

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



# Tropic Trooper TryHackMe Write-Up



Joseph Alan · [Follow](#)

3 min read · Jul 22, 2023



Listen



Share



More



A multinational technology company has been the target of several cyber attacks in the past few months. The attackers have been successful in stealing sensitive intellectual property and causing disruptions to the company's operations. A [threat advisory report](#) about similar attacks has been shared, and as a CTI analyst, your 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. For this task, you will utilize the [OpenCTI](#) platform as well as the MITRE ATT&CK navigator, linked to the details below.

## Assigned Tools

Start the virtual machine by clicking on the green “**Start Machine**” button on the upper right section of this task. Give it about **7 minutes** to fully load and use the credentials below to access the platforms via the AttackBox or VPN to conduct your investigations.

### Download The APT X Report

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

The downloaded document says

the Philippines, and Hong Kong, has been active since 2011. The group was reportedly using *spear-phishing emails* — *Answer*

#### Q 2. What is the name of the malware used by APT X?

The downloaded document says

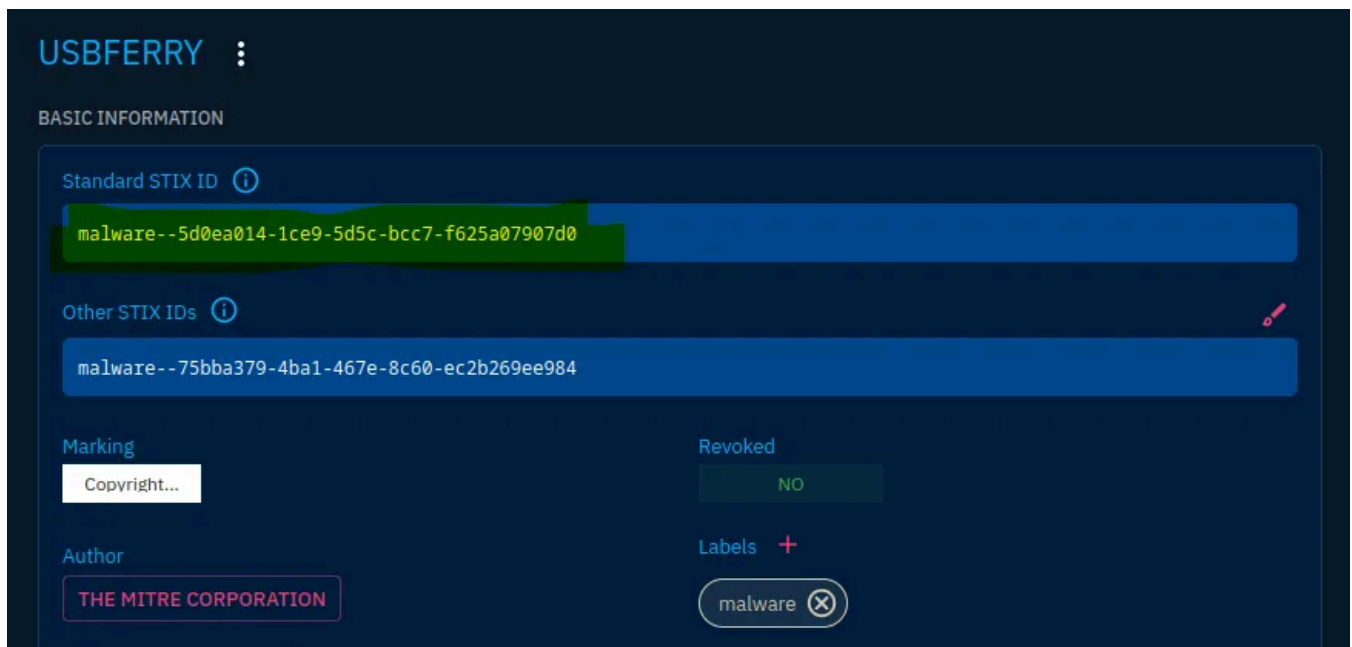
We found that APT X’s latest activities center on targeting Taiwanese and the Philippine military’s physically isolated networks through a *USBferry* — *Answer*  
**attack**

