



Eric Mwenda

THREAT INTELLIGENCE TOOLS

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

In this room this are the areas that I was supposed to have an understanding in:-

- Understanding the basics of threat intelligence & its classifications.
- Using UrlScan.io to scan for malicious URLs.
- Using Abuse.ch to track malware and botnet indicators.
- Investigate phishing emails using PhishTool
- Using Cisco's Talos Intelligence platform for intel gathering.

Lets get started

Threat Intelligence

We began by having an understanding of what threat intelligence is and we said 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.

For you to be able to mitigate against an attack there are a few questions you need to answer, for example:-

1. Who is attacking you?
2. What is their motivation?
3. What are their capabilities?
4. What areas and indicators that you have been compromised should we look out for?

We then proceeded to look into the various Threat Intelligence Classifications.

Threat intel is geared in understanding what is the relationship between your operations and the adversary.

Classifications are:-

Strategic Intel - High-level intel that looks into the organisation's threat landscape and maps out the risk areas based on trends, patterns and emerging threats that may impact business decisions.

Technical Intel - Looks into evidence and artefacts of attack used by an adversary. Incident Response teams can use this intel to create a baseline attack surface to analyse and develop defence mechanisms.

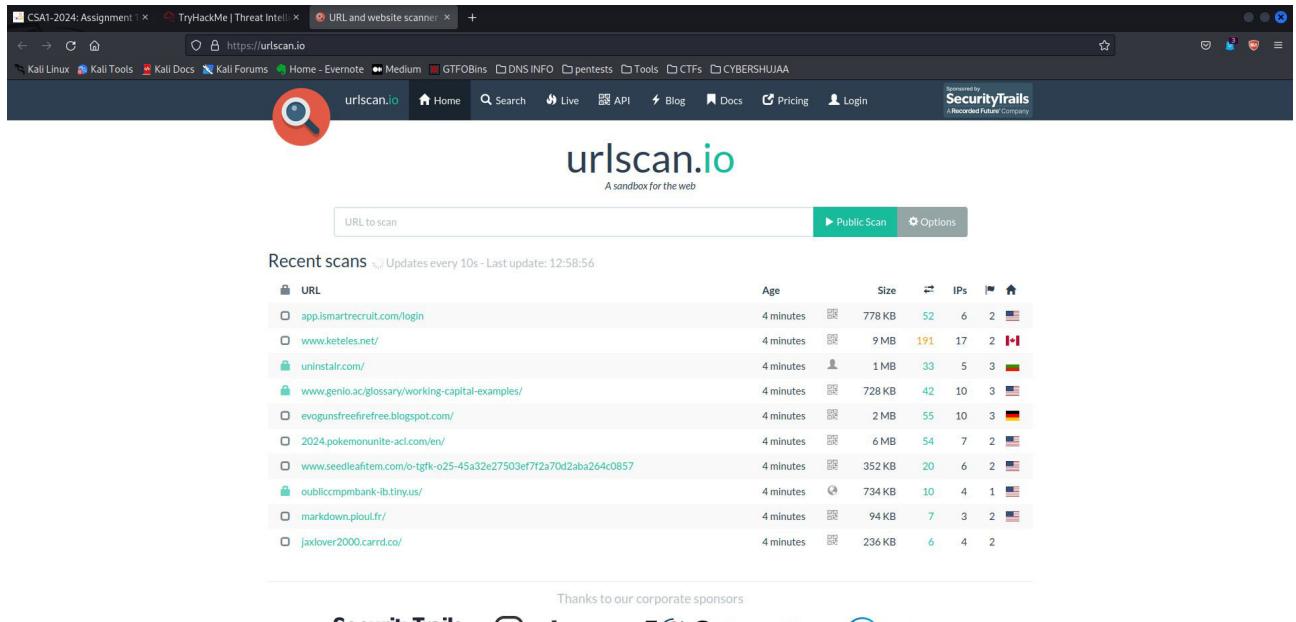
Tactical Intel - Assesses adversaries' tactics, techniques, and procedures (TTPs). This intel can strengthen security controls and address vulnerabilities through real-time investigations.

Operational Intel - Looks into an adversary's specific motives and intent to perform an attack. Security teams may use this intel to understand the critical assets available in the organisation (people, processes, and technologies) that may be targeted.

UrlScan.io

Urlscan.io is a free service developed to assist in scanning and analysing websites. It is used to automate the process of browsing and crawling through websites to record activities and interactions.

This service provides user with metadata about the target.



The screenshot shows the URL <https://urlscan.io>. At the top, there is a navigation bar with links for Home, Search, Live, API, Blog, Docs, Pricing, and Login. Below the navigation bar, the main header features the URLscan.io logo and the tagline "A sandbox for the web". A search bar labeled "URL to scan" is present, along with "Public Scan" and "Options" buttons. Below the search bar, a section titled "Recent scans" displays a table of 12 recent scans. The table includes columns for URL, Age, Size, IPs, and a flag icon. The URLs listed are: app.ismartrecruit.com/login, www.keteles.net/, uninstallr.com/, www.genio.ac/glossary/working-capital-examples/, evogunsfreefirefree.blogspot.com/, 2024.pokemonunite-acl.com/en/, www.seedleitem.com/o-tgfk-o25-45a32e27503ef7f2a70d2aba264c0857, oubliccmpbank-lb.tinyus/, markdown.pioufr/, and jaxlover2000.carrd.co/. The table shows varying sizes (778 KB to 94 KB), IP counts (52 to 2), and ages (4 minutes to 4 minutes).

Some of the results or information that the UrlScan.io gives include:-

Summary - Provides general information about the URL, ranging from the identified IP address, domain registration details, page history and a screenshot of the site.

HTTP - Provides information on the HTTP connections made by the scanner to the site, with details about the data fetched and the file types received.

Redirects - Shows information on any identified HTTP and client-side redirects on the site.

Links - Shows all the identified links outgoing from the site's homepage.

Behaviour - Provides details of the variables and cookies found on the site. These may be useful in identifying the frameworks used in developing the site.

Indicators - Lists all IPs, domains and hashes associated with the site. These indicators do not imply malicious activity related to the site.

Scenario

You have been tasked to perform a scan on TryHackMe's domain. The results obtained are displayed in the image below. Use the details on the image to answer the questions:

Before I proceeded to the questions, I first did my own scan to see the results I would get.

Here are my results immediately after the scan.

The screenshot shows the urlscan.io interface for the domain `tryhackme.com`. The main summary section indicates that the site was contacted by 39 IPs from 4 countries across 25 domains, performing 157 HTTP transactions. The main IP is `2606:4700:10::6816:37e4`, located in the United States. The effective URL is `https://tryhackme.com/`. The page title is `TryHackMe | Cyber Security Training`. The screenshot shows a fun, cartoonish character running through a digital landscape. The page URL history shows the initial request to `http://tryhackme.com/` followed by an HTTP 301 redirect to `https://tryhackme.com/`. The detected technologies include `PathJS (JavaScript Graphics)`.

Answer the questions below

Although I had tried out my own search, this question needed me to use the screenshot provided in the room.

Here it is:-

tryhackme.com
2606:4700:10::ac43:1b0a

Submitted URL: <http://www.tryhackme.com/>
Effective URL: <https://tryhackme.com/>
Submission: On April 20 via manual (April 20th 2022, 5:22:48 pm UTC) from KE — Scanned from DE

[Summary](#) [HTTP](#) [Redirects](#) [Links](#) [Behaviour](#) [Indicators](#) [Similar](#) [DOM](#) [Content](#) [API](#) [Verdicts](#)

Summary

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.
TLS certificate: Issued by E1 on March 25th 2022. Valid for: 3 months.

[www.tryhackme.com](#) scanned 30 times on urlscan.io [Show Scans](#)
[tryhackme.com](#) scanned 239 times on urlscan.io [Show Scans](#)
urlscan.io Verdict: No classification

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

Domain & IP information

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
1	2606:4700:10::6816:37e4		13335 (CLOUDFLARENET)			
11	2606:4700:10::ac43:1b0a		13335 (CLOUDFLARENET)			
47	2606:9000:225e:f400:1f:54cc:9ec0:93a1		16509 (AMAZON-02)			
3	2606:4700:6811:190e		13335 (CLOUDFLARENET)			
2	2606:4700:6812:1734		13335 (CLOUDFLARENET)			

Screenshot [Live screenshot](#) [Full Image](#)

Join over 1 million others learning Cyber Security with TryHackMe
Hands-on cyber security training through real-world scenarios
• Beginner friendly • Scalable challenges
• Auto-sized gamified lessons
• Learning never seems so “hacking” to the user interface. Our unique pedagogical approach, making our challenges fun and accessible to everyone.
• Challenge yourself to learn through real-life scenarios

Page URL History [Show full URLs](#)

1. <http://www.tryhackme.com/> [HTTP 201]
<https://tryhackme.com/> [Page URL]

Detected technologies

Path.js (JavaScript Graphics)	Expand
Bootstrap (Web Frameworks)	Expand
animate.css (Web Frameworks)	Expand
Font Awesome (Font Scripts)	Expand
Google Analytics (Analytics)	Expand
Google Tag Manager (Tag Managers)	Expand
Osano (Cookie compliance)	Expand
Slick (JavaScript Libraries)	Expand
jQuery (JavaScript Libraries)	Expand
reCAPTCHA (Captchas)	Expand

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

Ans: 345612

Summary

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.

