Get unlimited access to the best of Medium for less than $1/week. Become a member

TryHackMe : Trooper Writeup

Daouda Diallo · Follow

6 min read · Aug 15, 2024

Listen Share More

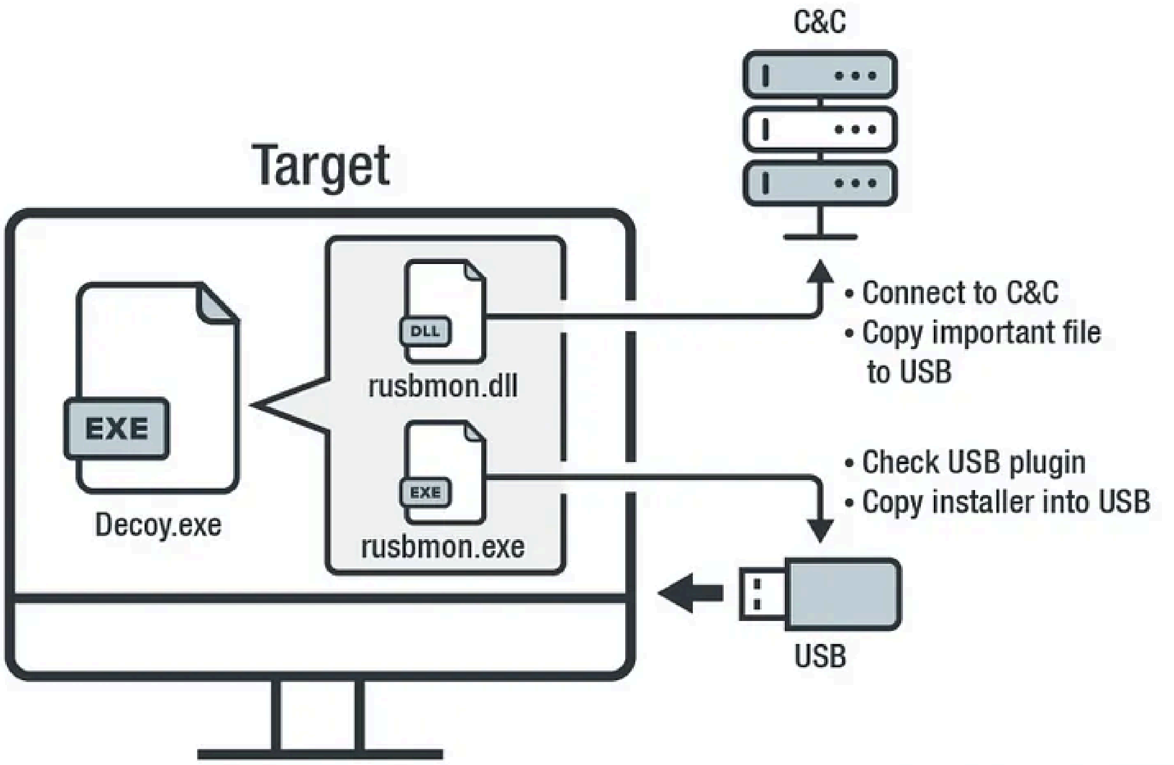
Synopsis : " A global tech company has suffered several cyber attacks recently, leading to stolen intellectual property and operational disruptions.
Our task as a CTI analyst is to identify the Tactics, Techniques, and Procedures (TTPs) used by the attackers and gather information on their identity and motives, using the OpenCTI platform and MITRE ATT&CK navigator. "

Intro (Based on APT X report sample provided by THM) :

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. Primarily motivated by **information theft** and **espionage**, the group has also been seen adopting different strategies such as fine-tuning tools with new behaviors and going mobile with surveillanceware.

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. Based on data from the Trend Micro™ Smart Protection Network™ security infrastructure, USBferry attacks have been active since 2014.
We found the group was focused on stealing defense-, ocean-, and ship-related documents from target networks, which led us to believe that APT X's main purpose is to exfiltrate confidential information or intelligence.



Open in app ↗

Medium Search

Source : **TrendMicro**

Challenge

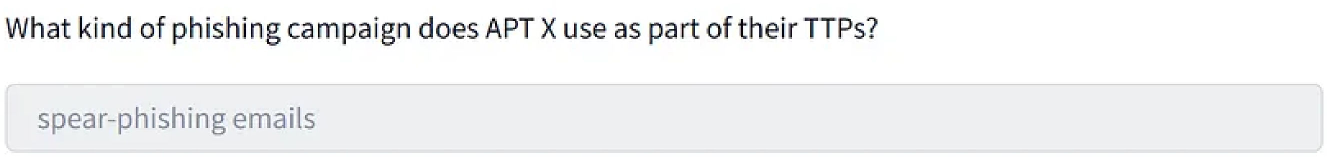
As a CTI analyst, our task is to identify the Tactics, Techniques, and Procedures (TTPs) being used by the Threat group and gather as much information as possible about their identity and motive.

Here is the report shared with us as a CTI analyst : Threat Advisory Report .

Question1 : What kind of phishing campaign does APT X use as part of their TTPs ?

The given report sample shows that APT X is known for using **spear-phishing emails as initial acces tactic .**

Answer :



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

spear-phishing emails

Phishing_campaign : Spear-phishing emails

Question2 : What is the name of the malware used by APT X ?

The report states 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).

Answer :

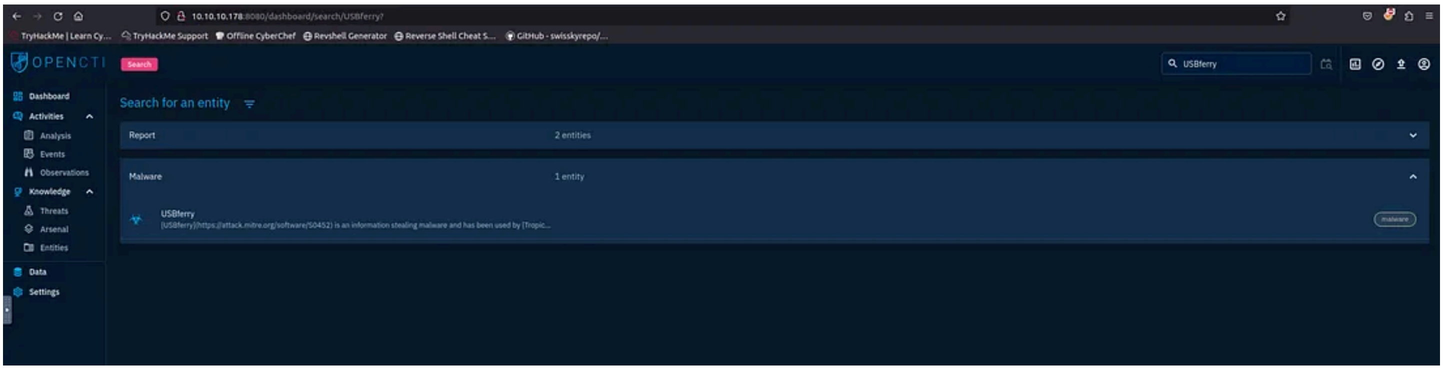
What is the name of the malware used by APT X?

USBferry

Malware_name : USBferry

Question3 : What is the malware’s STIX ID ?

We’ll utilize our threat intelligence platform, OpenCTI, for this task. After accessing OpenCTI, we need to check for the USBferry malware.



10.10.10.178:8080/dashboard/search/USBferry?

