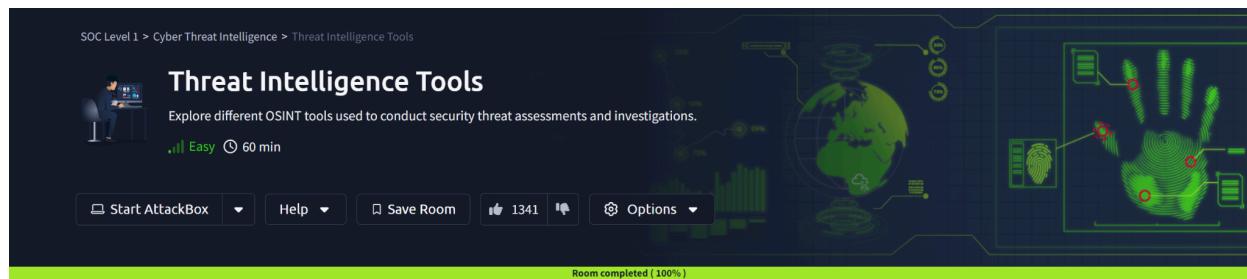


THREAT INTELLIGENCE TOOLS

ASSIGNMENT REPORT



**Peter Kinyumu,
cs-sa07-24067,
June 9th, 2024**

1. INTRODUCTION

This room focuses on the basics of cyber threat intelligence and its classifications. It also explores various open-source tools for threat intel analysis, such as Urlscan, Abuse.ch, Phishtool, and the Cisco Talos Intelligence platform, that are used for security investigations.

2. ANSWERS TO QUESTIONS

Urlscan.io

The screenshot shows the Urlscan.io interface for the URL <http://www.tryhackme.com/>. Key findings include:

- CISCO UMBRELLA RANK:** 345612
- DOMAINS:** 13 domains contacted.
- IP:** 2606:4700:10::ac43:1b0a
- Screenshot:** Shows the TryHackMe website with a live screenshot and full image options.
- Page URL History:** Shows the history of URLs visited, including [HTTP 301](http://www.tryhackme.com/) and [Page URL](https://tryhackme.com/).
- Detected technologies:** Paths.js (JavaScript Graphics).

The screenshot above highlights the answers to the questions below:

- What was TryHackMe's Cisco Umbrella Rank based on the screenshot?**
345612
- How many domains did UrlScan.io identify on the screenshot?**
13 domains.
- 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

Abuse.ch

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

Mirai

ThreatFox Database

Indicators of Compromise (IOCs) on ThreatFox are associated with a certain malware family. A malware sample can be associated with only one malware family. The page below gives you an overview on indicators of compromise associated with [elf.mirai](#).

You can also get this data through the [ThreatFox API](#).

Database Entry

Malware:	Mirai
Malware alias:	Katana
First seen:	2020-12-27 07:34:56 UTC
Last seen:	2024-05-31 06:25:21 UTC
Number of IOCs:	19'693
Malpedia:	https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai



- b. Which malware is associated with the JA3 Fingerprint

51c64c77e60f3980eea90869b68c58a8 on SSL Blacklist?

Dridex

JA3 Fingerprints

Here you can browse a list of malicious JA3 fingerprints identified by SSLBL. JA3 is an [open source tool](#) used to fingerprint SSL/TLS client applications. In the best case, you can use JA3 to identify malware traffic that is leveraging SSL/TLS.

Caution!

The JA3 fingerprints below have been collected by analysing more than 25,000,000 PCAPs generated by malware samples. These fingerprints have **not** been tested against known good traffic yet and may cause a significant amount of FPs!

Show	Search:		
50 entries	<input type="text" value="f3980eea90869b68c58a8"/>		
Listing Date (UTC)	JA3 Fingerprint	Listing Reason	Malware Samples
2018-12-17 07:47:19	51c64c77e60f3980eea90869b68c58a8	Dridex	227'010

Showing 1 to 1 of 1 entries (filtered from 96 total entries)

Previous 1 Next

© abuse.ch 2024



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

The chart below shows the top malware hosting network by ASN. Please consider that some of them just offer CDN or proxy services and are hence not hosting the malicious content it self rather than facilitate delivering the malicious payload to the user.

