TIMOTHY SEWE OGODE(CSSA0423076)

CYBER SHUJAA

WEEK 5

1. Threat intelligence tools

Table of Contents

[1. INTRODUCTION 2](#_Toc137584106)

[2. UrlScan.io 2](#_Toc137584107)

[Task 2](#_Toc137584108)

[3.Abuse.ch 3](#_Toc137584109)

[Task 3](#_Toc137584110)

[4.PhishTool 4](#_Toc137584111)

[Task 4](#_Toc137584112)

[5.Cisco Talos Intelligence 5](#_Toc137584113)

[Task 6](#_Toc137584114)

[6.Scenario 1 6](#_Toc137584115)

[Task 6](#_Toc137584116)

[7.Scenario 2 7](#_Toc137584117)

[Task 7](#_Toc137584118)

[3. CONCLUSION 7](#_Toc137584119)

# INTRODUCTION

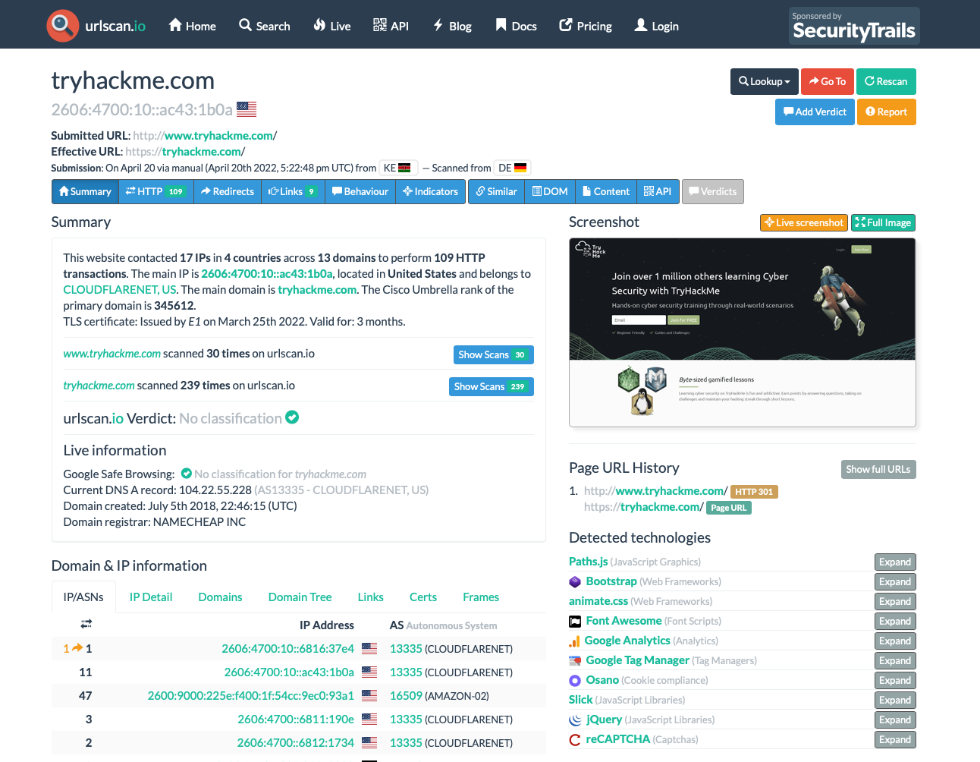
Threat Intelligence involves analyzing data to identify and mitigate risks from potential threats targeting organizations, industries, sectors, or governments. To effectively mitigate risks, it is important to understand the attackers, their motivations, capabilities, and indicators of compromise. Threat Intelligence can be classified into strategic, technical, tactical, and operational categories. Strategic Intelligence focuses on mapping risk areas based on emerging threats, while technical intelligence examines evidence of attacks to develop defense mechanisms. Tactical intelligence analyzes adversaries' tactics and procedures to enhance security controls, and operational intelligence investigates adversaries' motives and targets within an organization.