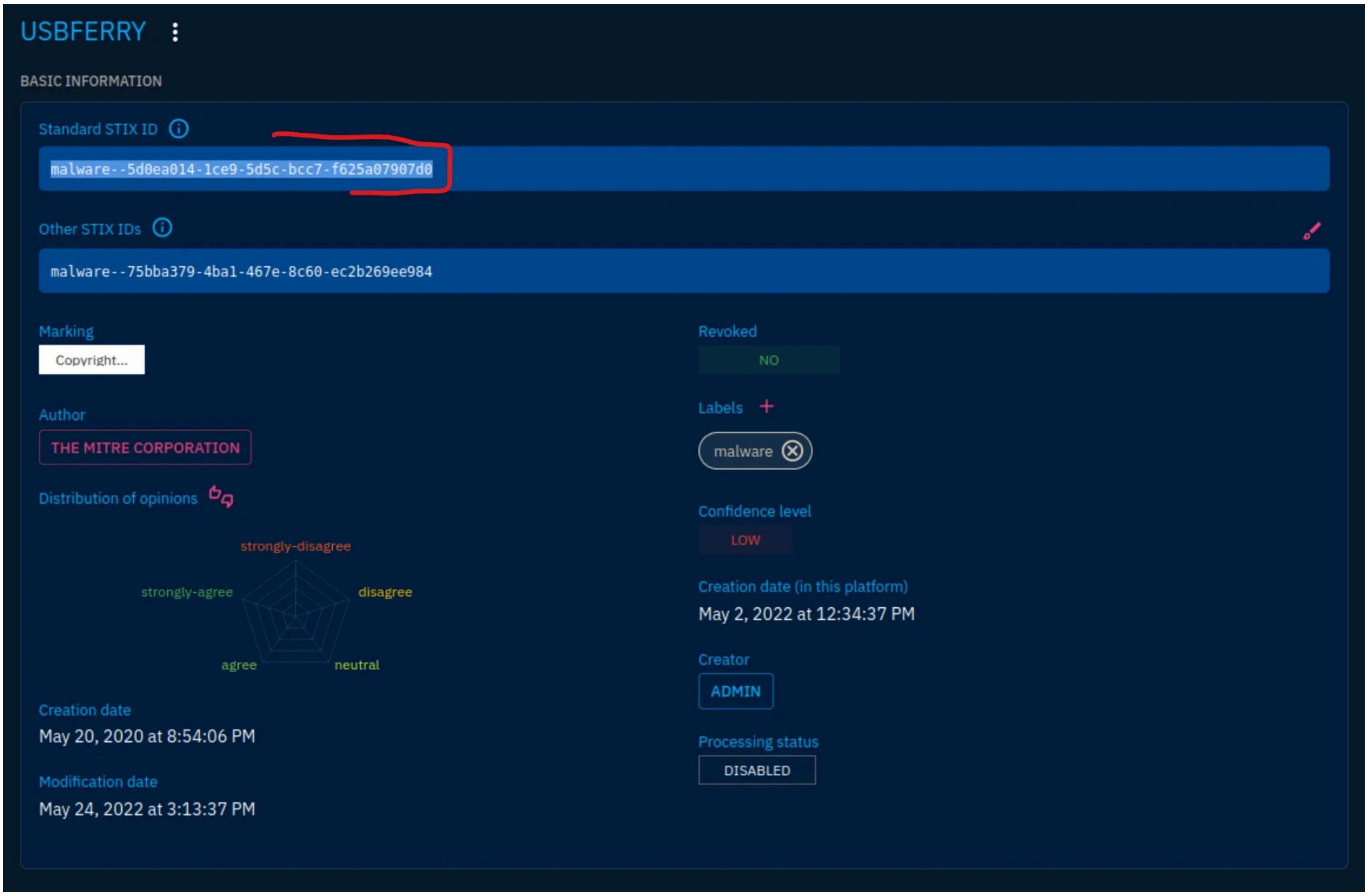
USBferry

Search for an entity

Report 2 entities

Malware 1 entity

USBferry
[USBferry](https://attack.mitre.org/software/S0452) is an information stealing malware and has been used by [Tropic...



USBFERRY

BASIC INFORMATION

Standard STIX ID: malware--5d0ea014-1ce9-5d5c-bcc7-f625a07907d0

Other STIX IDs: malware--75bba379-4ba1-467e-8c60-ec2b269ee984

Marking: Copyright...

Revoked: NO

Author: THE MITRE CORPORATION

Labels: malware

Distribution of opinions

Confidence level: LOW

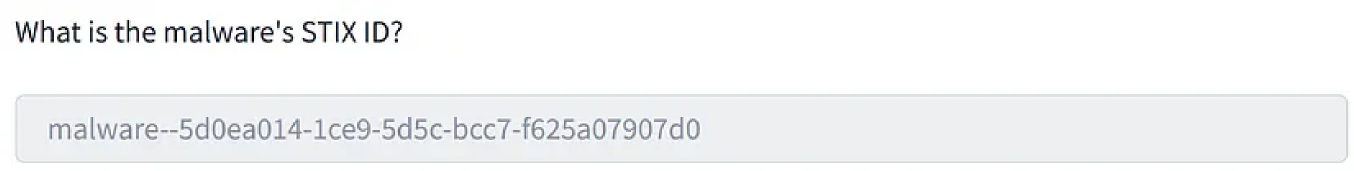
Creation date (in this platform): May 2, 2022 at 12:34:37 PM

Creator: ADMIN

Creation date: May 20, 2020 at 8:54:06 PM

Processing status: DISABLED

Modification date: May 24, 2022 at 3:13:37 PM



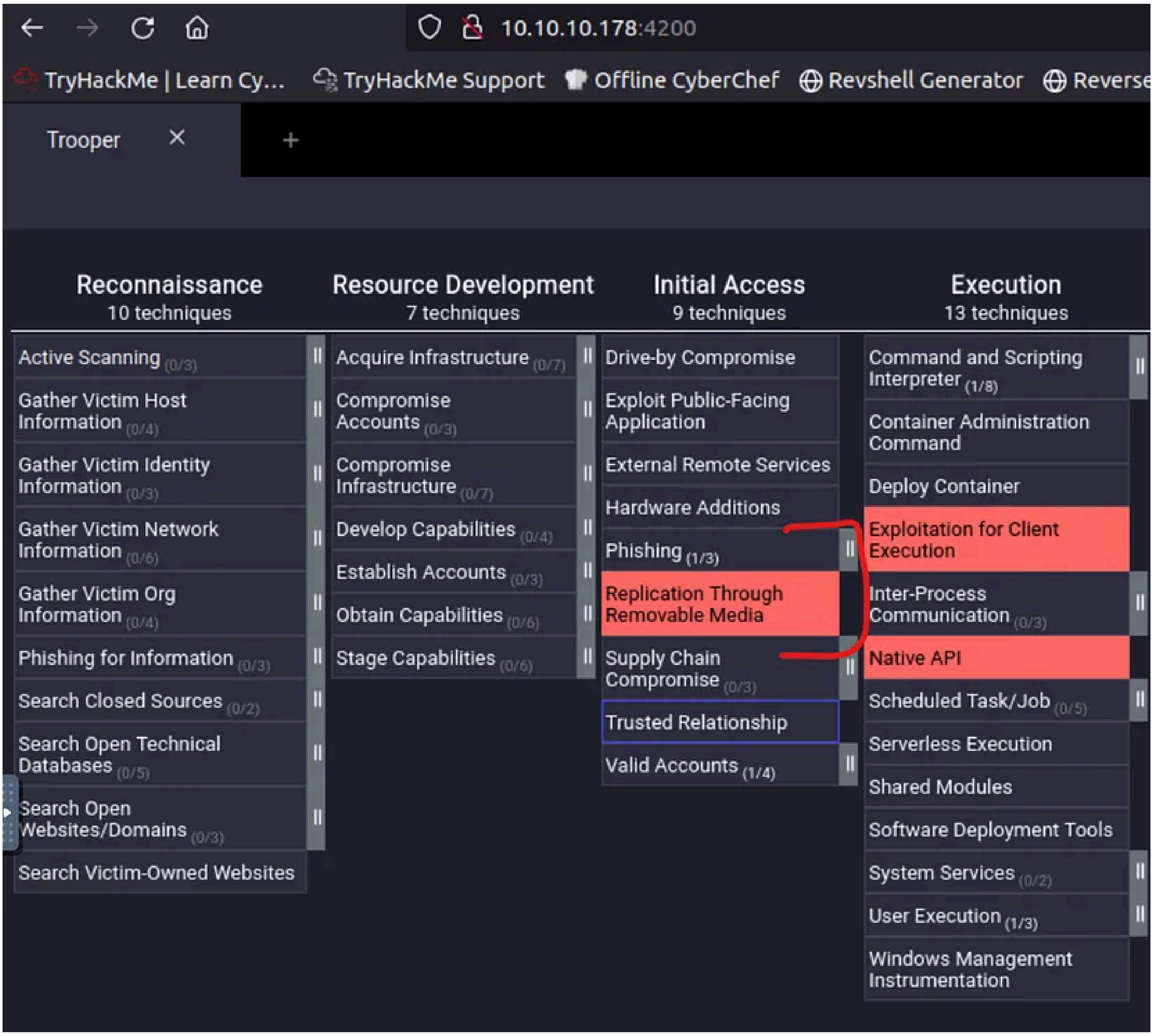
What is the malware's STIX ID?

