Cyber Threat Intelligence

CTI can be defined as evidence-based knowledge about adversaries, this can include:

- Tactics
- Motivation
- Indicators

This is how the CTI comes into play with Data, Information and intelligence:

- Data - Indicators associated with attackers, which could include IP addresses, URL or hashes
- Information - Multiple data points
- Intelligence - Correlation of data and information to extract patterns of actions based on contextual analysis

The main objective of the CTI is to understand the relationship between your operational environment and the adversary. How to defend against attacks/attackers

Questions to be asked in this model include:

- Who’s attacking you?
- What are their motivations?
- What are their capabilities?
- What artefacts and indicators of compromise (IOCs) should you look out for?

There are three sources where these questions could arise from:

Internal:

- Vulnerability assessments/Incident reports
- Cyber Awareness Training
- Logs/Events

Community:

- Web forums
- Dark web

External:

- News feeds
- Social Media
- Marketplaces

We can break down threat intel into four classifications:

- Strategic Intel - High-level intel that looks at the landscape and maps out vulnerable areas based on trends, patterns and threats
- Technical Intel - Analyses evidence of an attack used by the adversary, this helps incident response teams create defence mechanisms
- Tactical Intel - Assesses the adversaries TTPs
- Operational Intel - Figuring out the attackers motive and why they have intent to perform an attack on the organisation

What does CTI stand for?
Cyber Threat Intelligence

IP addresses, Hashes and other threat artefacts would be found under which Threat Intelligence classification?
Technical intel

CTI Lifecycle

There are 6 phases to the cyber threat intelligence lifecycle:

Direction:
The threat intel needs to have a sense of direction of how to defend themselves, these are the following that will need to be put in place:

- Assets that need to be defended
- Impact if assets are lost
- How to store data and assets securely
- Tools that will help defend data and assets

Collection:
Once an objective has been completed, security analysts will need to collect all data. They can collect this with public, private and open source tools, most of the time this will be automated

Processing:
Processing is the phase of ensuring that data is extracted, organised and correlates. SIEMs will be used to make sure this is completed

Analysis
After the data has been aggregated, it will be analysed and decisions are made:

- Investigating a potential threat through patterns and trends
- Action plan to defend against the attack
- Strengthening security controls

Dissemination:
Dissemination is the process of writing a report on the attack and reporting it to the technical teams with the TTPs, threats, IOCs and how it will be remediated

Feedback
The final phase is the feedback phase that is provided by stakeholders to strengthen the threat intelligence process and implementation

At which phase of the CTI lifecycle is data converted into usable formats through sorting, organising, correlation and presentation?
Processing

During which phase do security analysts get the chance to define the questions to investigate incidents?
Direction

CTI Standards & Frameworks

Standards and Frameworks can help with strengthening the cyber threat intelligence, here are some that are commonly used:

MITRE ATT&CK
This framework is a knowledge base of adversary behaviour to track and investigate

TAXII
TAXII stands for Trusted Automated eXchange of Indicator Information. This framework insists on having real-time detection, prevention and mitigation of threats. There are two sharing models the TAXII support:

- Collection - Collected and hosted by a producer upon request
- Channel - Pushed to users from a central server through a publish-subscribe model

STIX
Structured Threat Information Expression is a language developed for the "specification, capture, characterisation and communication of standardised cyber threat information". It provides defined relationships

between sets of threat info such as observables, indicators, adversary TTPs, attack campaigns, and more.

Cyber Kill Chain
As in previous writeups, this is a 7 step phase to an attack developed by Lockheed Martin:

- Reconnaissance
- Weaponisation
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objectives

Diamond Model
The diamond model is a four key intrusion analysis framework:

- Adversary
- Victim
- Infrastructure
- Capabilities

What sharing models are supported by TAXII?
Collection and Channel

When an adversary has obtained access to a network and is extracting data, what phase of the kill chain are they on?
Actions On Objective

Practical Analysis

In the practical analysis we have to review the logs in a SIEM and answer questions on the threat profile

"Pasted image 20230830200018.png" is not created yet. Click to create.