TLS certificate: Issued by E1 on March 25th 2022. Valid for: 3 months.

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

Ans: 13

Summary

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.

TLS certificate: Issued by E1 on March 25th 2022. Valid for: 3 months.

What was the main domain registrar listed on the screenshot?

Ans: NAMECHEAP INC

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?

Ans: 2606:4700:10::ac43:1b0a

Summary

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 **CLOUDFLARENED, US**. The main domain is **[tryhackme.com](#)**. The Cisco Umbrella rank of the primary domain is **345612**.
TLS certificate: Issued by E1 on March 25th 2022. Valid for: 3 months.

Abuse.ch

Next was to look at **Abuse.ch** which was a research project that was developed to identify and track malware and botnets through several operational platforms developed under the project. These platforms are:

- 1. Malware Bazaar** - A resource for sharing malware samples.
- 2. Feodo Tracker** - A resource used to track botnet command and control (C2) infrastructure linked with Emotet, Dridex and TrickBot.
- 3. SSL Blacklist** - A resource for collecting and providing a blocklist for malicious SSL certificates and JA3/JA3s fingerprints.
- 4. URL Haus** - A resource for sharing malware distribution sites.
- 5. Threat Fox** - A resource for sharing indicators of compromise (IOCs).

After stating them, we then proceeded to explain each one of them.

MalwareBazaar

This project is a one in all malware collection and analysis database supporting the following features:

1. Malware Samples Upload: Security analysts can upload their malware samples for analysis and build the intelligence database. This can be done through the browser or an API.

2. Malware Hunting: Hunting for malware samples is possible through setting up alerts to match various elements such as tags, signatures, YARA rules, ClamAV signatures and vendor detection.

FeodoTracker

For this project Abuse.ch is targets to share intelligence on botnet Command & Control (C&C) servers associated with Dridex, Emotes (aka Heodo), TrickBot, QakBot and BazarLoader/BazarBackdoor.

To achieve this a database is provided to the C&C servers so that security analysts can search through and investigate any suspicious IP addresses they have come across. Additionally, they provide various IP and IOC blocklists and mitigation information to be used to prevent botnet infections.

SSL Blacklist

Abuse.ch developed this tool to identify and detect malicious SSL connections. From these connections, SSL certificates used by botnet C2 servers would be identified and updated on a denylist that is provided for use. The denylist is also used to identify JA3 fingerprints that would help detect and block malware botnet C2 communications on the TCP layer.

URLhaus

As the name points out, this tool focuses on sharing malicious URLs used for malware distribution. As an analyst, you can search through the database for domains, URLs, hashes and filetypes that are suspected to be malicious and validate your investigations.

The tool also provides feeds associated with country, AS number and Top Level Domain that an analyst can generate based on specific search needs.

ThreatFox

With ThreatFox, security analysts can search for, share and export indicators of compromise associated with malware. IOCs can be exported in various formats such as MISP events, Suricata IDS Ruleset, Domain Host files, DNS Response Policy Zone, JSON files and CSV files.

Answer the questions below

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

Ans: Katana

First I visited the ThreatFox database and queried the search bar using this statement:-

ioc:212.192.246.30:5555

Browse Database

See search syntax see below, example: malware:ZLoader

Search Syntax ⓘ

Show entries

Search:

Date (UTC)	IOC	Malware	Tags	Reporter
2022-03-15 07:20	212.192.246.30:5555	Mirai	Mirai	abuse_ch

Showing 1 to 1 of 1 entries

Previous 1 Next

To view more details about this result found I clicked on the results which gave more insights about the malware including the alias name.

THREATfox

Browse IOCs | IOC Requests | Share IOCs | Request IOCs | Data | FAQ | About | Login

Database Entry

IOC ID:	395319	Actions ▾
IOC:	212.192.246.30:5555	
IOC Type ⓘ:	ip.port	
Threat Type ⓘ:	botnet_cc	
Malware:	Mirai	
Malware alias:	Katana	
Confidence Level ⓘ:	的信心等级提高 (75%)	
First seen:	2022-03-15 07:20:31 UTC	
Last seen:	never	
UUID:	65d0f100-a430-11ec-a022-42010aa4000a	
Reporter ⓘ:	abuse_ch	
Reward ⓘ:	5 credits from ThreatFox	
Tags:	Mirai	
Reference:	https://bazaar.abuse.ch/sample/8a510bb0ccdac2fec5f13fae389b6900624329303d8ec85190ebf594b60d94e2/	

abuse_ch
Mirai (aka Katana) botnet C2

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

First was to download the JA3 Fingerprint list.

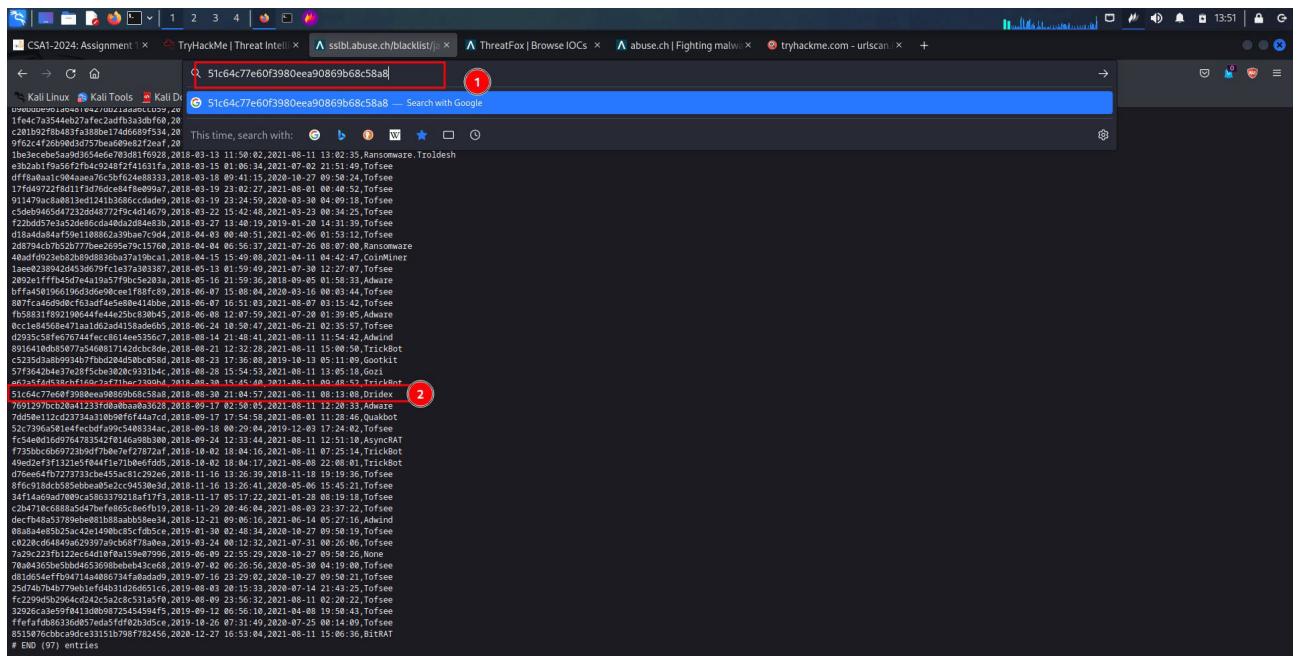
The JA3 Fingerprint Blacklist (CSV) gets generated every 5 minutes. Please do not fetch it more often than every 5 minutes.

Caution!

The JA3 fingerprints blacklisted on SSLBL 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!**

[Download JA3 Fingerprints](#)

After downloading the list, I double checked which index in the list matched the one provided in the question one by one till I found a match



```
51c64c77e60f3980eea90869b68c58a8
```