malware--5d0ea014-1ce9-5d5c-bcc7-f625a07907d0

STIX ID : malware — 5d0ea014–1ce9–5d5c-bcc7-f625a07907d0

Question4 : With the use of a USB, what technique did APT X use for initial access ?

You can find this information using the MITRE ATT&CK Navigator. By examining the initial access tactics associated with this group, you can identify the techniques employed by the threat actor.



Reconnaissance 10 techniques

- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/3)
- Search Victim-Owned Websites

Resource Development 7 techniques

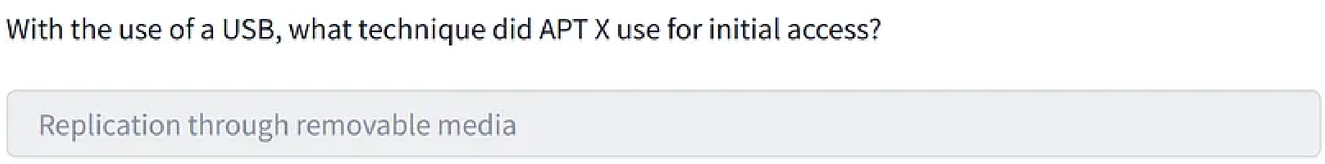
- Acquire Infrastructure (0/7)
- Compromise Accounts (0/3)
- Compromise Infrastructure (0/7)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/6)

Initial Access 9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (1/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (1/4)

Execution 13 techniques

- Command and Scripting Interpreter (1/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (1/3)
- Windows Management Instrumentation



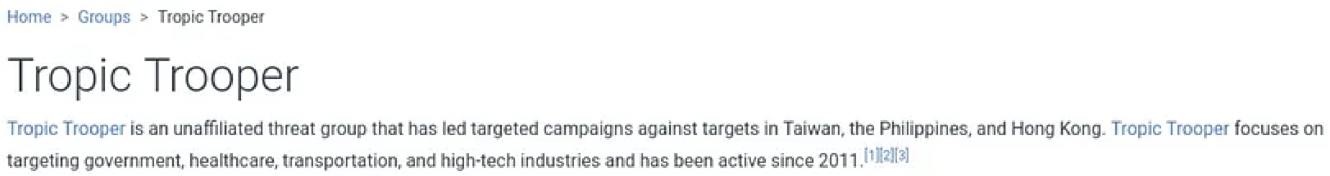
With the use of a USB, what technique did APT X use for initial access?

Replication through removable media

Initial_access : Replication through removable media

Question5 : What is the identity of APT X ?

APT X is known by **Tropic Trooper** .

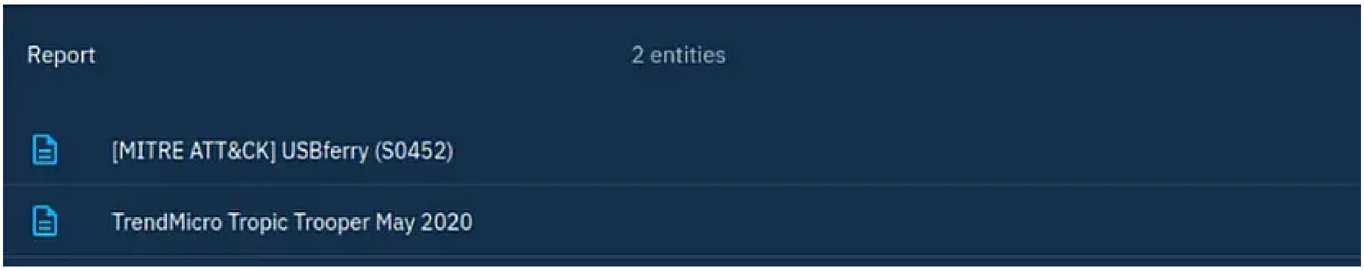


Home > Groups > Tropic Trooper

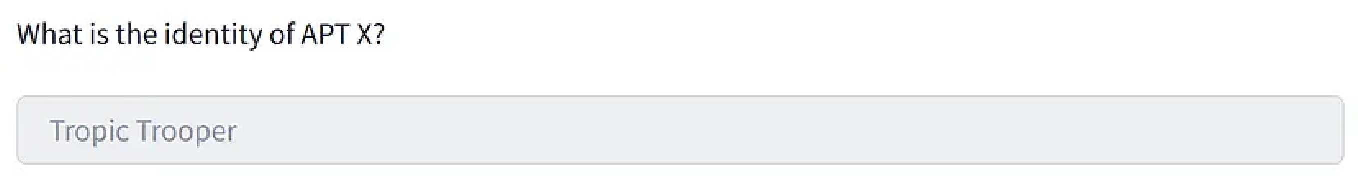
Tropic Trooper

Tropic Trooper is an unaffiliated threat group that has led targeted campaigns against targets in Taiwan, the Philippines, and Hong Kong. Tropic Trooper focuses on targeting government, healthcare, transportation, and high-tech industries and has been active since 2011.[1][2][3]

This can also be found using OpenCTI, by checking the reports related to USBferry.



Report	2 entities
[MITRE ATT&CK] USBferry (S0452)	
TrendMicro Tropic Trooper May 2020	

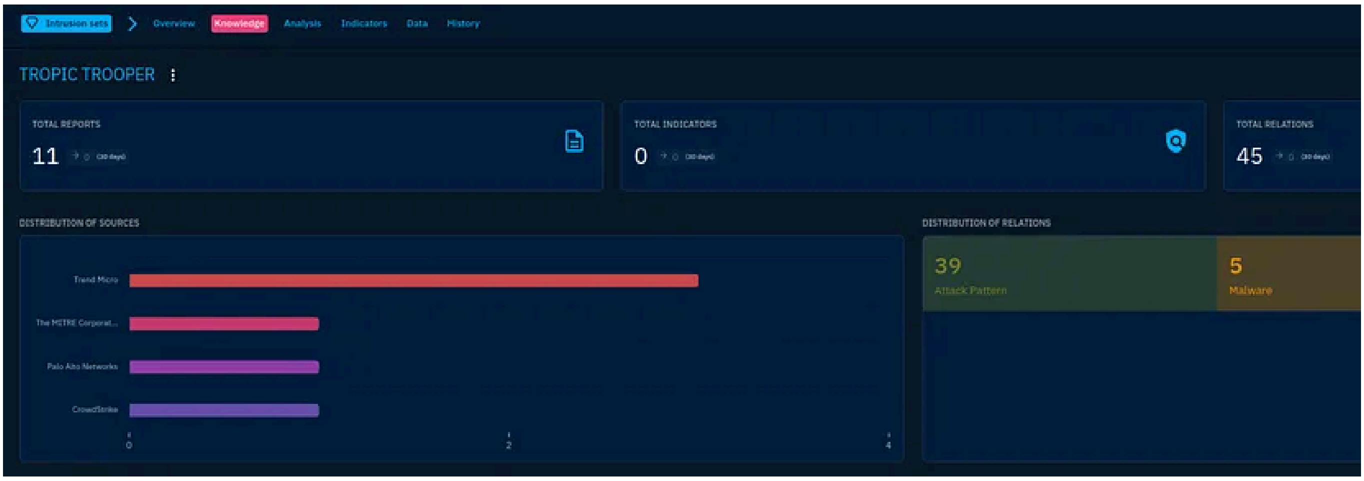


What is the identity of APT X?