Top malware hosting networks in total (counting online and offline malware distribution sites):

Rank	ASN	Country	Average Reaction Time	Malware URLs
1	AS4837 CHINA169-Backbone	CN	2 days, 14 hours, 16 minutes	784'672
2	AS9829 BSNL-NIB	IN	9 hours, 36 minutes	278'447
3	AS4134 CHINANET-BACKBONE	CN	4 days, 1 hours, 59 minutes	171'455
4	AS17488 HATHWAY-NET-AP	IN	5 hours, 56 minutes	141'875
5	AS8661 PTK	AL	2 days, 1 hours, 28 minutes	97'550
6	AS17816 CHINA169-GZ	CN	1 day, 8 hours, 25 minutes	82'768
7	AS13335 CLOUDFLARENET	US	3 days, 11 hours, 19 minutes	66'391
8	AS14061 DIGITALOCEAN-ASN	US	4 days, 9 hours, 44 minutes	56'818
9	AS17622 CNCGROUP-GZ	CN	22 hours, 37 minutes	50'855
10	AS46606 UNIFIEDLAYER-AS-1	US	13 days, 23 hours, 32 minutes	46'879
11	AS19871 NETWORK-SOLUTIONS-HOSTING	US	13 days, 6 hours, 11 minutes	37'061
12	AS16276 OVH	FR	10 days, 16 hours, 48 minutes	31'200
13	AS15169 GOOGLE	US	10 days, 14 hours, 35 minutes	30'087

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

IP address, AS number or AS name

Search

Filter for: Emotet (aka Heodo) TrickBot Dridex QakBot BazarLoader BumbleBee Pikabot

Show entries Search:

Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Country
2021-04-22 22:04:30	178.134.47.166	TrickBot	Offline	AS35805 SILKNET-AS	GE

© abuse.ch 2024

Phishtool

- What social media platform is the attacker trying to pose as in the email?
Linkedin
- What is the sender's email address?
darkabutla@sc500.whpservers.com
- What is the recipient's email address?
cabbagecare@hotmail.com

The screenshot below showcases the answers to the questions above.

You are a SOC Analyst and have been tasked to analyse a suspicious email, **Email1.eml**. To solve the task, open the email using **Thunderbird** on the attached VM, analyse it and answer the questions below.

Answer the questions below

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

LinkedIn ✓ Correct Answer ? Hint

What is the senders email address?

darkabutla@sc500.whpservers.com ✓ Correct Answer

What is the recipient's email address?

cabbagecare@hotmail.com ✓ Correct Answer

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

Answer format: *.*.*.* ? Submit ? Hint

Room progress (59%)

You can now add **PhishTool** to your list of email analysis tools.

Scenarios

File Edit View Go Message Applications Places System Sun Jun 9, 14:04

From Patrick Cook <darkabutla@sc500.whpservers.com> *

Subject: You have 5 new message(s) *

To cabbagecare@hotmail.com <cabbagecare@hotmail.com> *

You have 5 new message(s)

by Patrick Cook Show message

Attacker poses as linkedin

Never miss an update with LinkedIn app

Download the app

53min 12s

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

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

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

In the screenshot below, the received lines marked 1, 2, and 3,4 provide details on the email traversal process across various SMTP servers for tracing purposes. These are the number of hops the email went through. It took 4 hops to get to the recipient.

You are a SOC Analyst and have been tasked to analyse a suspicious email, **Email1.eml**. To solve the task, open the email using **Thunderbird** on the attached VM, analyse it and answer the questions below.

Answer the questions below

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

LinkedIn ✓ Correct Answer ? Hint

What is the senders email address?

darkabutla@sc500.whpservers.com ✓ Correct Answer

What is the recipient's email address?

cabbagecare@hotmail.com ✓ Correct Answer

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

Answer format: *.*.*.* ? Submit ? Hint

Room progress (59%)

You can now add **PhishTool** to your list of email analysis tools.