# UrlScan.io

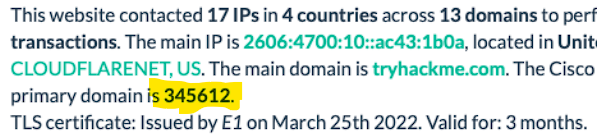
Urlscan.io is a free website scanning and analysis service. It automates the process of browsing and crawling websites to gather information such as contacted domains, IP addresses, requested resources, webpage snapshots, and utilized technologies. The site offers two views: recent scans and live scans. Scan results include essential areas like summary (IP address, domain details, page history, screenshot), HTTP connections, redirects, links, behavior (variables, cookies), and indicators (associated IPs, domains, hashes). Note that indicators do not necessarily indicate malicious activity.

### Task

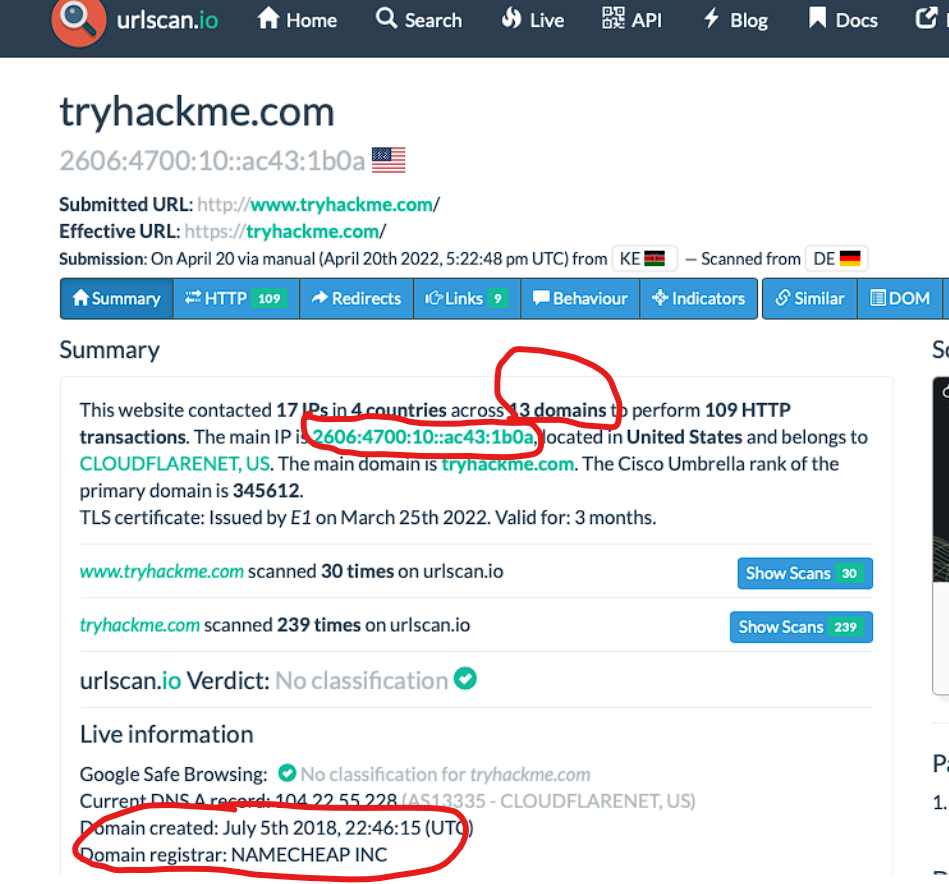
You have been tasked to perform a scan on TryHackMe's domain. The results obtained are displayed in the image below. Use the details on the image to answer the questions:



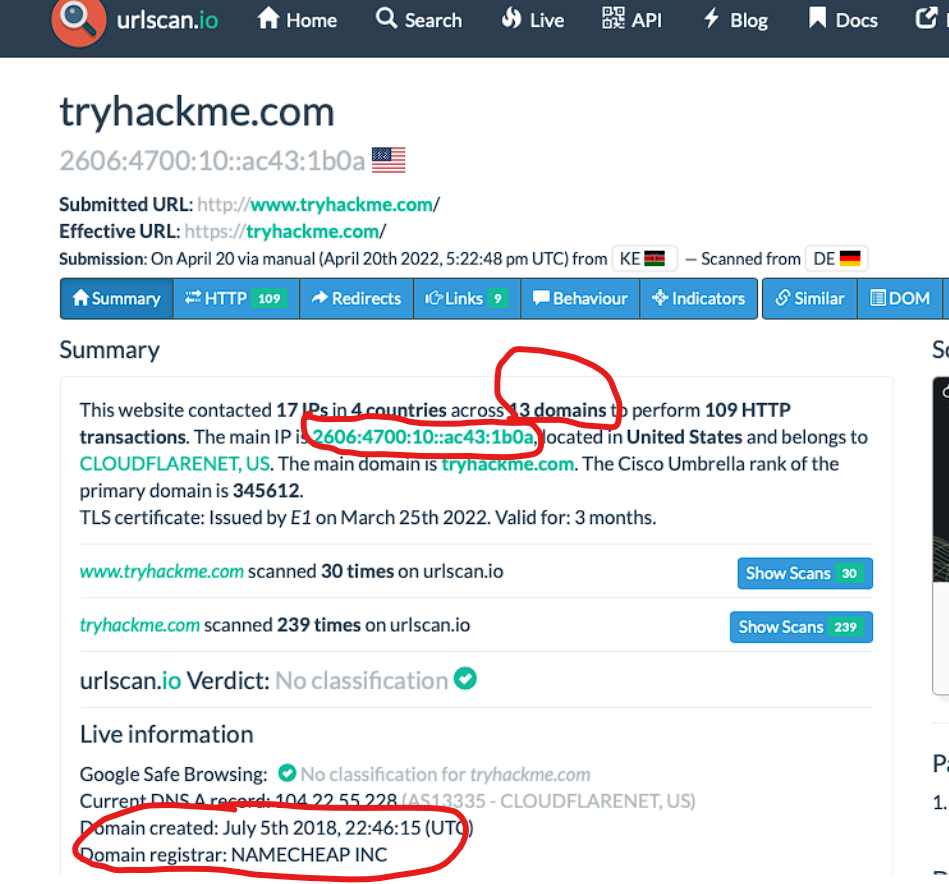
What is TryHackMe's Cisco Umbrella Rank? 345612



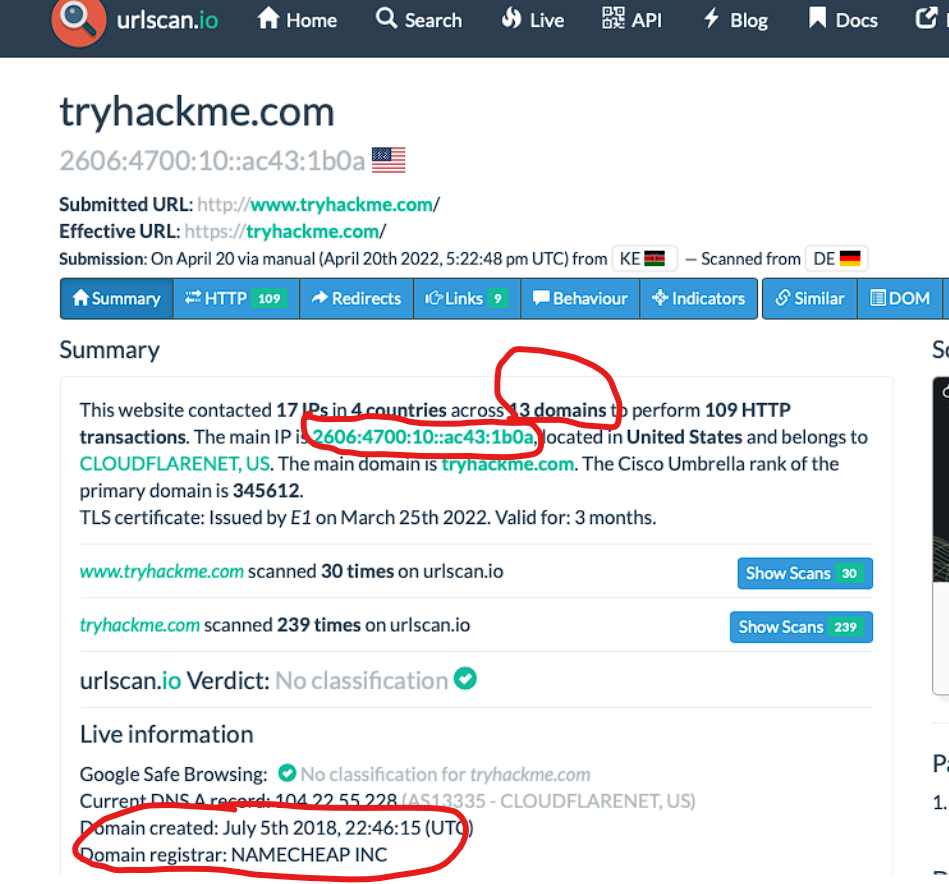
How many domains did UrlScan.io identify? 13 ()