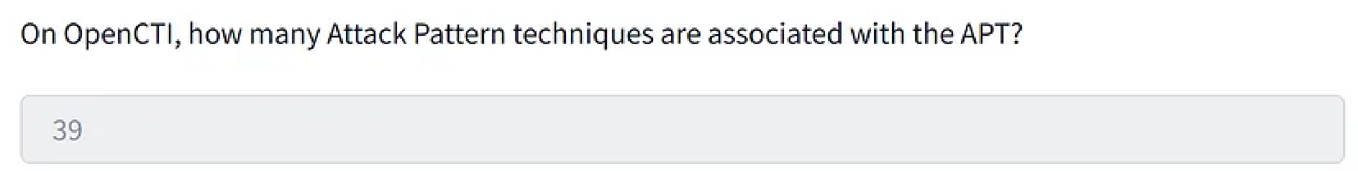
Tropic Trooper

Identity : Tropic Trooper

Question6 : On OpenCTI, how many Attack Pattern techniques are associated with the APT ?



39 attack patterns are associated with Tropic Trooper threat actor .



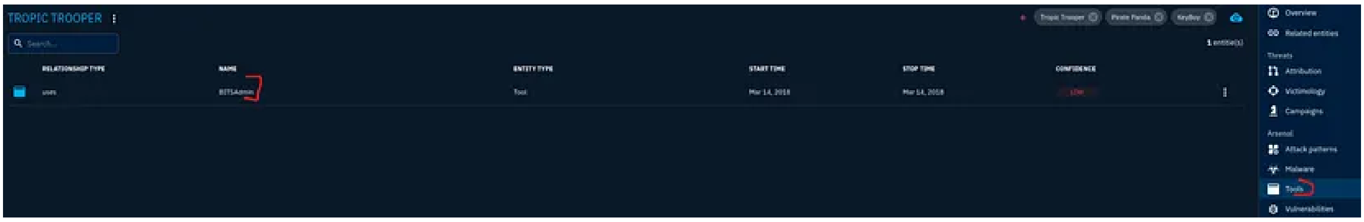
On OpenCTI, how many Attack Pattern techniques are associated with the APT?

39

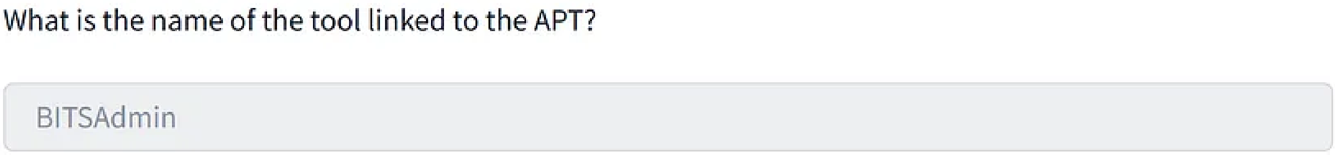
Attack_patterns : 39

Question7 : What is the name of the tool linked to the APT ?

Using OPENCTI, we can find tools used by Tropic Trooper group, but checking the **arsenal menu** related to the threat actor in the right corner, then **tools.**



RELATIONSHIP TYPE	NAME	ENTITY TYPE	START TIME	STOP TIME	CONFIDENCE
uses	BITSAdmin	Tool	Mar 14, 2018	Mar 14, 2018	LOW



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

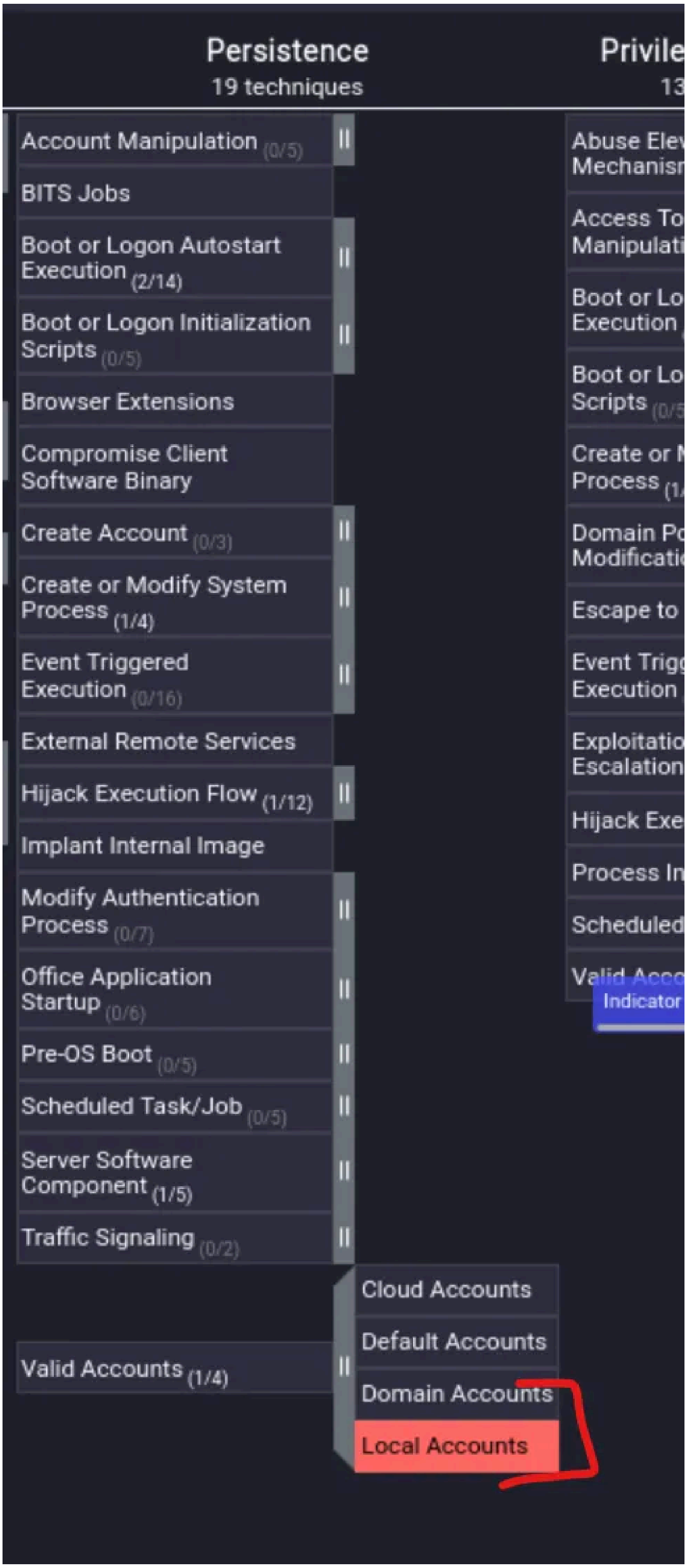
BITSAdmin

Tool : BITSAdmin

Question8 :

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

Review the persistence tactic, then expand the “**Valid Accounts**” technique at the bottom.

