



THM SOC LEVEL 1

CYBER THREAT INTELLIGENCE

Mikhail Amzar

5/13/2024

Try Hack Me's SOC
Level 1 Training Course
self-notes 2/7.

CONTENTS

Cyber Threat Intelligence	2
Intro to Cyber Threat Intel	2
1.Introduction.....	2
2.CTI Lifecycle.....	3
3.CTI Standards and & Frameworks	3
4.Additionals on CTI	4
Threat Intelligence Tools.....	4
1.Threat Intelligence	4
2.Abuse.ch.....	4
3.PhishTool	5
4.Cisco Talos Intelligence	6
Yara.....	8
1.What is Yara?.....	8
2.Yara Rule	8
3.Yara Modules.....	11
4.Other tools.....	11
OpenCTI.....	15
1.Intro to OpenCTI.....	15
2.OpenCTI Data Model.....	15
3.Dashboard.....	17
4.Investigative Scenario using OpenCTI	20
MISP (Malware Information Sharing Platform)	24
1.What is MISP?.....	24
2.Using the system – MISP	25
Holotapes.....	26

CYBER THREAT INTELLIGENCE

INTRO TO CYBER THREAT INTEL

1.Introduction

Def: Evidence-based knowledge about adversaries, their indicator, motivation, tactics. CTI is vital for investigation and reporting against attacks.

Objectives:

- The basics of CTI.
- Lifecycle to deploy and use intelligence during investigations.
- Frameworks and standards used in distributing intelligence.

Primary goal of CTI is to understand relationship between your operational environment and your adversary & how to defend your environment.

- Who is attacking you?
- What are their motivations?
- What are their capabilities?
- What artefacts & indicators of compromise should you look out for?

The sources of threat intelligence you can look from:

- **Internal** (Corpo sec events, vuln assessments, IR report, system logs & events)
- **Community** (Forums etc)
- **External** (Threat intel feed, publications, socmed, government data)

2.CTI Lifecycle



6 phases to gather and analyze threat intel.

3.CTI Standards and & Frameworks

- MITRE ATT&CK
- TAXII
 - Trusted Automated eXchange of Indicator Information.
 - Defines transport protocols for securely exchanging threat intel to have near real-time detection, prevention and mitigation of threats. The protocol supports two sharing models:
 - Collection: Threat intel is collected and hosted by a producer upon request by users using a request-response model.
 - Channel: Threat intel is pushed to users from a central server through a publish-subscribe model.
- STIX
 - Structured Threat Information Expression
 - It's a language developed for the "specification, capture, characterization and communication of standardized cyber threat information.
- Cyber Kill Chain
 - Breaking down adversary actions into steps.
- The Diamond Model

4.Additionals on CTI

Some notable threat reports come from [Mandiant](#), [Recorded Future](#) and [AT&TCybersecurity](#).

THREAT INTELLIGENCE TOOLS

1.Threat Intelligence

Objectives:

- Understanding the basics of threat intelligence & its classifications.
- Using UrlScan.io to scan for malicious URLs.
- Using Abuse.ch to track malware and botnet indicators.
- Investigate phishing emails using PhishTool
- Using Cisco's Talos Intelligence platform for intel gathering.

Classification of Threat Intelligence:

Strategic Intel – Technical Intel – Tactical Intel – Operational Intel

Urlscan.io

Website analyzer and scanner.

- **Summary:**
Provides general information about the URL, ranging from the identified IP address, domain registration details, page history and a screenshot of the site.
- **HTTP:**
Provides information on the HTTP connections made by the scanner to the site, with details about the data fetched and the file types received.
- **Redirects:**
Shows information on any identified HTTP and client-side redirects on the site.
- **Links:**
Shows all the identified links outgoing from the site's homepage.
- **Behaviour:**
Provides details of the variables and cookies found on the site. These may be useful in identifying the frameworks used in developing the site.
- **Indicators:**
Lists all IPs, domains and hashes associated with the site. These indicators do not imply malicious activity related to the site.

2.Abuse.ch

Platform encompassing resources for malware and botnets etc.

MalwareBazaar

Sharing malware samples and malware hunting for investigative and analysis efforts.

<https://bazaar.abuse.ch/browse/>

FeodoTracker

Intelligence on botnet Command & Control (C&C) servers associated with Dridex, Emotes (aka Heodo), TrickBot, QakBot and BazarLoader/BazarBackdoor.

<https://feodotracker.abuse.ch/>

SSL Blacklist

Tool to identify and detect malicious SSL connections.

<https://sslbl.abuse.ch/>

URLhaus

This tool focuses on sharing malicious URLs used for malware distribution. As an analyst, you can search through the database for domains, URLs, hashes and filetypes that are suspected to be malicious and validate your investigations.

<https://urlhaus.abuse.ch/>

ThreatFox

With ThreatFox, security analysts can search for, share and export indicators of compromise associated with malware. IOCs can be exported in various formats such as MISP events, Suricata IDS Ruleset, Domain Host files, DNS Response Policy Zone, JSON files and CSV files.

<https://threatfox.abuse.ch/>

3. PhishTool

[Extensive email analysis tool for phishing emails](#). Uncover email IOCs, prevent breaches, provide forensic reports, and understand TTPs used to evade (security controls and perform social engineering).

<https://app.phishtool.com/sign-up/community>

[PhishTool](#) seeks to elevate the perception of phishing as a severe form of attack and provide a responsive means of email security. Through email analysis, security analysts can uncover email IOCs, prevent breaches and provide forensic reports that could be used in phishing containment and training engagements.

Features:

- **Perform email analysis:** PhishTool retrieves metadata from phishing emails and provides analysts with the relevant explanations and capabilities to follow the email's actions, attachments, and URLs to triage the situation.

- **Heuristic intelligence:** OSINT is baked into the tool to provide analysts with the intelligence needed to stay ahead of persistent attacks and understand what TTPs were used to evade security controls and allow the adversary to social engineer a target.
 - **Classification and reporting:** Phishing email classifications are conducted to allow analysts to take action quickly. Additionally, reports can be generated to provide a forensic record that can be shared.
- [Phishing Emails 1](#)
 - [Phishing Emails 2](#)
 - [Phishing Emails 3](#)
 - [Phishing Emails 4](#)
 - [Phishing Emails 5](#)

4.Cisco Talos Intelligence

A solution by Cisco Talos to provide intelligence on emerging threats.