What is the main domain registrar listed? NAMECHEAP INC



What is the main IP address identified? 2606:4700:10::ac43:1b0a

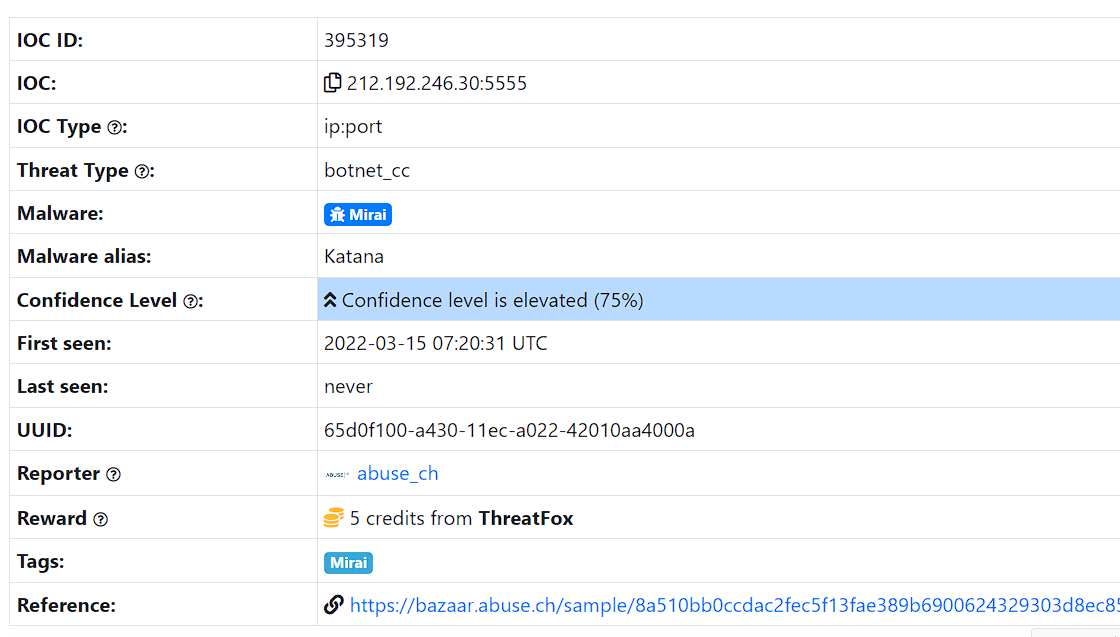


# 3.Abuse.ch

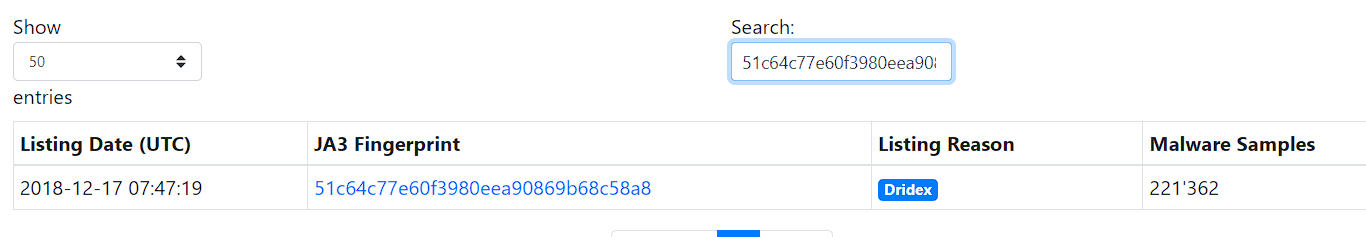
Abuse.ch tracks malware and botnets through multiple platforms. These platforms include Malware Bazaar for sharing malware samples, Feodo Tracker for monitoring botnet command and control infrastructure, SSL Blacklist for identifying malicious SSL certificates, URL Haus for sharing malware distribution sites, and ThreatFox for sharing indicators of compromise. Each platform offers specific features such as malware sample analysis, C&C server database search, SSL connection detection, malicious URL validation, and IOC export in various formats.

