Cyber Threat Intelligence

-Mesai-

Chapter này gồm 5 mục chính:

1.Intro to Cyber Threat Intel

2.Threat Intelligence Tools

3.Yara

4.Open CTI

5.MISP

1. Intro to Cyber Threat Intel

Task 2 Cyber Threat Intelligence

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

Task 3 CTI Lifecycle

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

Task 4 CTI Standards & Frameworks

What sharing models are supported by TAXII?

Collection and chanels

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

Actions on Objectives

Task 5 Practical Analysis

What was the source email address?

vipivillain@badbank.com

What was the name of the file downloaded?

flbpfuh.exe

After building the threat profile, what message do you receive?

THM{NOW_I_CAN_CTI}

2. Threat Intelligence Tools

Task 2 Threat Intelligence

What was TryHackMe's Cisco Umbrella Rank based on the screenshot?

345612

How many domains did UrlScan.io identify on the screenshot?

13

What was the main domain registrar listed on the screenshot?

NAMECHEAP INC

What was the main IP address identified for TryHackMe on the screenshot?

2606:4700:10::ac43:1b0a

Task 3 Urlscan.io

What was TryHackMe's Cisco Umbrella Rank based on the screenshot?

345612

How many domains did UrlScan.io identify on the screenshot?

13

What was the main domain registrar listed on the screenshot?

NAMECHEAP INC

What was the main IP address identified for TryHackMe on the screenshot?

2606:4700:10::ac43:1b0a

Task 4 Abuse.ch

The IOC 212.192.246.30:5555 is identified under which malware alias name on ThreatFox?

katana

Which malware is associated with the JA3 Fingerprint 51c64c77e60f3980eea90869b68c58a8 on SSL Blacklist?

Dridex

From the statistics page on URLHaus, what malware-hosting network has the ASN number AS14061?

DIGITALOCEAN-ASN

Which country is the botnet IP address 178.134.47.166 associated with according to FeodoTracker?

Georgia

Task 5 PhishTool

What social media platform is the attacker trying to pose as in the email?

linkedIn

What is the senders email address?

darkabutla@sc500.whpservers.com

What is the recipient's email address?

cabbagecare@hotsmail.com

What is the Originating IP address? Defang the IP address.

204[.]93[.]183[.]11

How many hops did the email go through to get to the recipient?

4

Task 6 Cisco Talos Intelligence

What is the listed domain of the IP address from the previous task?

scnet.net

What is the customer name of the IP address?

Complete Web Reviews

Task 7 Scenario 1

According to Email2.eml, what is the recipient's email address?

chris.lyons@supercarcenterdetroit.com

From Talos Intelligence, the attached file can also be identified by the Detection Alias that starts with an H...

HIDDENEXT/Worm.Gen

Task 8 Scenario 2

What is the name of the attachment on Email3.eml?

Sales_Receipt 5606.xls

What malware family is associated with the attachment on Email3.eml?

Dridex

3. Yara

Task 2 What is Yara?

What is the name of the base-16 numbering system that Yara can detect?

hexadecimal

Would the text "Enter your Name" be a string in an application? (Yay/Nay)

Yay

Task 8

Scan file 1. Does Loki detect this file as suspicious/malicious or benign?

suspicious

What Yara rule did it match on?

webshell_metaslsoft

What does Loki classify this file as?

Web shell

Based on the output, what string within the Yara rule did it match on?

Str1

What is the name and version of this hack tool?

b374k 2.2

Inspect the actual Yara file that flagged file 1. Within this rule, how many strings are there to flag this file?

1

Scan file 2. Does Loki detect this file as suspicious/malicious or benign?

bengin

Inspect file 2. What is the name and version of this web shell?

b374k 3.2.3

Task 9

From within the root of the suspicious files directory, what command would you run to test Yara and your Yara rule against file 2?

yara file2.yar file2/1ndex.php

Did Yara rule flag file 2? (Yay/Nay)

yay

Copy the Yara rule you created into the Loki signatures directory.

Test the Yara rule with Loki, does it flag file 2? (Yay/Nay)

yay

What is the name of the variable for the string that it matched on?

zepto

Inspect the Yara rule, how many strings were generated?

20

One of the conditions to match on the Yara rule specifies file size. The file has to be less than what amount?

700kb

Task 10

Enter the SHA256 hash of file 1 into Valhalla. Is this file attributed to an APT group? (Yay/Nay)

yay

Do the same for file 2. What is the name of the first Yara rule to detect file 2?

Webshell_b374k_rule1

Examine the information for file 2 from Virus Total (VT). The Yara Signature Match is from what scanner?

THOR APT Scanner

Enter the SHA256 hash of file 2 into Virus Total. Did every AV detect this as malicious? (Yay/Nay)

nay

Besides .PHP, what other extension is recorded for this file?

exe

What JavaScript library is used by file 2?

zepto

Is this Yara rule in the default Yara file Loki uses to detect these type of hack tools? (Yay/Nay)

nay

4. OpenCTI

Task 4

What is the name of the group that uses the 4H RAT malware?

Putter Panda

What kill-chain phase is linked with the Command-Line Interface Attack Pattern?

execution-ics

Within the Activities category, which tab would house the Indicators?

observations

Task 5

What Intrusion sets are associated with the Cobalt Strike malware with a Good confidence level? (Intrusion1, Intrusion2)

CopyKittens, FIN7

Who is the author of the entity?

The MITRE Corporation

Task 6

What is the earliest date recorded related to CaddyWiper? Format: YYYY/MM/DD

2022/03/15

Which Attack technique is used by the malware for execution?

Native API

How many malware relations are linked to this Attack technique?

113

Which 3 tools were used by the Attack Technique in 2016? (Ans: Tool1, Tool2, Tool3)

ShimRatReporter, Empire, Bloodhound

What country is APT37 associated with?

North Korean

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

T1189, T1566

5. MISP

Task 3 Using the System

How many distribution options does MISP provide to share threat information?

4

Which user has the role to publish events?

organisation admin

Task 5: Scenario Event

What event ID has been assigned to the PupyRAT event?

1145

The event is associated with the adversary gaining ______ into organisations.

remote access

What IP address has been mapped as the PupyRAT C2 Server

89.107.62.39

From the Intrusion Set Galaxy, what attack group is known to use this form of attack?

Magic Hound

There is a taxonomy tag set with a Certainty level of 50. Which one is it?

osint