# Try Hack Me — Trooper — Walkthrough

0x4C1D · Follow

5 min read · Sep 19, 2023

Listen Share More

So as a drive by I came across this fun first looking box called "Trooper".

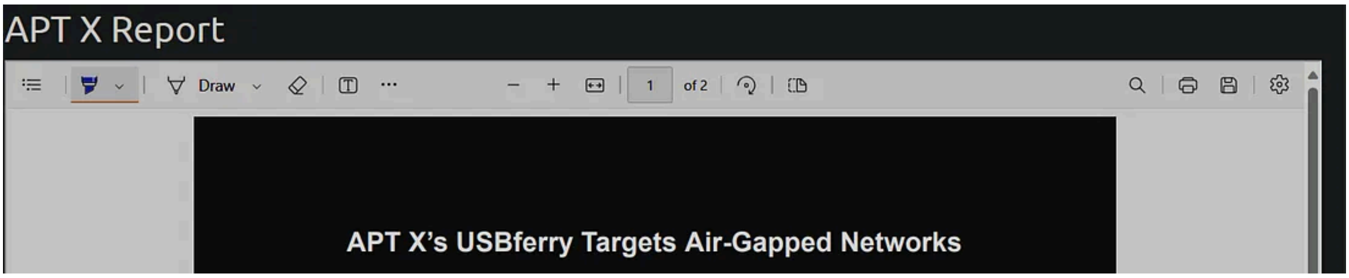
Link to the Box: https://tryhackme.com/room/trooper

Now it turns out this is my kind of box :D since it is a box using
- CTI
- Mitre Att&ck Framework
- and Report understanding.
So basically it is a Blue teamers fun all day Box.

So It got me right away. Specially when I saw the question I knew I have to do this one. So lets do this :)

Answer the questions below

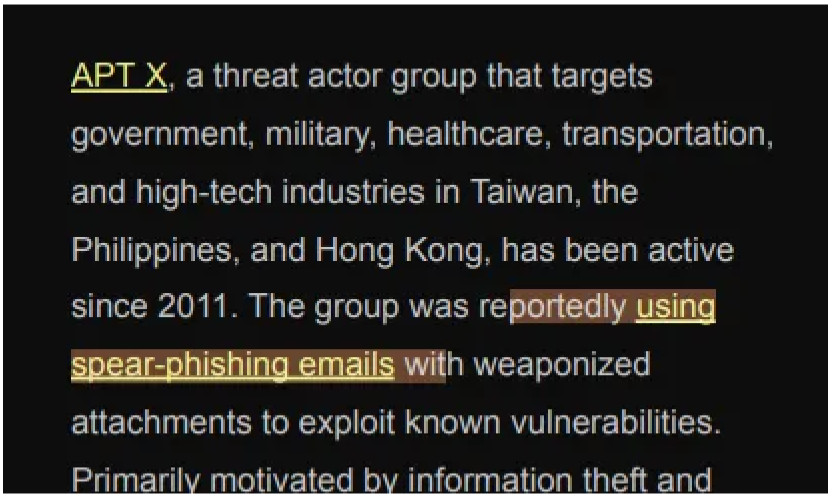
## Question 1:: What kind of phishing campaign does APT X use as part of their TTPs?



APT X Report

APT X's USBferry Targets Air-Gapped Networks

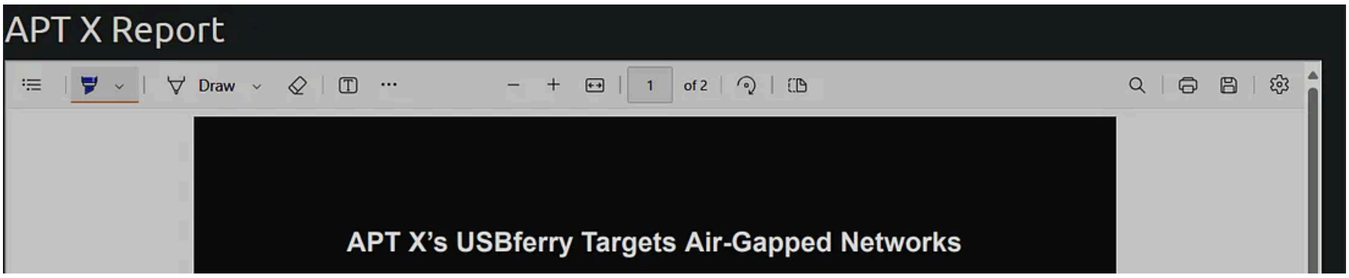
It is basically within the report provided so we just need to read it carefully at least once.



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

> *Answer:: Spear-Phising emails*

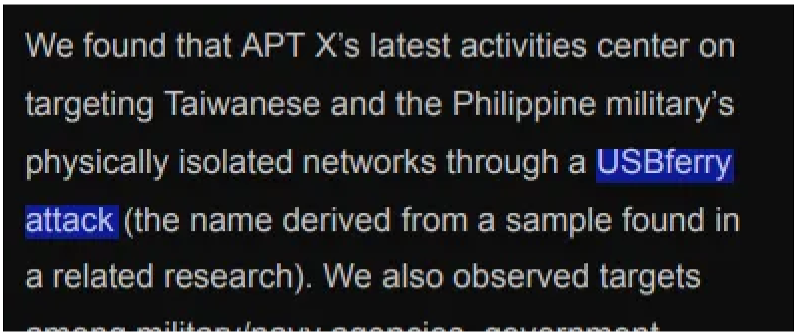
## Question 2:: What is the name of the malware used by APT X?



APT X Report

APT X's USBferry Targets Air-Gapped Networks

Same as question 1. We just need to read the report and it is provided :)



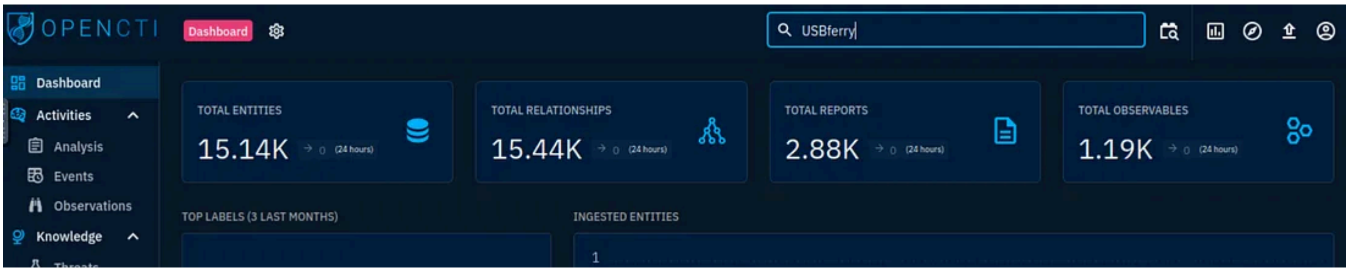
We found that APT X's latest activities center on targeting Taiwanese and the Philippine military's physically isolated networks through a USBferry attack (the name derived from a sample found in a related research). We also observed targets