Index	Fingerprint	Date	Description
1	51c64c77e60f3980eea90869b68c58a8	2018-03-13	Ransomware.Trollstore
2	51c64c77e60f3980eea90869b68c58a8	2018-03-15	Tofsee
3	51c64c77e60f3980eea90869b68c58a8	2018-03-19	Tofsee
4	51c64c77e60f3980eea90869b68c58a8	2018-03-22	Tofsee
5	51c64c77e60f3980eea90869b68c58a8	2018-03-27	Tofsee
6	51c64c77e60f3980eea90869b68c58a8	2018-03-29	Ransomware
7	51c64c77e60f3980eea90869b68c58a8	2018-04-15	CoinMiner
8	51c64c77e60f3980eea90869b68c58a8	2018-05-16	Adware
9	51c64c77e60f3980eea90869b68c58a8	2018-06-07	Tofsee
10	51c64c77e60f3980eea90869b68c58a8	2018-06-08	Adware
11	51c64c77e60f3980eea90869b68c58a8	2018-06-24	Tofsee
12	51c64c77e60f3980eea90869b68c58a8	2018-06-26	Adwind
13	51c64c77e60f3980eea90869b68c58a8	2018-07-01	TrickBot
14	51c64c77e60f3980eea90869b68c58a8	2018-07-02	Adwind
15	51c64c77e60f3980eea90869b68c58a8	2018-07-17	Tofsee
16	51c64c77e60f3980eea90869b68c58a8	2018-08-03	Dridex
17	51c64c77e60f3980eea90869b68c58a8	2018-09-17	Tofsee
18	51c64c77e60f3980eea90869b68c58a8	2018-09-17	Adware
19	51c64c77e60f3980eea90869b68c58a8	2018-09-17	Quakbot
20	51c64c77e60f3980eea90869b68c58a8	2018-09-24	AsyncRAT
21	51c64c77e60f3980eea90869b68c58a8	2018-09-24	TrickBot
22	51c64c77e60f3980eea90869b68c58a8	2018-10-02	Adwind
23	51c64c77e60f3980eea90869b68c58a8	2018-10-10	Adwind
24	51c64c77e60f3980eea90869b68c58a8	2018-11-10	Adwind
25	51c64c77e60f3980eea90869b68c58a8	2018-11-16	Adwind
26	51c64c77e60f3980eea90869b68c58a8	2018-11-17	Adwind
27	51c64c77e60f3980eea90869b68c58a8	2018-11-29	Adwind
28	51c64c77e60f3980eea90869b68c58a8	2018-12-21	Adwind
29	51c64c77e60f3980eea90869b68c58a8	2018-12-24	Adwind
30	51c64c77e60f3980eea90869b68c58a8	2018-12-25	Adwind
31	51c64c77e60f3980eea90869b68c58a8	2018-12-26	Adwind
32	51c64c77e60f3980eea90869b68c58a8	2018-12-27	Adwind
33	51c64c77e60f3980eea90869b68c58a8	2018-12-28	Adwind
34	51c64c77e60f3980eea90869b68c58a8	2018-12-29	Adwind
35	51c64c77e60f3980eea90869b68c58a8	2018-12-30	Adwind
36	51c64c77e60f3980eea90869b68c58a8	2018-12-31	Adwind
37	51c64c77e60f3980eea90869b68c58a8	2019-01-01	Adwind
38	51c64c77e60f3980eea90869b68c58a8	2019-01-02	Adwind
39	51c64c77e60f3980eea90869b68c58a8	2019-01-03	Adwind
40	51c64c77e60f3980eea90869b68c58a8	2019-01-04	Adwind
41	51c64c77e60f3980eea90869b68c58a8	2019-01-05	Adwind
42	51c64c77e60f3980eea90869b68c58a8	2019-01-06	Adwind
43	51c64c77e60f3980eea90869b68c58a8	2019-01-07	Adwind
44	51c64c77e60f3980eea90869b68c58a8	2019-01-08	Adwind
45	51c64c77e60f3980eea90869b68c58a8	2019-01-09	Adwind
46	51c64c77e60f3980eea90869b68c58a8	2019-01-10	Adwind
47	51c64c77e60f3980eea90869b68c58a8	2019-01-11	Adwind
48	51c64c77e60f3980eea90869b68c58a8	2019-01-12	Adwind
49	51c64c77e60f3980eea90869b68c58a8	2019-01-13	Adwind
50	51c64c77e60f3980eea90869b68c58a8	2019-01-14	Adwind
51	51c64c77e60f3980eea90869b68c58a8	2019-01-15	Adwind
52	51c64c77e60f3980eea90869b68c58a8	2019-01-16	Adwind
53	51c64c77e60f3980eea90869b68c58a8	2019-01-17	Adwind
54	51c64c77e60f3980eea90869b68c58a8	2019-01-18	Adwind
55	51c64c77e60f3980eea90869b68c58a8	2019-01-19	Adwind
56	51c64c77e60f3980eea90869b68c58a8	2019-01-20	Adwind
57	51c64c77e60f3980eea90869b68c58a8	2019-01-21	Adwind
58	51c64c77e60f3980eea90869b68c58a8	2019-01-22	Adwind
59	51c64c77e60f3980eea90869b68c58a8	2019-01-23	Adwind
60	51c64c77e60f3980eea90869b68c58a8	2019-01-24	Adwind
61	51c64c77e60f3980eea90869b68c58a8	2019-01-25	Adwind
62	51c64c77e60f3980eea90869b68c58a8	2019-01-26	Adwind
63	51c64c77e60f3980eea90869b68c58a8	2019-01-27	Adwind
64	51c64c77e60f3980eea90869b68c58a8	2019-01-28	Adwind
65	51c64c77e60f3980eea90869b68c58a8	2019-01-29	Adwind
66	51c64c77e60f3980eea90869b68c58a8	2019-01-30	Adwind
67	51c64c77e60f3980eea90869b68c58a8	2019-01-31	Adwind
68	51c64c77e60f3980eea90869b68c58a8	2019-02-01	Adwind
69	51c64c77e60f3980eea90869b68c58a8	2019-02-02	Adwind
70	51c64c77e60f3980eea90869b68c58a8	2019-02-03	Adwind
71	51c64c77e60f3980eea90869b68c58a8	2019-02-04	Adwind
72	51c64c77e60f3980eea90869b68c58a8	2019-02-05	Adwind
73	51c64c77e60f3980eea90869b68c58a8	2019-02-06	Adwind
74	51c64c77e60f3980eea90869b68c58a8	2019-02-07	Adwind
75	51c64c77e60f3980eea90869b68c58a8	2019-02-08	Adwind
76	51c64c77e60f3980eea90869b68c58a8	2019-02-09	Adwind
77	51c64c77e60f3980eea90869b68c58a8	2019-02-10	Adwind
78	51c64c77e60f3980eea90869b68c58a8	2019-02-11	Adwind
79	51c64c77e60f3980eea90869b68c58a8	2019-02-12	Adwind
80	51c64c77e60f3980eea90869b68c58a8	2019-02-13	Adwind
81	51c64c77e60f3980eea90869b68c58a8	2019-02-14	Adwind
82	51c64c77e60f3980eea90869b68c58a8	2019-02-15	Adwind
83	51c64c77e60f3980eea90869b68c58a8	2019-02-16	Adwind
84	51c64c77e60f3980eea90869b68c58a8	2019-02-17	Adwind
85	51c64c77e60f3980eea90869b68c58a8	2019-02-18	Adwind
86	51c64c77e60f3980eea90869b68c58a8	2019-02-19	Adwind
87	51c64c77e60f3980eea90869b68c58a8	2019-02-20	Adwind
88	51c64c77e60f3980eea90869b68c58a8	2019-02-21	Adwind
89	51c64c77e60f3980eea90869b68c58a8	2019-02-22	Adwind
90	51c64c77e60f3980eea90869b68c58a8	2019-02-23	Adwind
91	51c64c77e60f3980eea90869b68c58a8	2019-02-24	Adwind
92	51c64c77e60f3980eea90869b68c58a8	2019-02-25	Adwind
93	51c64c77e60f3980eea90869b68c58a8	2019-02-26	Adwind
94	51c64c77e60f3980eea90869b68c58a8	2019-02-27	Adwind
95	51c64c77e60f3980eea90869b68c58a8	2019-02-28	Adwind
96	51c64c77e60f3980eea90869b68c58a8	2019-02-29	Adwind
97	51c64c77e60f3980eea90869b68c58a8	2019-03-01	Adwind
98	51c64c77e60f3980eea90869b68c58a8	2019-03-02	Adwind
99	51c64c77e60f3980eea90869b68c58a8	2019-03-03	Adwind
100	51c64c77e60f3980eea90869b68c58a8	2019-03-04	Adwind
101	51c64c77e60f3980eea90869b68c58a8	2019-03-05	Adwind
102	51c64c77e60f3980eea90869b68c58a8	2019-03-06	Adwind
103	51c64c77e60f3980eea90869b68c58a8	2019-03-07	Adwind
104	51c64c77e60f3980eea90869b68c58a8	2019-03-08	Adwind
105	51c64c77e60f3980eea90869b68c58a8	2019-03-09	Adwind
106	51c64c77e60f3980eea90869b68c58a8	2019-03-10	Adwind
107	51c64c77e60f3980eea90869b68c58a8	2019-03-11	Adwind
108	51c64c77e60f3980eea90869b68c58a8	2019-03-12	Adwind
109	51c64c77e60f3980eea90869b68c58a8	2019-03-13	Adwind
110	51c64c77e60f3980eea90869b68c58a8	2019-03-14	Adwind
111	51c64c77e60f3980eea90869b68c58a8	2019-03-15	Adwind
112	51c64c77e60f3980eea90869b68c58a8	2019-03-16	Adwind
113	51c64c77e60f3980eea90869b68c58a8	2019-03-17	Adwind
114	51c64c77e60f3980eea90869b68c58a8	2019-03-18	Adwind
115	51c64c77e60f3980eea90869b68c58a8	2019-03-19	Adwind
116	51c64c77e60f3980eea90869b68c58a8	2019-03-20	Adwind
117	51c64c77e60f3980eea90869b68c58a8	2019-03-21	Adwind
118	51c64c77e60f3980eea90869b68c58a8	2019-03-22	Adwind
119	51c64c77e60f3980eea90869b68c58a8	2019-03-23	Adwind
120	51c64c77e60f3980eea90869b68c58a8	2019-03-24	Adwind
121	51c64c77e60f3980eea90869b68c58a8	2019-03-25	Adwind
122	51c64c77e60f3980eea90869b68c58a8	2019-03-26	Adwind
123	51c64c77e60f3980eea90869b68c58a8	2019-03-27	Adwind
124	51c64c77e60f3980eea90869b68c58a8	2019-03-28	Adwind
125	51c64c77e60f3980eea90869b68c58a8	2019-03-29	Adwind
126	51c64c77e60f3980eea90869b68c58a8	2019-03-30	Adwind
127	51c64c77e60f3980eea90869b68c58a8	2019-03-31	Adwind
128	51c64c77e60f3980eea90869b68c58a8	2019-04-01	Adwind
129	51c64c77e60f3980eea90869b68c58a8	2019-04-02	Adwind
130	51c64c77e60f3980eea90869b68c58a8	2019-04-03	Adwind
131	51c64c77e60f3980eea90869b68c58a8	2019-04-04	Adwind
132	51c64c77e60f3980eea90869b68c58a8	2019-04-05	Adwind
133	51c64c77e60f3980eea90869b68c58a8	2019-04-06	Adwind
134	51c64c77e60f3980eea90869b68c58a8	2019-04-07	Adwind
135	51c64c77e60f3980eea90869b68c58a8	2019-04-08	Adwind
136	51c64c77e60f3980eea90869b68c58a8	2019-04-09	Adwind
137	51c64c77e60f3980eea90869b68c58a8	2019-04-10	Adwind
138	51c64c77e60f3980eea90869b68c58a8	2019-04-11	Adwind
139	51c64c77e60f3980eea90869b68c58a8	2019-04-12	Adwind
140	51c64c77e60f3980eea90869b68c58a8	2019-04-13	Adwind
141	51c64c77e60f3980eea90869b68c58a8	2019-04-14	Adwind
142	51c64c77e60f3980eea90869b68c58a8	2019-04-15	Adwind
143	51c64c77e60f3980eea90869b68c58a8	2019-04-16	Adwind
144	51c64c77e60f3980eea90869b68c58a8	2019-04-17	Adwind
145	51c64c77e60f3980eea90869b68c58a8	2019-04-18	Adwind
146	51c64c77e60f3980eea90869b68c58a8	2019-04-19	Adwind
147	51c64c77e60f3980eea90869b68c58a8	2019-04-20	Adwind
148	51c64c77e60f3980eea90869b68c58a8	2019-04-21	Adwind
149	51c64c77e60f3980eea90869b68c58a8	2019-04-22	Adwind
150	51c64c77e60f3980eea90869b68c58a8	2019-04-23	Adwind
151	51c64c77e60f3980eea90869b68c58a8	2019-04-24	Adwind
152	51c64c77e60f3980eea90869b68c58a8	2019-04-25	Adwind
153	51c64c77e60f3980eea90869b68c58a8	2019-04-26	Adwind
154	51c64c77e60f3980eea90869b68c58a8	2019-04-27	Adwind
155	51c64c77e60f39		