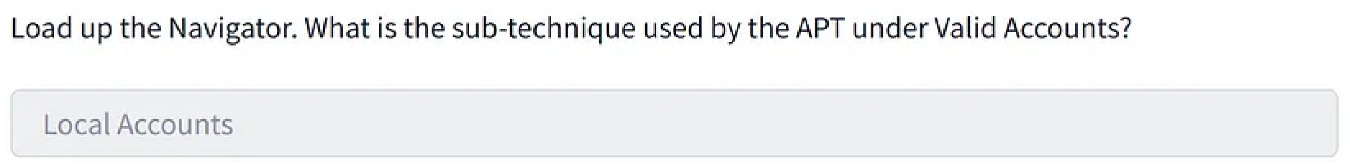


Persistence
19 techniques

Privile
13

Account Manipulation (0/5)
BITS Jobs
Boot or Logon Autostart Execution (2/14)
Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Client Software Binary
Create Account (0/3)
Create or Modify System Process (1/4)
Event Triggered Execution (0/16)
External Remote Services
Hijack Execution Flow (1/12)
Implant Internal Image
Modify Authentication Process (0/7)
Office Application Startup (0/6)
Pre-OS Boot (0/5)
Scheduled Task/Job (0/5)
Server Software Component (1/5)
Traffic Signaling (0/2)
Valid Accounts (1/4)
Cloud Accounts
Default Accounts
Domain Accounts
Local Accounts

Abuse Elev Mechanism
Access To Manipulati
Boot or Lo Execution
Boot or Lo Scripts (0/5
Create or M Process (1/
Domain Po Modificati
Escape to
Event Trigg Execution
Exploitatio Escalation
Hijack Exe
Process In
Scheduled
Valid Acco



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

Local Accounts

sub-technique : Local Accounts

Question9 : Under what Tactics does the technique above fall ?

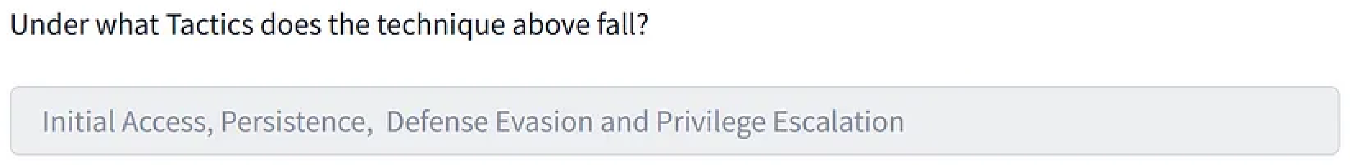
The "**local accounts**" technique can be classified under four distinct tactics in the MITRE ATT&CK framework: Initial Access, Persistence, Defense Evasion, and Privilege Escalation. This classification highlights the versatility and impact of local accounts in a cybersecurity context.

Initial Access: Local accounts can be used by attackers to gain initial access to a system, particularly if they exploit weak or default credentials that provide entry points into a network or system.

Persistence: Once inside a system, attackers can create or manipulate local accounts to maintain access over time. By establishing local accounts with persistent access, they ensure that they can return to the system even if other access methods are discovered and removed.

Defense Evasion: Local accounts may help in evading detection by blending in with legitimate accounts or avoiding monitoring systems that focus on network or domain-level activities. Attackers might use local accounts to avoid triggering security alerts that are typically configured for network-based threats.

Privilege Escalation: Attackers might leverage local accounts to escalate privileges. For instance, if they manage to create or modify local administrator accounts, they can gain elevated privileges that allow them to perform actions with higher levels of access and control.



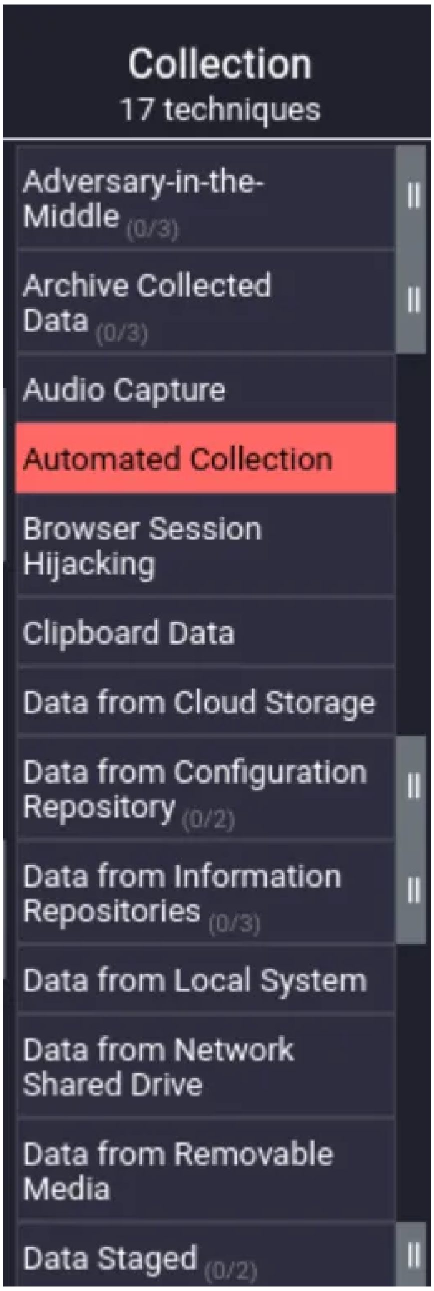
Under what Tactics does the technique above fall?

Initial Access, Persistence, Defense Evasion and Privilege Escalation

Tactics : Initial Access, Persistence, Defense Evasion and Privilege Escalation

Question9 : What technique is the group known for using under the tactic Collection?

The group is known for using an "**automated collection**" technique as part of their **collection** strategy.



Collection
17 techniques

Adversary-in-the-Middle (0/3)

Archive Collected Data (0/3)

Audio Capture

Automated Collection

Browser Session Hijacking

Clipboard Data

Data from Cloud Storage

Data from Configuration Repository (0/2)

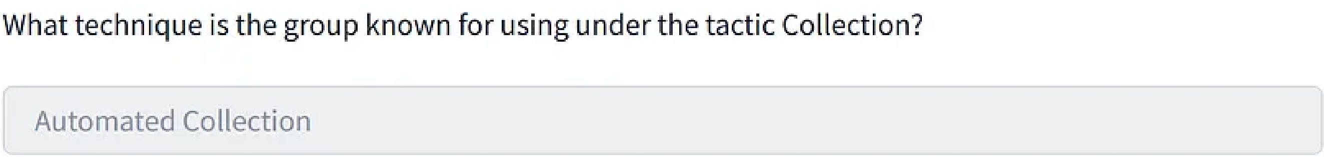
Data from Information Repositories (0/3)

Data from Local System

Data from Network Shared Drive

Data from Removable Media

Data Staged (0/2)



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

Automated Collection

Technique : Automated Collection

The room was straightforward but engaging, offering valuable insights into the Tropic Trooper threat actor and threat intelligence analysis.
It provides a detailed look at their tactics and helps understanding of how threat intelligence is used to counteract such threats.

Overall, it was both informative and enjoyable.

Thanks for reading !