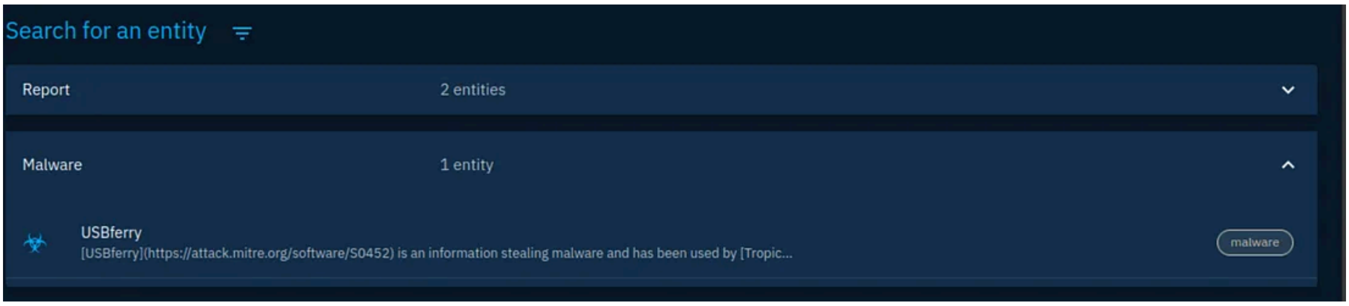
> *Answer:: USBferry*

## Question 3:: What is the malware's STIX ID?

Now this is not within the report obviously. So we need to use the provided Open CTI instance. All credentials are provided just log in.

Once logged in click into the "Search" box and type in "USBferry"



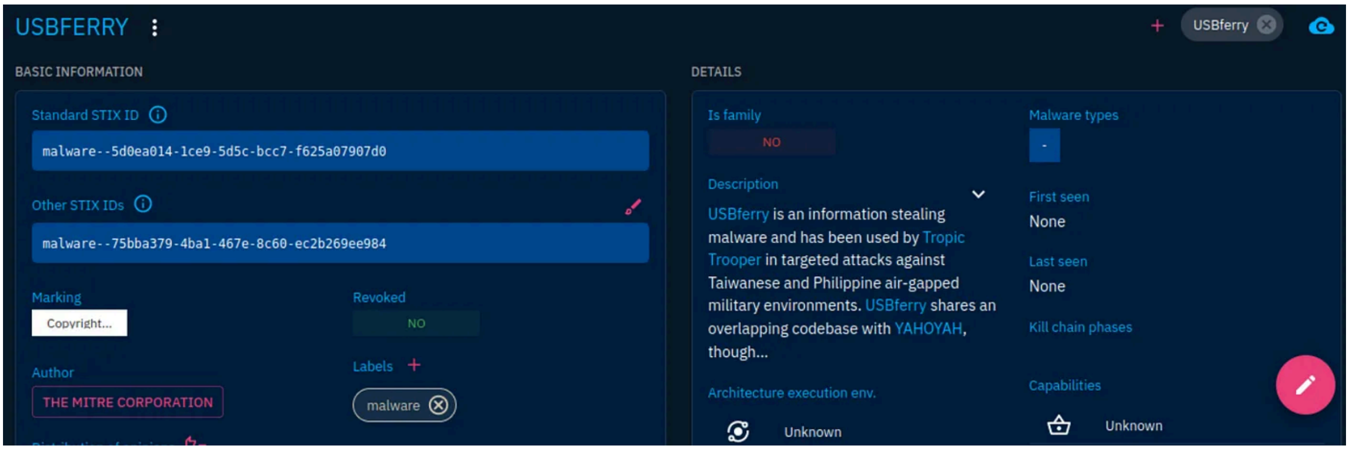


Search for an entity

| | |
|---|---|
| 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...
malware

You will see two options coming up but select the Malware option



USBFERRY

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

DETAILS

Is family: NO

Malware types: -

Description: USBferry is an information stealing malware and has been used by Tropic Trooper in targeted attacks against Taiwanese and Philippine air-gapped military environments. USBferry shares an overlapping codebase with YAHOYAH, though...

First seen: None

Last seen: None

Kill chain phases

Architecture execution env.: Unknown

Capabilities: Unknown

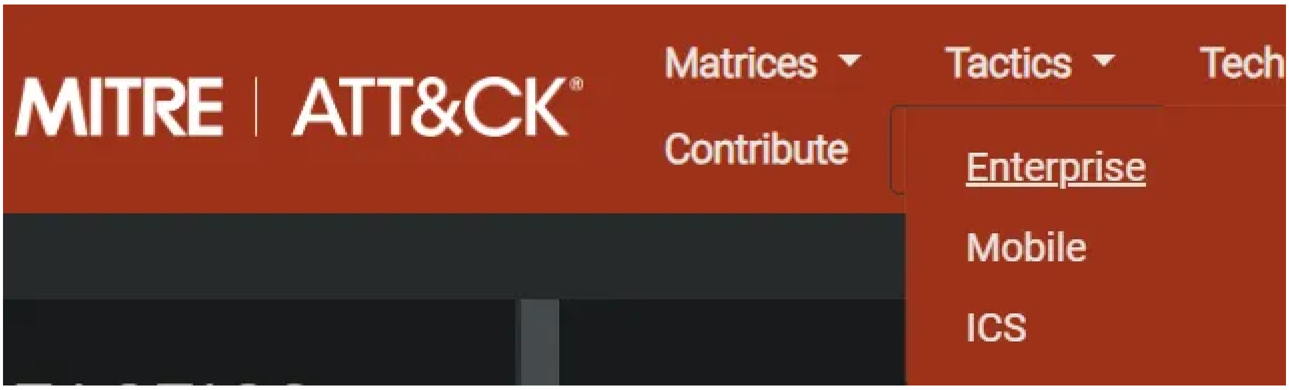
Once done you will see the answer.