Rank	ASN	Country	Average Reaction Time	Malware URLs
1	AS4837 CHINA169-BACKBONE CHINA UNICOM China169 Backbone	CN	2 days, 15 hours, 12 minutes	742210
2	AS9829 BSNL-NIB National Internet Backbone	IN	9 hours, 41 minutes	254839
3	AS4134 CHINANET-BACKBONE No.3,Jin-rong Street	CN	4 days, 2 hours, 29 minutes	167454
4	AS17488 HATHWAY-NETAP Hathway IP Over Cable Internet	IN	5 hours, 54 minutes	141488
5	AS8661 PTK PTK IPMPLS Network	AL	2 days, 1 hours, 28 minutes	97550
6	AS17816 CHINA169-GZ China Unicom IP network China169 Guangdong province	CN	1 day, 8 hours, 8 minutes	83328
7	AS13335 CLOUDFLARENET	US	3 days, 11 hours, 16 minutes	64870
8	AS14061 DIGITALOCEAN-ASN	US	4 days, 10 hours, 36 minutes	54894
9	AS17622 CNCGROUP-GZ China Unicom Guangzhou network	CN	22 hours, 37 minutes	50853
10	AS46606 UNIFIEDLAYER-AS-1	US	13 days, 22 hours, 37 minutes	46586
11	ASNone None	-	1 day, 14 hours, 14 minutes	38557
12	AS19871 NETWORK-SOLUTIONS-HOSTING	US	13 days, 4 hours, 33 minutes	37040
13	AS15169 GOOGLE	US	10 days, 15 hours, 29 minutes	29705
14	AS16276 OVH	FR	10 days, 6 hours, 12 minutes	29680
15	AS8075 MICROSOFT-CORP-MSN-AS-BLOCK	US	17 days, 21 hours, 30 minutes	28455

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

Ans: Georgia

Once on the FeodoTracker page I located the Botnet C&Cs section and clicked on the View Details button.

Next I just copied the IP address given in the question and pasted it on the search bar which revealed the answer to our question.

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

In the first I thought GE represented Germany only to search and find they represent the country Georgia

PhishTool

In my understanding from the introduction given in this section I understood PhishTool, as a tool that can be useful in email analysis.

PhishTool has two accessible versions that is the Community and Enterprise.

Email Phishing

In Email Phishing adversaries send malicious links using the email, tricking the target to open and access the sent malicious files and links sent as they appear to be legitimate. As a result, adversaries infect their victims' systems with malware, harvesting their credentials and personal data and performing other actions such as financial fraud or conducting ransomware attacks.

PhishTool seeks to elevate the perception of phishing as a severe form of attack and provide a responsive means of email security. Through email analysis, security analysts can uncover email IOCs, prevent breaches and provide forensic reports that could be used in phishing containment and training engagements.

The core features of PhishTool include:-

Perform email analysis - PhishTool retrieves metadata from phishing emails and provides analysts with the relevant explanations and capabilities to follow the email's actions, attachments, and URLs to triage the situation.

Heuristic intelligence - OSINT is baked into the tool to provide analysts with the intelligence needed to stay ahead of persistent attacks and understand what TTPs were used to evade security controls and allow the adversary to social engineer a target.

Classification and reporting - Phishing email classifications are conducted to allow analysts to take action quickly. Additionally, reports can be generated to provide a forensic record that can be shared.

Analysis Tab

Once a file is uploaded, details about our email are provided more in-depth look. Tabs that are available include:-

Headers - Provides the routing information of the email, such as source and destination email addresses, Originating IP and DNS addresses and Timestamp.

Received Lines – Gives information on the email traversal process across various SMTP servers for tracing purposes.

X-headers - These are extension headers added by the recipient mailbox to provide additional information about the email.

Security - Details on email security frameworks and policies such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC).

Attachments - Lists any file attachments found in the email.

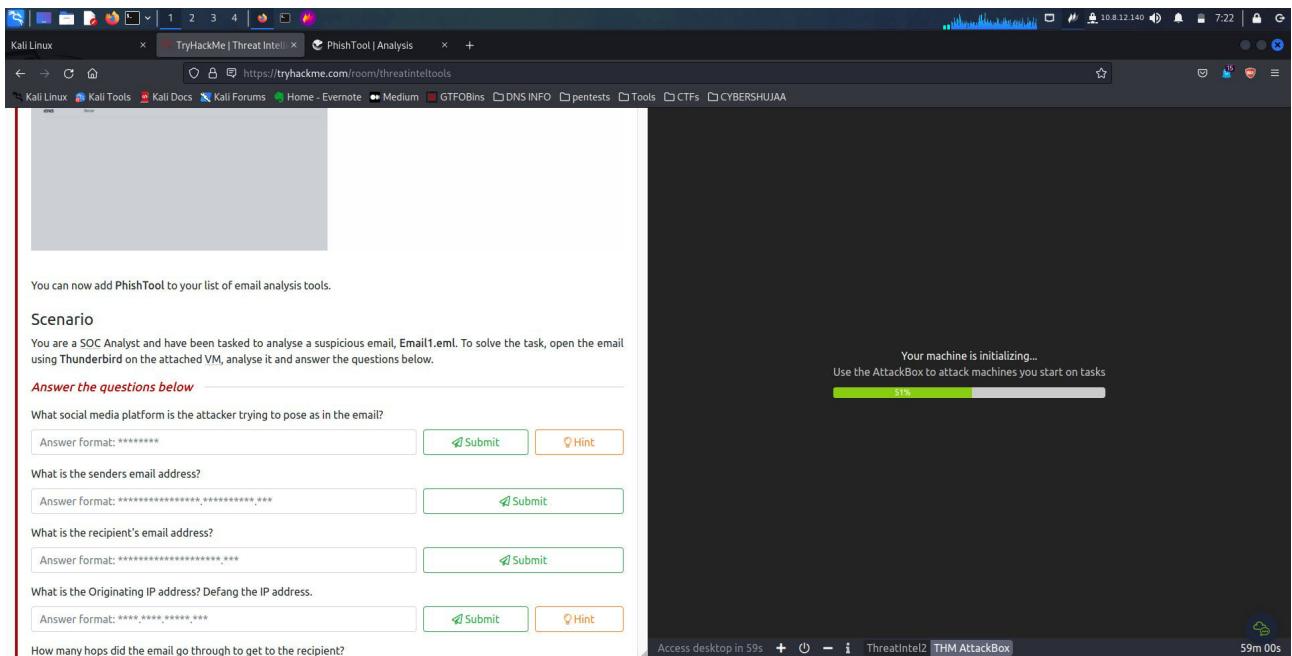
Message URLs – Gives any URL provided in the email that reference to external sources.