Six key teams:

- **Threat Intelligence & Interdiction:** Quick correlation and tracking of threats provide a means to turn simple IOCs into context-rich intel.
- **Detection Research:** Vulnerability and malware analysis is performed to create rules and content for threat detection.
- **Engineering & Development:** Provides the maintenance support for the inspection engines and keeps them up to date to identify and triage emerging threats.
- **Vulnerability Research & Discovery:** Working with service and software vendors to develop repeatable means of identifying and reporting security vulnerabilities.
- **Communities:** Maintains the image of the team and the open-source solutions.

- **Global Outreach:** Disseminates intelligence to customers and the security community through publications.

Talos Dashboard:

Vulnerability Information

Vulnerability reports with CVE& CVSS scores, any disclosed vuln either zero-day or not. Details of vuln provided.

Reputation Center

Access to searchable threat data related to IPs and files using their SHA256 hashes.

YARA

1.What is Yara?

Yara is a tool that can identify information based on both binary and textual patterns, such as hexadecimal and strings contained within a file.

<https://github.com/virustotal/yara>

Exm: Write a Yara rule to search for "hello world" in every program in our OS

```
print("Hello World!")
```

So, in malware you might be searching for a string of data like bitcoin wallet (ransomware) and IP address of C2 server (botnet).

2.Yara Rule

Every **yara** command needs 2 arguments, which is the rule file you made, and name of the file, directory, or process ID to use the rule for.

<https://yara.readthedocs.io/en/stable/writingrules.html>

```
cmnatic@thm nano myfirstrule.yar
rule exemplerule {
    condition: true
}
```

```
cmnatic@thm-yara:~$ yara myfirstrule.yar somefile
exemplerule somefile
```

Checking if the subject contains "Hello World!" string.

```
rule helloworld_checker{
    strings:
        $hello_world = "Hello World!"

    condition:
        $hello_world
}

rule helloworld_checker{
    strings:
        $hello_world = "Hello World!"
        $hello_world_lowercase = "hello world"
        $hello_world_uppercase = "HELLO WORLD"
```

```
    condition:
        any of them
}
```

What about other operation like >, <, != ?

```
rule helloworld_checker{
    strings:
        $hello_world = "Hello World!"

    condition:
        #hello_world <= 10
}
```

- Look for the "Hello World!" string.
- Only say the rule matches if there are less than or equal to ten occurrences of the "Hello World!" string.

And – Not – Or

```
rule helloworld_checker{
    strings:
        $hello_world = "Hello World!"

    condition:
        $hello_world and filesize < 10KB
}
```

Check if a file has a string and id less than <10 kb and has "Hello World!".

ANATOMY OF A YARA RULE



Yara is a tool used to identify file, based on **textual or binary pattern**.



A rule consists of a **set of strings and conditions** that determine its logic.



Rules can be compiled with "yara" to **increase the speed** of multiple Yara scans.

1

IMPORT MODULE

Yara modules allow you to extend its functionality. The PE module can be used to match specific data from a PE:

- `pe.number_of_exports`
- `pe.sections[0].name`
- `pe.imphash()`
- `pe.imports("kernel32.dll")`
- `pe.is_dll()`

List of modules: `pe`, `elf`, `hash`, `math`, `cuckoo`, `dotnet`, `time`

2

RULE NAME

The rule name identifies your Yara rule. It is recommended to add a meaningful name. There are different types of rules:

- Global rules: applies for all your rules in the file.
- Private rules: can be called in a condition of a rule but not reported.
- Rule tags: used to filter yara's output.

3

METADATA

Rules can also have a metadata section where you can put additional information about your rule.

- Author
- Date
- Description
- Etc...

4

STRINGS

The field strings is used to define the strings that should match your rule. It exists 3 type of strings:

- Text strings
- Hexadecimal strings
- Regex

5

CONDITION

Conditions are Boolean expressions used to match the defined pattern.

- Boolean operators:
 - `and`, `or`, `not`
 - `<`, `>`, `==`, `<`, `>`, `!=`
- Arithmetic operators:
 - `+`, `-`, `*`, `\`, `%`
- Bitwise operators:
 - `&`, `|`, `<<`, `>>`, `^`, `~`
- Counting strings:
 - `#string0 == 5`
- Strings offset:
 - `$string1 at 100`

```
import "pe"

rule demo_rule : Tag1 Demo
{
  meta:
    author = "Thomas Roccia"
    description = "demo"
    hash = ""

  strings:
    $string0 = "hello" nocase wide
    $string1 = "world" fullword ascii
    $hex1 = { 01 23 45 ?? 89 ab cd ef }
    $rel1 = /md5: [0-9a-zA-Z]{32}/

  condition:
    uint16(0) == 0x5A4D and filesize < 2000KB
    or pe.number_of_sections == 1 and
    any of ($string*) and (not $hex1 or $rel1)
}
```

TEXT STRINGS

Text strings can be used with modifiers:

- `nocase`: case insensitive
- `wide`: encoded strings with 2 bytes per character
- `fullword`: non alphanumeric
- `xor(0x01-0xff)`: look for xor encryption
- `base64`: base64 encoding

HEXADECIMAL

Hex strings can be used to match piece of code:

- Wild-cards: `{ 00 ?2 A? }`
- Jump: `{ 3B [2-4] B4 }`
- Alternatives: `{ F4 (B4 | 56) }`

REGEX

Regular expression can also be used and defined as text strings but enclosed in forward slash.

ADVANCED CONDITION

- Accessing data at a given position: `uint16(0) == 0x5A4D`
- Check the size of the file: `filesize < 2000KB`
- Set of strings: `any of ($string0, $hex1)`
- Same condition to many strings: for all of them: `(# > 3)`
- Scan entry point: `$value at pe.entry_point`
- Match length: `!rel[1] == 32`
- Search within a range of offsets: `$value in (0,100)`

 @FR0GGER_
THOMAS ROCCIA

3.Yara Modules

Frameworks such as the [Cuckoo Sandbox](#) or [Python's PE Module](#) allow you to improve the technicality of your Yara rules ten-fold.

[Cuckoo Sandbox](#) is an automated malware analysis environment. This module allows you to generate Yara rules based upon the behaviors discovered from Cuckoo Sandbox. As this environment executes malware, you can create rules on specific behaviors such as runtime strings and the like.

[Python's PE](#) module allows you to create Yara rules from the various sections and elements of the Windows Portable Executable (PE) structure.

<https://github.com/Neo23x0/yarGen>

<https://www.bsk-consulting.de/2015/02/16/write-simple-sound-yara-rules/>

<https://www.bsk-consulting.de/2015/10/17/how-to-write-simple-but-sound-yara-rules-part-2/>

<https://www.bsk-consulting.de/2016/04/15/how-to-write-simple-but-sound-yara-rules-part-3/>

<https://github.com/Neo23x0/yarAnalyzer/>

YarGen to help generate rules.