> *Answer:: malware — 5d0ea014–1ce9–5d5c-bcc7-f625a07907d0*

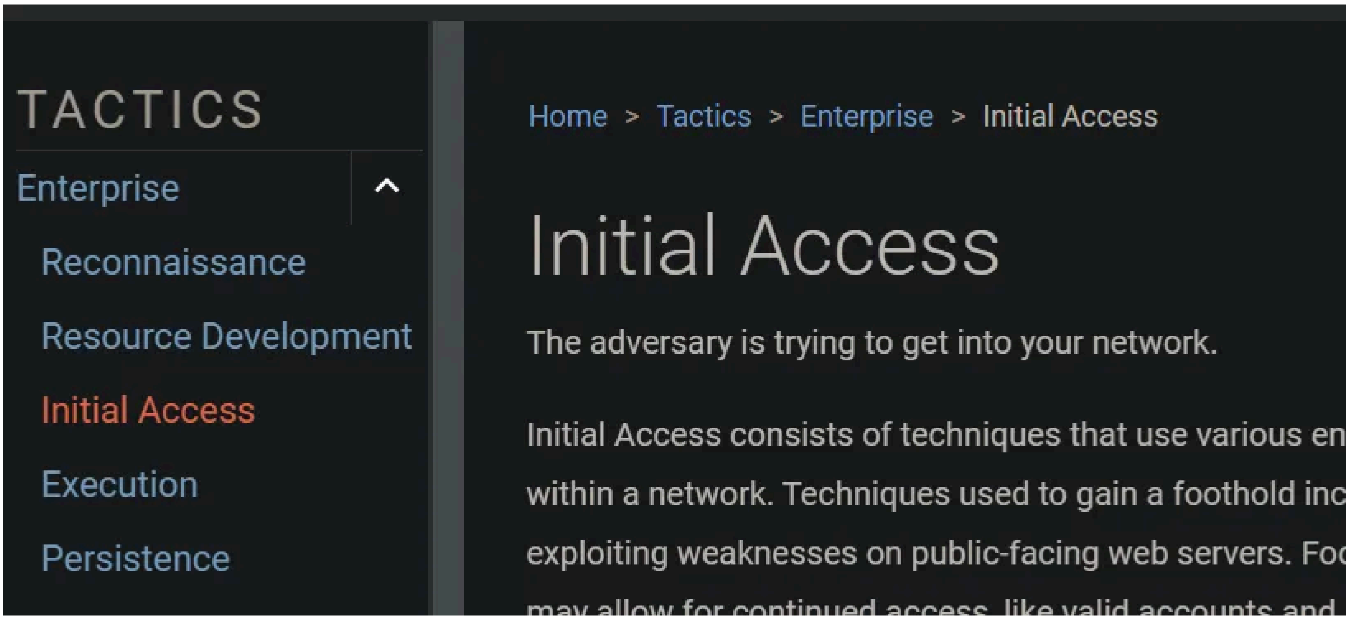
## Question 4:: With the use of a USB, what technique did APT X use for initial access?

This has multiple solutions I picked the easiest for myself.

Go to Mitre Att&ck website. Select Tactics -> Enterprise



Then within the “Enterprise” section under Tactics on the left you can find “Initial Access”



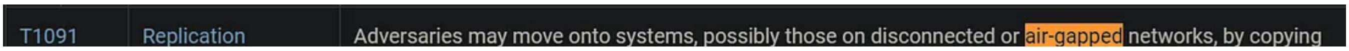
Initial Access

The adversary is trying to get into your network.

Initial Access consists of techniques that use various en
within a network. Techniques used to gain a foothold inc
exploiting weaknesses on public-facing web servers. Fo
may allow for continued access, like valid accounts and

Once this is picked we just need to find the answer here. We know from the report that they use “USB” and they operate within “Air-gapped” networks.

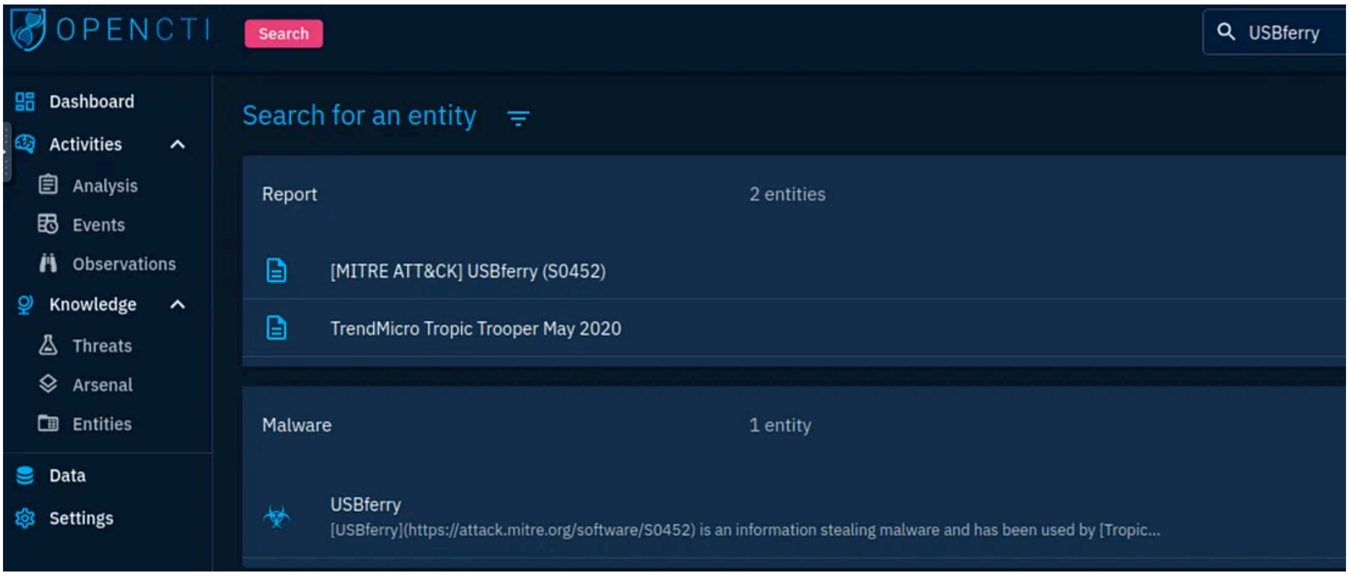
I wont pull this but if you look for “USB” aka “Removable Media” you get a lot of results but only one with a mach with “Air-gapped” networks and that is?



| | | |
|---|---|---|
| T1091 | Replication | Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying |

## Question 5:: What is the identity of APT X?

This is an easy one. The answer is basically within the Open CTI search we did earlier.



Report 2 entities

[MITRE ATT&CK] USBferry (S0452)

TrendMicro Tropic Trooper May 2020

Malware 1 entity

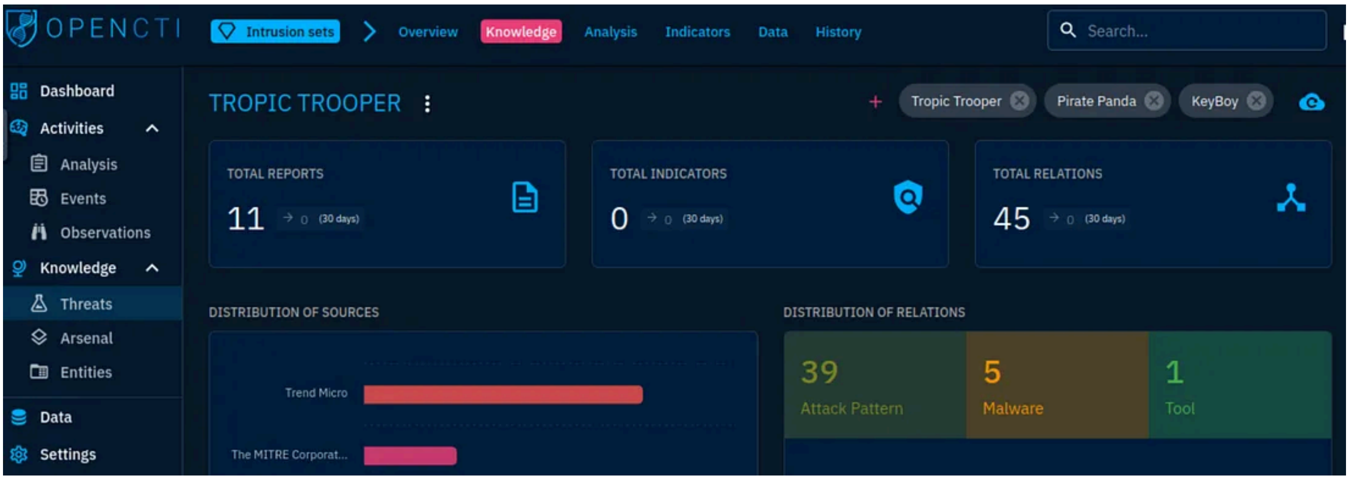
USBferry
[USBferry](https://attack.mitre.org/software/S0452) is an information stealing malware and has been used by [Tropic...

