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.

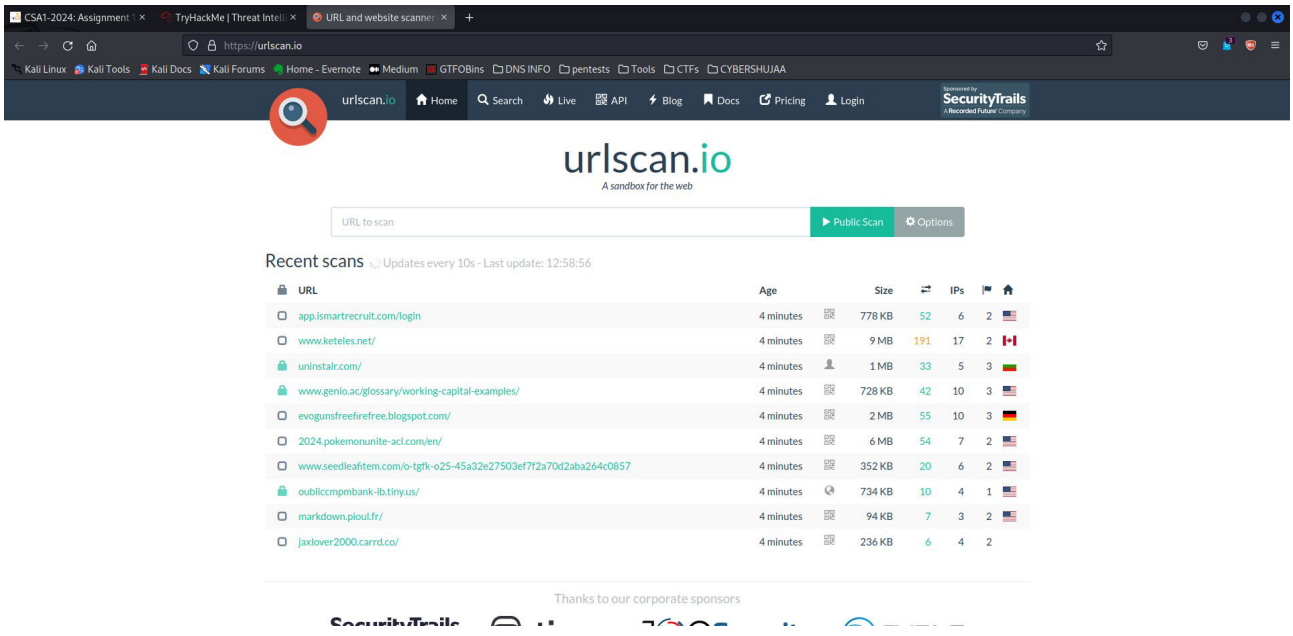
Tactical Intel - Assesses adversaries' tactics, techniques, and procedures (TTPs). This intel can strengthen security controls and address vulnerabilities through real-time investigations.

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.



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.

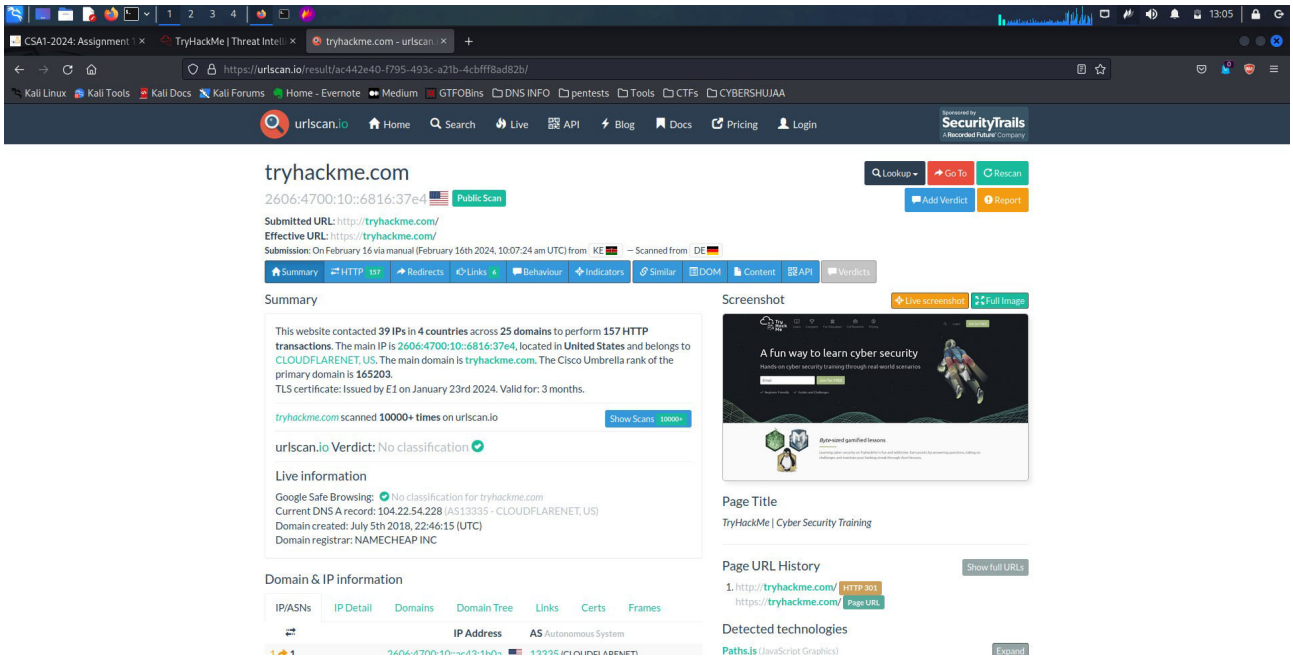
Indicators - Lists all IPs, domains and hashes associated with the site. These indicators do not imply malicious activity related to the site.

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.

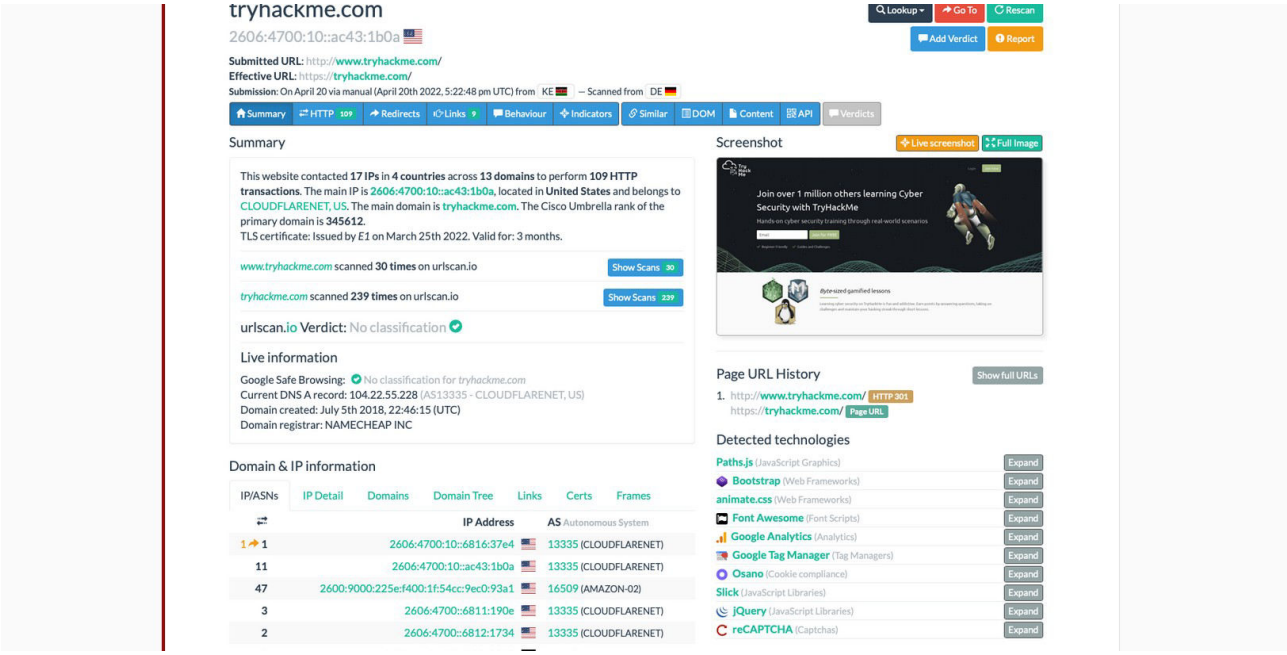
Here are my results immediately after the scan.



Answer the questions below

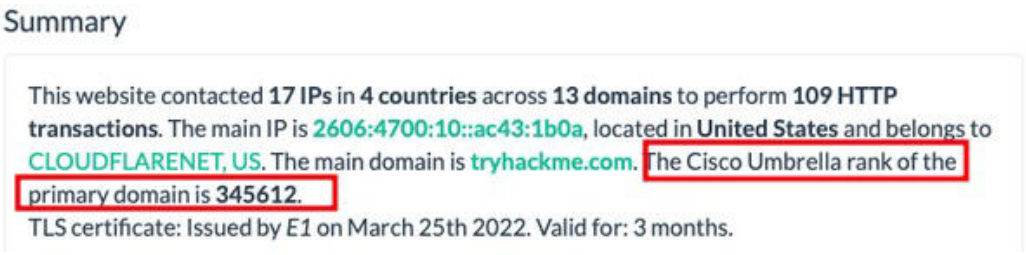
Although I had tried out my own search, this question needed me to use the screenshot provided in the room.

Here it is:-



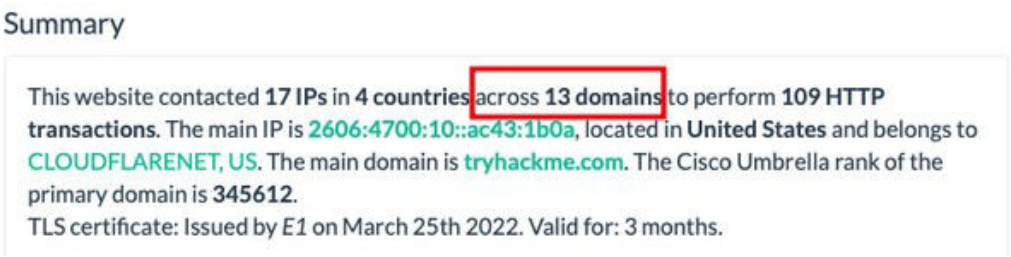
What was TryHackMe's Cisco Umbrella Rank based on the screenshot?