### Task

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



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

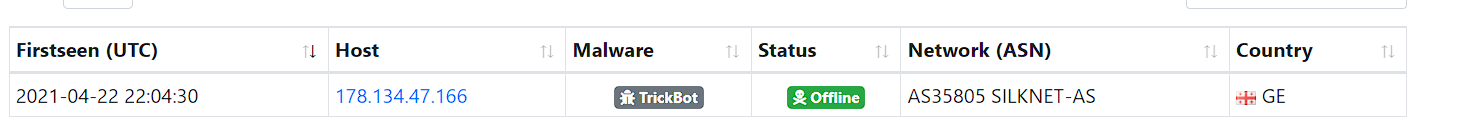


From the statistics page on URLHaus, what malware-hosting network has the ASN number AS14061?

DIGITALOCEAN-ASN



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



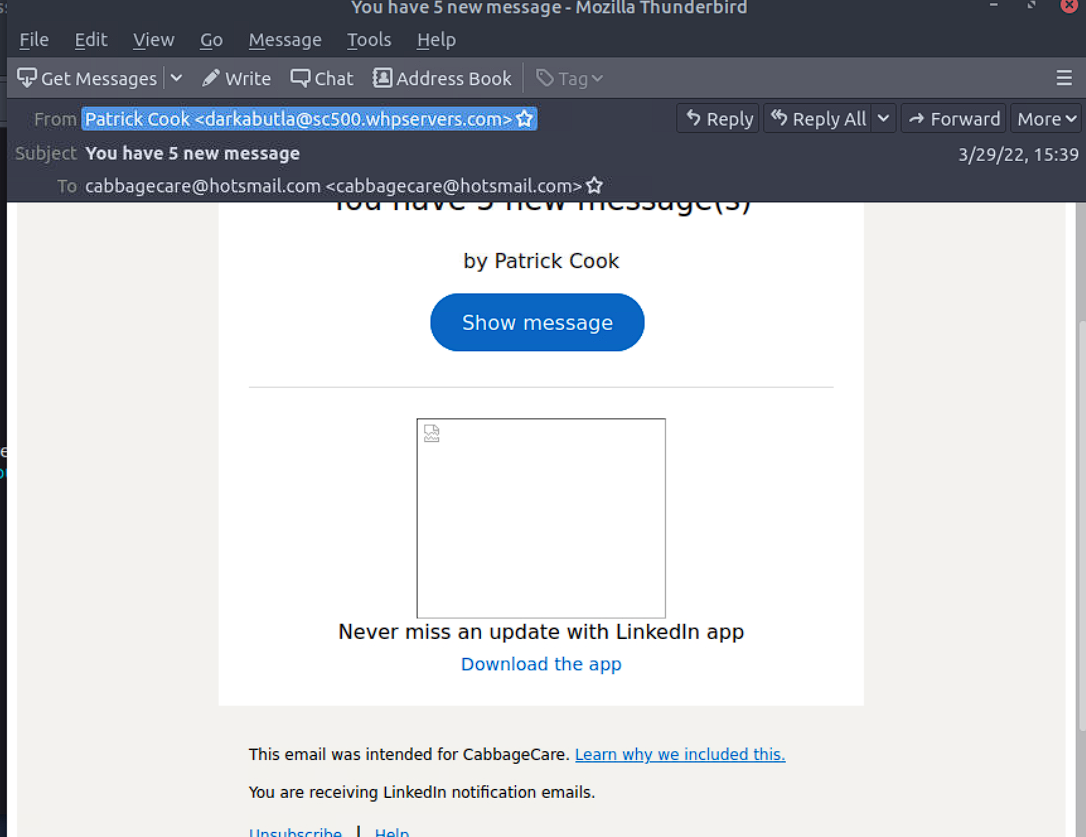
# 4.PhishTool

PhishTool is a tool that enhances email security and combats phishing attacks. It offers email analysis, heuristic intelligence, and classification features. The Community version focuses on email analysis, intelligence gathering, and reporting, while the Enterprise version includes additional features such as managing user-reported phishing events and integrating with Microsoft 365 and Google Workspace. The interface provides tabs for analysis, history, and in-tray, with details on email headers, received lines, security frameworks, attachments, and message URLs. The Resolve feature allows for email classification and artifact flagging.