"The main principle is the creation of yara rules from strings found in malware files while removing all strings that also appear in goodware files. Therefore, yarGen includes a big goodware strings and opcode database as ZIP archives that have to be extracted before the first use."

4.Other tools

LOKI

LOKI is a free open-source IOC (*Indicator of Compromise*) scanner.

<https://github.com/Neo23x0/Loki/releases>

```

cmnatic@thm:~/Loki$ python3 loki.py -h
usage: loki.py [-h] [-p path] [-s kilobyte] [-l log-file] [-r remote-loghost]
               [-t remote-syslog-port] [-a alert-level] [-w warning-level]
               [-n notice-level] [--allhds] [--alldrives] [--printall]
               [--allreasons] [--noprocsan] [--nofilescan] [--vulnchecks]
               [--nolevcheck] [--scriptanalysis] [--rootkit] [--noindicator]
               [--dontwait] [--intense] [--csv] [--onlyrelevant] [--nolog]
               [--update] [--debug] [--maxworkingset MAXWORKINGSET]
               [--syslogtcp] [--logfolder log-folder] [--nopesieve]
               [--pesieveshellc] [--python PYTHON] [--nolisten]
               [--excludeprocess EXCLUDEPROCESS] [--force]

Loki - Simple IOC Scanner

optional arguments:
  -h, --help            show this help message and exit

```

THOR

THOR *Lite* is Florian's newest multi-platform IOC AND YARA scanner. (THOR lite is free, THOR is more meant for corpo)

<https://www.nextron-systems.com/thor-lite/>

Fenrir

Simple bash IoC checker

<https://github.com/Neo23x0/Fenrir>

YAYA (Yet Another YARA Automaton)

"YAYA is a new open-source tool to help researchers manage multiple YARA rule repositories. YAYA starts by importing a set of high-quality YARA rules and then lets researchers add their own rules, disable specific rulesets, and run scans of files."

<https://github.com/EFForq/yaya>

Exms:

One of the YARA file in Loki signature-base directory:

```

import "pe"

rule Win32 Ransomware WannaCry : tc detection malicious
{
    meta:
        author = "ReversingLabs"
        source = "ReversingLabs"
        status = "RELEASED"
        sharing = "TLP:WHITE"
        category = "MALWARE"
        malware = "WANNACRY"
        description = "Yara rule that detects WannaCry ransomware."

        tc detection type = "Ransomware"
        tc detection name = "WannaCry"
        tc detection factor = 5

    strings:
        $main 1 = {
            A0 ?? ?? ?? ?? 56 57 6A ?? 88 85 ?? ?? ?? ?? 59 33 C0 8D BD ?? ?
            AA 8D 85 ?? ?? ?? ?? 68 ?? ?? ?? ?? 50 53 FF 15 ?? ?? ?? ?? 8B 3
            ?? ?? ?? ?? 6A ?? 50 FF D6 59 85 C0 59 74 ?? 8D 85 ?? ?? ?? ?? 6
            18 59 8D 85 ?? ?? ?? ?? 50 FF 15 ?? ?? ?? ?? 68 ?? ?? ?? ?? 53 E
            8D 8D ?? ?? ?? ?? E8 ?? ?? ?? ?? 53 53 53 8D 8D ?? ?? ?? ?? E8 ?
            C0 74 ?? 8D 45 ?? 8D 8D ?? ?? ?? ?? 50 68 ?? ?? ?? ?? 89 5D
        }

        $main 2 = {
            68 ?? ?? ?? ?? 33 DB 50 53 FF 15 ?? ?? ?? ?? 68 ?? ?? ?? ?? E8 ?
            ?? ?? ?? ?? 83 38 ?? 75 ?? 68 ?? ?? ?? ?? FF 15 ?? ?? ?? ?? 8B 0
            ?? ?? 59 85 C0 59 75 ?? 53 E8 ?? ?? ?? ?? 85 C0 59 74 ?? BE ?? ?
            ?? ?? ?? 56 50 FF 15 ?? ?? ?? ?? 56 FF 15 ?? ?? ?? ?? 83 F8 ?? 7
            85 C0 0F 85 ?? ?? ?? ?? 8B 35 ?? ?? ?? ?? 8D 85 ?? ?? ?? ?? 6A ?
            59 74 ?? 8D 85 ?? ?? ?? ?? 6A ?? 50 FF D6 59 88 18 59 8D 85 ?? ?
            ?? ?? ?? 6A ?? E8 ?? ?? ?? ?? C7 04 24 ?? ?? ?? ?? 53 E8 ?? ?? ?
            53 53 68 ?? ?? ?? ?? E8 ?? ?? ?? ?? 53 53 68 ?? ?? ?? ?? E8
        }
}


```

Theres more ofc in the signature-base:

cn pentestset tools.yar	Win32.Ransomware.Maktub.yara
cn pentestset webshells.yar	Win32.Ransomware.Marlboro.yara
crime academic data centers camp may20.yar	Win32.Ransomware.MarsJoke.yara
crime andromeda jun17.yar	Win32.Ransomware.Matsnu.yara
crime antifw installrex.yar	Win32.Ransomware.MedusaLocker.yara
crime atm dispenserxfs.yar	Win32.Ransomware.Montserrat.yara
crime atm javadipcash.yar	Win32.Ransomware.MZP.yara
crime atm loup.yar	Win32.Ransomware.NanoLocker.yara
crime atm xfsadm.yar	Win32.Ransomware.Nefilim.yara
crime atm xfscashocr.yar	Win32.Ransomware.Nemty.yara

Valhalla – by Florian Roth (just like most previous tool)

[Online Yara feed.](#)



VALHALLA
 SUPERCHARGE YOUR DETECTION

Keyword: 53fe44b4753874f079a936325d1fdc9b1691956a29c3aaf8643cddb49f5984bf (Results: 4)

Query Search

Type	Rule Name	Description	Date	Reference	Ref	VT	Info
YARA	WebshellRepo_convert	Detects Webshell - file convert.php	2016-12-09	Webshell Repos			
YARA	Operation_Email_Webshell_plugins.php	Detects an Operation Email Webshell - file plugins.php	2016-07-29	Operation Email			
YARA	Webshell_b374k_rule1	Detects b374k webshell	2015-10-16	https://github.com/b374k/b374k			
YARA	Webshell_b374k_rule2	Detects b374k webshell	2015-10-16	https://github.com/b374k/b374k			


Checking VT results from Valhalla:


thor
 2 days ago [ce39a9115aaadd201e06c186d6a2ea68703dc1db06a33050607f35ec647d3d0e](#)