Ans: 345612



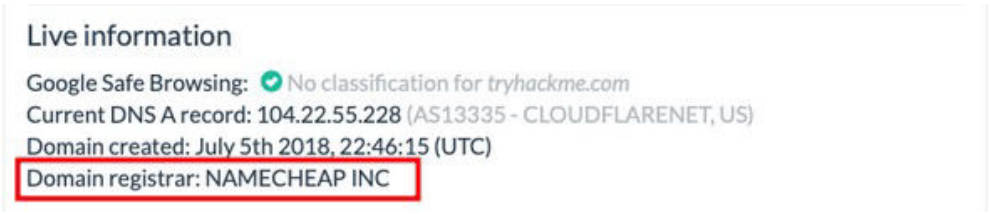
How many domains did UrlScan.io identify on the screenshot?

Ans: 13



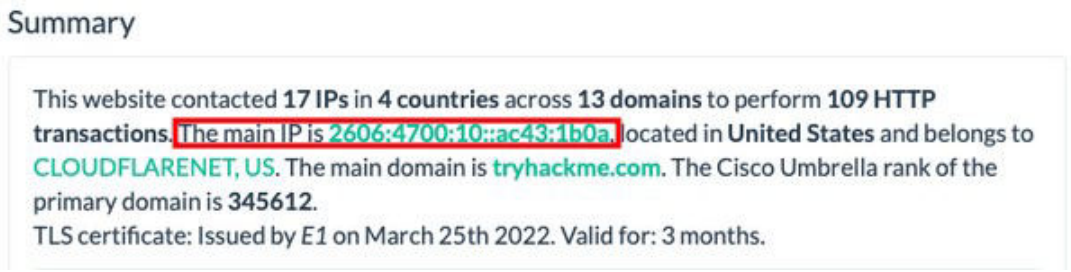
What was the main domain registrar listed on the screenshot?

Ans: NAMECHEAP INC



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

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



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.

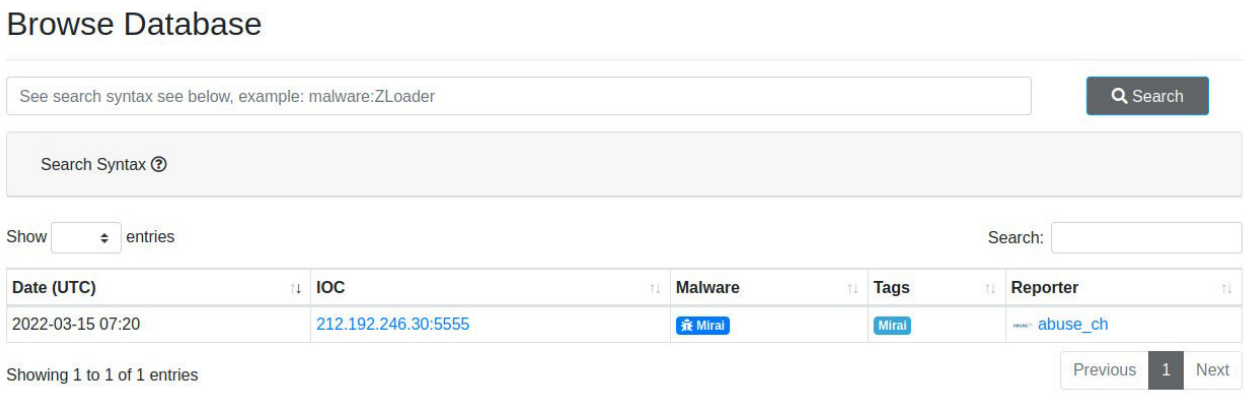
Answer the questions below

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

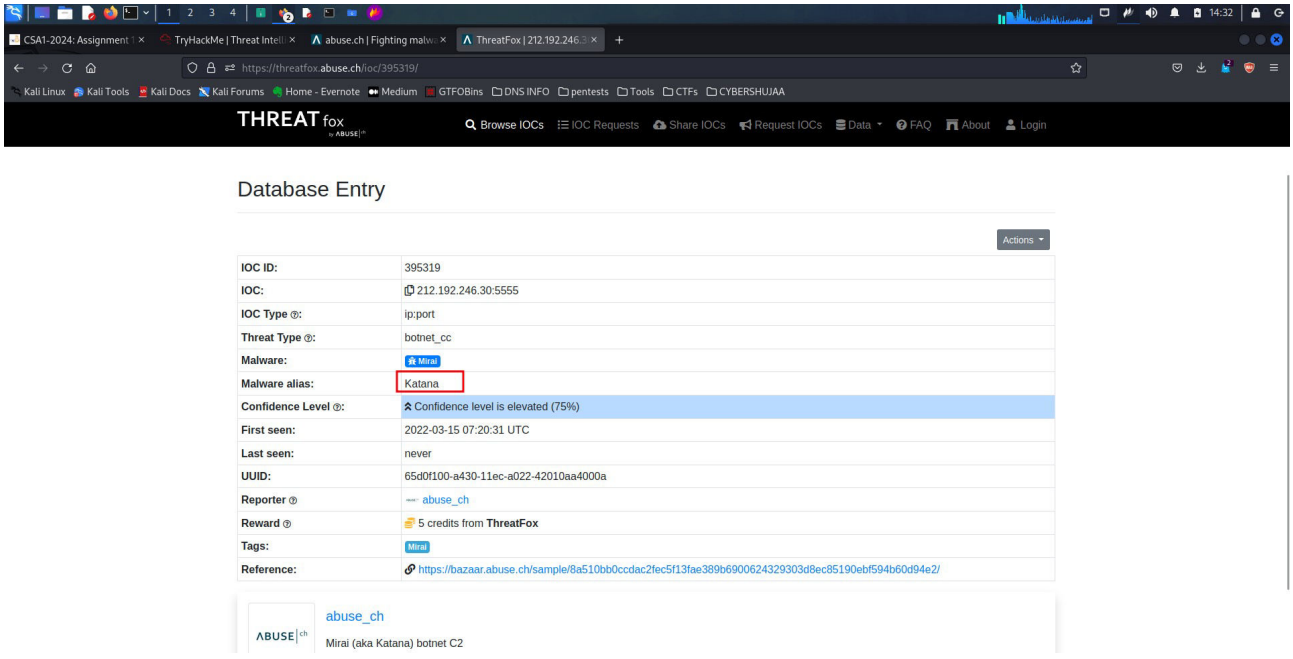
Ans: Katana

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

ioc:212.192.246.30:5555



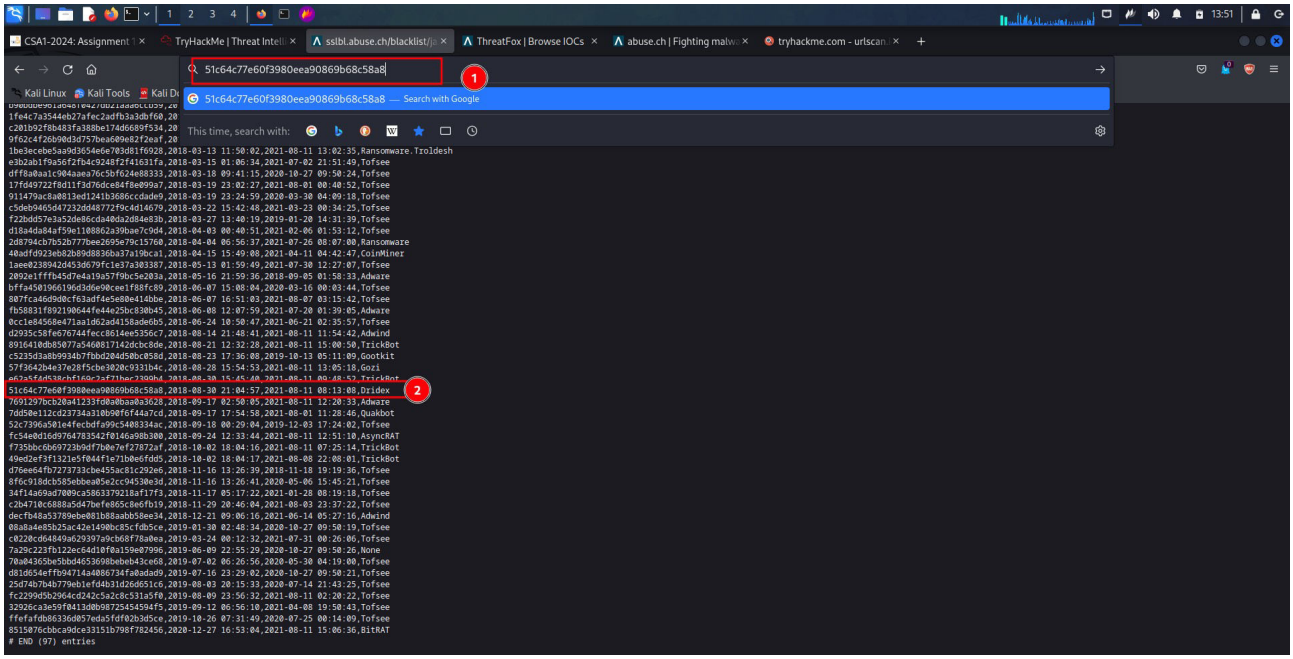
To view more details about this result found I clicked on the results which gave more insights about the malware including the alias name.



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

First was to download the JA3 Fingerprint list.