### Task

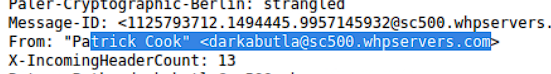
You are a SOC Analyst and have been tasked to analyse a suspicious email Email1.eml. With the skills learnt on this task and using Thunderbird, answer the questions below.

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

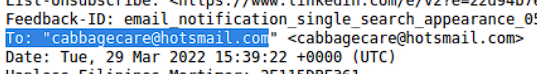


What is the senders email address? darkabutla@sc500.whpservers.com

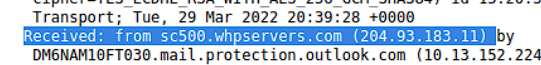
After opening headers you can get all this info. Ans= darkabutla@sc500.whpservers.com



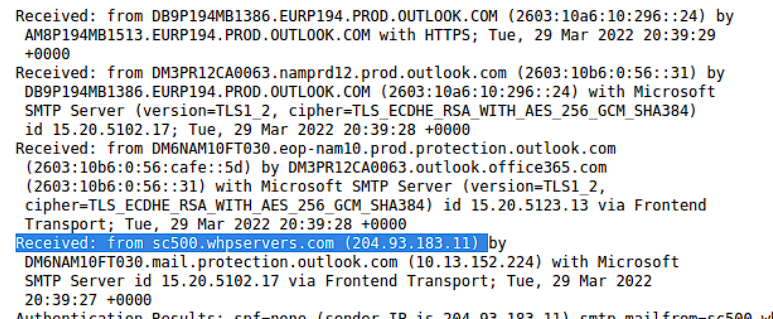
What is the recipient's email address? Ans= [cabbagecare@hotsmail.com](mailto:cabbagecare@hotsmail.com)



What is the Originating IP address? Defang the IP address. ans=204[.]93[.]183[.]11(go to cyberchef)



How many hops did the email go through to get to the recipient? Ans=4



# 5.Cisco Talos Intelligence

Cisco Talos is a team within Cisco that collects and analyses data to provide threat intelligence and protection against emerging threats. It consists of six teams focused on threat intelligence, detection research, engineering, vulnerability research, communities, and global outreach. Talos Intelligence offers a reputation lookup dashboard and tabs for accessing vulnerability information and searchable threat data. The dashboard provides an overview of email traffic across countries, indicating whether emails are legitimate, spam, or malware. The vulnerability information tab includes disclosed and zero-day vulnerability reports, while the reputation centre allows for searching threat data related to IPs and files.

### Task

What is the listed domain of the IP address from the previous task? Ans : scnet.net

What is the customer name of the IP address? Ans : Complete Web Reviews

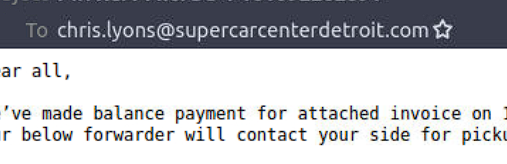
# 6.Scenario 1

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

### Task

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

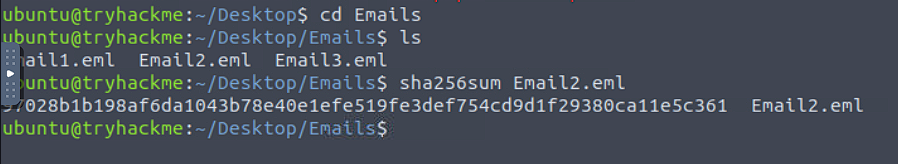
According to Email2.eml, what is the recipient's email address? Ans=chris.lyons@supercarcenterdetroit.com