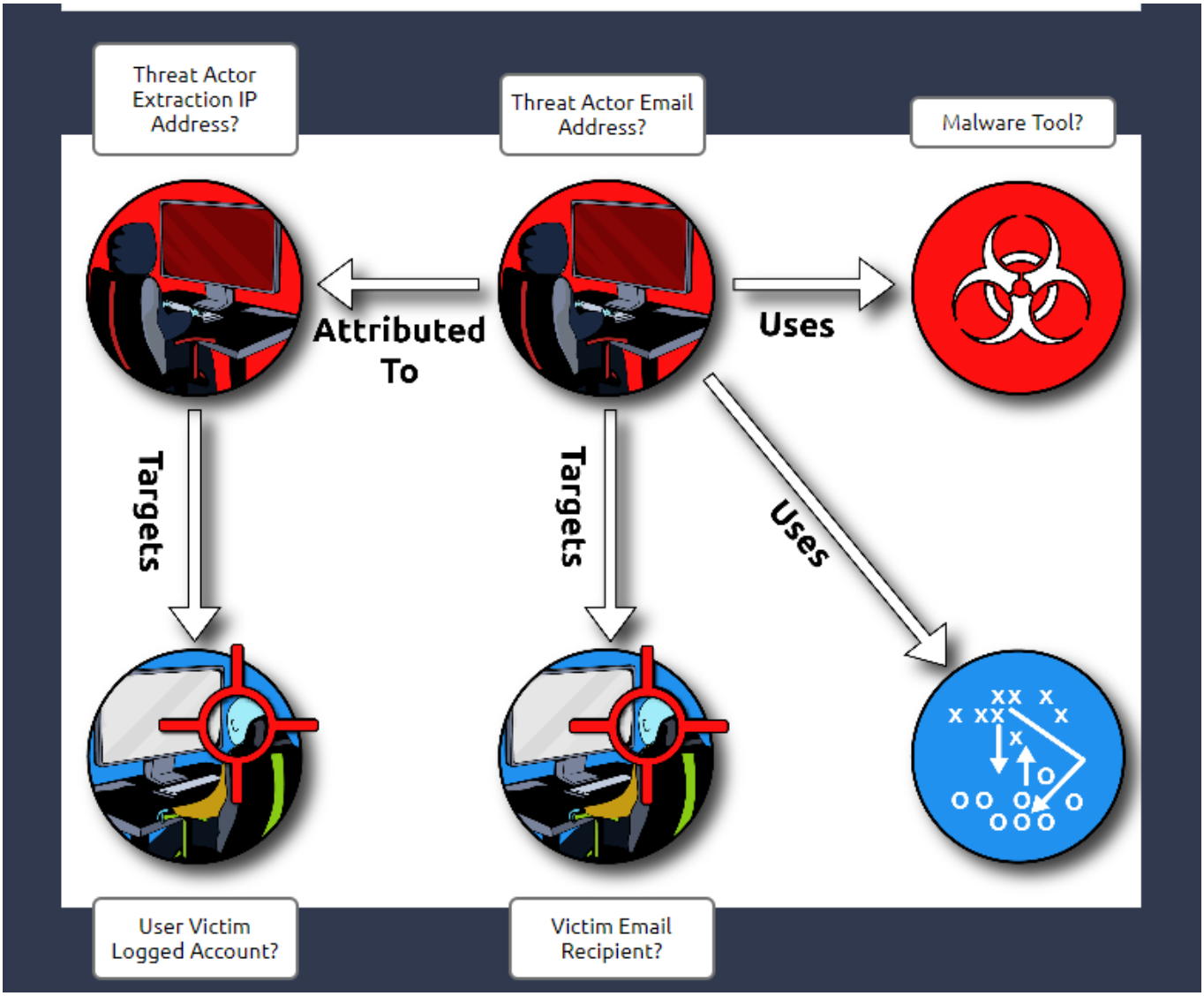
As we can see the email was received by John doe on Sept 10th 2020, 08:40:20:091

What was the source email address?
vipivillain@badbank.com

John Doe downloads an attachment from the email

What was the name of the file downloaded?
flbpfuh.exe

Now to receive the flag we have to build the threat profile by answering these questions:



What was the threat actor's extraction IP address?

91.185.23.222

What was the threat actor email address?

vipivillain@badbank.com

What software tool was used in the extraction?

flbpfuh.exe

What user account was logged in by the threat actor?

Administrator

Who was the targeted victim?

John Doe

Once we have answered all the questions we receive the flag

After building the threat profile, what message do you receive?
THM{NOW_I_CAN_CTI}