#### Q 3. What is the malware’s STIX ID?

**Step 1** — Login to OPENCTI with the provided credentials

**Step 2** — Search for USBferry

**Answer:**



**Q 4. With the use of a USB, what technique did APT X use for initial access?**

**Step 1** — Download a detailed technical report from trend micro from [here](#)

**Step 2** — ctrl+f and search initial access

**Answer:** Replication Through Removable Media

**Q 5. What is the identity of APT X?**

**Answer:** Tropic Trooper (aka KeyBoy) — *Found in the detailed document*

**Q 6. On OpenCTI, how many Attack Pattern techniques are associated with the APT?**

**Step 1** — Search Tropic Trooper on OpenCTI

**Step 2** — Click Arsenal → Attack Patterns

**Answer:** 39

**Q 7. What is the name of the tool linked to the APT?**

**Step 1** — Search Tropic Trooper on OpenCTI

**Step 2** — Click Arsenal → Tools

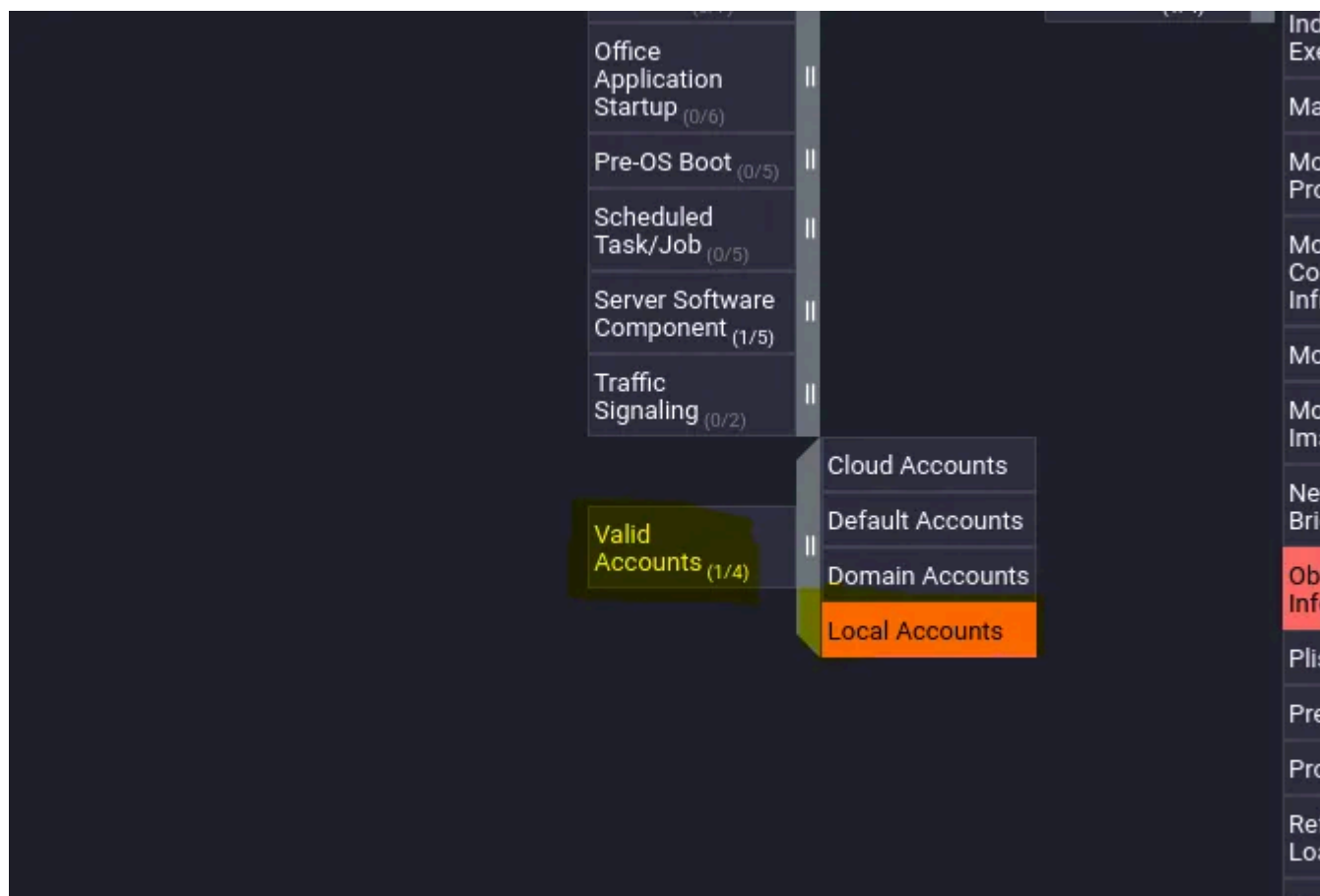
Open in app ↗

## Accounts?

**Step 1** — Login to the ATT&CK Navigator with the given credentials

**Step 2** — ctrl+f valid accounts

**Answer: Local Accounts**



**Q 9. Under what Tactics does the technique above fall?**

**Step 1** — Right-click the Local Accounts on the image above and select View tactic

### Valid Accounts: Local Accounts

#### Other sub-techniques of Valid Accounts (4)

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

Version: 1.3

Created: 13 March 2020

Last Modified: 13 April 2023

Version Permalink