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

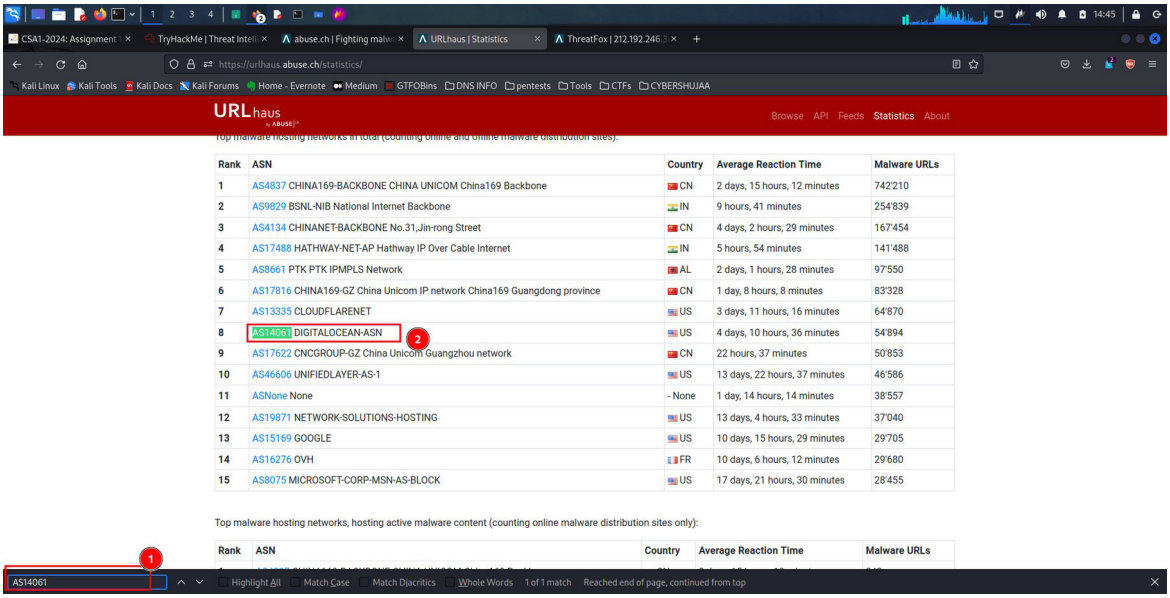


From the statistics page on URLHaus, what malware-hosting network has the ASN number AS14061?

Ans: DIGITALOCEAN-ASN

At first I was unable to find on how to find an Asn number, I tried using the search bar on the browsers tab but nothing was displaying till I did some search that game me the guidelines below.

Once you are on the Statistics page, use ctrl+f to get search bar and enter the ASN number and press enter. This will take you to the one result on the page. The answer to the question will be located right next to the ASN number.

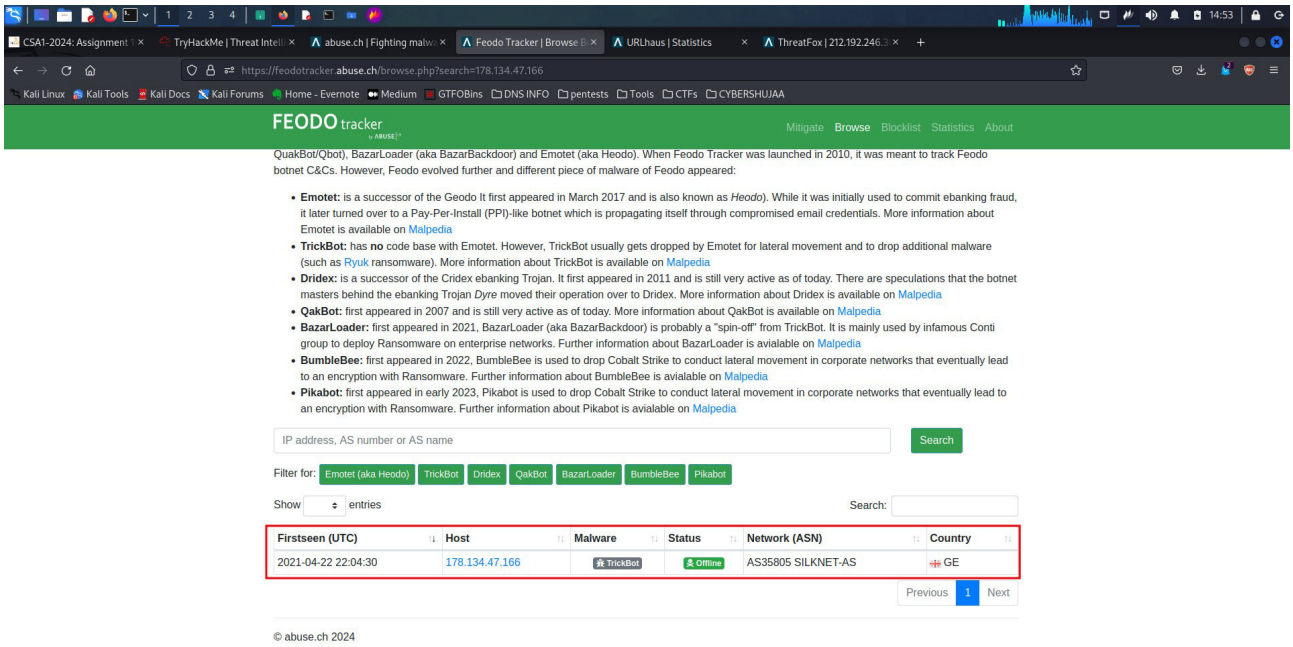


Which country is the botnet IP address 178.134.47.166 associated with according to FeodoTracker?

Ans: Geogia

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.



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.

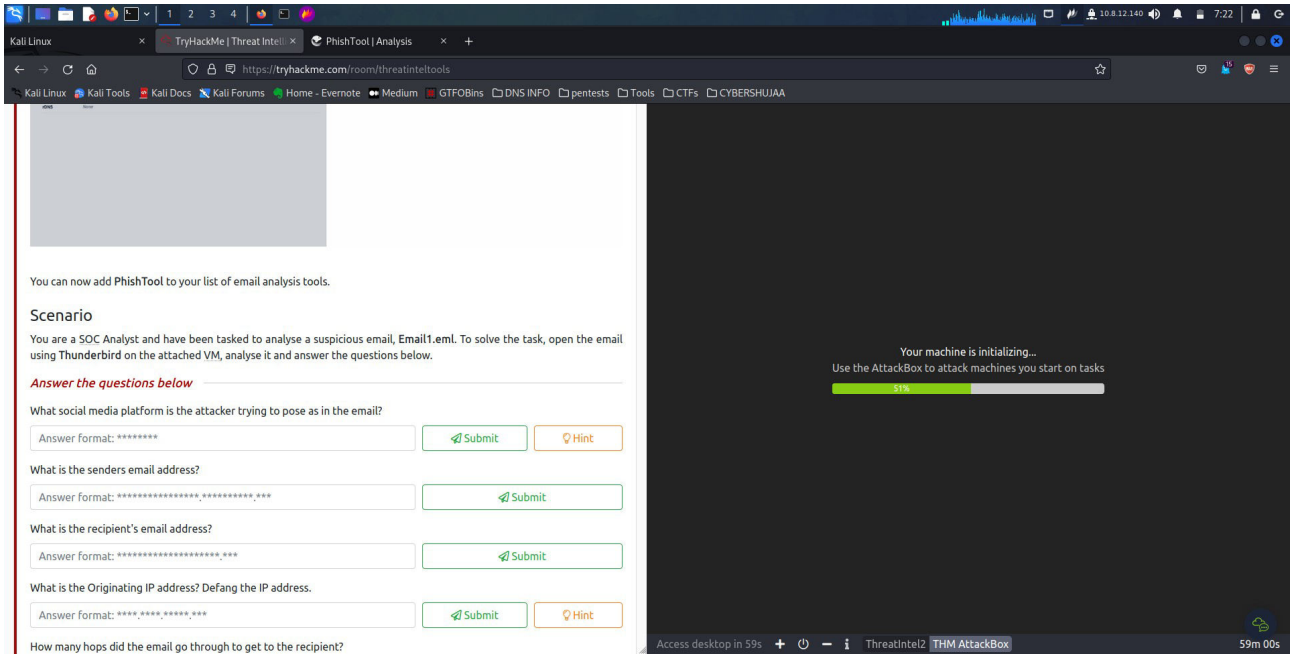
Message URLs – Gives any URL provided in the email that reference to external sources.

Scenario

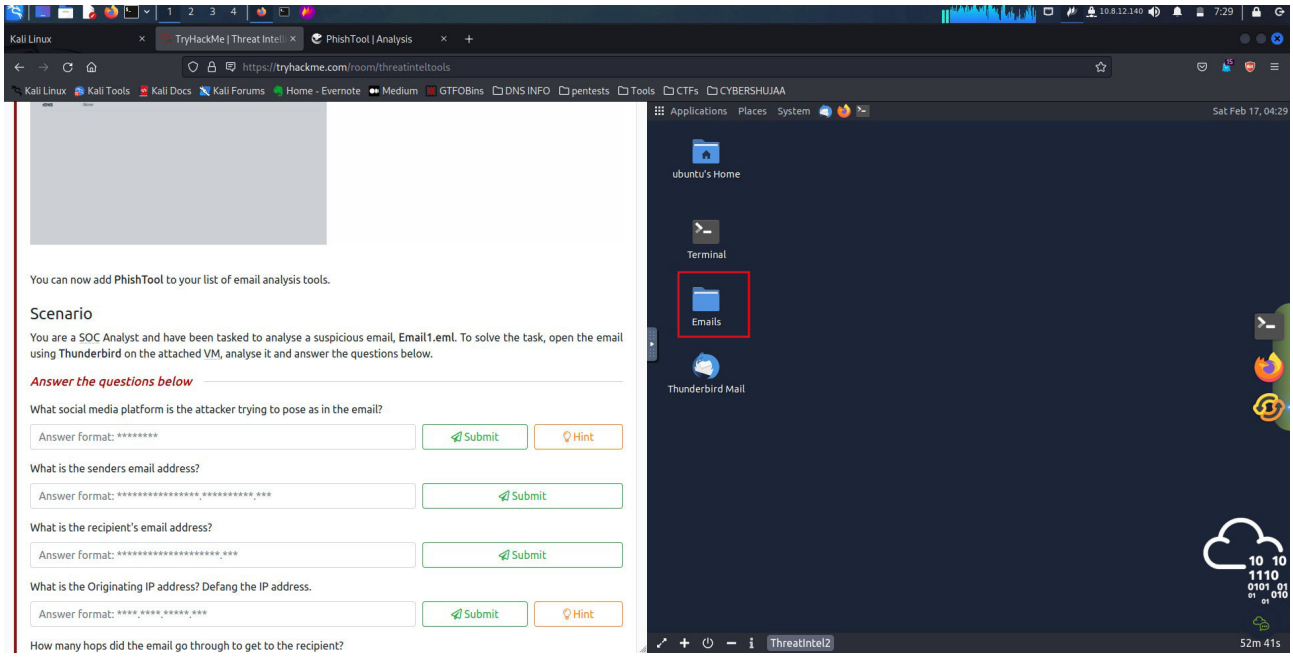
You are a SOC Analyst and have been tasked to analyze a suspicious email, Email1.eml. To solve the task, open the email using Thunderbird on the attached VM, analyze it and answer the questions below.