Scenario

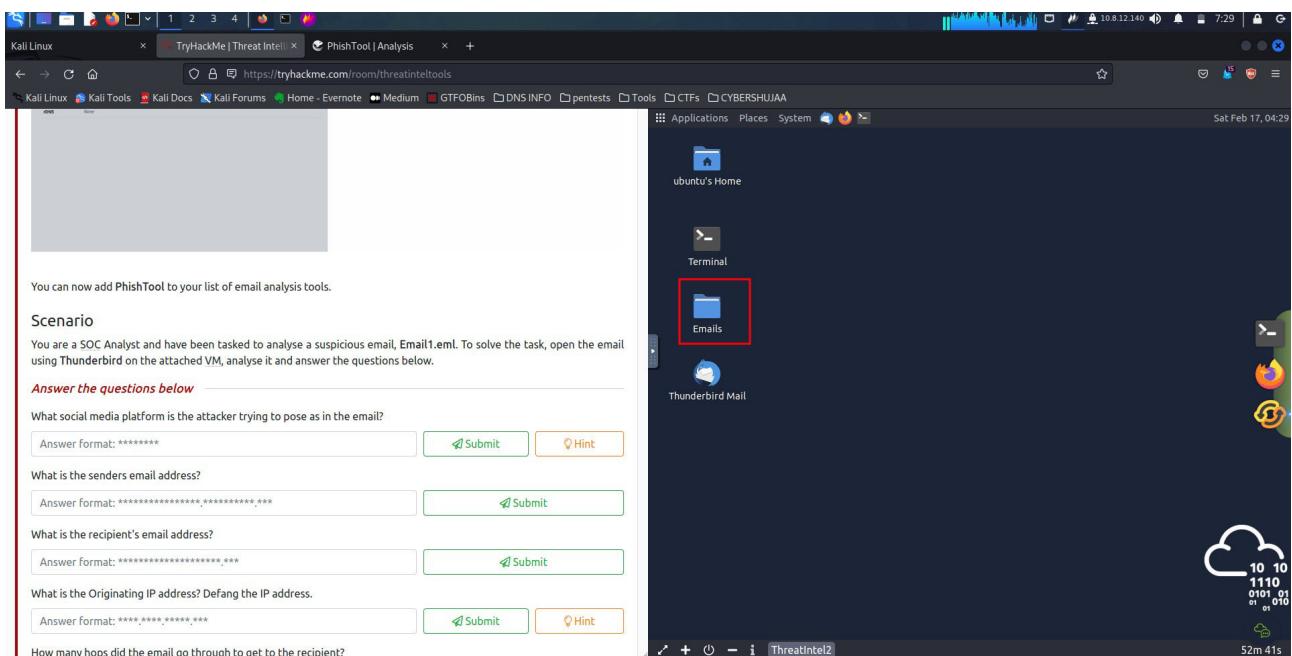
You are a SOC Analyst and have been tasked to analyze a suspicious email, Email1.eml. To solve the task, open the email using Thunderbird on the attached VM, analyze it and answer the questions below.

Answer the questions below

First step was to start a machine then start an attack box.

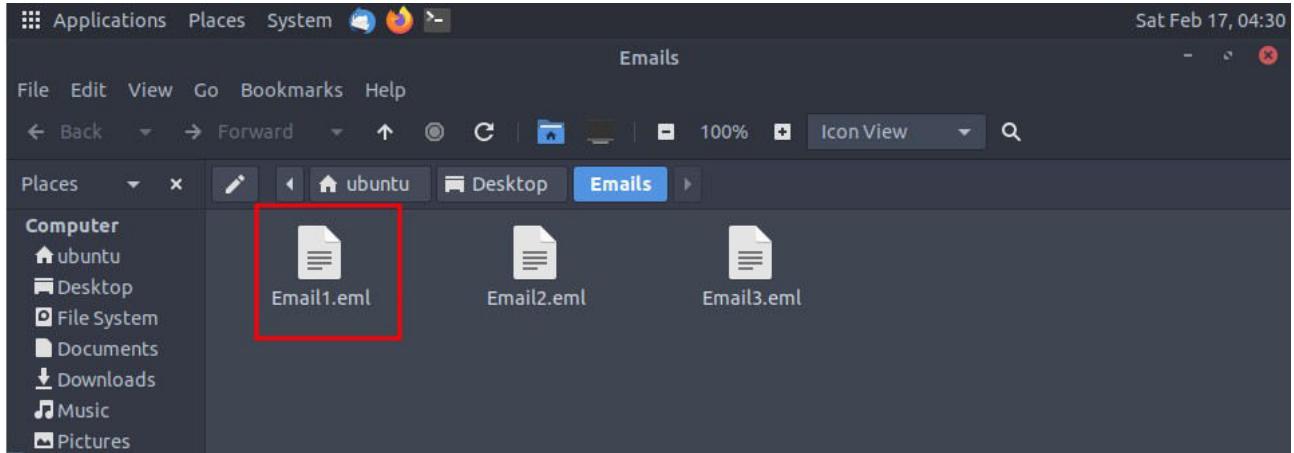


After the attack box had started, I then opened the email directory on the desktop to take a look at what was saved there.

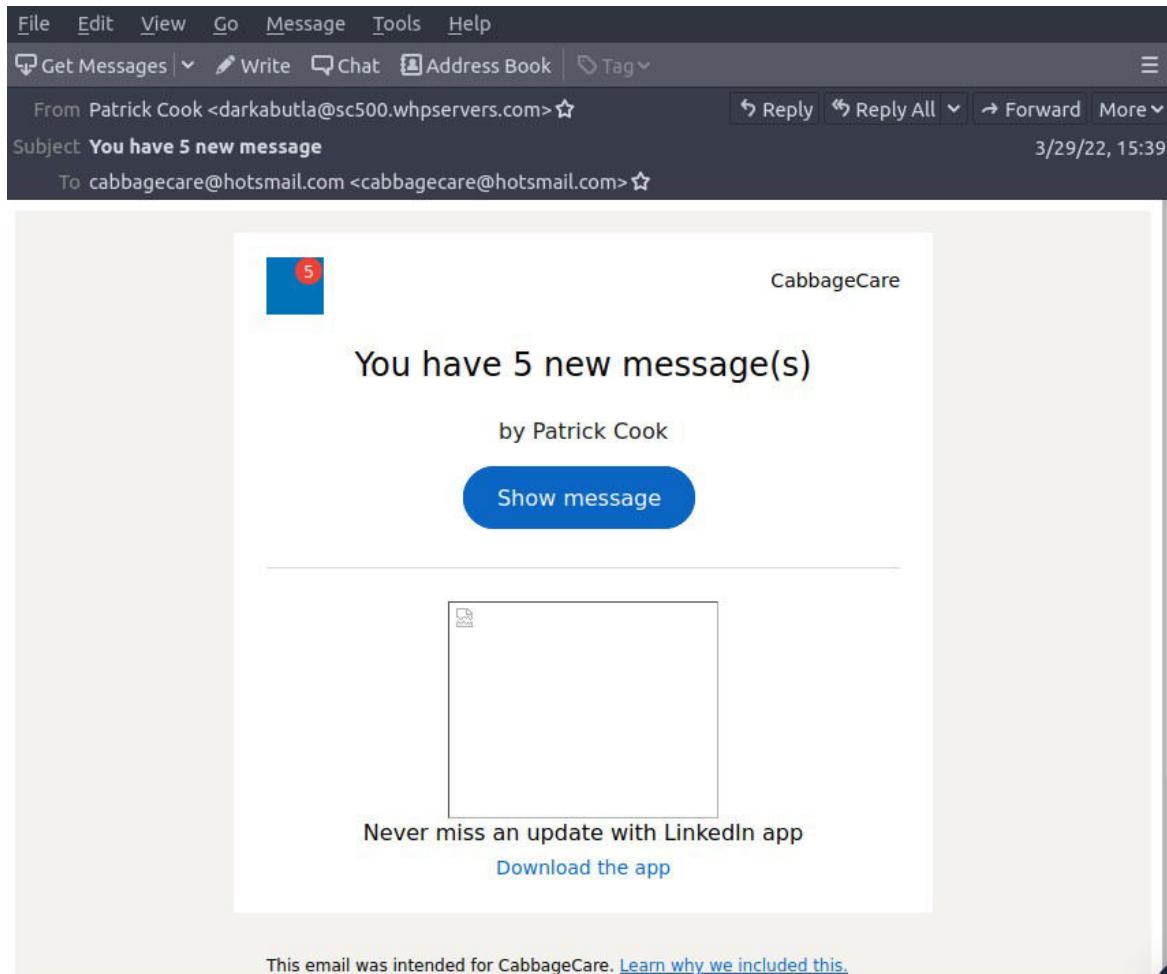


In the question we are told to analyze the file Email1.eml.