……………

Tropic Trooper Threat Intelligence Apt Cybersecurity Ctf Writeup

Follow

Written by Daouda Diallo

118 Followers · 35 Following

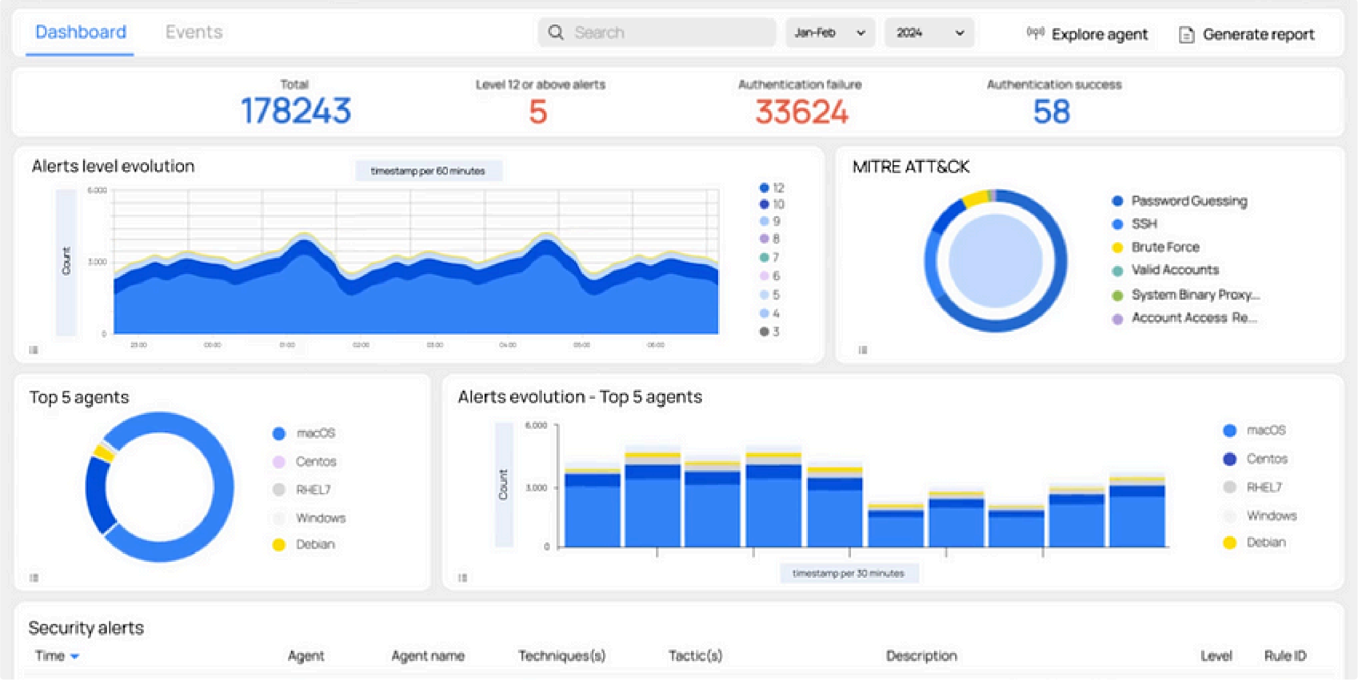
SOC Analyst 📌 | Cybersécurity 🛡 | BlueTeam ⚔️ | To sopprt my blog : https://buymeacoffee.com/daoudad

No responses yet

What are your thoughts?

Respond

More from Daouda Diallo

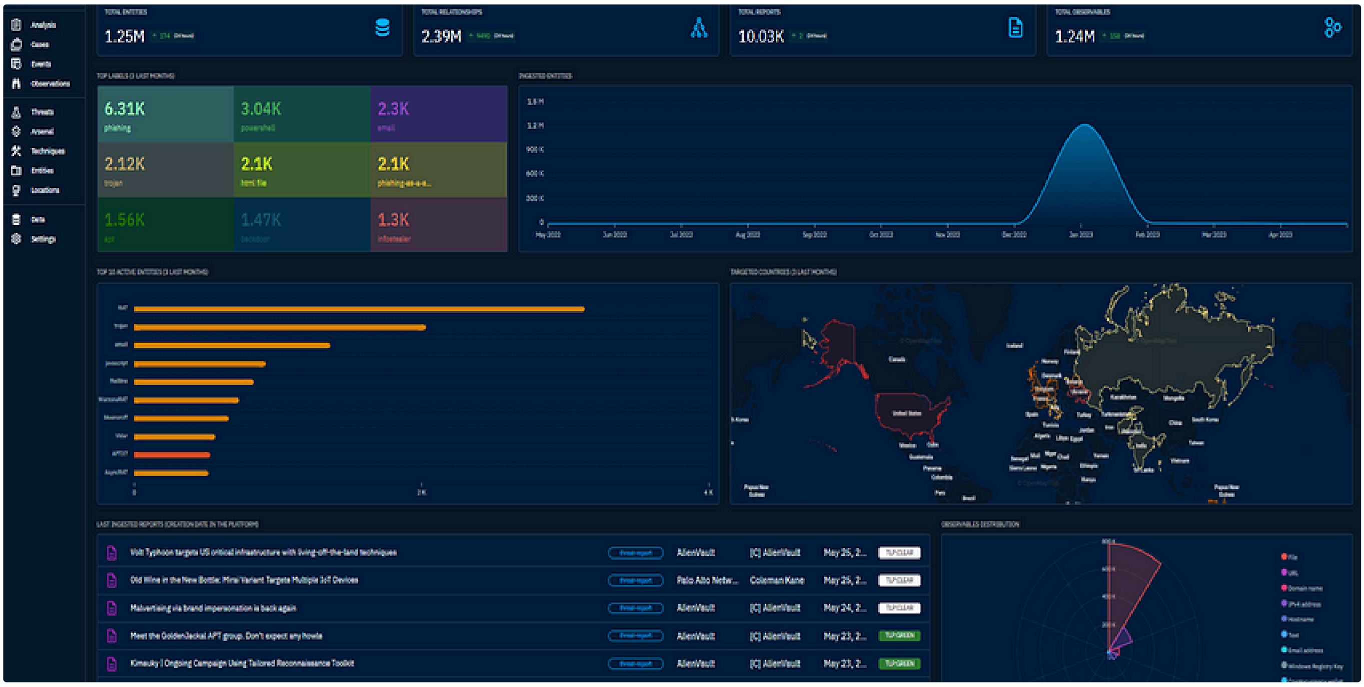


Daouda Diallo

Wazuh-Partie1 : Présentation & Mise en place

Wazuh est une plateforme de sécurité SI tout-en-un, open source et puissante, conçue pour protéger les organisations contre les menaces…