Answer the questions below

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

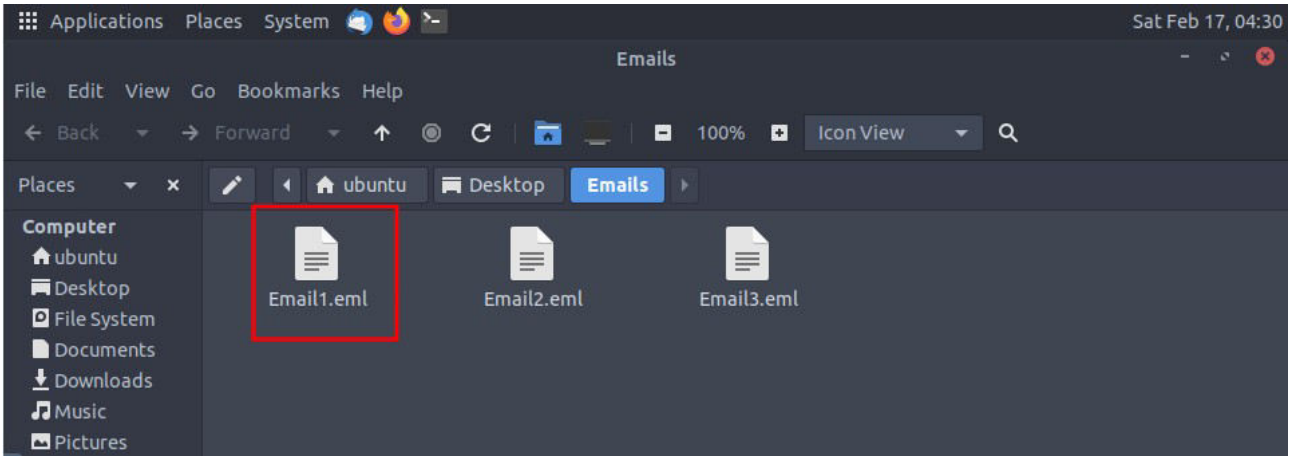


After the attack box had started, I then opened the email directory on the desktop to take a look at what was saved there.

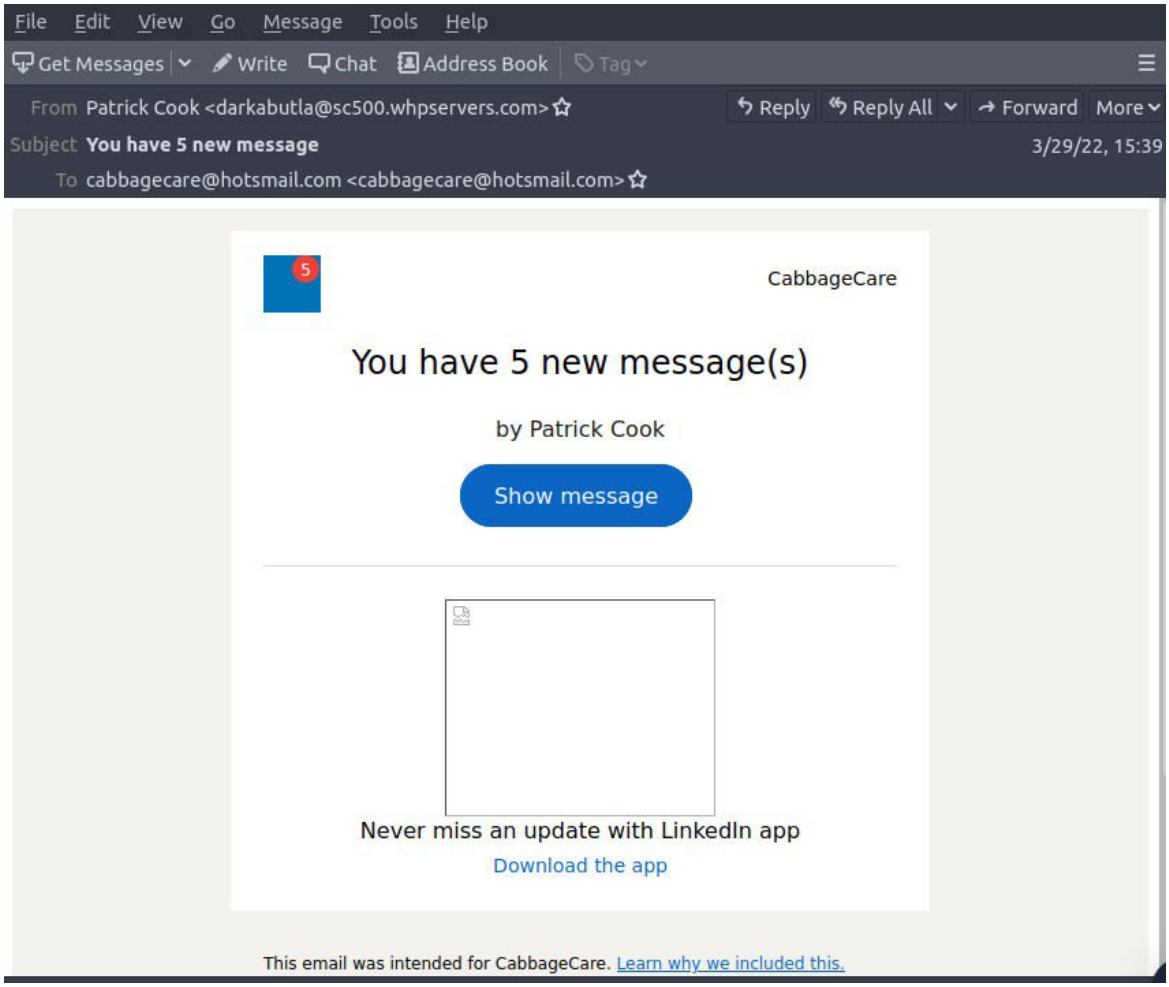


In the question we are told to analyze the file Email1.eml.