On opening the Email directory I found the Email1.eml file which I opened using Thunderbird mail as requested in the question.



Opening the file using Thunderbird:-



What social media platform is the attacker trying to pose as in the email? **ANS: LinkedIn**

To solve this question I clicked on the more tab above the mail server webpage on the right end, clicked on the drop-down arrow and choose option view source to get more information about this mail.

The screenshot shows a Firefox browser window with several tabs open. One tab is titled "PhishTool | Analysis" and contains a challenge from TryHackMe. The challenge asks what social media platform the attacker is posing as. Below the question are four input fields with placeholder text: "Answer format: *****@*****.***". To the right of each field are "Correct Answer" and "Hint" buttons. The "Submit" button is green with a white icon. A message box in the top right corner says "Woop woop! Your answer is correct." Another message box at the bottom right says "Never miss an update with LinkedIn app Download the app".

The right side of the screen shows an open Thunderbird window displaying an email message. The message header includes:

```
Received: from DB9P194B1386.EURP194.PROD.OUTLOOK.COM (2683:10a6:10:296::24) by
+0000
Received: from DM3P12CA0603.nampdr12.prod.outlook.com (2603:10b6:10:296::24) by Microsoft
SMTP Server (version=TLS_1_2_CTLS1_2_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
id 15.20.5102.17; Tue, 29 Mar 2022 20:39:28 +0000
Received: from DMNAM10FT030.eop-nan10.prod.protection.outlook.com
(2601:10b6:10:296::31) with Microsoft SMTP Server (version=TLS_1_2
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5123.13 via Frontend
Transport; Tue, 29 Mar 2022 20:39:28 +0000
Received: from DMNAM10FT030.mail.protection.outlook.com [10.13.12.224] with Microsoft
SMTP Server id 15.20.5102.17 via Frontend Transport; Tue, 29 Mar 2022
20:39:28 +0000
Authentication-Results: spf=None (sender IP is 204.93.183.11) smtp.mailfrom=sc500
dkim=none (message not signed) header.d=none;dmarc=none action=none
header.x-dmav=500.whpservers.com;comauth=pass reason=105
Received-Spf: pass (cabbagecare@hotmail.com: sc500.whpservers.com does not designate
permitted sender hosts)
X-IncomingToHeaderMarker: OriginalChecksum=33F3B6E550223B0251007520BE45C841D
Received-From-Email-Header: <[redacted]> <[redacted]> <[redacted]>
Feedback-ID: email_notification_single_search_appearance_05 [redacted]
To: <cabbagecare@hotmail.com> <cabbagecare@hotmail.com>
Date: Tue, 29 Mar 2022 20:39:28 +0000 (UTC)
Hapless-Filipinos-Mortimer: ZE115DBE361
Subject: You have 5 new message
```

The message body starts with "Never miss an update with LinkedIn app Download the app". At the bottom right of the Thunderbird window, it says "Your streak has increased. You're 5 away from a badge!"

What is the senders email address?

ANS: darkabutla@sc500.whpservers.com

Again to solve this I had to go though the source file information.

The screenshot shows a Firefox browser window with several tabs open. One tab is titled "PhishTool | Analysis" and contains a challenge from TryHackMe. The challenge asks what social media platform the attacker is posing as. Below the question are four input fields with placeholder text: "Answer format: *****@*****.***". To the right of each field are "Correct Answer" and "Hint" buttons. The "Submit" button is green with a white icon. A message box in the top right corner says "You have 5 new message - Mozilla Thunderbird". Another message box at the bottom right says "Never miss an update with LinkedIn app Download the app".

The right side of the screen shows an open Thunderbird window displaying an email message. The message header includes:

```
Source of file:///home/ubuntu/Desktop/Emails/Email1.eml?type=application/x-mail
File Edit View Help
Source of file:///home/ubuntu/Desktop/Emails/Email1.eml?type=application/x-mail
File Edit View Help
Received-Recipient-Valid-Since: cabbagecare@hotmail.com;Tue, 29 Mar 2022 15:39:28
List-Unsubscribe:<[redacted]>
Feedback-ID: email_notification_single_search_appearance_05 [redacted]
To: <cabbagecare@hotmail.com> <cabbagecare@hotmail.com>
Date: Tue, 29 Mar 2022 15:39:22 +0000 (UTC)
Hapless-Filipinos-Mortimer: ZE115DBE361
Subject: You have 5 new message
Paler-Cryptographic-Berlin: strangled
Message-ID: <1125793712_149445_95371459320sc500.whpservers.com>
From: "Patrick Cook" <[redacted]>
X-IncomingToHeaderMarker: 13
Return-Path: darkabutla@sc500.whpservers.com
X-MS-Exchange-Organization-Event-Start-Interval: 29 Mar 2022 20:39:28.0476 (UTC)
X-MS-Exchange-Organization-Expiration-Interval: OriginalSubmit
X-MS-Exchange-Organization-Expiration-Reason: OriginalSubmit
X-MS-Exchange-Organization-Expiration-Interval: 1:00:00:00,0000000
X-MS-Exchange-Organization-Expiration-Reason: OriginalSubmit
X-MS-Exchange-Organization-Network-Message-Id: 40748f1c-0a74-4678-08d11c43833
X-CPRA-Header: 0
X-EP0TenantAttributeMessage: 84df9e7f-f096-40af-b435-aaaaaaaaaaaa:0
X-MS-Exchange-Organization-MessageDirectionality: Incoming
X-MS-Exchange-Organization-Auth-Source: DMNAM10FT030.eop-nan10.prod.protection.outw
X-MS-Exchange-Organization-Auths: Anonymous
X-MS-UserLastLogonTime: 3/29/2022 8:38:46 AM
X-MS-UserLogonCount: 1
X-MS-TrafficTypeDiagnostic: DB9P194B1386:EE
X-MS-Exchange-Organization-ED0Direct: true
X-Header-IP: 204.93.183.11
X-SID-PRA: DARKABUTLA@SC500.NHPSERVERS.COM
X-CTD-Processor: [redacted]
```

The message body starts with "Never miss an update with LinkedIn app Download the app". At the bottom right of the Thunderbird window, it says "Your streak has increased. You're 5 away from a badge!"

What is the recipient's email address?

ANS: cabbagecare@hotmail.com

The screenshot shows a Kali Linux desktop environment with a Firefox browser window open to the TryHackMe Threat Intel page. On the left, there's a sidebar with various tools like Kali Tools, Kali Docs, Kali Forums, Home - Evernote, Medium, GTFOBins, DNS INFO, pentests, Tools, CTFs, and CYBERSHUJAA. The main content area has tabs for 'PhishTool | Analysis' and 'PhishTool | Tools'. Below these tabs, there's a message: 'You can now add PhishTool to your list of email analysis tools.' A 'Scenario' section describes a SOC Analyst task involving a suspicious email named 'Email1.eml'. Below this, a 'Answer the questions below' section contains several questions with input fields and 'Correct Answer' buttons:

- What social media platform is the attacker trying to pose as in the email? (Answer: LinkedIn)
- What is the senders email address? (Answer: darkabutla@sc500.whpservers.com)
- What is the recipient's email address? (Answer: cabbagecare@hotmail.com)
- What is the Originating IP address? Defang the IP address. (Answer format: *.*.*.*)
- How many hops did the email go through to get to the recipient? (Answer format: *)

To the right of the browser, a separate Thunderbird window is open, showing an email from 'Patrick Cook <darkabutla@sc500.whpservers.com>' to 'cabbagecare@hotmail.com'. The email body contains a message: 'Woop woop! Your answer is correct.' and a link to 'https://www.linkedin.com/e/v2e+22d94b7e8b-b2317916t+lnkMldt0'. The email header is visible, showing various X-MS-Exchange headers related to the email's path and delivery.