Mar 2, 2024



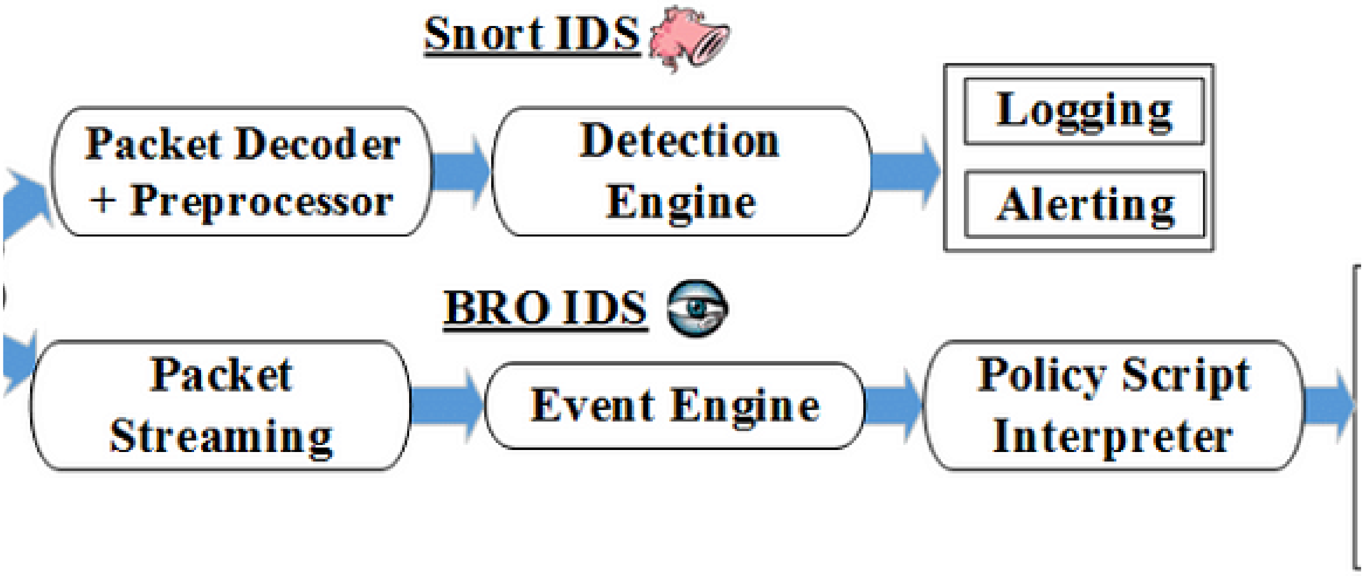
Volt Typhoon targets US critical infrastructure with living-off-the-land techniques AlienVault [C] AlienVault May 25, 2... TLP:CLEAR
Old Wine in the New Bottle: Mirai Variant Targets Multiple IoT Devices Palo Alto Netw... Coleman Kane May 25, 2... TLP:CLEAR
Malvertising via brand impersonation is back again AlienVault [C] AlienVault May 24, 2... TLP:CLEAR
Meet the GoldenJackal APT group. Don't expect any howls AlienVault [C] AlienVault May 23, 2... TLP:GREEN
Kimsuky | Ongoing Campaign Using Tailored Reconnaissance Toolkit AlienVault [C] AlienVault May 23, 2... TLP:GREEN

Daouda Diallo

La Plateforme OpenCTI

Installation guidée

Nov 8, 2023 2



In OSINT Team by Daouda Diallo

SNORT essentials

Network intrusion detection and prevention system

Dec 25, 2024

In OSINT Team by Daouda Diallo

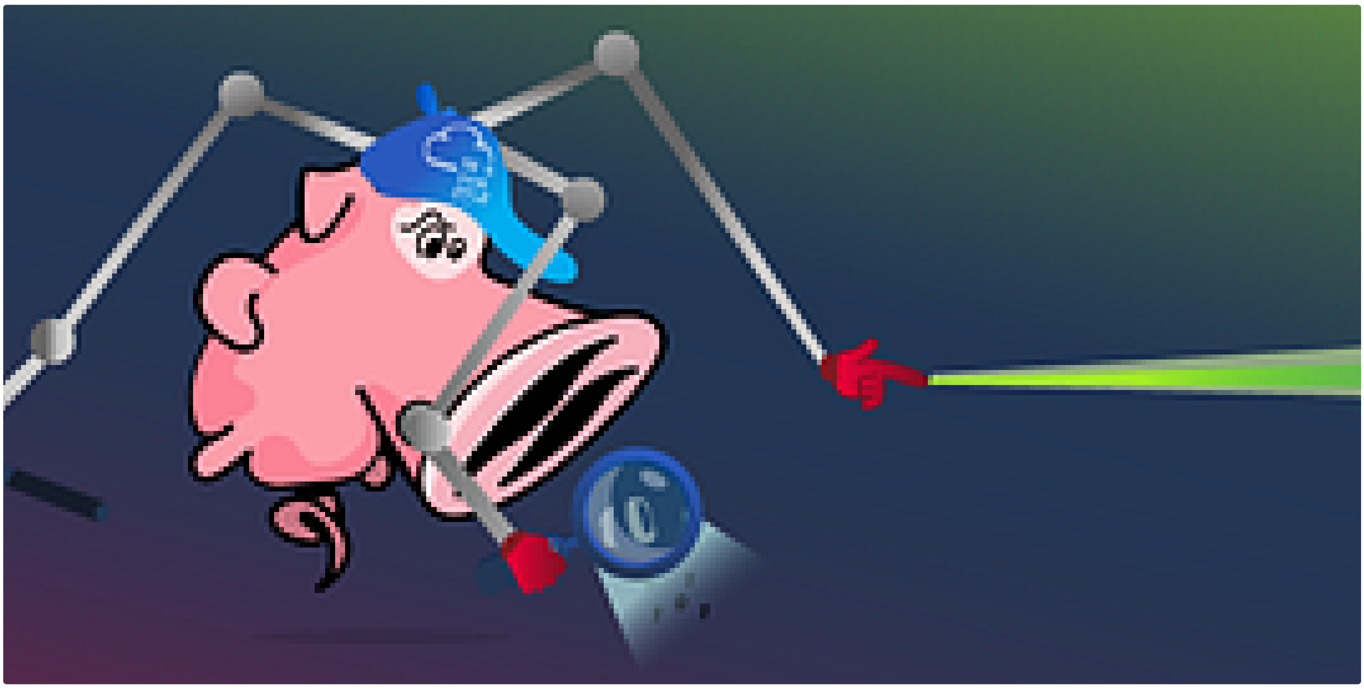
Wireshark: Keys to analyzing and identifying network packets

Wireshark is an open-source software that allows real-time network traffic analysis on various operating systems such as Windows, Linux…

Sep 4, 2024

See all from Daouda Diallo

Recommended from Medium



In T3CH by Axoloth

TryHackMe | Snort Challenge — The Basics | WriteUp

Put your snort skills into practice and write snort rules to analyse live capture network traffic

✦ Nov 9, 2024

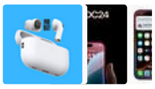
In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

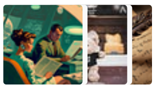
Nov 28, 2024

Lists



Tech & Tools

22 stories · 380 saves

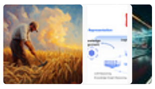


Medium's Huge List of Publications Accepting Submissions

377 stories · 4341 saves

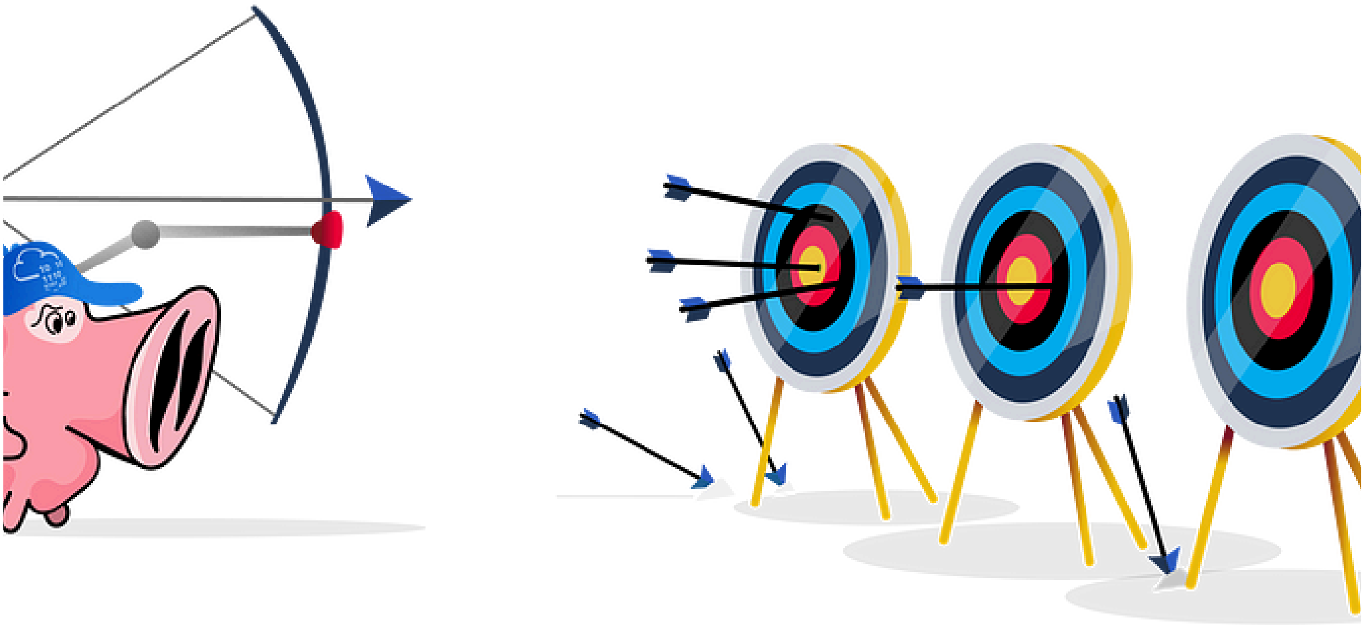
Staff picks

796 stories · 1558 saves



Natural Language Processing

1884 stories · 1529 saves



Manivel

Snort Challenge — The Basics : TryHackMe — Medium

Snort Challenge — The Basics by TryHackMe. Writeup and Answers the question below