> *Answer:: Tropic Trooper*

## Question 6:: On OpenCTI, how many Attack Pattern techniques are associated with the APT?

So we need Open CTI for this as well. Lets search for “Tropic Trooper”.

Once done select “Knowledge” on the top bar.



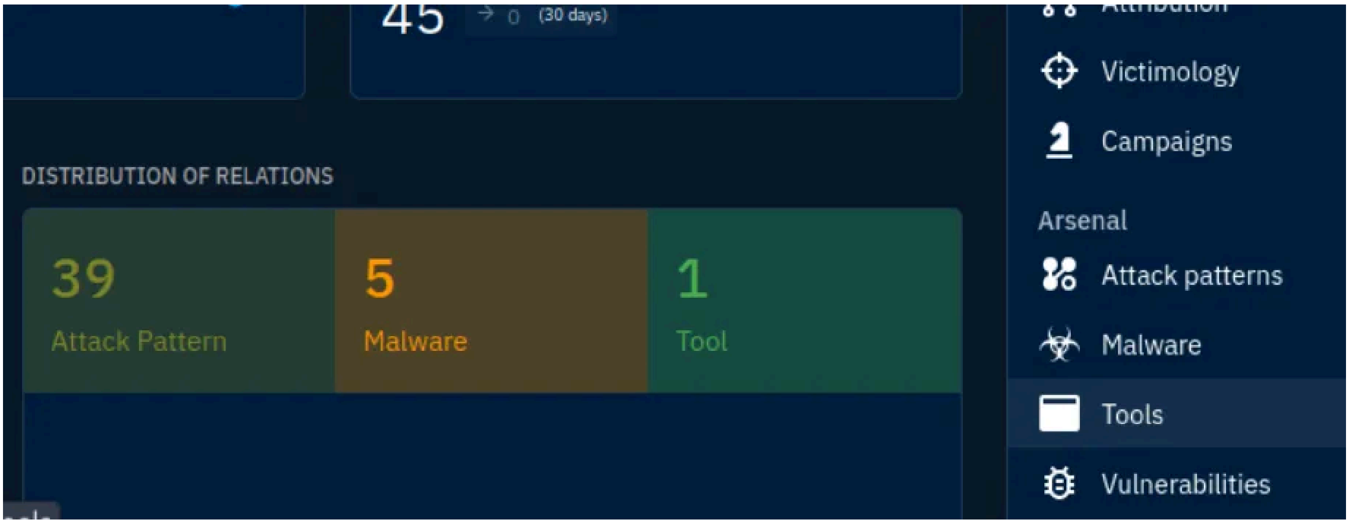
Under Distribution of Relations you can see that they have 39 known attack petterns by Open CTI.

> *Answer:: 39*

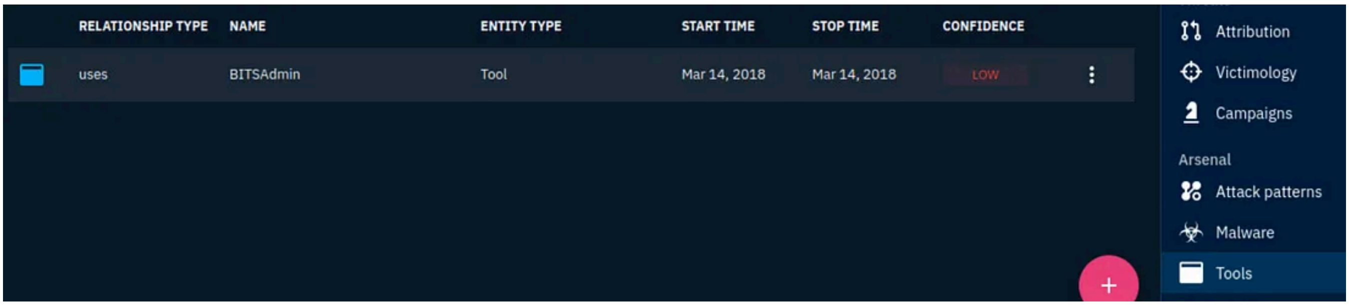
## Question 7:: What is the name of the tool linked to the APT?

Same place dont go anywhere :)

On the right you see a menu element called “Arsenal” and no its not the football team :D



There click the “Tools” submenu.



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

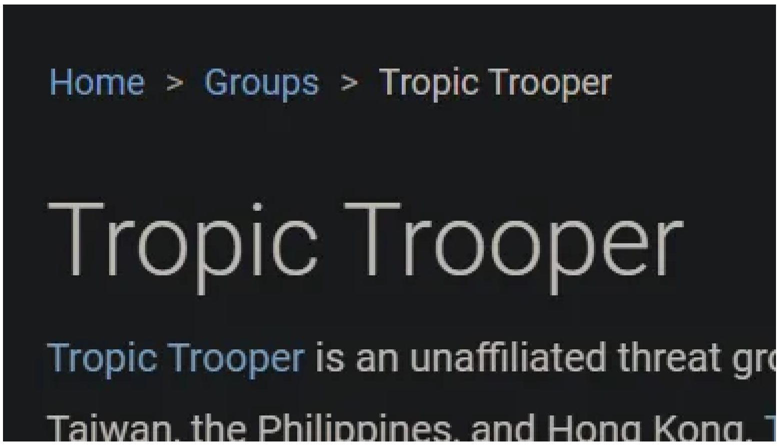
And we have a winner for thisone too.

> *Answer:: BITSAdmin*

### Question 8:: Load up the Navigator. What is the sub-technique used by the APT under Valid Accounts?

Just for the record this has multiple ways to solve it.

Load up Mitre page and under the groups look for the “Tropic Trooper”



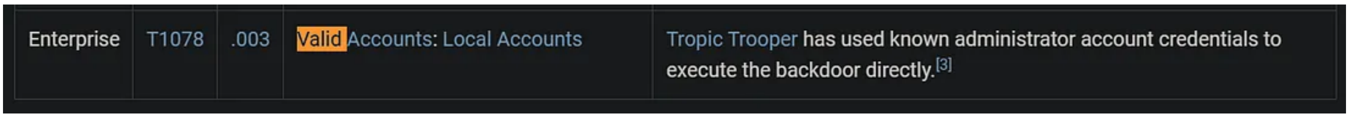
Home > Groups > Tropic Trooper

Tropic Trooper

Tropic Trooper is an unaffiliated threat gr

Taiwan, the Philippines, and Hong Kong. T

Then hit “Ctrl + f” and search for Valid Accounts.