Scenarios

File Edit View Go Message Applications Places System Sun Jun 9, 14:04

From Patrick Cook <darkabutla@sc500.whpservers.com> *

Subject: You have 5 new message(s) *

To cabbagecare@hotmail.com <cabbagecare@hotmail.com> *

You have 5 new message(s)

by Patrick Cook Show message

Attacker poses as linkedin

Never miss an update with LinkedIn app

Download the app

53min 12s

Cisco Talos Intelligence

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

The screenshot shows the Cisco Talos Reputation Lookup interface. The search bar at the top contains the IP address 204.93.183.11. Below the search bar, there are three main sections: LOCATION DATA, REPUTATION DETAILS, and EMAIL VOLUME DATA. In the LOCATION DATA section, it shows Chicago, United States. In the REPUTATION DETAILS section, it shows SENDER IP REPUTATION as Neutral and WEB REPUTATION as Unknown. In the EMAIL VOLUME DATA section, it shows email volume for the last day and month. The DOMAIN field in the OWNER DETAILS section is highlighted with a red box and contains scinet.net. The CONTENT DETAILS section shows a list of files. The BLOCK LISTS section shows a list of block lists. The taskbar at the bottom of the screen shows various icons and the system tray.

b. What is the customer name of the IP address?

We can identify the customer name of the IP address from the **whois** records.

The screenshot shows a terminal window displaying whois results for the IP address 204.93.183.0. The results show the customer name as Complete Web Reviews, along with other contact information like address, city, state, and postal code. The taskbar at the bottom of the screen shows various icons and the system tray.

```
ciph3rbnuk@DESKTOP-D970INA: ~
Updated: 2014-06-06
Ref: https://rdap.arin.net/registry/ip/204.93.183.0

CustName: Complete Web Reviews
Address: 415 W Golf Rd
Address: Suite #
City: Arlington Heights
StateProv: IL
PostalCode: 60005
Country: US
RegDate: 2014-06-06
Updated: 2014-06-06
Ref: https://rdap.arin.net/registry/entity/c05082466
```

Scenario 1

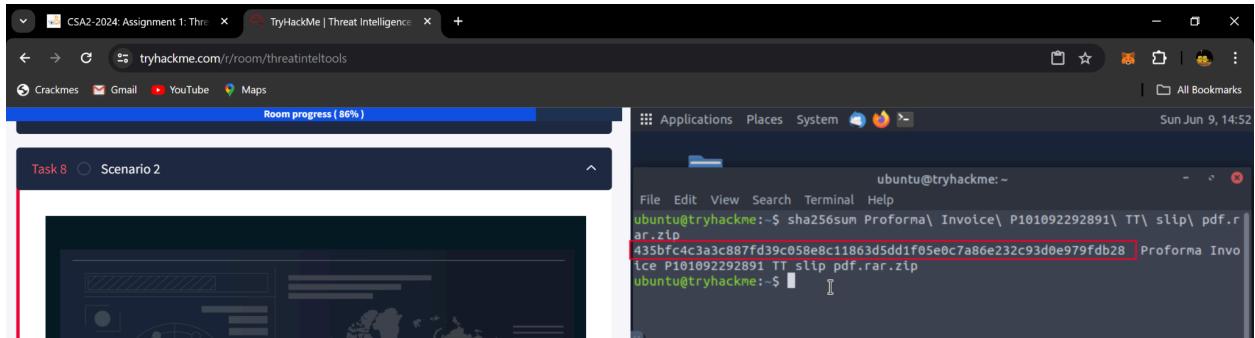
You are a SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email to triage the incidents reported.

Task: Use the tools and knowledge discussed throughout this room (or use your resources) to help you analyze Email2.eml found on the VM attached to **Task 5** and use the information to answer the questions.

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

chris.lyons@supercarcenterdetroit.com

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



A screenshot of the Talos File Reputation Lookup website. The page displays the following information for the SHA256 hash `435bf4c3a3c887fd39c058e8c11863d5dd1f05e0c7a86e232c93d0e979fdb28`:

- FILE REPUTATION:** Malicious
- FILE SIZE:** 228458 bytes
- SAMPLE TYPE:** Zip archive data, at least v2.0 to extract, compression method: deflate
- CISCO SECURE ENDPOINT DETECTION NAME:** Formbook::gravity::ARC.INV.435BFC4C.CAE.Talos
- TALOS WEIGHTED FILE REPUTATION SCORE:** Score not available.
- ASSOCIATED DOMAINS FOR THIS HASH:** Domains not available.
- DETECTION ALIASES:** Win-Trojan/VBKrypt.RP02.X1828, HIDDENEXT/Worm.Gen (highlighted with a red box), Win32-Evo-gen [Trj], Trojan.GenericKD.36883201, virus, Win.Malware.Noon-6903088-0, Trojan.PWS.Stealer.20273

Scenario 2

You are a SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email to triage the incidents reported.