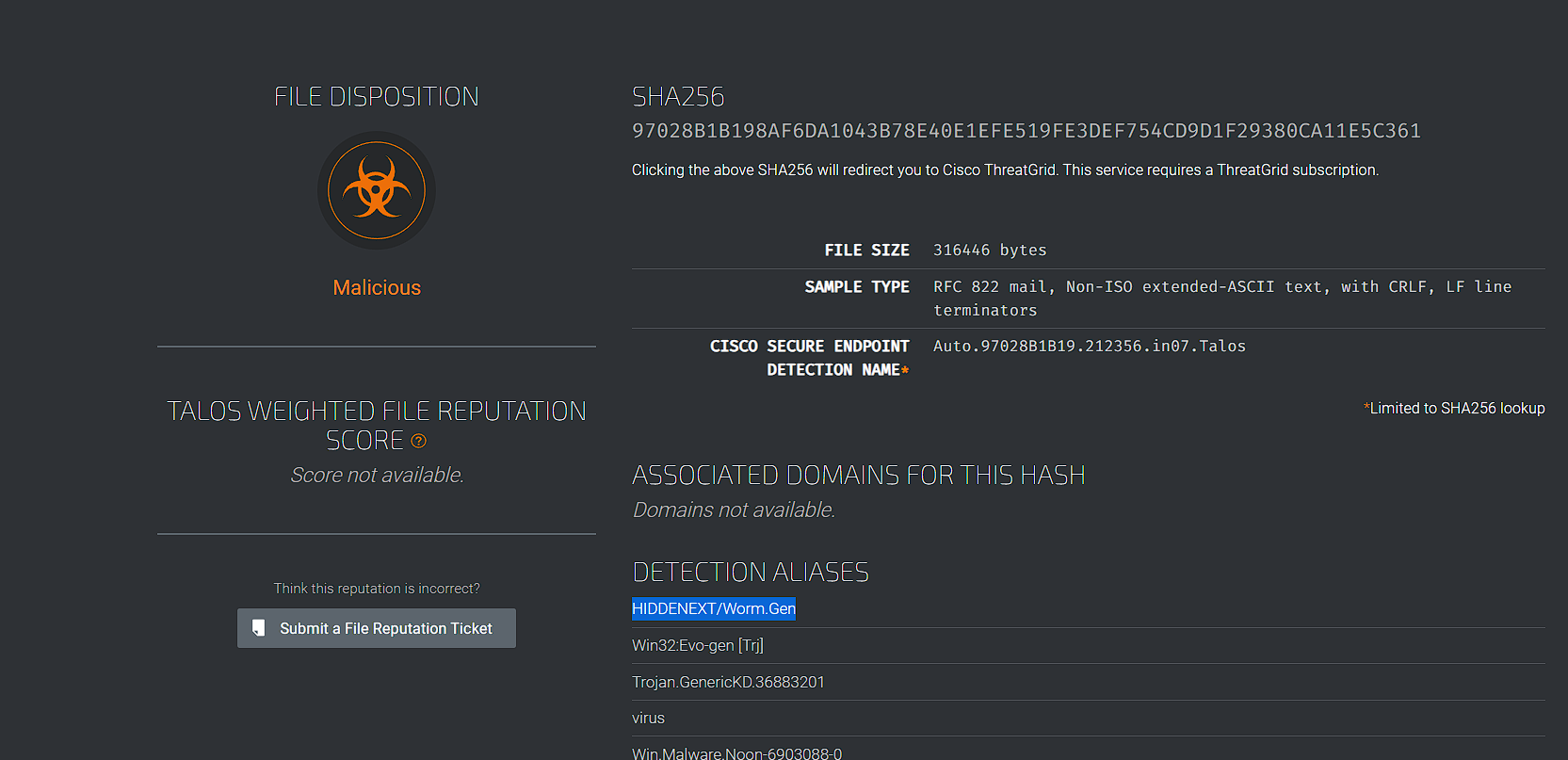


From Talos Intelligence, the attached file can also be identified by the Detection Alias that starts with an H... ans= HIDDENEXT/Worm.Gen

Get the has value first 97028b1b198af6da1043b78e40e1efe519fe3def754cd9d1f29380ca11e5c361