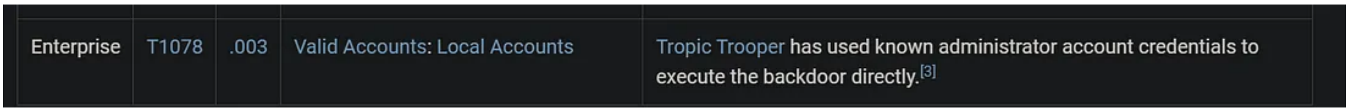


| | | | | |
|---|---|---|---|---|
| Enterprise | T1078 | .003 | Valid Accounts: Local Accounts | Tropic Trooper has used known administrator account credentials to execute the backdoor directly.[3] |

> *Answer:: Local Accounts*

## Question 9:: Under what Tactics does the technique above fall?

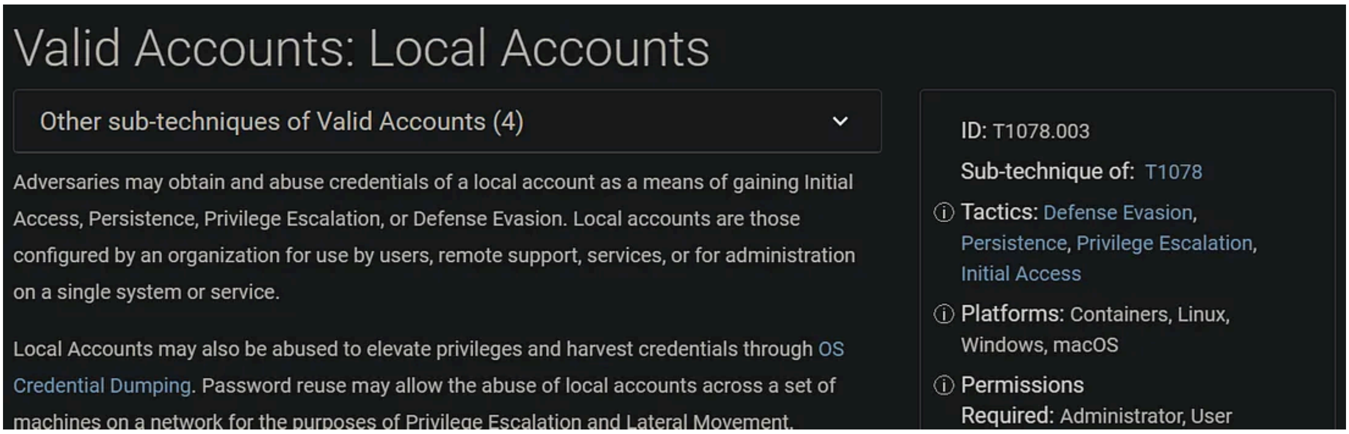
Easy one on the same page we were previously.



| | | | | |
|---|---|---|---|---|
| Enterprise | T1078 | .003 | Valid Accounts: Local Accounts | Tropic Trooper has used known administrator account credentials to execute the backdoor directly.[3] |

Click the T1078 tactic link.

Will get you here.



Valid Accounts: Local Accounts

Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.

Local Accounts may also be abused to elevate privileges and harvest credentials through OS Credential Dumping. Password reuse may allow the abuse of local accounts across a set of machines on a network for the purposes of Privilege Escalation and Lateral Movement.

ID: T1078.003

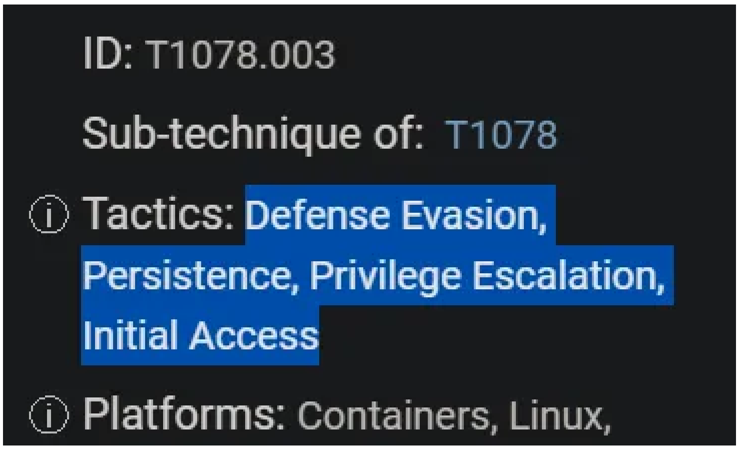
Sub-technique of: T1078

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

Platforms: Containers, Linux, Windows, macOS

Permissions Required: Administrator, User

On the right we can already see what Tactics does this fall under.



ID: T1078.003

Sub-technique of: T1078

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

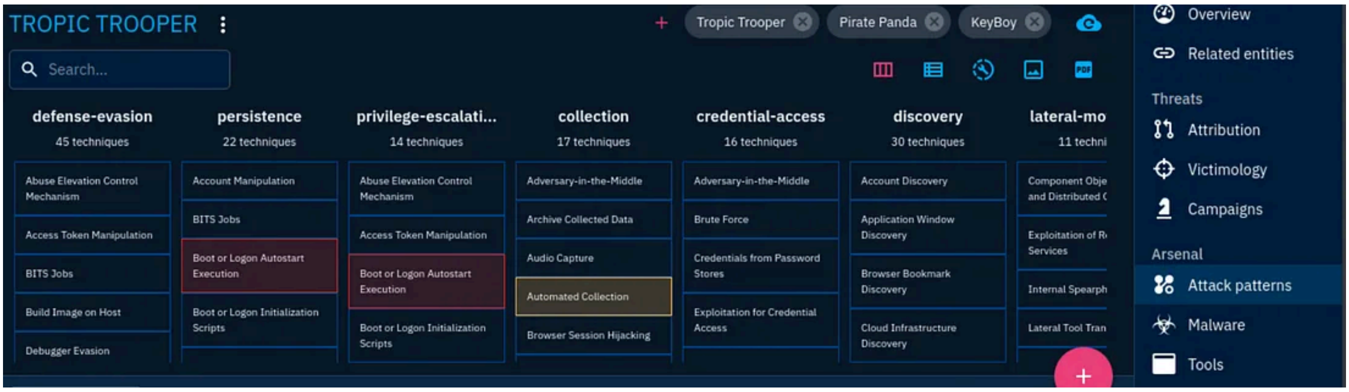
Platforms: Containers, Linux,

> *Answer:: Defense Evasion, Persistence, Privilege Escalation, Initial Access*

## Question 10:: What technique is the group known for using under the tactic Collection?

For fun and to switch lets use Open CTI for this.

Go to Open CTI page where we were previously and on the right side under “Arsenal” select “Attack patterns”



| defense-evasion<br>45 techniques | persistence<br>22 techniques | privilege-escalati...<br>14 techniques | collection<br>17 techniques | credential-access<br>16 techniques | discovery<br>30 techniques | lateral-mo<br>11 techni |
|---|---|---|---|---|---|---|
| Abuse Elevation Control Mechanism | Account Manipulation | Abuse Elevation Control Mechanism | Adversary-in-the-Middle | Adversary-in-the-Middle | Account Discovery | Component Obje and Distributed ( |
| Access Token Manipulation | BITS Jobs | Access Token Manipulation | Archive Collected Data | Brute Force | Application Window Discovery | Exploitation of R Services |
| BITS Jobs | Boot or Logon Autostart Execution | Boot or Logon Autostart Execution | Audio Capture | Credentials from Password Stores | Browser Bookmark Discovery | Internal Spearph |
| Build Image on Host | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Automated Collection | Exploitation for Credential Access | Cloud Infrastructure Discovery | Lateral Tool Tran |
| Debugger Evasion | | | Browser Session Hijacking | | | |

Look for the “collection” column. The answer is already highlighted by Open CTI.