YARA Signature Match - THOR APT Scanner

RULE: Webshell_b374k_rule2
 RULE_SET: Livehunt - Webshells4 Indicators 🍷
 RULE_TYPE: VALHALLA rule feed only ⚡
 RULE_LINK: https://valhalla.nexttron-systems.com/info/rule/Webshell_b374k_rule2
 DESCRIPTION: Detects b374k webshell
 REFERENCE: <https://github.com/b374k/b374k>
 RULE_AUTHOR: Florian Roth

Show more


thor
 3 days ago [0e9da58fb0bbd4d95ba1ecec6578b8aefca67a729c415e8362b3d498a50a0e82](#)

YARA Signature Match - THOR APT Scanner

RULE: Webshell_b374k_rule2
 RULE_SET: Livehunt - Webshells35 Indicators 🍷
 RULE_TYPE: VALHALLA rule feed only ⚡

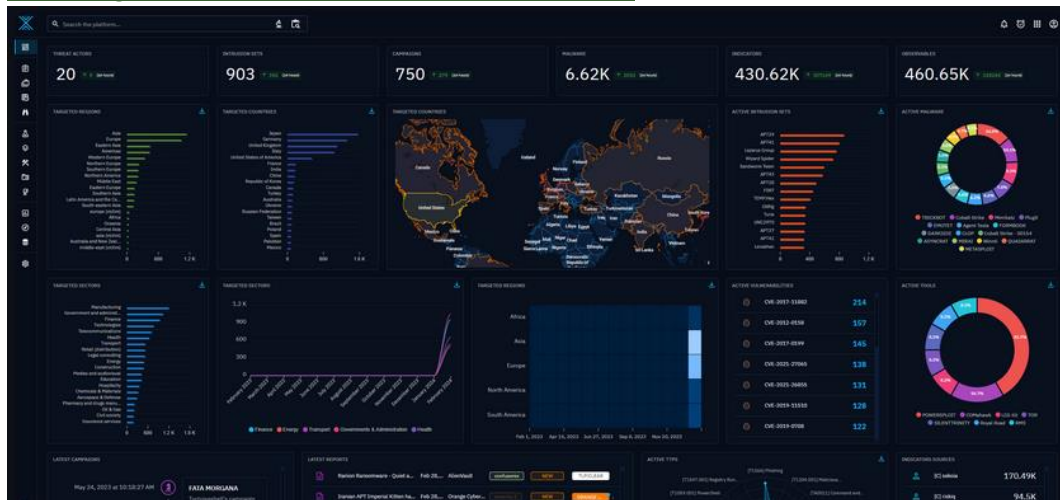
OPENCTI

1.Intro to OpenCTI

What is Open CTI?

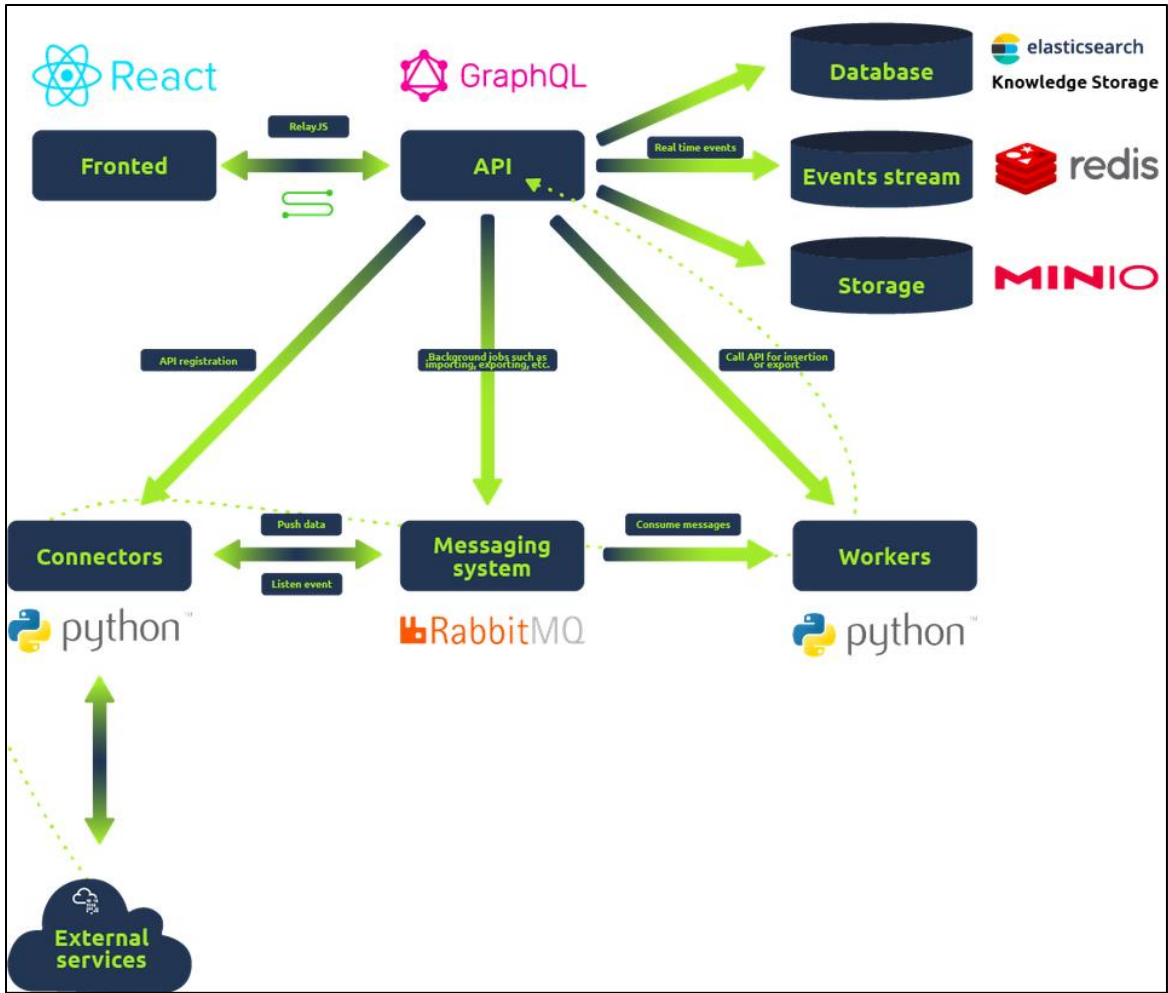
Open-sourced platform designed to provide organizations with the means to manage CTI through the storage, analysis, visualization and presentation of threat campaigns, malware, and IOCs.