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

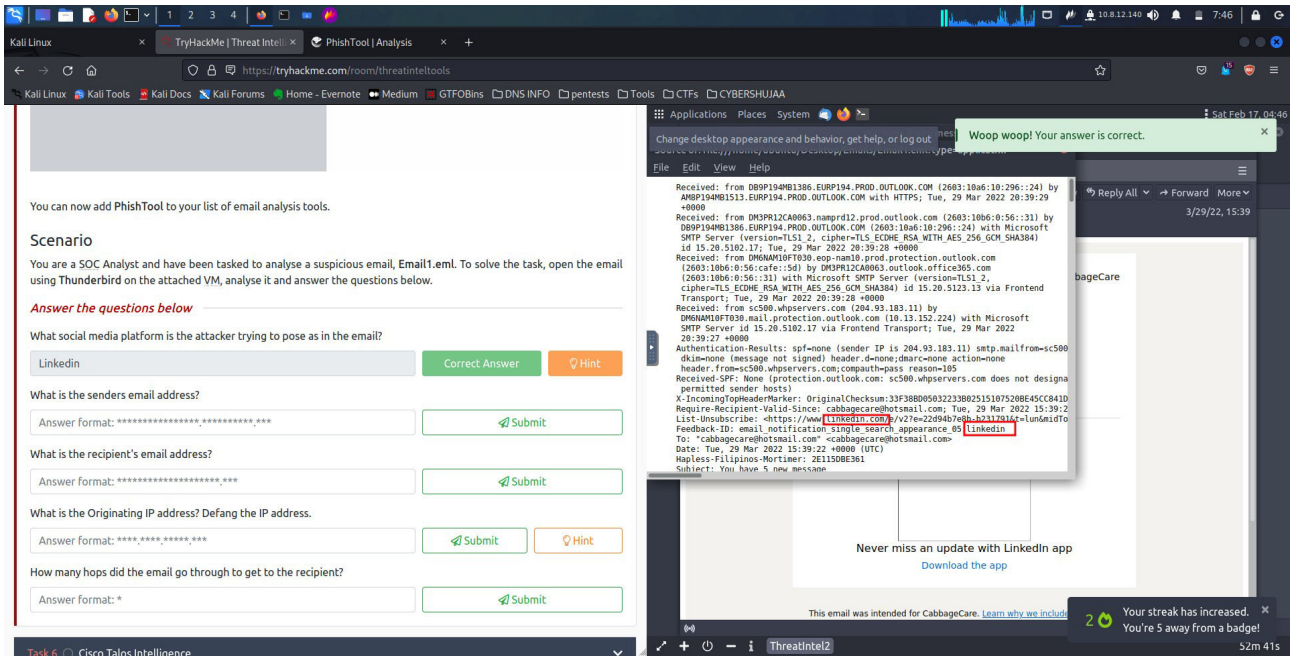


Opening the file using Thunderbird:-



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

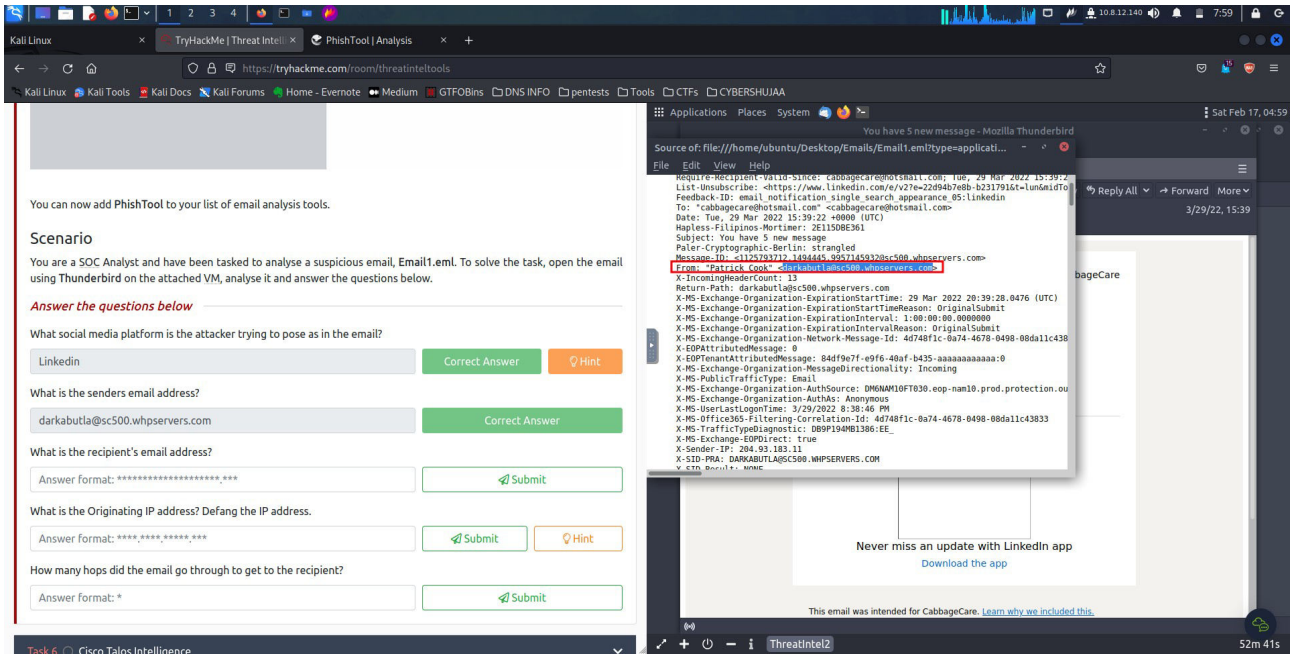
To solve this question I clicked on the more tab above the mail server webpage on the right end, clicked on the drop-down arrow and choose option view source to get more information about this mail.



What is the senders email address?

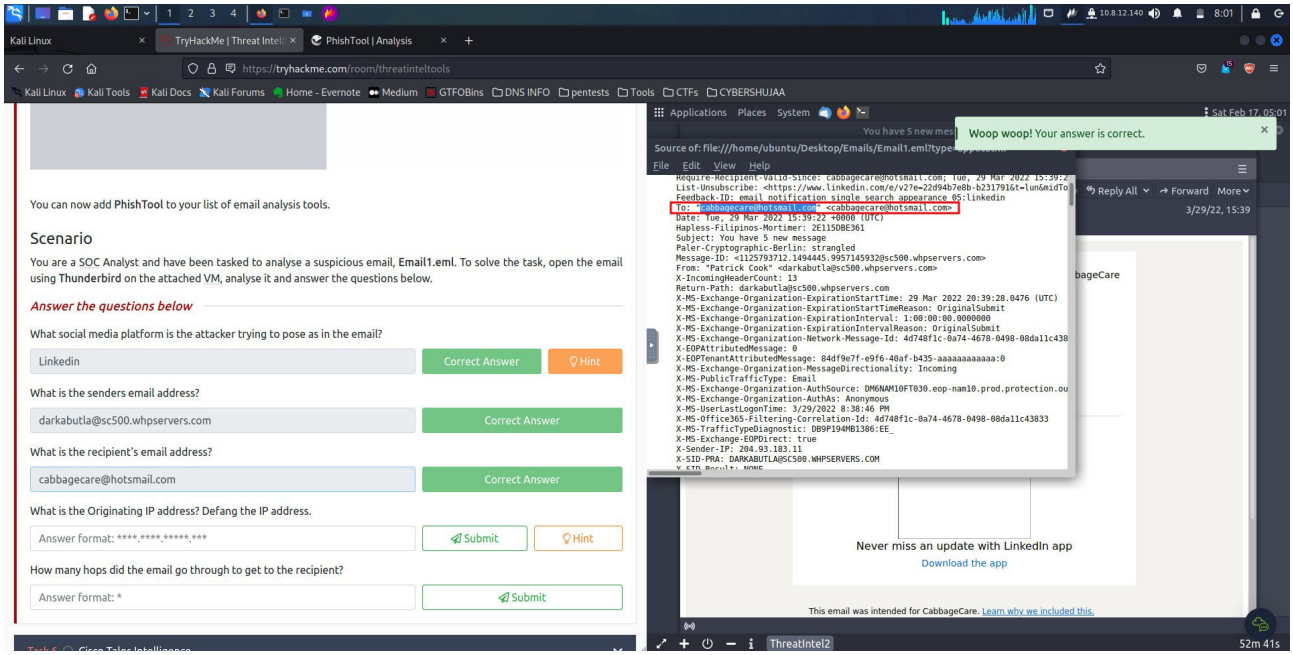
ANS: darkabutla@sc500.whpservers.com

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



What is the recipient's email address?

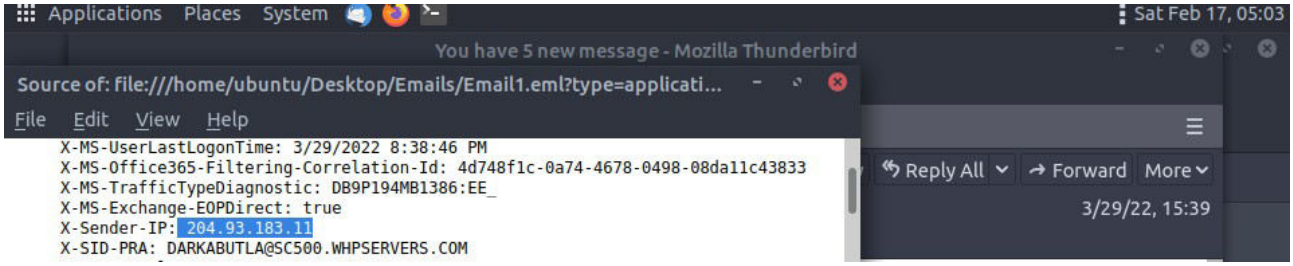
ANS: cabbagecare@hotsmail.com



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**

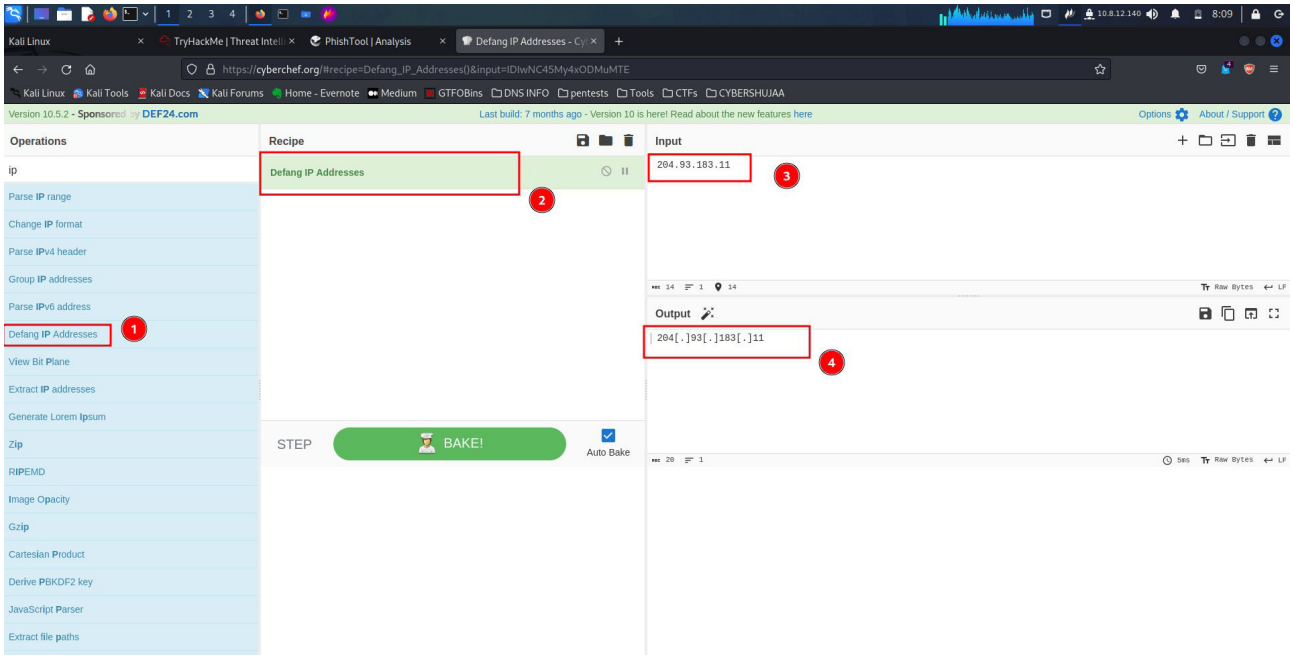


Next step was to defang the IP address.

What does Defanging an IP address mean?

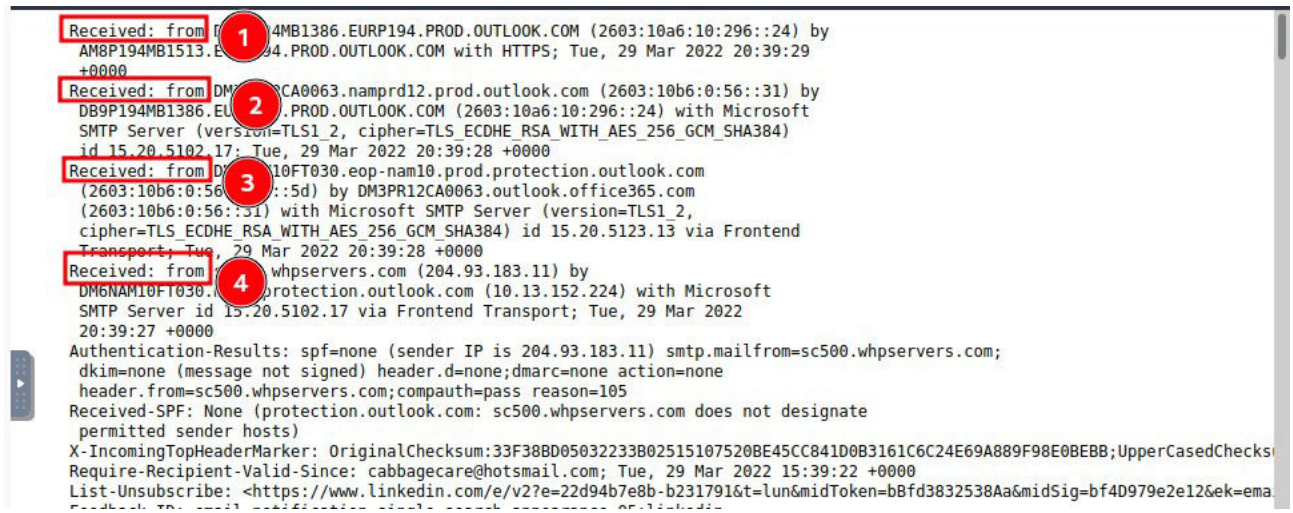
When sharing suspicious or malicious URLs, IP addresses, and email addresses, you don't want people to accidentally click those links. To prevent this, you defang the URLs or IP addresses, so that software doesn't convert them into clickable links.