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

**Q 10. What technique is the group known for using under the tactic Collection?**

**Answer: Automated Collection**

Initial Access Techniques	Collection 17 techniques	Command and Control 16 techniques
Application of e es	Adversary-in-the-Middle (0/3)	Application Layer Protocol (
phishing	Archive Collected Data (0/3)	Communi Through Removabl Media
Tool er	Audio Capture	Data Encoding
e e n ng (0/2)	Automated Collection	Data Obfuscati
e es (0/6)	Browser Session Hijacking	Dynamic Resolution
tion	Clipboard Data	Encrypted
	Data from Cloud	

**TTP Has Been Identified Successfully As Required By The Questionnaire!!!**

Tryhackme Walkthrough

Tryhackme Writeup

Ctf Writeup

Cybersecurity

Opencti



Follow

**Written by Joseph Alan**

217 Followers · 225 Following

Cloud Security Engineer | AWS Solutions Architect Professional | CompTIA Cysa+|AWS sysops admin with LAB | TryHackMe top 1%| HackTheBox Rank - Pro Hacker

No responses yet




What are your thoughts?

Respond

## More from Joseph Alan



 Joseph Alan

## Expose TryHackMe Write-Up


Expose

Sep 24, 2023  5








 Joseph Alan

## Threat Hunting Introduction

### Task 1 Introduction

Sep 26, 2023  7  1



 In Dev Genius by Joseph Alan

## TryHackMe HTTP/2 Request Smuggling Write-Up

Learning Objectives: Gain a foundational understanding of HTTP/2, master the exploitation of HTTP request smuggling through HTTP/2 or...

