

THREAT-INTELLIGENCE-TOOLS

INTRODUCTION

Threat Intelligence is the analysis of data and information using tools and techniques to generate meaningful patterns on how to mitigate against potential risks associated with existing or emerging threats targeting organizations, industries, sectors or governments.

This room will cover the concepts of Threat Intelligence and various open-source tools that are useful.

I came to have a grip of the various classification of threat intelligence namely;

- Strategic Intel: High-level intelligence focused on the broader trends and patterns in the threat landscape.

- Tactical Intel: Intelligence that provides specific information on tactics, techniques, and procedures (TTPs) used by threat actors.

- Operational Intel: Intelligence focused on the details of specific, imminent threats or incidents.

Now here are the questions and how I solved them.

Read the description! Continue to the next task.

No answer needed

✓ Correct

I've read on Threat Intel and the classifications

No answer needed

✓ Correct

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

345612

✓ Correct

Looking closely on the screenshot provided in this room, the rank was 345612. And this can be proven from the image below.

This website contacted **17 IPs** in **4 countries** across **13 domains** to perform **109 HTTP transactions**. The main IP is **2606:4700:10::ac43:1b0a**, located in **United States** and belongs to **CLOUDFLARENET, US**. The main domain is **tryhackme.com**. The Cisco Umbrella rank of the primary domain is **345612**.

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

13

✓ Correct

This website contacted **17 IPs** in **4 countries** across **13 domains** to perform **109 HTTP**

What was the main domain registrar listed on the screenshot?

NAMECHEAP INC

✓ Correct

The domain registrar is NAMECHEAP INC as it can be seen from the image below.

Live information

Google Safe Browsing:  No classification for *tryhackme.com*
Current DNS A record: 104.22.55.228 (AS13335 - CLOUDFLARENET, US)
Domain created: July 5th 2018, 22:46:15 (UTC)
Domain registrar: NAMECHEAP INC

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

2606:4700:10::ac43:1b0a

✓ Correct

This website contacted **17 IPs** in **4 countries** across **13 domains** to perform **109 HTTP transactions**. The main IP is **2606:4700:10::ac43:1b0a**, located in **United States** and belongs to

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

Katana

✓ Correct

For this question, I did some little google search and the results were as shown below.


15 Mar 2022 — IOC ID: 395319. IOC: 212.192.246.30:5555. IOC Type : ip:port. Threat Type : botnet_cc. Malware: Mirai. Malware alias: Katana.

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

Dridex

✓ Correct

Dridex, is the malware as you can see from the image below.

JA3 Fingerprint:	51c64c77e60f3980eea90869b68c58a8
First seen:	2018-08-30 21:04:57 UTC
Last seen:	2021-08-11 08:13:08 UTC
Status:	Blacklisted
Malware samples:	227'014
Destination IPs:	5'216
Malware:	Dridex 
Listing date:	2018-12-17 07:47:19

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

DIGITALOCEAN-ASN




✓ Correct

8	AS14061 DIGITALOCEAN-ASN	 US	4 days, 9 hours, 43 minutes	56'828
---	--	--	-----------------------------	--------

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

Georgia

✓ Correct

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

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

LinkedIn

✓ Correct Answer

💡 Hint

I used to the phish tools and talos to analyse for this information and the screenshots below summarizes how I got the answers.

This email was intended for CabbageCare. [Learn why we included this.](#)

You are receiving LinkedIn notification emails.

What is the senders email address?

darkabutla@sc500.whpservers.com

✓ Correct Answer

By simply looking at the header information, I was able to retrieve the senders email.

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

What is the recipient's email address?

cabbagecare@hotmail.com

✓ Correct Answer

By simply looking at the header information, I was able to retrieve the recipient's email.

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

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

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

✓ Correct Answer

💡 Hint

I used the phishtool to analyse the email and got this information (basically the IP).
Visited the cyberchef and to defang the ip address as shown in the image below.

Received: from sc500.whpservers.com (204.93.183.11) by
DM6NAM10FT030.mail.protection.outlook.com (10.13.152.224) with Microsoft
SMTP Server id 15.20.5102.17 via Frontend Transport; Tue, 29 Mar 2022
20:39:27 +0000

Recipe

Defang IP Addresses

^

📁

🗑️

^

🚫

⏸️

Input

204.93.183.11

rec 13 1

Output

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

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

✓ Correct Answer

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

✓ Correct Answer

💡 Hint

```
NetRange:      204.93.183.0 - 204.93.183.255
CIDR:          204.93.183.0/24
NetName:       SCNET-204-93-183-0-24
NetHandle:     NET-204-93-183-0-1
Parent:        SCN-6 (NET-204-93-128-0-1)
NetType:       Reassigned
OriginAS:
Customer:      Complete Web Reviews (C05082466)
RegDate:       2014-06-06
Updated:       2014-06-06
Ref:           https://rdap.arin.net/registry/ip/204.93.183.0
```

What is the customer name of the IP address?

Complete Web Reviews

✓ Correct Answer


💡 Hint

I visited the whois.org to extract this information just as shown in the screenshot below.

204.93.183.11 was found in our database!

This IP was reported 17 times. Confidence of Abuse is 0%: ?

0%

ISP	Complete Web Reviews
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	sc500.whpservers.com
Domain Name	completewebreviews.com
Country	 United States of America
City	Chicago, Illinois

IP info including ISP, Usage Type, and Location provided by [IP2Location](#)

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

ris.lyons@supercarcenterdetroit.com

✓ Correct Answer

I uploaded the email to the phishtool and did some analysis on the analysis tab. And below was the output.