<https://github.com/OpenCTI-Platform/opencti>



2.OpenCTI Data Model

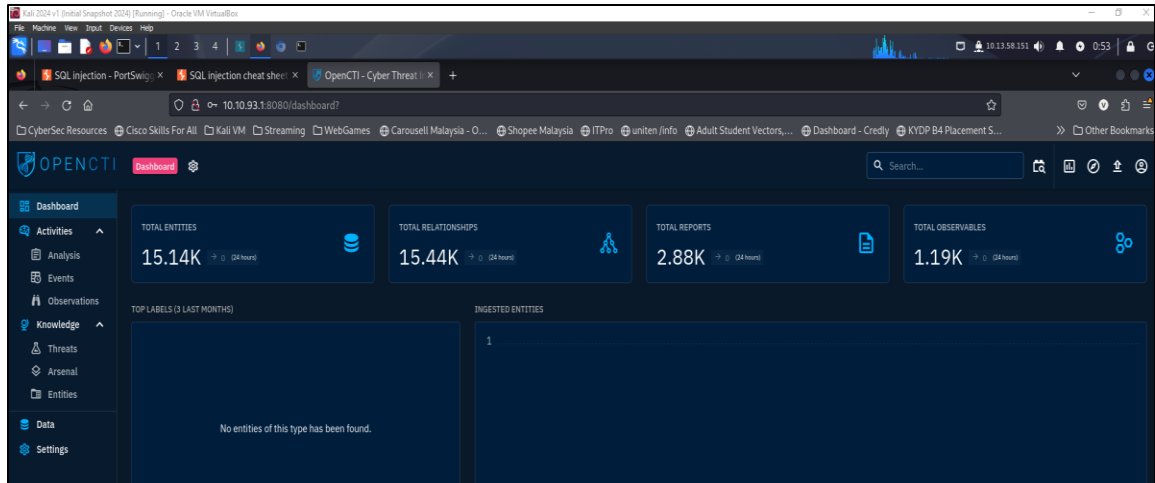
Platform Architecture:



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

Exm Using Kali > VPN connection to THM's network to access the machine hosting OpenCTI:



3. Dashboard

Analysis

The Analysis tab contains the input entities in reports analyzed and associated external references. They allow for easier identification of the source of information by analysts.

<input type="checkbox"/>	TITLE	AUTHOR	LABELS	DATE	STATUS
<input type="checkbox"/>	[MITRE ATT&CK] Gelsemium (S0666)	The MITRE Corporation	No label	May 6, 2022	
<input type="checkbox"/>	[MITRE ATT&CK] VPNFilter (S1010)	The MITRE Corporation	No label	May 6, 2022	
<input type="checkbox"/>	[MITRE ATT&CK] Triton (S1009)	The MITRE Corporation	No label	May 6, 2022	
<input type="checkbox"/>	[MITRE ATT&CK] PLC-Blaster (S1006)	The MITRE Corporation	No label	May 6, 2022	

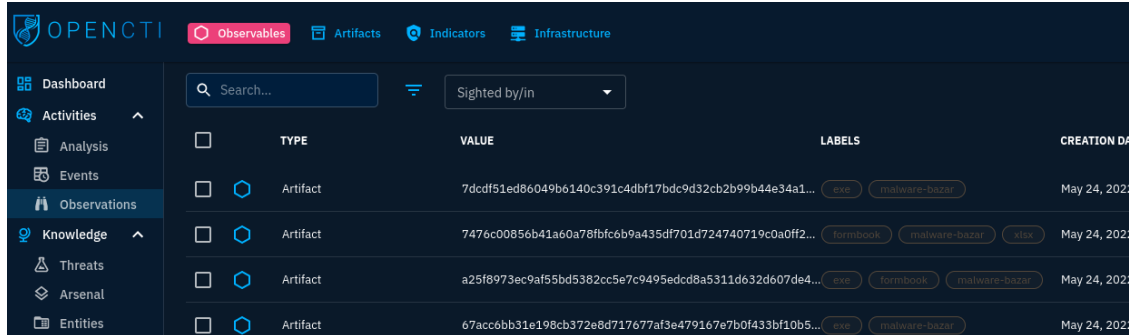
Events

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



Observations

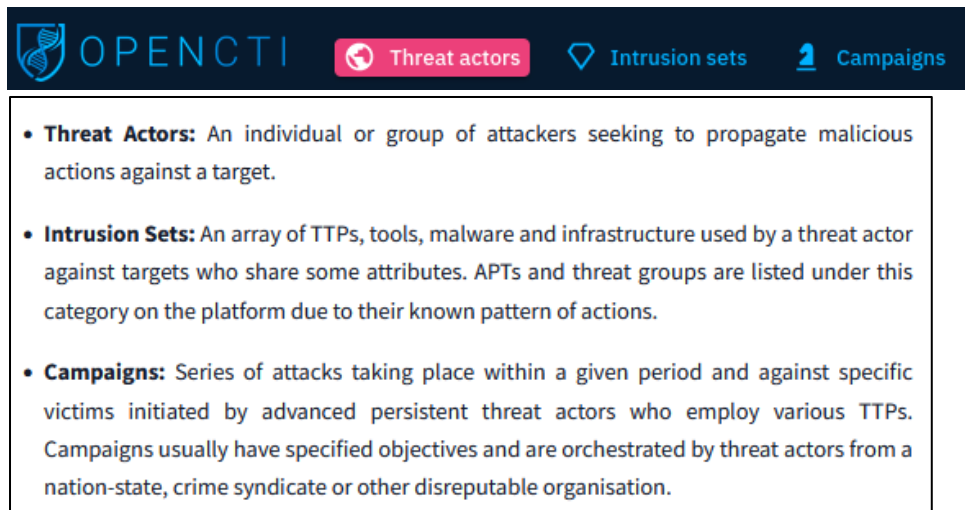
Technical elements, detection rules and artefacts identified during a cyber-attack. These elements assist analysts in mapping out threat events during a hunt and perform correlations between what they observe in their environments against the intel feeds.



The screenshot shows the OpenCTI Observations page. The left sidebar contains navigation links: Dashboard, Activities (Analysis, Events), Observations (selected), Knowledge (Threats, Arsenal, Entities). The main area has a search bar and a filter dropdown set to 'Sighted by/in'. Below is a table of artifacts.