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



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

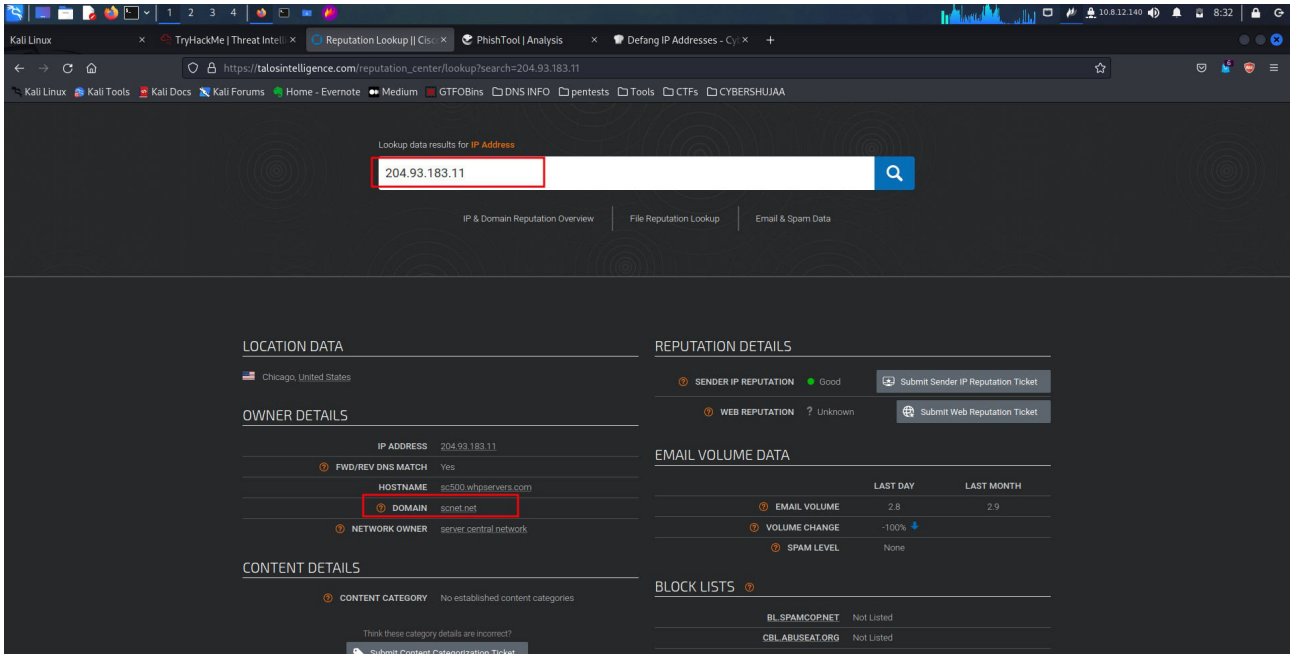
Use the information gathered from inspecting the Email1.eml file from Task 5 to answer the following questions using Cisco Talos Intelligence. Please note that the VM launched in Task 5 would not have access to the Internet.

Answer the questions below

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

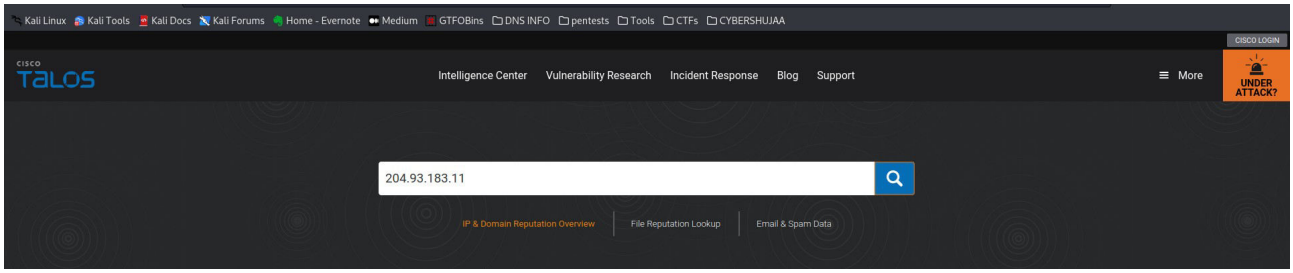
ANS: scnet.net

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.

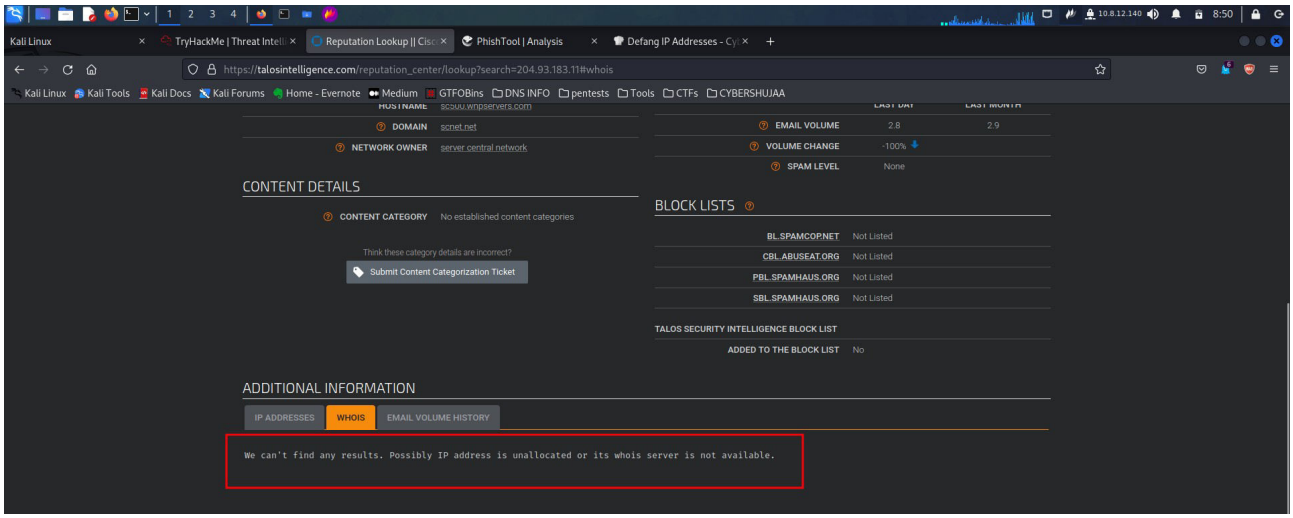


What is the customer name of the IP address?

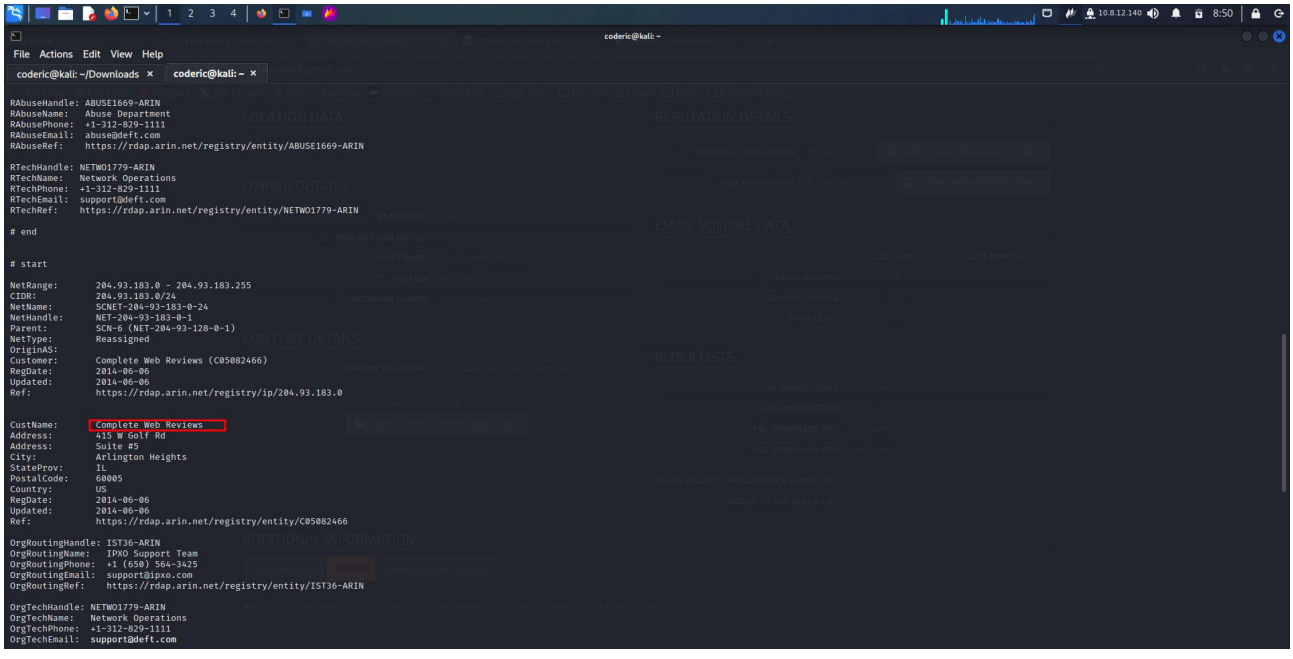
ANS: Complete Web Reviews



While using the Talos Intelligence platform, the whois tab didint 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

Task 7 ○ Scenario 1

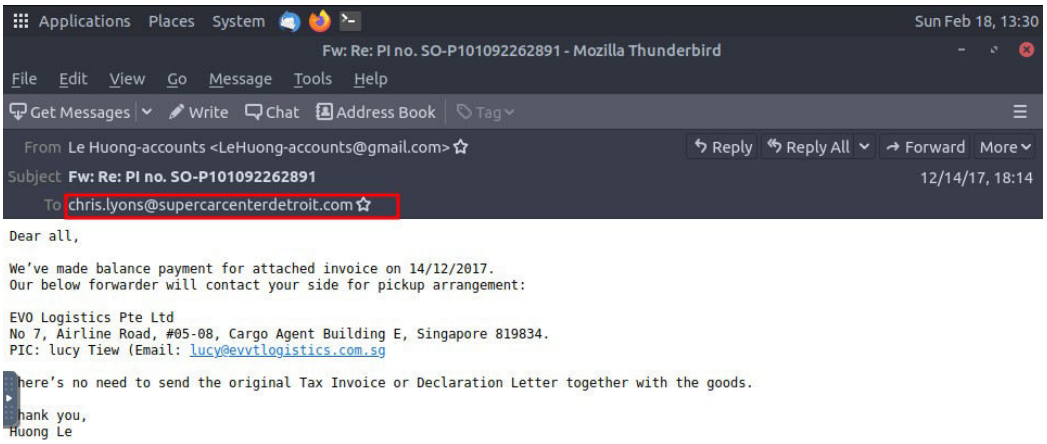
Scenario: You are a SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email to triage the incidents reported.