Mar 15, 2024 🖱 1



Joseph Alan

## Custom Alert Rules in Wazuh TryHackMe Write-Up

Custom Alert Rules in Wazuh

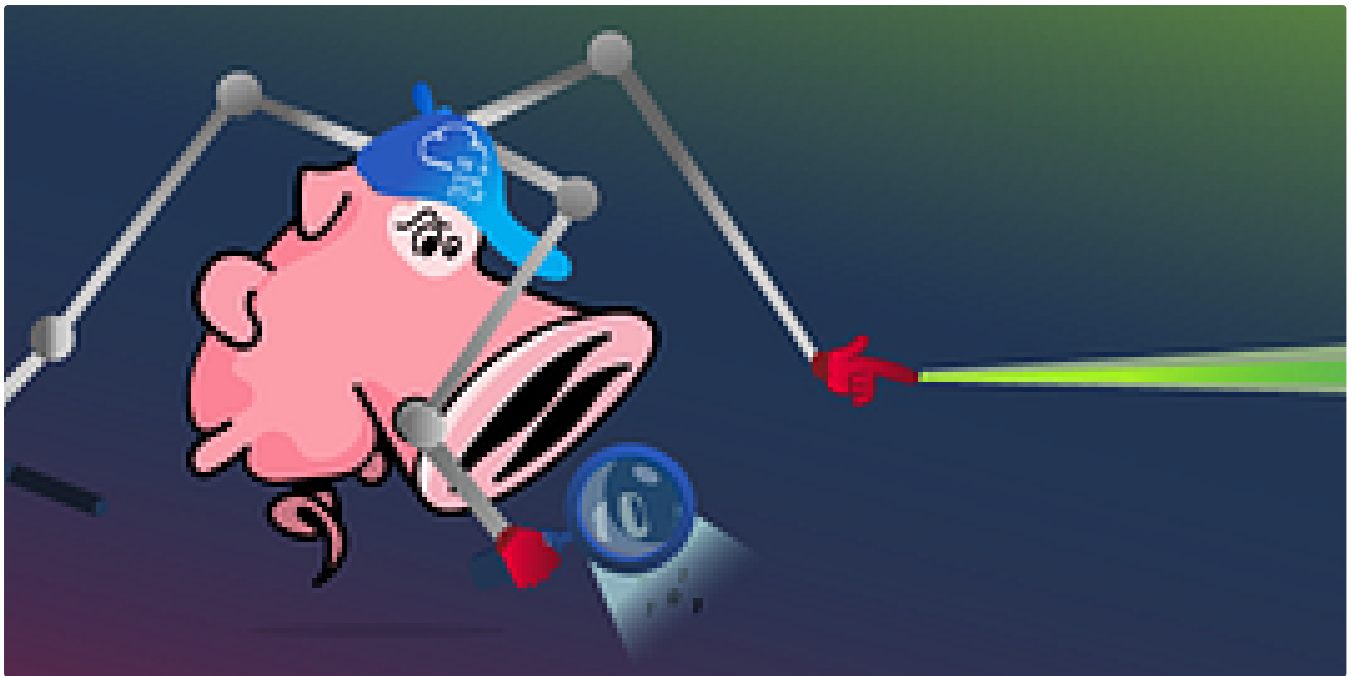
Sep 20, 2023 🖱 76 💬 1



See all from Joseph Alan

## 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



The Devops Girl

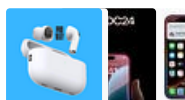
## How to Set Up Fluent Bit for CloudWatch Logs in EKS : A Complete Guide