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

ANS: 204[.]93[.]183[.]11

First I obtained the senders IP address which was: **204.93.183.11**

A screenshot of Mozilla Thunderbird showing an incoming email. The subject is 'You have 5 new message - Mozilla Thunderbird'. The source of the email is 'file:///home/ubuntu/Desktop/Emails>Email1.eml?type=application'. The header information includes:

- X-MS-UserLastLogonTime: 3/29/2022 8:38:46 PM
- X-MS-Office365-Filtering-Correlation-Id: 4d748f1c-0a74-4678-0498-08da11c43833
- X-MS-TrafficTypeDiagnostic: DB9P194MB1386:EE_
- X-MS-Exchange-EOPDirect: true
- X-Sender-IP: 204.93.183.11
- X-SID-PRA: DARKABUTLA@SC500.WHPSERVERS.COM

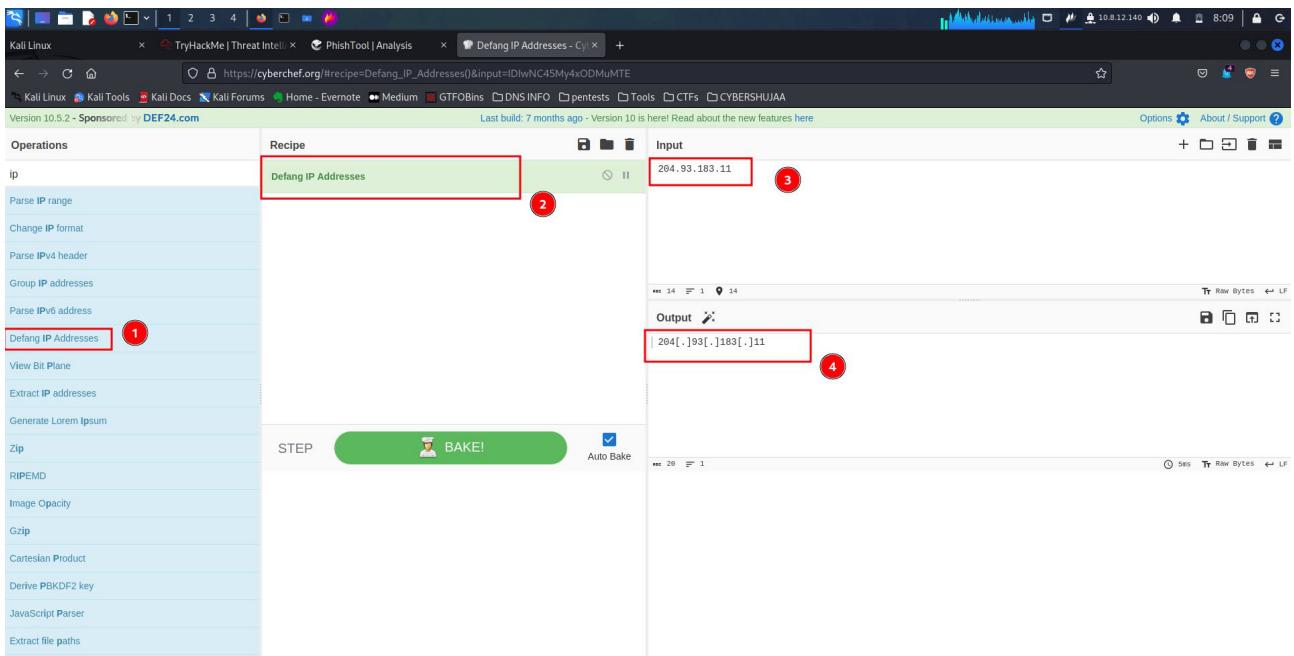
The email body contains a message: 'Never miss an update with LinkedIn app Download the app' and a note: 'This email was intended for CabbageCare. Learn why we included this.'

Next step was to defang the IP address.

What does Defanging an IP address mean?

When sharing suspicious or malicious URLs, IP addresses, and email addresses, you don't want people to accidentally click those links. To prevent this, you defang the URLs or IP addresses, so that software doesn't convert them into clickable links.

Cyberchef.org gives this tool therefore I used it for this next step.



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

ANS: 4

```

1 Received: from [REDACTED]4MB1386.EURP194.PROD.OUTLOOK.COM (2603:10a6:10:296::24) by
AMBP194MB1513.EURP194.PROD.OUTLOOK.COM with HTTPS; Tue, 29 Mar 2022 20:39:29
+0000
2 Received: from DM3PR12CA0063.namprd12.prod.outlook.com (2603:10b6:0:56::31) by
DB9P194MB1386.EURP194.PROD.OUTLOOK.COM (2603:10a6:10:296::24) with Microsoft
SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
id 15.20.5102.17; Tue, 29 Mar 2022 20:39:28 +0000
3 Received: from DMGNAME10FT030.eop-nam10.prod.protection.outlook.com
(2603:10b6:0:56::5d) by DM3PR12CA0063.outlook.office365.com
(2603:10b6:0:56::51) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5123.13 via Frontend
Transport; Tue, 29 Mar 2022 20:39:28 +0000
4 Received: from [REDACTED]whpservers.com (204.93.183.11) by
DMGNAM10FT030.eop-nam10.prod.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
Authentication-Results: spf=none (sender IP is 204.93.183.11) smtp.mailfrom=sc500.whpservers.com;
dkim=none (message not signed) header.d=none;dmarc=none action=none
header.from=sc500.whpservers.com;compauth-pass reason=105
Received-SPF: None (protection.outlook.com: sc500.whpservers.com does not designate
permitted sender hosts)
X-IncomingTopHeaderMarker: OriginalChecksum:33F38BD05032233B02515107520BE45CC841D0B3161C6C24E69A889F98E0BEBB;UpperCasedChecks
Require-Recipient-Valid-Since: cabbagecare@hotmail.com; Tue, 29 Mar 2022 15:39:22 +0000
List-Unsubscribe: <https://www.linkedin.com/e/v2?e=22d94b7e8b-b231791&t=lun&midToken=bBfd3832538Aa&midSig=bf4D979e2e12&ek=ema>

```

Cisco Talos Intelligence

In this section we looked at Cisco Talos which is a large team of security practitioners called Cisco Talos to provide actionable intelligence, visibility on indicators, and protection against emerging threats through data collected from their products. IT and Cybersecurity companies collect massive amounts of information that could be used for threat analysis and intelligence

Cisco Talos encompasses six key teams:

Threat Intelligence & Interdiction: Quick correlation and tracking of threats provide a means to turn simple IOCs into context-rich intel.

Detection Research: Vulnerability and malware analysis is performed to create rules and content for threat detection.

Engineering & Development: Provides the maintenance support for the inspection engines and keeps them up-to-date to identify and triage emerging threats.

Vulnerability Research & Discovery: Working with service and software vendors to develop repeatable means of identifying and reporting security vulnerabilities.

Communities: Maintains the image of the team and the open-source solutions.

Global Outreach: Disseminates intelligence to customers and the security community through publications.

Task

Use the information gathered from inspecting the Email1.eml file from Task 5 to answer the following questions using Cisco Talos Intelligence. Please note that the VM launched in Task 5 would not have access to the Internet.

Answer the questions below

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

ANS: scnet.net

Once the Cisco Talos page loaded, there was a search box with a placeholder URL, IP etc. In this search box I put the IP address from the previous task and begun my search.

The screenshot shows the Cisco Talos Reputation Lookup interface. The search bar at the top contains the IP address 204.93.183.11. The results are displayed in several sections:

- LOCATION DATA:** Chicago, United States
- OWNER DETAILS:** IP ADDRESS: 204.93.183.11; FWD/REV DNS MATCH: Yes; HOSTNAME: sc500.whpservers.com; DOMAIN: **scnet.net** (highlighted with a red box); NETWORK OWNER: server.central.network
- REPUTATION DETAILS:** SENDER IP REPUTATION: Good; WEB REPUTATION: Unknown
- EMAIL VOLUME DATA:** LAST DAY: 2.8; LAST MONTH: 2.9; VOLUME CHANGE: -100% (with a downward arrow); SPAM LEVEL: None
- CONTENT DETAILS:** CONTENT CATEGORY: No established content categories
- BLOCK LISTS:** BLSPAMCOP.NET: Not Listed; CBLABUSEAT.ORG: Not Listed

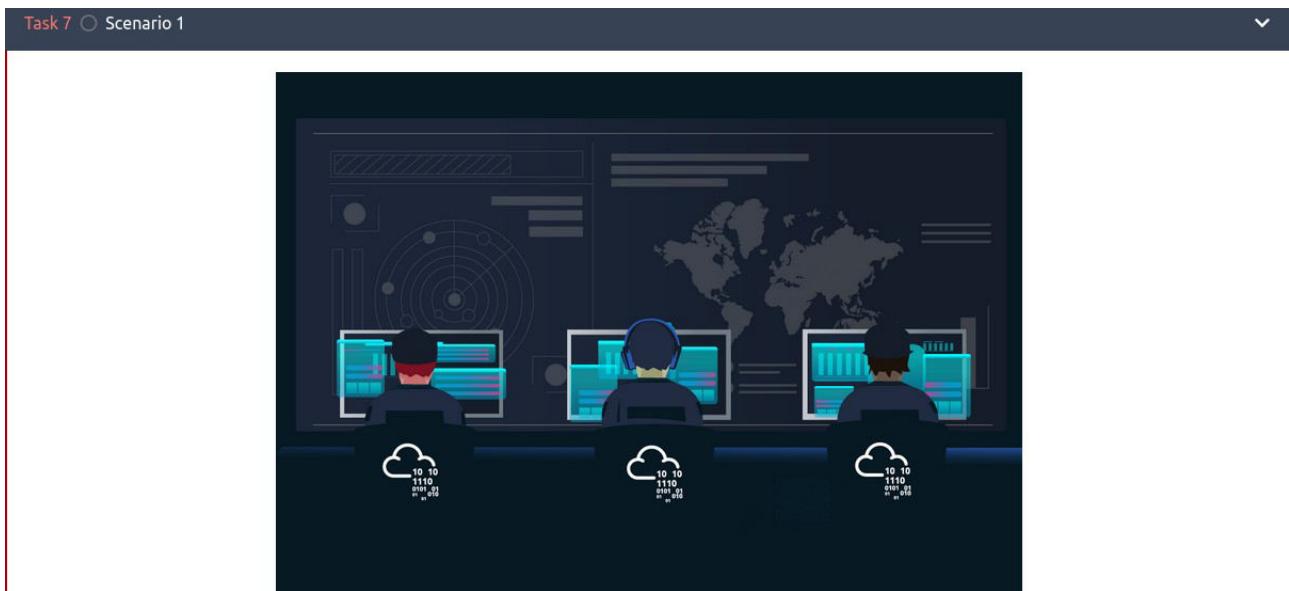
What is the customer name of the IP address?