Fw: Re: PI no. SO-P101092262891

✓ Resolve

Headers	Received lines	X-headers	Security	Attachments	Message URLs	Plaintext	Source
From	LeHuong-accounts@gmail.com					Dear all,	
Display name	Le Huong-accounts					We've made balance payment for attached invoice on 14/12/2017.	
To	chris.lyons@supercarcenterdetroit.com					Our below forwarder will contact your side for pickup arrangement:	
CC	None					EVO Logistics Pte Ltd	
Timestamp	01:14 pm, Dec 14th 2017					No 7, Airline Road, #05-08, Cargo Agent Building E, Singapore 819834.	
Reply-To	None					PIC: Lucy Tiew (Email: lucy@evtlogistics.com.sg)	
Return-Path	None					There's no need to send the original Tax Invoice or Declaration Letter together with the goods.	
Originating IP	134.19.187.230 (Hop 1) ▼					Thank you,	
rDNS	hyp07-nl-ams.gowhitelabel.com					Huong Le	

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

HIDDENEXT/Worm.Gen

✓ Correct Answer

I went to the attachments and copied the SHA-256 hash. I Opened Cisco Talos and checked the reputation of the file. I then got the alias name

DETECTION	DETAILS	RELATIONS	COMMUNITY 2
Security Vendors' Analysis ⓘ			
Acronis (Static ML)	ⓘ Suspicious	Ad-Aware	ⓘ Trojan.GenericKD.36883201
AhnLab-V3	ⓘ Win-Trojan/VBKrypt.RP02.X1828	Alibaba	ⓘ Trojan.Package/phishing.8
ALYac	ⓘ Gen.Heur.PonyStealer.Cm0@daFRfHob	Antiy-AVL	ⓘ HackTool[VirTool]/Win32.VBInject
Arcabit	ⓘ Trojan.Generic.D232CB01	Avast	ⓘ Win32.Evo-gen [Trj]
AVG	ⓘ Win32.Evo-gen [Trj]	Avira (no cloud)	ⓘ HIDDENEXT/Worm.Gen
BitDefender	ⓘ Trojan.GenericKD.36883201	BitDefenderTheta	ⓘ Gen.NN.ZevbaF.34796.Cm0@aaFRfHob
ClamAV	ⓘ Win.Malware.Noan-6903088-0	Comodo	ⓘ Malware@#19q3jlbqycech
Cylance	ⓘ Unsafe	Cynet	ⓘ Malicious (score: 99)
Cyren	ⓘ W32/VBInject.NO.genIEldorado	DrWeb	ⓘ Trojan.PWS.Stealer.20273
Elastic	ⓘ Malicious (high Confidence)	Emsisoft	ⓘ Trojan.GenericKD.36883201 (B)
eScan	ⓘ Trojan.GenericKD.36883201	ESET-NOD32	ⓘ A Variant Of Win32/Injector.DUOO
Fortinet	ⓘ W32/VBKryptik.DZKHftr	GData	ⓘ Trojan.GenericKD.36883201
Google	ⓘ Detected	Gridinsoft (no cloud)	ⓘ Spy.Win32.Gen.sbls1


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

Sales_Receipt 5606.xls

✓ Correct

On the phishtool, I uploaded the email, analysed it and then checked on the attachments tab for detailed information pertaining this email. And it can be seen fromt the image below the file name is Sales_Receipt 5606.xls


Purchase Order Receipt

 Headers



Received lines

X-headers

Security

 **Attachments**

Message URLs

  1 ...

File name Sales_Receipt 5606.xls

File type CFB

File size 82.50 KB

VirusTotal [Configure](#)

OLE analysis Macro

File hashes

MD5 e63deaaa51f7cc2064ff808e11e1ad55

SHA-1 4d58ec4c978988f16468cda2323103ae62b2baea

SHA-256 b8ef959a9176aef07fdca8705254a163b50b49a17217a4ff0107487f59d4a35d

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

Dridex

✓ Correct

For this question, I used the MalwareBazaar tool. I provided the hash and analyzed it and here there were intel of importance as shown in the image below. The malware family is dridex.



Vendor detections: 9



Maldoc score: 4

Intelligence 9	IOCs	YARA	File information	Comments	Actions
----------------	------	------	------------------	----------	---------

SHA256 hash:	b8ef959a9176aef07fdca8705254a163b50b49a17217a4ff0107487f59d4a35d
SHA3-384 hash:	353bbefd55bc4c0f08736fd2e6a2f39f319a1d92ffd2aed003cc483a3f823c2315efa9364653bb048d573deadc2f06af
SHA1 hash:	4d58ec4c978988f16468cda2323103ae62b2baea
MD5 hash:	e63deaea51f7cc2064ff808e11e1ad55
humanhash:	triple-salami-item-fanta
File name:	Purchase_Order 2412.xls
Download:	download sample
Signature ⓘ	Alert
File size:	84'480 bytes
First seen:	2021-10-13 13:47:49 UTC
Last seen:	2022-08-06 12:18:08 UTC
File type:	xls
MIME type:	application/vnd.ms-excel
ssdeep ⓘ	1536:LFk3hbdlylKsgqopeJBWhZFGkE+cL2NdAA5eSUpIbjB59ZYiosYvvXvTWbxgXTPE:LFk3hbdlylKsgqopeJBWhZFGkE+cL2Nn
TLSH ⓘ	T184835BA6F682E909D95917754CE683E26727FC115F53C3887288F72F0F727808A03656
Reporter ⓘ	Anonymous
Tags:	



Congratulations!

You've completed the room! Share this with your friends:

 Twitter

 Facebook

 LinkedIn

[Leave feedback](#)

<https://tryhackme.com/r/room/threatinteltools>

CONCLUSION

This room majorly was to introduce me to the various threat intelligence tools to analyse data and information to generate meaningful patterns to mitigate potential threats to the organisations systems and operations.