	TYPE	VALUE	LABELS	CREATION DATE
<input type="checkbox"/>	Artifact	7dcd51ed86049b6140c391c4dbf17bdc9d32cb2b99b44e34a1...	exe malware-bazar	May 24, 2022
<input type="checkbox"/>	Artifact	747ec00856b41a60a78fbfc6b9a435df701d724740719c0a0ff2...	formbook malware-bazar	May 24, 2022
<input type="checkbox"/>	Artifact	a25f8973ec9af55bd5382cc5e7c9495edcd8a5311d632d607de4...	exe formbook malware-bazar	May 24, 2022
<input type="checkbox"/>	Artifact	67acc6bb31e198cb372e8d717677af3e479167e7b0f433bf10b5...	exe malware-bazar	May 24, 2022

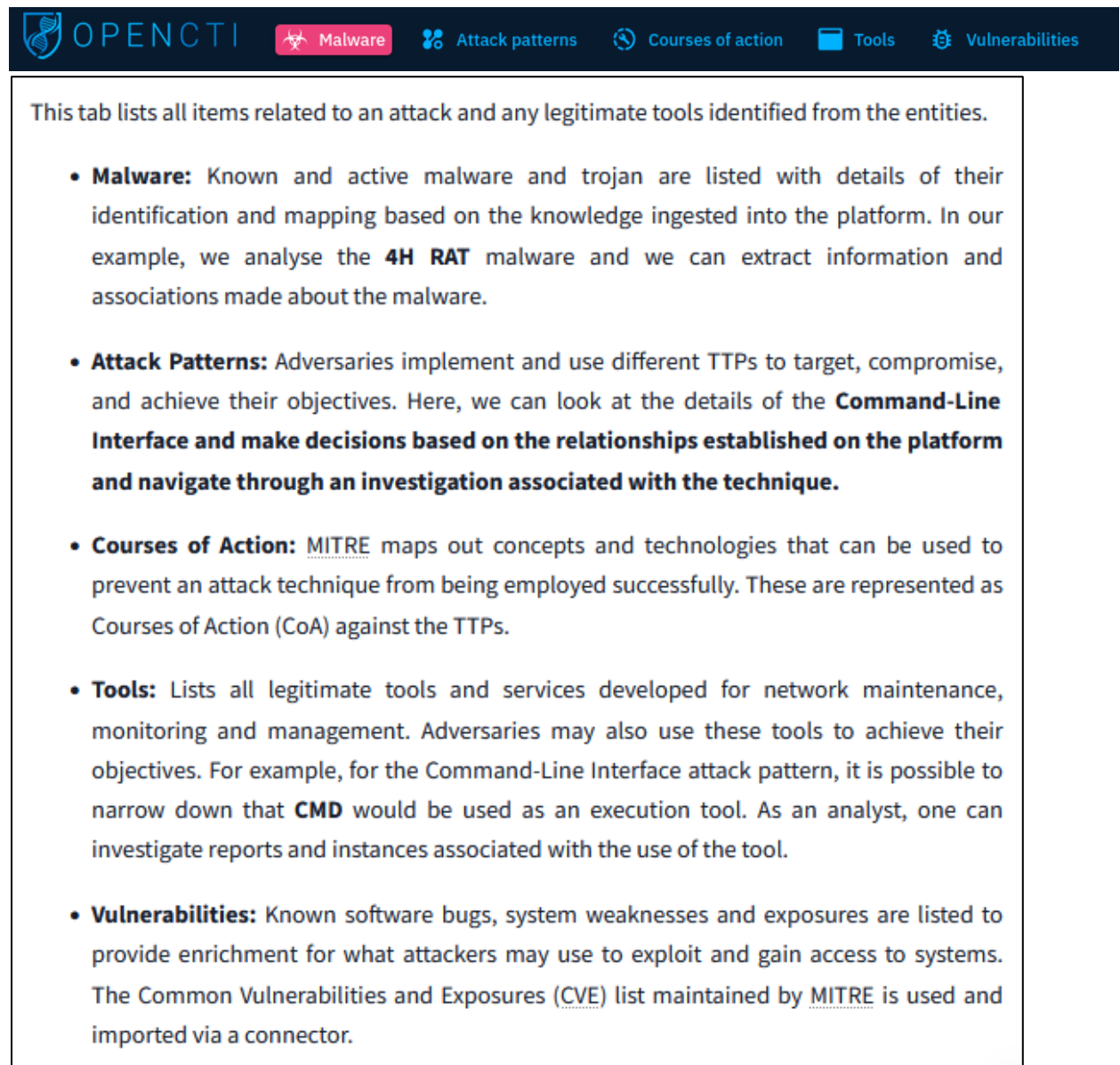
Threats



The screenshot shows the OpenCTI Threats page with tabs for Threat actors, Intrusion sets, and Campaigns. The content area contains definitions for these three concepts.

- **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

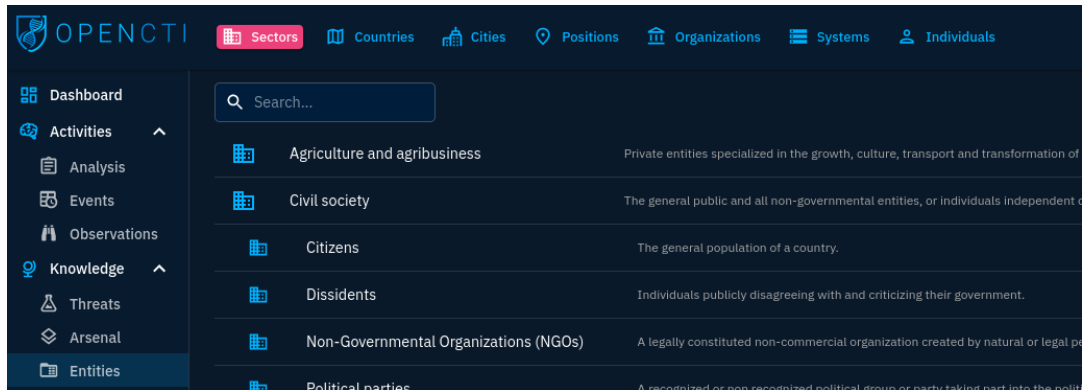


The screenshot shows the OpenCTI interface with the 'Arsenal' tab selected. The top navigation bar includes icons for Malware, Attack patterns, Courses of action, Tools, and Vulnerabilities. The main content area is titled 'This tab lists all items related to an attack and any legitimate tools identified from the entities.' and contains a list of five items:

- **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

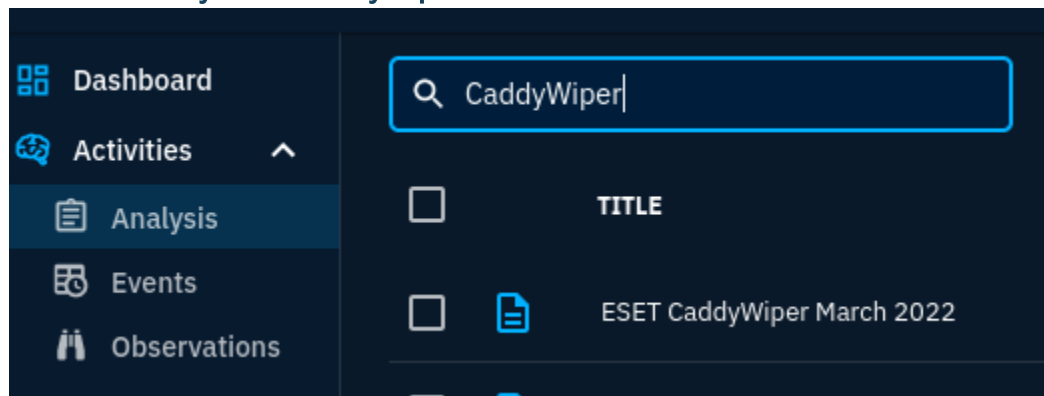
This tab categorizes all entities based on operational sectors, countries, organizations and individuals. This information allows for knowledge enrichment on attacks, organizations, or intrusion sets.