> *Answer:: Automated Collection*

## 0x4C1D review

I personally think this was a really fun and interesting box. If you are already familiar with Open CTI and Mitre Att&ck framework then this is a really nice and easy walk in the park.

On the other hand. If someone is just getting around or does not know these frameworks then it can be a pain to differentiate Tactics, Techniques and Procedures.

Mitre can be a lot at the start but once you get to know it then you realize it is easy and very helpfull.

I do suggest everyone to take a peak of this box and have a go at it.

Have fun ya all and remember that the Sky is Blue :D

Tryhackme Thm Trooper Mitre Attack Walkthrough

Follow

## Written by 0x4C1D

62 Followers · 1 Following

I am a Cyber Security Specialist at a Telco company so mainly dealing with Blue Team stuff. Also during night time I like to practice Red Teaming and CTFs.

## No responses yet

What are your thoughts?

Respond

## More from 0x4C1D

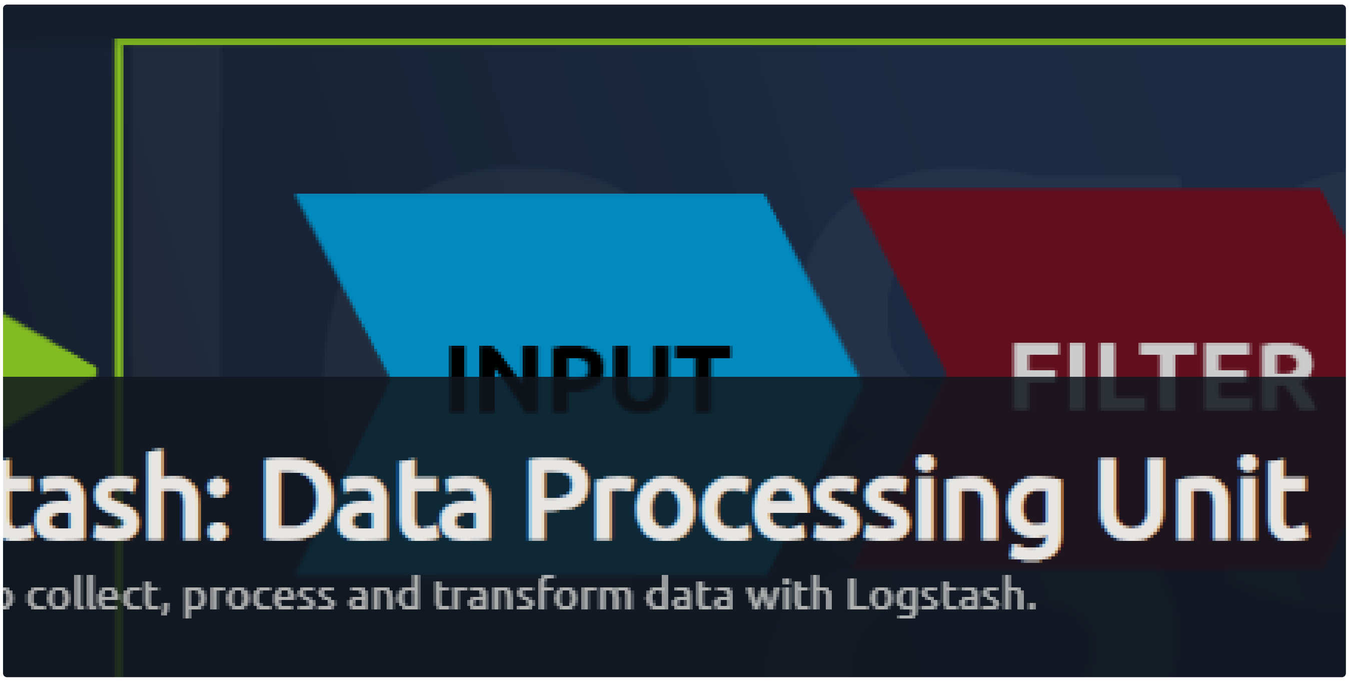
Rule
t Intelligence for SOC
utilise Threat Intelligence to improve the Security Operations

0×4C1D

## Try Hack Me — Threat Intelligence for SOC — Walkthrough

Room Link:: https://tryhackme.com/room/threatintelligenceforsoc Level:: Medium Tags:: SOC, Threat Intelligence, Uncoder, Kibana

Sep 26, 2023 5

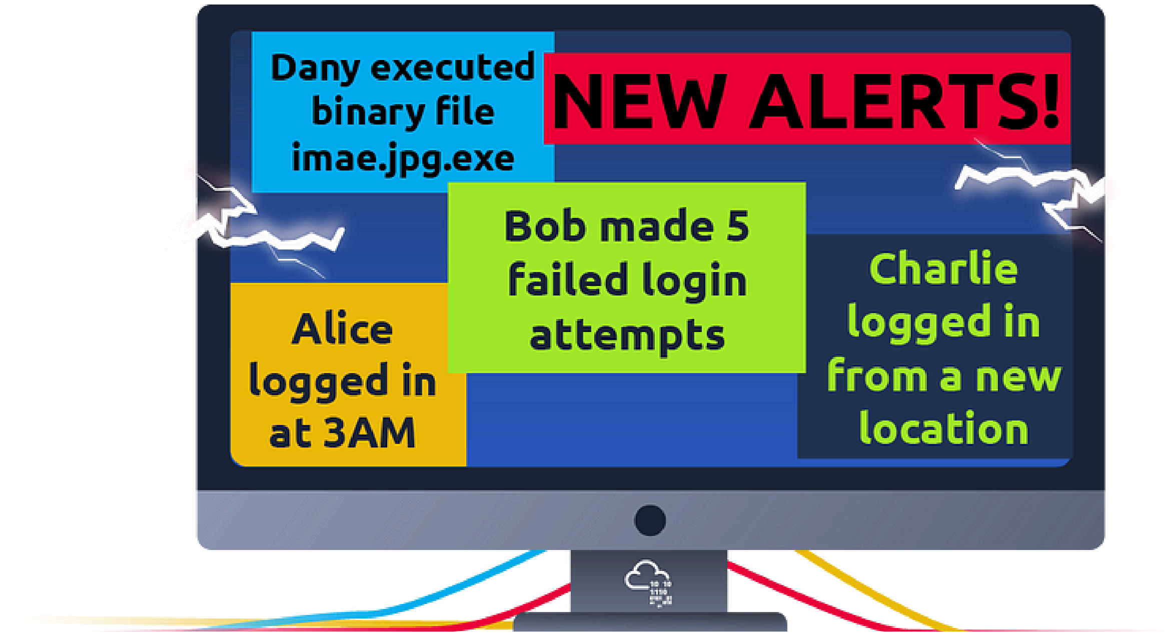

INPUT
FILTER
tash: Data Processing Unit
collect, process and transform data with Logstash.