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

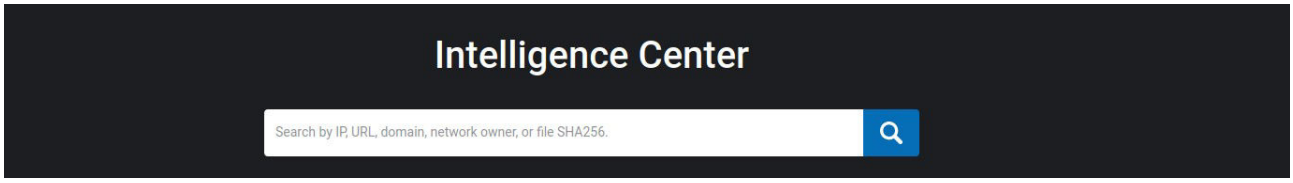


From Talos Intelligence, the attached file can also be identified by the Detection Alias that starts with an H…

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.

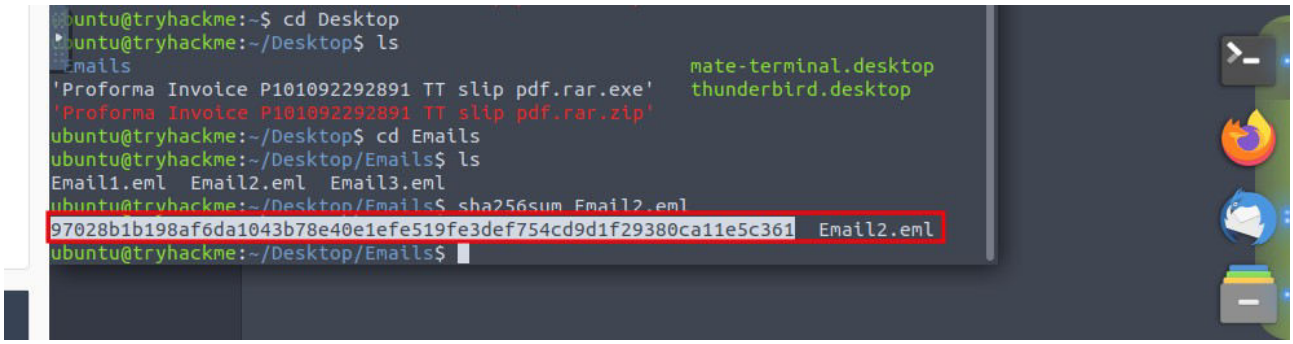
Talos Intelligence only runs a search on specific strings from the placeholder on the search bar they include:-



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

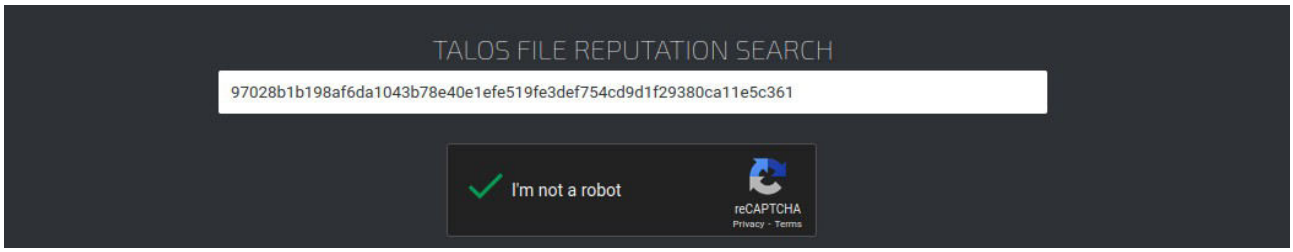
For this task since it was a file, I can get a sha256 value if there is one, so I went on to find if there was this kind of value using the attack box terminal.

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.

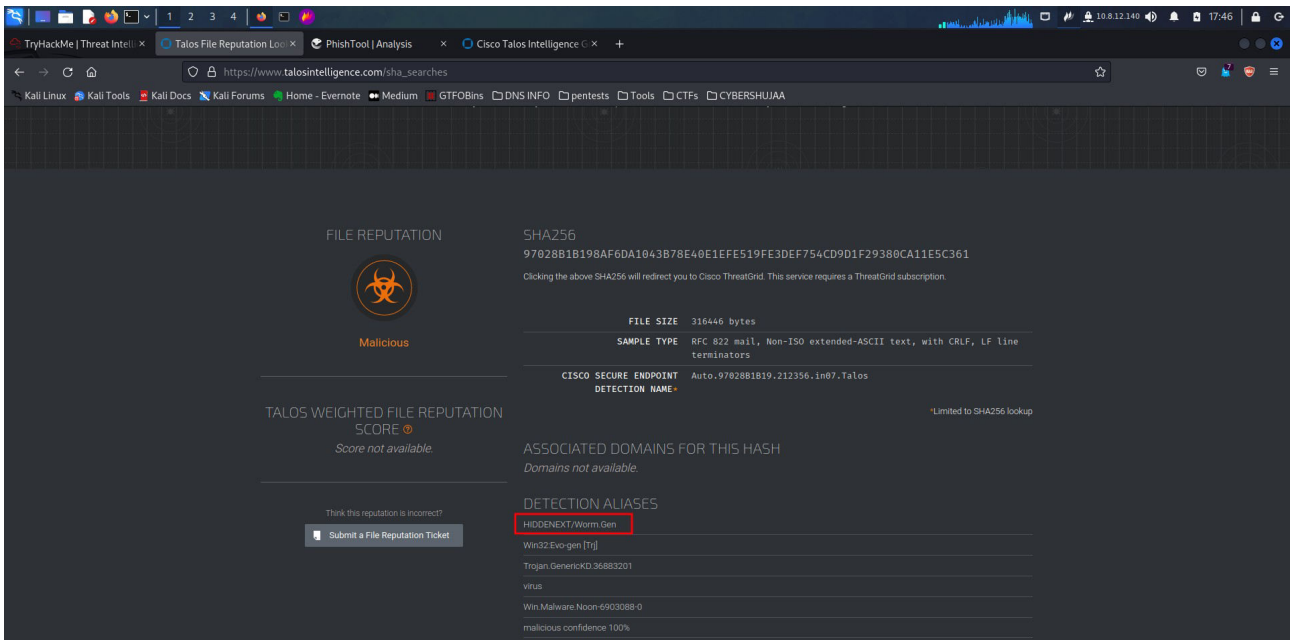


There it was a shs256 value which was:-
97028b1b198af6da1043b78e40e1efe519fe3def754cd9d1f29380ca11e5c361

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

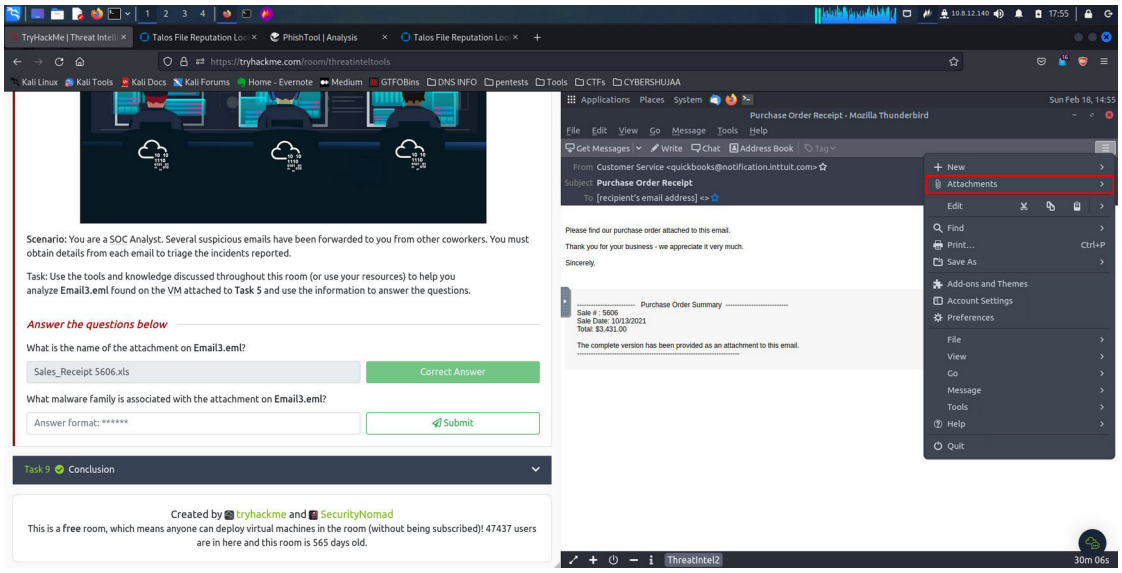
Scenario: You are a SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email to triage the incidents reported.