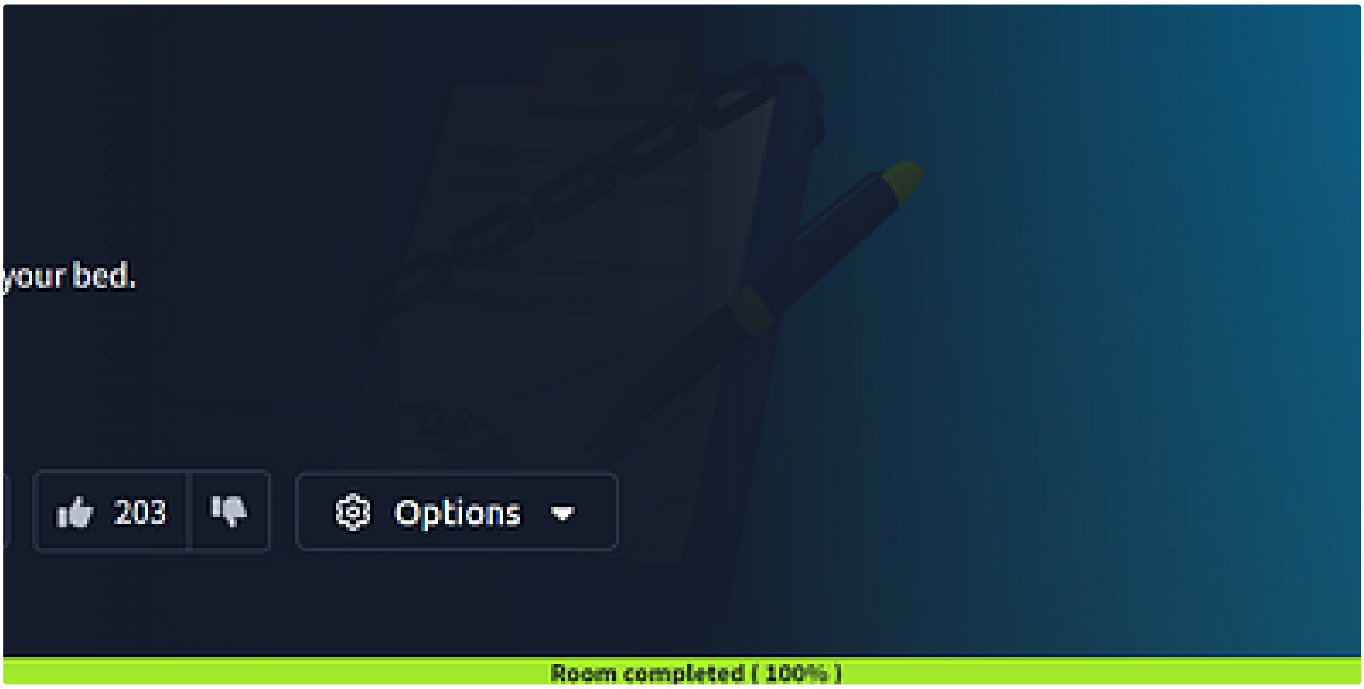
Dec 30, 2024

IritT

Windows Event Logs — Cyber Defense-Security Operations & Monitoring — TryHackMe Walkthrough

Introduction to Windows Event Logs and the tools to query them.

Oct 15, 2024

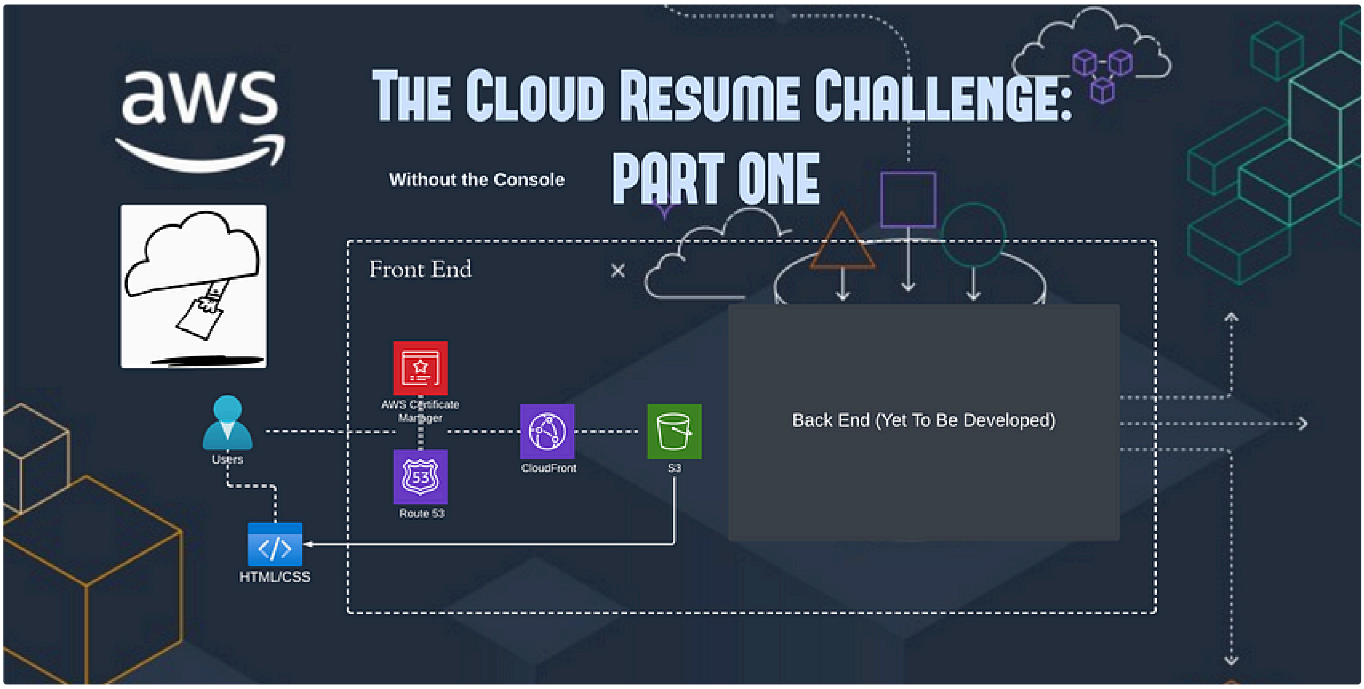


L4V4NY4 AGR3

Eviction — Tryhackme writeup

Sunny is a SOC analyst at E-corp, which manufactures rare earth metals for government and non-government clients. She receives a...

Jul 27, 2024



Gabriel Binion

The Cloud Resume Challenge (AWS): Part One

Hello everyone, this is part one of my documentation of 'The Cloud Resume Challenge' my first cloud project where I showcase my knowledge...

Nov 18, 2024

See more recommendations