddyWiper
Updated the May 24, 2022
CaddyWiper is a destructive data wiper that has been used in attacks against organizations in...
malware


OPENCTI
Malware
Overview
Knowledge
Analysis
Indicators
Data
History
Search...
CADDYWIPER
CaddyWiper
Arsenal
Variants
Attack patterns
Tools
Vulnerabilities
Observations
Observables
Infrastructure
Events
mitre-attack


OPENCTI
Attack patterns
Overview
Knowledge
Analysis
Indicators
History
Search...
NATIVE API
TOTAL REPORTS
149
TOTAL OBSERVABLES
0
TOTAL RELATIONS
135
DISTRIBUTION OF SOURCES
ESET
Trend Micro
McAfee
DISTRIBUTION OF RELATIONS
113
Malware
14
Intrusion Set
6
Tool
Overview
Related entities
Threats
Threat actors
Intrusion sets
Campaigns
Arsenal
Malware
Tools
Vulnerabilities


OPENCTI
Attack patterns
Overview
Knowledge
Analysis
Indicators
History
Search...
RELATIONSHIP TYPE
NAME
ENTITY TYPE
START TIME
STOP TIME
CONFIDENCE
uses
ShimRatReporter
Tool
May 17, 2016
May 17, 2016
uses
BloodHound
Tool
Apr 17, 2016
Apr 17, 2016
uses
SILENTTRINITY
Tool
Aug 6, 2019
Aug 6, 2019
uses
Donut
Tool
May 9, 2019
May 9, 2019
uses
Imminent Monitor
Tool
Feb 18, 2019
Feb 18, 2019
uses
Empire
Tool
Apr 28, 2016
Apr 28, 2016
Overview
Related entities
Threats
Threat actors
Intrusion sets
Campaigns
Arsenal
Malware
Tools
Vulnerabilities





That is all for this Write-up, hoping this will help you in solving the challenges of OpenCTI. Have Fun and Enjoy Hacking! Do visit other rooms and modules on TryHackMe for more learning.

-by Shefali Kumai

For more cyber security learning follow me here-

https://github.com/ctf-time

https://www.youtube.com/channel/UCf-F-eATCUXYaUVk8Xl7OOQ

https://www.instagram.com/cybersecurity.cyber_seek/

https://twitter.com/Shefali37920461