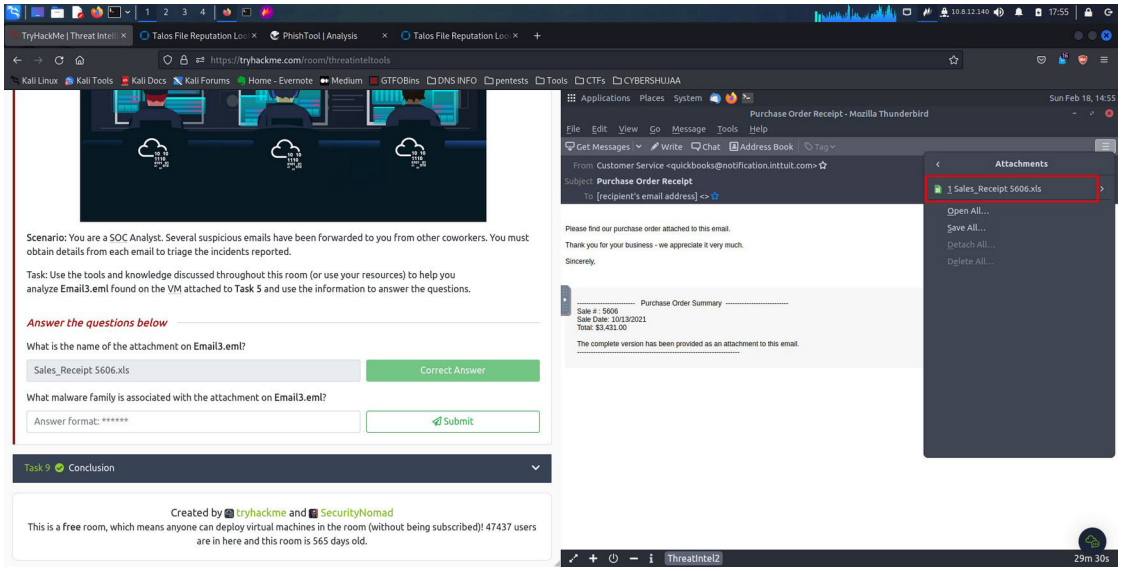
Task: Use the tools and knowledge discussed throughout this room (or use your resources) to help you analyze Email3.eml found on the VM attached to Task 5 and use the information to answer the questions.

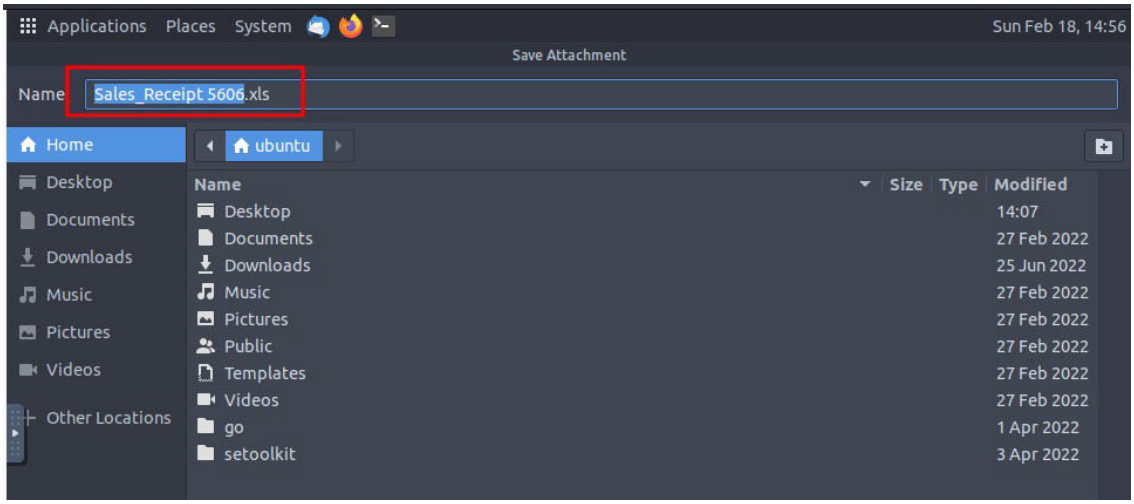
Answer the questions below

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.



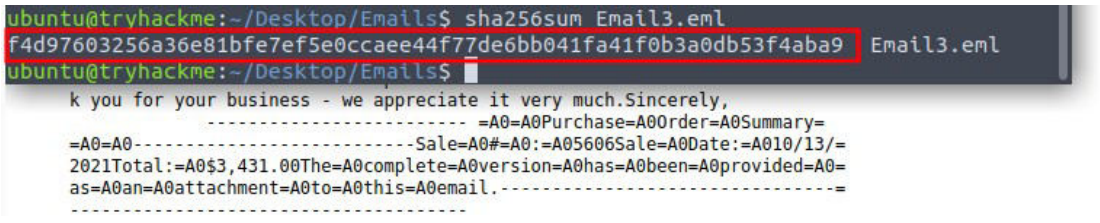




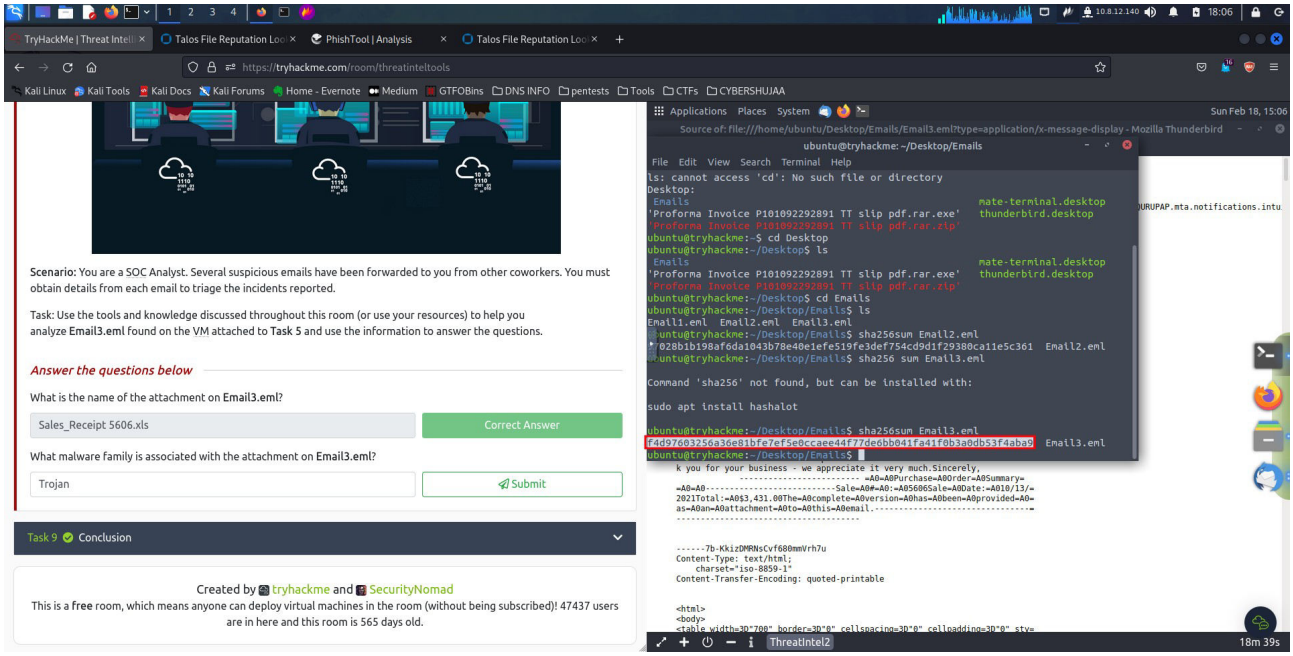
What malware family is associated with the attachment on Email3.eml?

Ans: Dridex

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

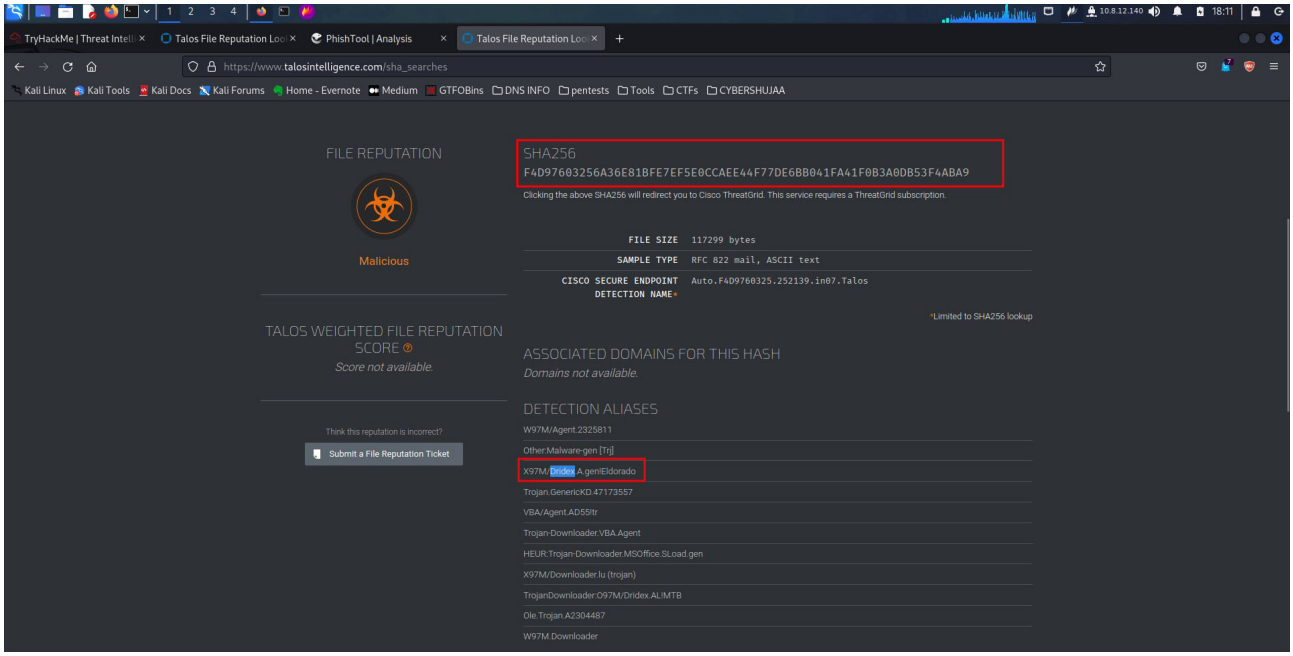


Sha256 value is:- **f4d97603256a36e81bfe7ef5e0ccaee44f77de6bb041fa41f0b3a0db53f4aba9**



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



Conclusion

In this lab several concepts of Threat Intelligence and various open-source tools that are useful in carrying out a good anaysis. 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.