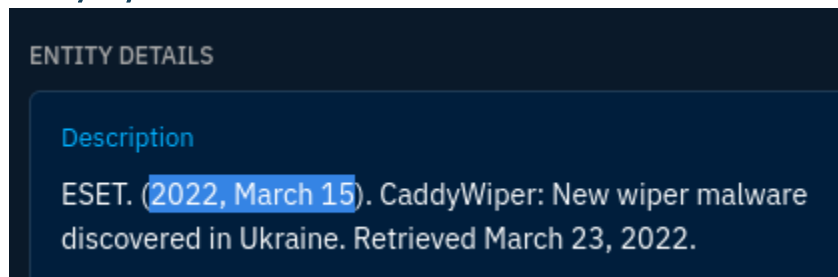
4. Investigative Scenario using OpenCTI

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

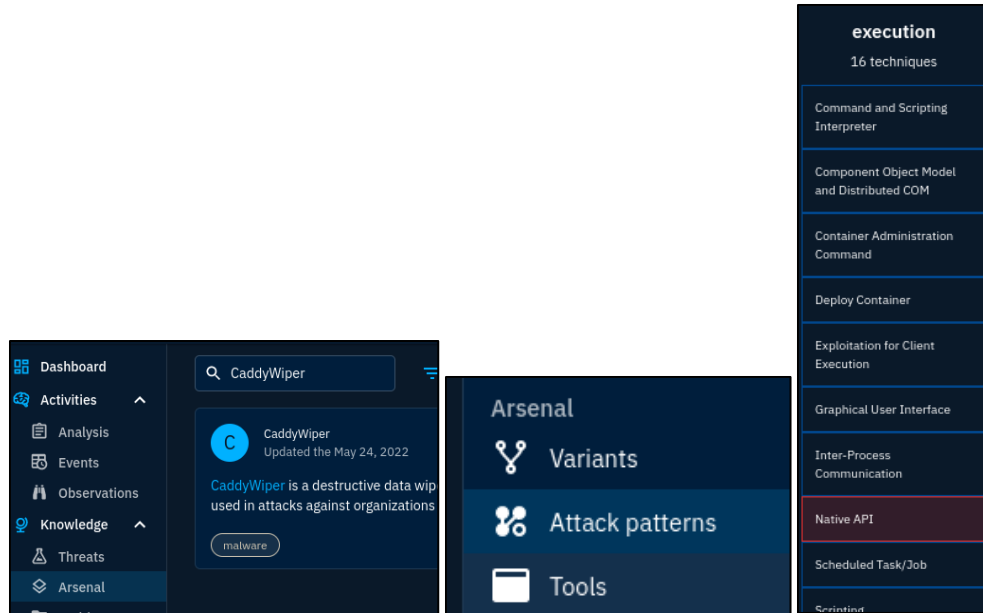
1. What is the earliest date recorded related to **CaddyWiper**? Format: YYYY/MM/DD
Search in Analysis for CaddyWiper



2022/03/15



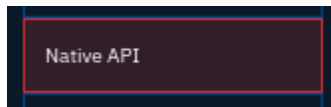
2. Which **Attack technique** is used by the malware for execution?



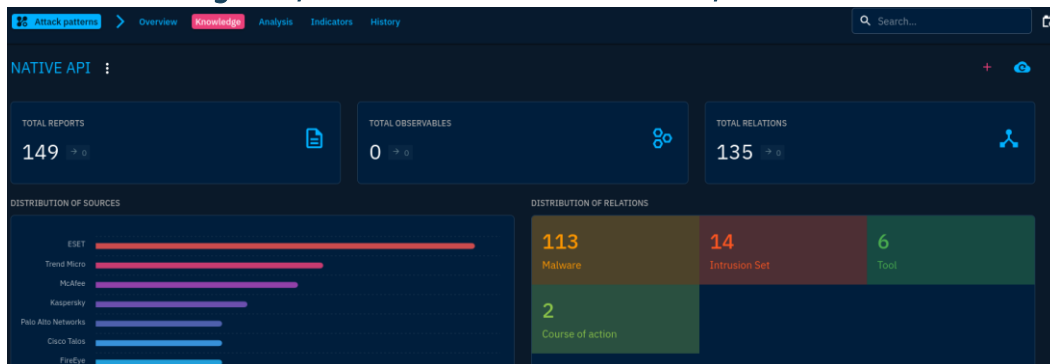
Arsenal search for CaddyWiper > Knowledge tab of the malware > Attack pattern details on right tab > execution details you will see the answer.

Native API

- How many malware relations are linked to this Attack technique?
Click the Native API to know more details about this technique.



Under Knowledge tab, observe the malware relations, there is 113.



- Which 3 tools were used by the Attack Technique in 2016? (Ans: Tool1, Tool2, Tool3)
Still under Knowledge tab, click on Tools to see what tools use this attack technique.

RELATIONSHIP TYPE	NAME	ENTITY TYPE	START TIME	STOP TIME	CONFIDENCE
uses	BloodHound	Tool	Apr 16, 2016	Apr 16, 2016	LOW
uses	Empire	Tool	Apr 27, 2016	Apr 27, 2016	LOW
uses	ShimRatReporter	Tool	May 16, 2016	May 16, 2016	LOW
uses	Imminent Monitor	Tool	Feb 17, 2019	Feb 17, 2019	LOW

BloodHound, Empire, ShimRatReporter

5. What country is **APT37** associated with?

Search in Analysis for **APT37**, the entry mentions North Korea to be the origin of the group.