0×4C1D

## Try Hack Me — Logstash: Data Processing Unit — Walkthrough

So Logstash is part of the new SOC L2 paths advanced ELK section.

Oct 16, 2023 54 1

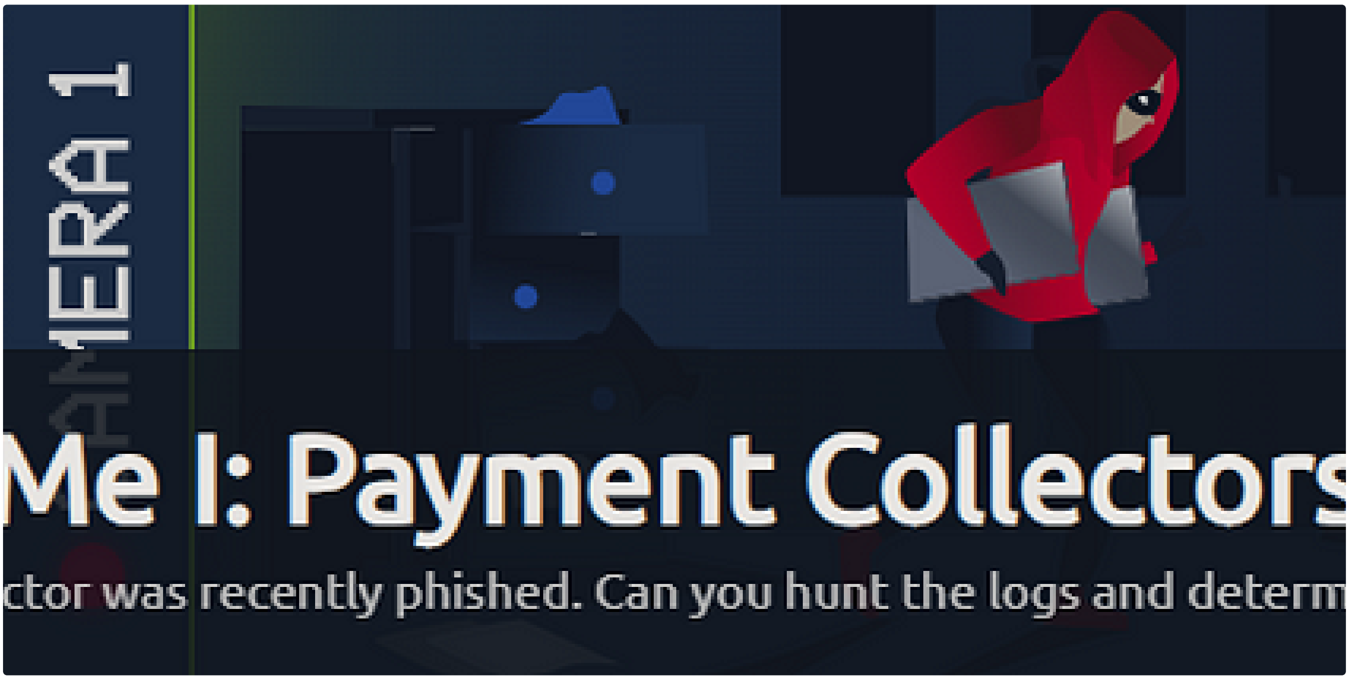

Dany executed binary file imae.jpg.exe
NEW ALERTS!
Bob made 5 failed login attempts
Alice logged in at 3AM
Charlie logged in from a new location

0×4C1D

## TryHackMe—Identification & Scoping walkthrough

So this is a fairly new room which got released fairly recently on THM.

Aug 24, 2023 1



0×4C1D

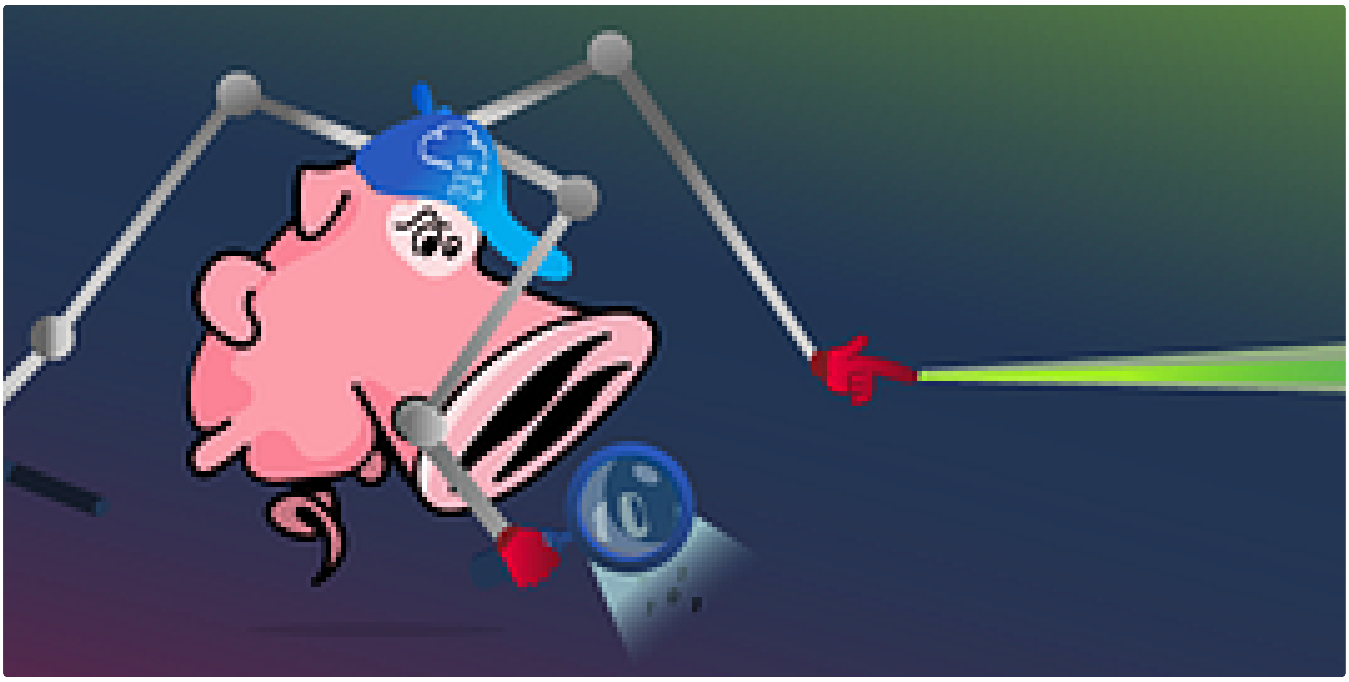
## Try Hack Me—Hunt Me I: Payment Collectors—Walkthrough

Link to room:: https://tryhackme.com/room/threathuntingendgame Level:: Medium Tags:: #ThreatHunting, #Kibana, #Security, #ELK, #Phishing

Oct 2, 2023 7

See all from 0×4C1D

## 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 100

Trnty

## TryHackMe | Introduction To Honeypots Walkthrough

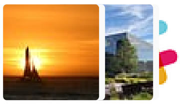
A guided room covering the deployment of honeypots and analysis of botnet activities

Sep 7, 2024 10

## Lists

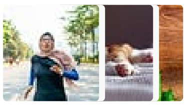
### Staff picks

796 stories · 1558 saves



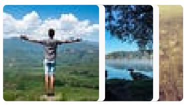
### Stories to Help You Level-Up at Work

19 stories · 912 saves



### Self-Improvement 101

20 stories · 3191 saves



### Productivity 101

20 stories · 2704 saves

The Devops Girl

## How to Set Up Fluent Bit for CloudWatch Logs in EKS : A Complete Guide

Learn how to configure Fluent Bit to stream logs from your Amazon EKS cluster to CloudWatch in simple, detailed steps. This guide will walk...