Then look it up in Talos and look for an alias that starts with H





# 7.Scenario 2

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

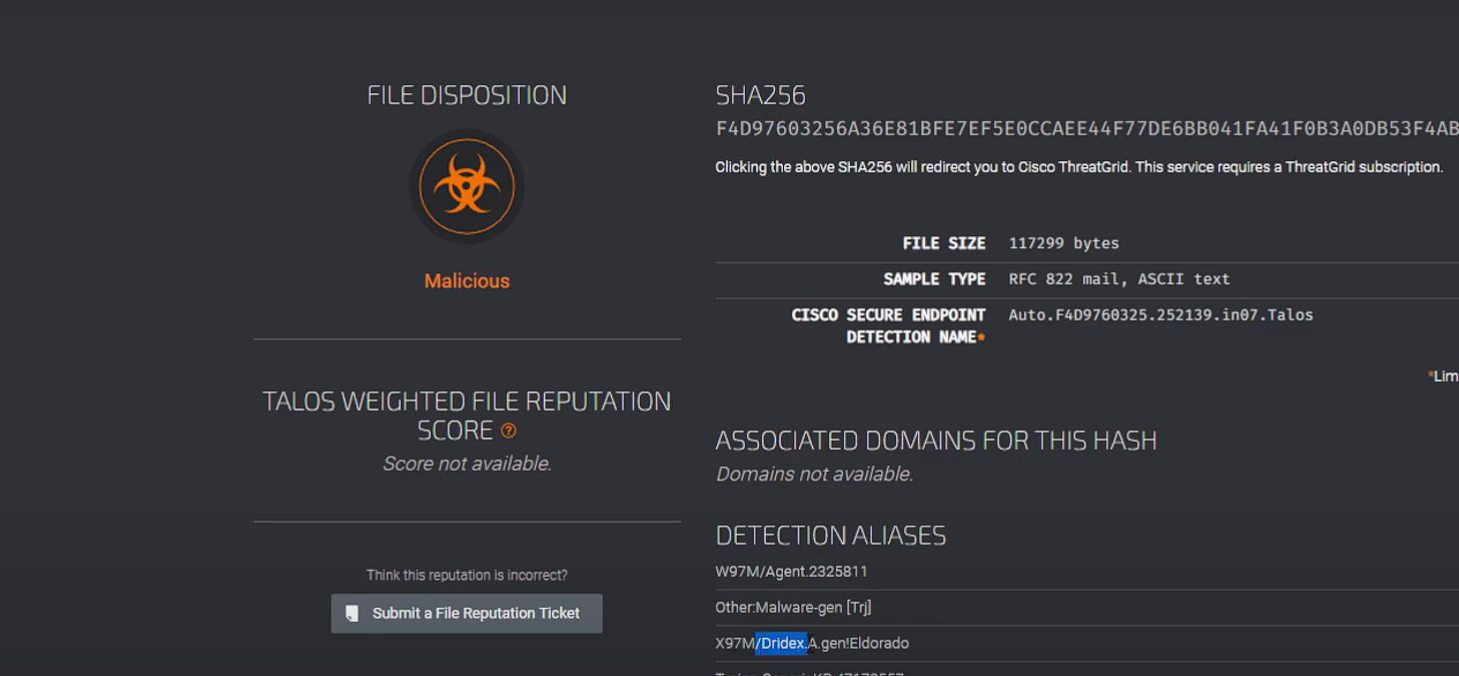
### Task

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

What is the name of the attachment on Email3.eml? Sales\_Receipt 5606.xls

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

Same process to get the hash as above.



# CONCLUSION

In conclusion, we have explored various topics related threat intelligence. We discussed the importance of threat intelligence in mitigating risks and understanding adversaries. We learned about tools like Urlscan.io for website scanning and analysis, Abuse.ch's platforms for tracking malware and botnets, and PhishTool for combating email phishing. Additionally, we discovered Cisco Talos as a leading provider of threat intelligence, offering actionable insights and protection against emerging threats. These discussions highlight the significance of staying informed, proactive, and leveraging advanced tools and intelligence to enhance cybersecurity measures. [**LINK**](https://tryhackme.com/p/Timothy254)