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

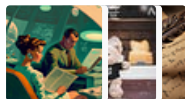


## Lists



### 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



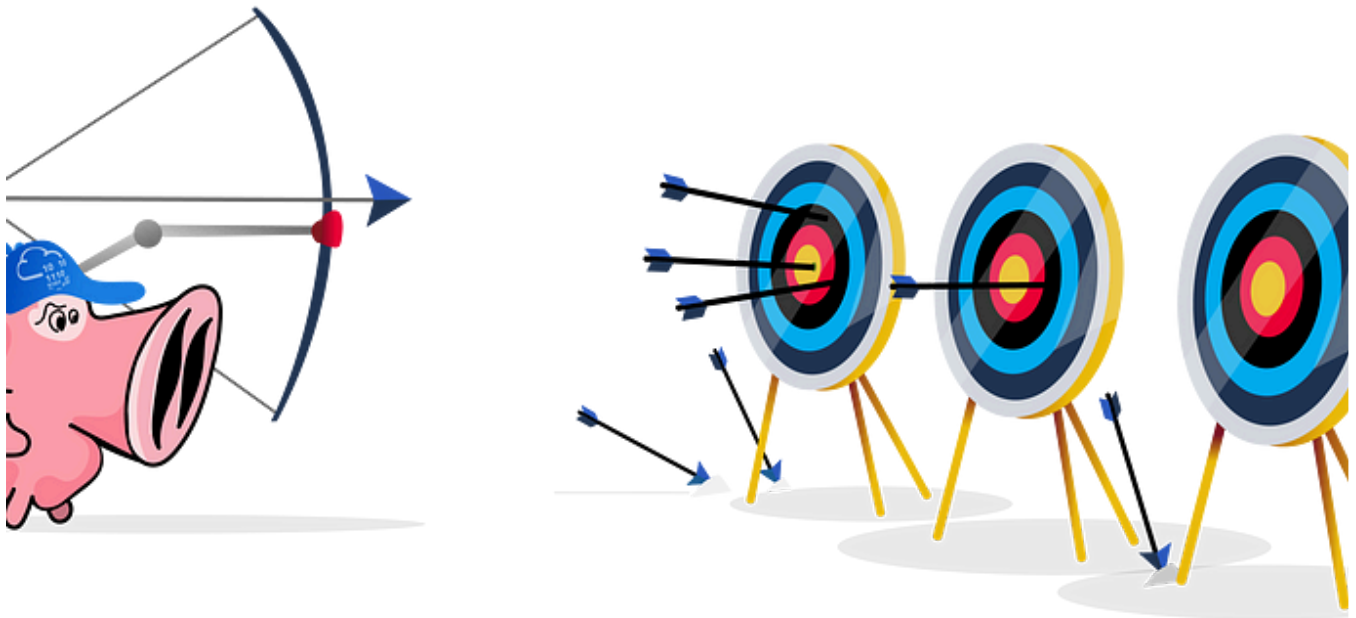
In T3CH by Axoloth

## TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

★ Nov 28, 2024 🖱 50



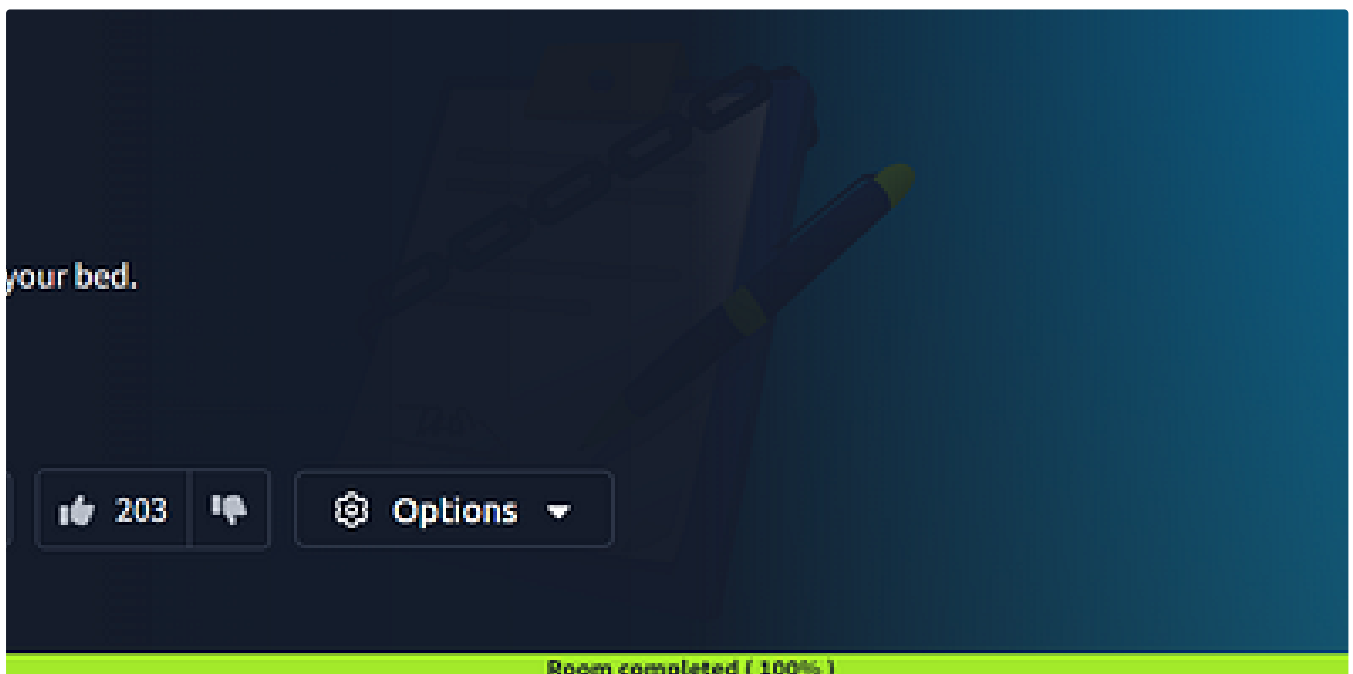


 Manivel

## Snort Challenge—The Basics : TryHackMe—Medium

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

Dec 30, 2024  3



 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



IritT

## Becoming a First Responder — Managing Incidents — TryHackMe Walkthrough

Explaining how first responders work and what to do if you are a first responder to a cyber incident.

Dec 16, 2024

[See more recommendations](#)