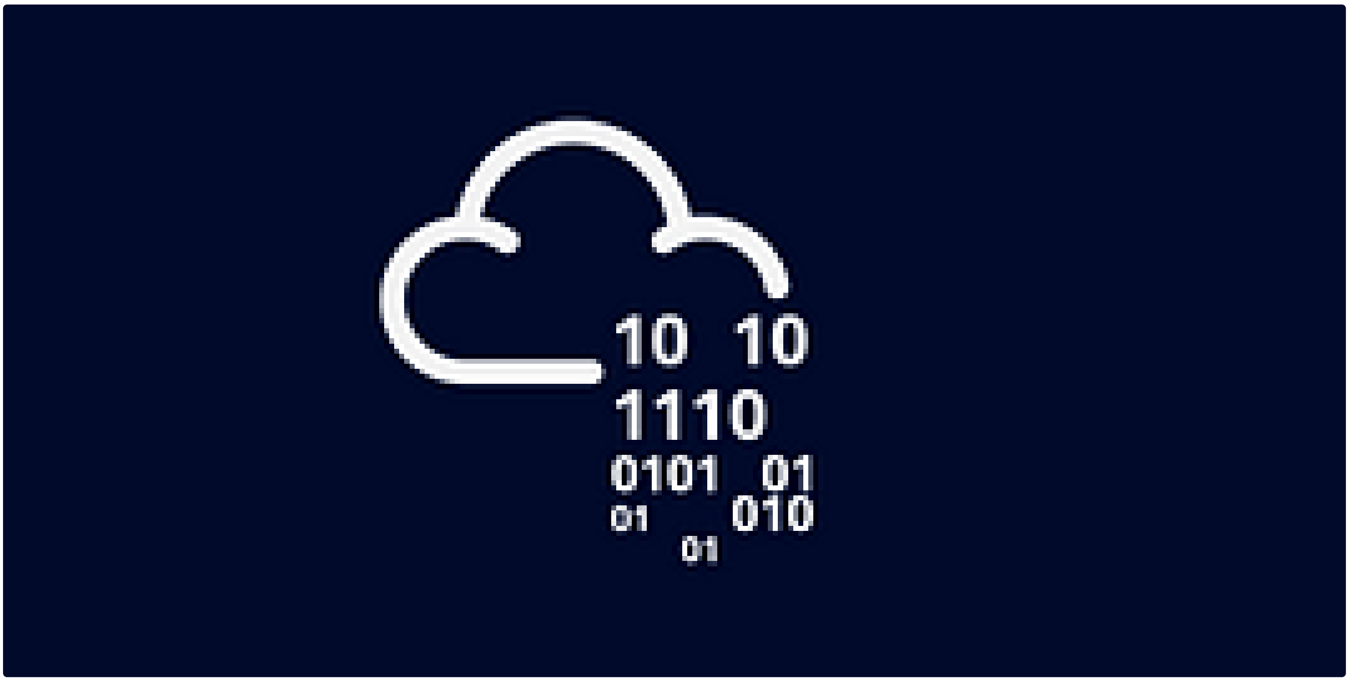
Jul 30, 2024 50

In T3CH by Axoloth

## TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50

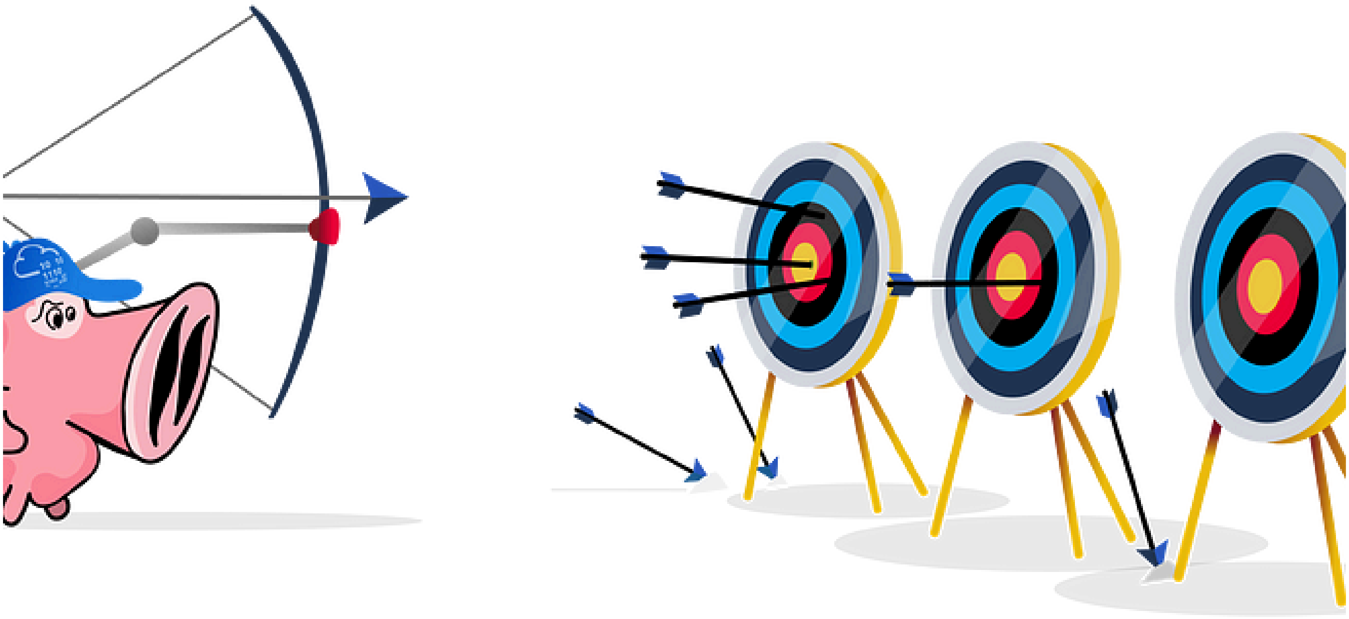


In T3CH by Axoloth

## TryHackMe | AD Certificate Templates | WriteUp

Walkthrough on the exploitation of misconfigured AD certificate templates

Sep 11, 2024 70



Manivel

## Snort Challenge — The Basics : TryHackMe — Medium

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

Dec 30, 2024 👏 3

See more recommendations