Task: Use the tools and knowledge discussed throughout this room (or use your resources) to help you analyze Email3.eml found on the VM attached to Task 5 and use the information to answer the questions.

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

The screenshot shows a dual-monitor setup. On the left monitor, a browser window displays the TryHackMe Threat Intelligence Tools room progress at 86%. It contains two questions: "What is the name of the attachment on Email3.eml?" and "What malware family is associated with the attachment on Email3.eml?". Both questions have input fields and "Submit" buttons. Below the browser is a task summary for "Task 9 Conclusion" showing "Created by tryhackme" and "Room Type Free Room". On the right monitor, a Mozilla Thunderbird window shows an incoming email from "Customer Service <quickbooks@notification.intuit.com>" titled "Purchase Order Receipt". The email body says "Please find our purchase order attached to this email." and "thank you for your business - we appreciate it very much." Sincerely, The complete version has been provided as an attachment to this email. The attachment is a Microsoft Excel file named "Sales_Receipt 5606.xls" (82.5 KB). A red arrow points from the question "What is the name of the attachment on Email3.eml?" to the attachment filename in the email client.

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

The screenshot shows a dual-monitor setup. On the left monitor, the TryHackMe room progress is now at 95%. It contains the same two questions as before. The first question has the correct answer "Sales_Receipt 5606.xls" entered, and the second question has the correct answer "Dridex" entered. Both answers have "Correct Answer" buttons. On the right monitor, a terminal window on an Ubuntu system shows the command "sha256sum Sales_Receipt\ 5606.xls" being run, followed by the output "b8ef959a9176aeff07fdca8705254a163b50b49a17217a4ff0107487f59d4a35d". A green checkmark and the message "Woop woop! Your answer is correct" are displayed above the terminal window.

The screenshot shows the Talos File Reputation Lookup interface. At the top, it displays the SHA256 hash: B8EF959A9176AEF07FDCA8705254A163B50B49A17217A4FF0107487F59D4A35D. Below the hash, there's a biohazard icon and the word "Malicious". To the right, detailed information is provided: FILE SIZE (84480 bytes), SAMPLE TYPE (OLE 2 Compound Document, v3.62, SecID 0x1, 2 FAT sectors, Mini FAT start sector 0x7f, 2 Mini FAT sectors : Microsoft Excel 97-2003 addin), and CISCO SECURE ENDPOINT (XLS.INV.B8EF959A.CAE.Talos) with DETECTION NAME*. A note states: "Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription." A red arrow points from the text "Dridex malware family" to the detection alias "Downloader/XLS.Dridex" which is highlighted with a red box. Other detection aliases listed include W97M/Agent.2325811, VBA-Dropper.GX [Trj], VB.Trojan.Valyria.5569, virus, and malicious confidence 100%. The bottom status bar shows YOTAM/Dridex A nonIEEdition.

3. MODULE COMPLETION

<https://tryhackme.com/p/c1ph3rbnuk>

The screenshot shows the TryHackMe Threat Intelligence room completion screen. A central modal window displays a green checkmark and the message "Woop woop! Your answer is correct". Below this, a large green banner says "Congratulations!". The message "You've completed the room! Share this with your friends:" is followed by social sharing buttons for Twitter, Facebook, and LinkedIn. On the left, a sidebar lists tasks: Task 1 (Room Outline), Task 2 (Threat Intelligence), Task 3 (UrlScan.io), and Task 4 (Abuse.ch). The main interface features a dashboard with various threat intelligence feeds and a handprint analysis section. The bottom status bar shows Sunset, 18:02, and other system icons.

4. CONCLUSION

This assignment gave me a basic foundation for threat intelligence using open-source tools like Abuse.ch, Urlscan.io and Cisco Talos Intelligence to triage through incidents. It was really engaging and informative. I look forward to applying these investigative skills that I have learned in an incident response process.