BASIC INFORMATION	ENTITY DETAILS
<p>Standard STIX ID</p> <p>report--ac24f595-9d8d-5a46-9f1d-99c8242b432d</p> <p>Other STIX IDs</p>	<p>Description</p> <p>FireEye. (2018, February 20). APT37 (Reaper): The Overlooked North Korean Actor. Retrieved March 1, 2018.</p>

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

Searching from the whole website work as well.

Report	3 entities
Intrusion Set	2 entities
APT37	(APT37)(https://attack.mitre.org/groups/G0067) is a North Korean state-sponsored cyber espionage group that has been active since at least 2012. The...
Lazarus Group	(Lazarus Group)(https://attack.mitre.org/groups/G0032) is a North Korean state-sponsored cyber threat group that has been attributed to the...

Attack patterns show 2 techniques used for initial access.

initial-access 9 techniques	impact 13 techniques	Threats
Drive-by Compromise	Account Access Removal	Attribution
Exploit Public-Facing Application	Data Destruction	Victimology
External Remote Services	Data Encrypted for Impact	Campaigns
Hardware Additions	Data Manipulation	Arsenal
Phishing	Defacement	Attack patterns
Replication Through	Disk Wipe	Malware
		Tools

Note both technique codes.

External ID	External ID
T1189	T1566

T1189, T1566

Drive By Compromise, Phishing

MISP (MALWARE INFORMATION SHARING PLATFORM)

Objectives of learning:

- Introduction to MISP and why it was developed.
- Use cases MISP can be applied to
- Core features and terminologies.
- Dashboard Navigation.
- Event Creation and Management.
- Feeds and Taxonomies.

1.What is MISP?



Open-source **threat information platform** that facilitates the collection, storage and distribution of threat intelligence and Indicators of Compromise (IOCs) related to malware, cyber-attacks, financial fraud.

Additional Resources:

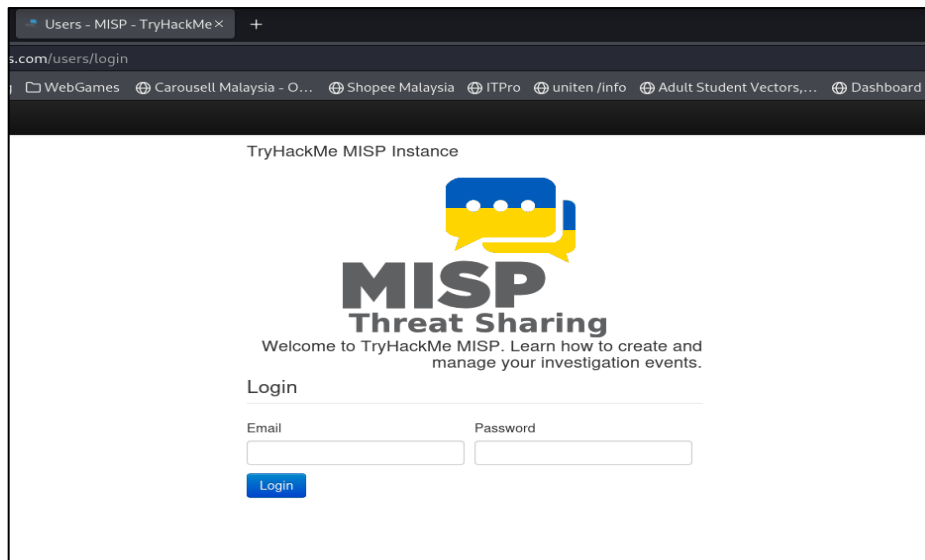
- [MISP Book](#)
- [MISP GitHub](#)
- [CIRCL MISP Training Module 1](#)
- [CIRCL MISP Training Module 2](#)

What does MISP support?	
IOC database	This allows for the storage of technical and non-technical information about malware samples, incidents, attackers, and intelligence.
Automatic Correlation	Identification of relationships between attributes and indicators from malware, attack campaigns or analysis.
Data Sharing	This allows for sharing of information using different models of distributions and among different MISP instances.
Import & Export features	This allows the import and export of events in different formats to integrate other systems such as NIDS, HIDS, and OpenIOC.

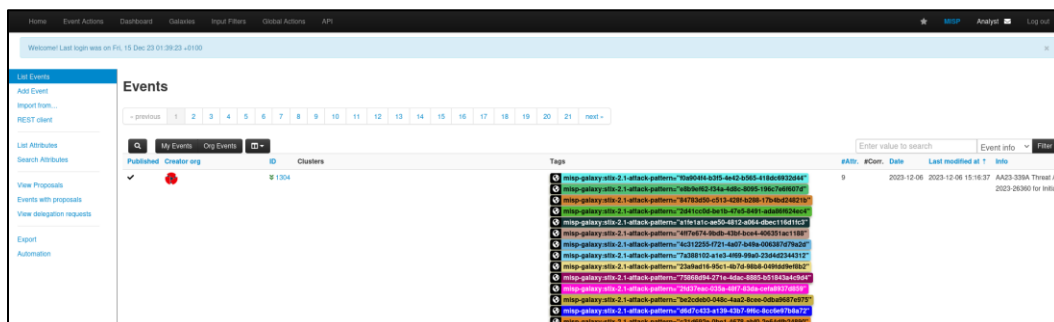
Event Graph	Showcases the relationships between objects and attributes identified from events.
API support	Supports integration with own systems to fetch and export events and intelligence.

2.Using the system – MISP

Hosted by TryHackMe's machine, connected to the site using own Kali to VPN to THM network.



First look:



HOLOTAPES

C2



Command and Control (C2) Infrastructure are a set of programs used to communicate with a victim machine. This is comparable to a reverse shell, but is generally more advanced and often communicate via common network protocols, like HTTP, HTTPS and DNS.

FTP



File Transfer Protocol (FTP) is a protocol designed to help the efficient transfer of files between different and even non-compatible systems. It supports two modes for file transfer: binary and ASCII (text).

CVE



Common Vulnerabilities and Exposures (CVE), this term is given to a publicly disclosed vulnerability

CVSS



Common Vulnerability Scoring System

IOC



Indicator of Compromise is a forensic artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion.


API



API, which stands for Application Programming Interface, is a set of rules and protocols for building software and applications. An API allows different software programs to communicate with each other. It defines methods of communication between various components, including the kinds of requests that can be made, how they're made, the data formats that should be used, and conventions to follow.

SOC

AB ✓



Security Operations Center (SOC) is a team of IT security professionals tasked with monitoring, preventing, detecting, investigating, and responding to threats within a company's network and systems.


MISP

AB ✓

Malware Information Sharing Platform is an open-source threat information platform used to facilitate the collection and sharing of threat information.

HIDS

AB ✓



Host Intrusion Detection System (HIDS) analyzes system state, system calls, file-system modifications, application logs, and other system activity.