ANS: Complete Web Reviews

While using the Talos Intelligence platform, the whois tab didnt give any responses:-

This being so I used my terminal “**whois**” command to see if I would get a respond and there it was, the customer name of the IP address

Scenario 1



Scenario: 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.

Answer the questions below

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

Ans: chris.lyons@supercarcenterdetroit.com

Fw: Re: PI no. SO-P101092262891 - Mozilla Thunderbird

Sun Feb 18, 13:30

File Edit View Go Message Tools Help

Get Messages | Write Chat Address Book Tag

From Le Huong-accounts <LeHuong-accounts@gmail.com>☆

Subject Fw: Re: PI no. SO-P101092262891

To chris.lyons@supercarcenterdetroit.com☆

12/14/17, 18:14

Dear all,

We've made balance payment for attached invoice on 14/12/2017.
Our below forwarder will contact your side for pickup arrangement:

EVO Logistics Pte Ltd
No 7, Airline Road, #05-08, Cargo Agent Building E, Singapore 819834.
PIC: lucy Tiew (Email: lucy@evvlogistics.com.sg)

There's no need to send the original Tax Invoice or Declaration Letter together with the goods.

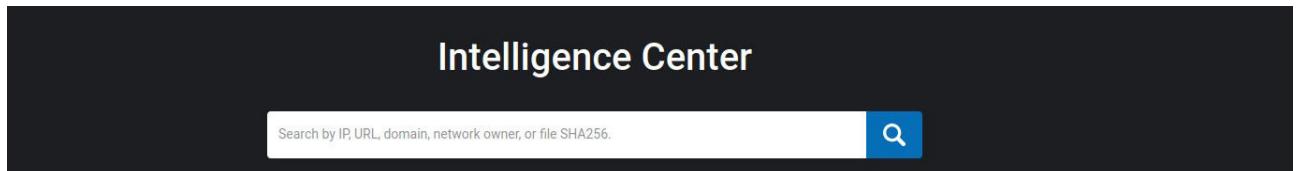
Thank you,
Huong Le

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

Ans: HIDDENEXT/Worm.Gen

In this task I got a little bit stuck but with some research I was able to go around it, this is what I did.

Talos Intelligence only runs a search on specific strings from the placeholder on the search bar they include:-



For me to have a successful search my values have to be in one of this specified format.

For this task since it was a file, I can get a sha256 value if there is one, so I went on to find if there was this kind of value using the attack box terminal.

All I had to do was to navigate to the file and run command sha256sum on that file and see if there is a sha256 value.

```
ubuntu@tryhackme:~$ cd Desktop
ubuntu@tryhackme:~/Desktop$ ls
-mails
'Proforma Invoice P101092292891 TT slip pdf.rar.exe'
'Proforma Invoice P101092292891 TT slip pdf.rar.zip'
ubuntu@tryhackme:~/Desktop$ cd Emails
ubuntu@tryhackme:~/Desktop/Emails$ ls
Email1.eml Email2.eml Email3.eml
ubuntu@tryhackme:~/Desktop/Emails$ sha256sum Email2.eml
97028b1b198af6da1043b78e40e1efe519fe3def754cd9d1f29380ca11e5c361 Email2.eml
ubuntu@tryhackme:~/Desktop/Emails$
```

There it was a sha256 value which was:-

97028b1b198af6da1043b78e40e1efe519fe3def754cd9d1f29380ca11e5c361

Having this value, next step was to run a search on the Talos Intelligence database and find out if there is a valuable information I could gather.



Well there was, this is how I found the alias name.

Scenario 2

Scenario: 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.

Answer the questions below

What is the name of the attachment on Email3.eml? Ans: Sales_ Receipt 5606.xls

First I opened the file using thunderbird then clicked on the more options icon with the 3 bars > Attachments > 1_Sales_Receipt 5606.xls > open us > save where before the file gets saved it displays the real name of the file.

The screenshot shows a Linux desktop environment with several windows open. One window is a web browser displaying the TryHackMe ThreatIntel room. Another window is Mozilla Thunderbird showing an email titled 'Purchase Order Receipt'. The attachment 'Sales_Receipt 5606.xls' is listed in the attachments panel. A third window is a file manager showing the contents of the attachment, which is a Microsoft Excel spreadsheet containing a purchase order summary.

The screenshot shows a file manager window titled 'Save Attachment' with the file name 'Sales_Receipt 5606.xls' highlighted. The file manager lists various folders and files on the left, and the contents of the selected file on the right. The file is a Microsoft Excel spreadsheet containing a purchase order summary.

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

Ans: Dridex

First again I will find the sha256 value then search for an attached malware analysis on the value.

```
ubuntu@tryhackme:~/Desktop/Emails$ sha256sum Email3.eml
f4d97603256a36e81bfe7ef5e0ccae44f77de6bb041fa41f0b3a0db53f4aba9 Email3.eml
ubuntu@tryhackme:~/Desktop/Emails$
```

K you for your business - we appreciate it very much. Sincerely,
----- =A0=A0Purchase=A0Order=A0Summary=
=A0=A0-----=Sale=A0#=A0:=A05606Sale=A0Date:=A010/13/=
2021Total:=A0\$3,431.00The=A0complete=A0version=A0has=A0been=A0provided=A0=
as=A0an=A0attachment=A0to=A0this=A0email.-----=

Sha256 value is:- **f4d97603256a36e81bfe7ef5e0ccae44f77de6bb041fa41f0b3a0db53f4aba9**

The screenshot shows a Linux desktop environment with several windows open. In the top right, a terminal window displays a command-line session:

```

Sun Feb 18, 15:06
Source of file:///home/ubuntu/Desktop/Emails/Email3.eml?type=application/x-message-display - Mozilla Thunderbird
ubuntu@tryhackme: ~/Desktop/Emails
ls: cannot access 'cd': No such file or directory
Desktop:
'Emails'                                         mate-terminal.desktop
'Proforma Invoice P101092292891 TT sli... pdf.rar.exe'   thunderbird.desktop
'Proforma Invoice P101092292891 TT sli... pdf.rar.zip'   JURUPAP.mta.notifications.intu
ubuntu@tryhackme:~/Desktop/Emails$ ls
Emails                                         mate-terminal.desktop
'Proforma Invoice P101092292891 TT sli... pdf.rar.exe'   thunderbird.desktop
'Proforma Invoice P101092292891 TT sli... pdf.rar.zip'   JURUPAP.mta.notifications.intu
ubuntu@tryhackme:~/Desktop/Emails$ ls
Emails                                         mate-terminal.desktop
Email1.eml                                     Email1.eml
Email1.eml.sha256                               Email1.eml.sha256
Email2.eml                                     Email2.eml
Email2.eml.sha256                               Email2.eml.sha256
Email3.eml                                     Email3.eml
Email3.eml.sha256                               Email3.eml.sha256
Command 'sha256' not found, but can be installed with:
sudo apt install hashalot
ubuntu@tryhackme:~/Desktop/Emails$ sha256sum Email3.eml
f4d97603256A36E81BFE7EF5E0CCAEE44F77DE6BB041FA41F0B3A0DB53F4ABA9  Email3.eml
ubuntu@tryhackme:~/Desktop/Emails$ 

```

In the bottom right, a browser window titled "ThreatIntel2" shows a ThreatGrid search result for the SHA256 value f4d97603256A36E81BFE7EF5E0CCAEE44F77DE6BB041FA41F0B3A0DB53F4ABA9. The results page includes sections for FILE REPUTATION, TALOS WEIGHTED FILE REPUTATION, ASSOCIATED DOMAINS FOR THIS HASH, and DETECTION ALIASES.

Next was to key in the sha256 value and check for the available database record collected in the Talos Intelligence about this sha256.

I tried a few aliases but in the end the answer to which malware it was was Dridex

The screenshot shows a detailed view of a file reputation search result for the SHA256 value f4d97603256A36E81BFE7EF5E0CCAEE44F77DE6BB041FA41F0B3A0DB53F4ABA9. The page includes sections for FILE REPUTATION, TALOS WEIGHTED FILE REPUTATION, ASSOCIATED DOMAINS FOR THIS HASH, and DETECTION ALIASES. The DETECTION ALIASES section lists various aliases, with "X97M/Dridex.Agent/Ildorado" highlighted.

Conclusion

In this lab several concepts of Threat Intelligence and various open-source tools that are useful in carrying out a good analysis. On the learning objectives for this lab included, Understanding the basics of threat intelligence & its classifications, using UrlScan.io to scan for malicious URLs, using Abuse.ch to track malware and botnet indicators, investigate phishing emails using PhishTool and using Cisco's Talos Intelligence platform for intel gathering I am glad to say that all of this areas I have a solid ground and I have an added milestone in the skills that I have gained from this room. This room has surely enlarged my knowledge in threat intelligence and tools to rely on in the process of such an analysis.

Thank You.