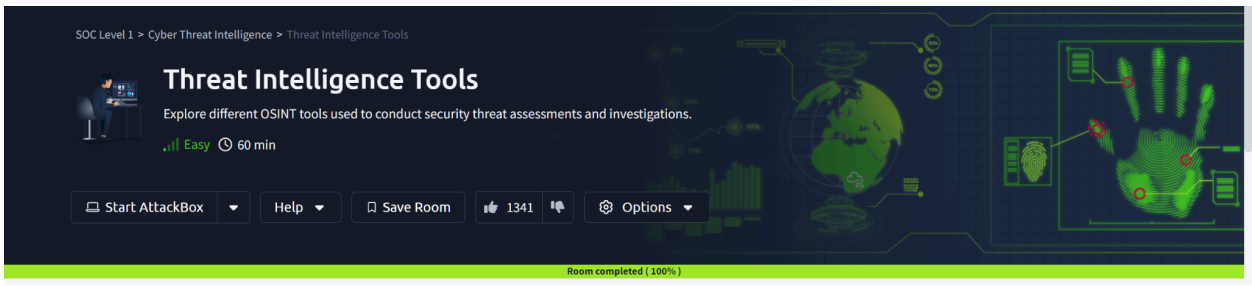
THREAT INTELLIGENCE TOOLS

ASSIGNMENT REPORT



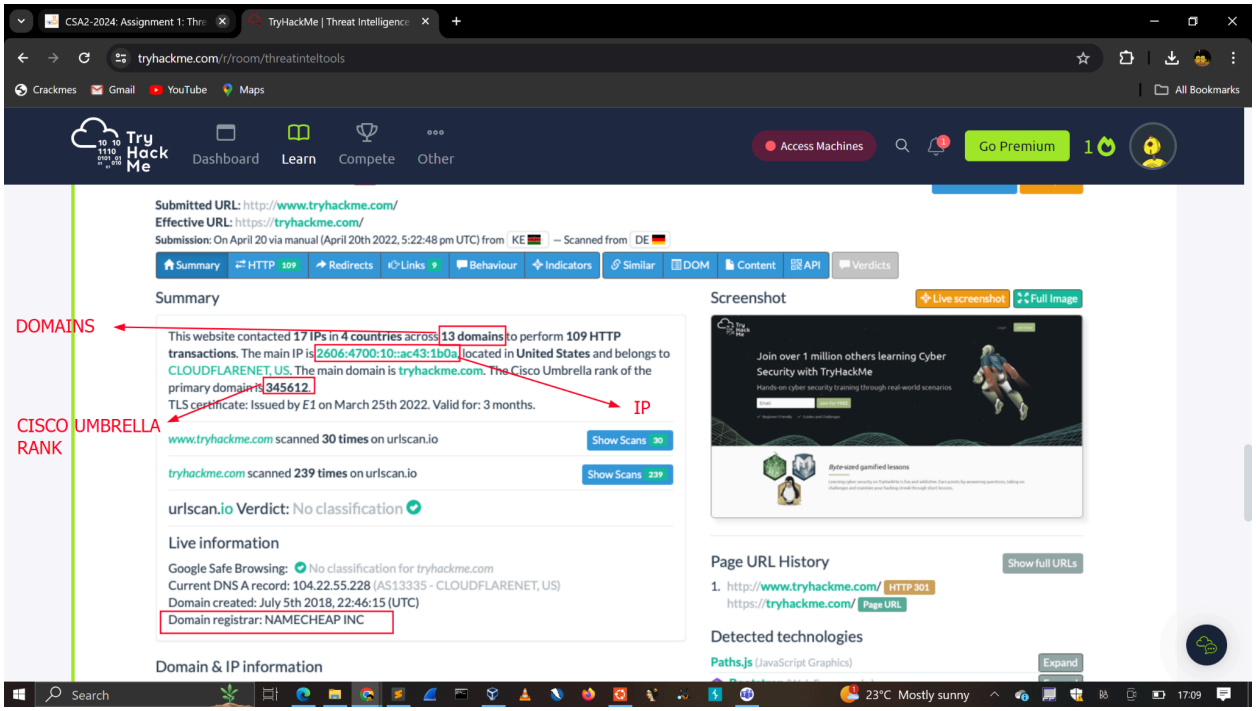
Peter Kinyumu,
cs-sa07-24067,
June 9th, 2024

1. INTRODUCTION

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

2. ANSWERS TO QUESTIONS

Urlscan.io



The screenshot above highlights the answers to the questions below:

a. **What was TryHackMe's Cisco Umbrella Rank based on the screenshot?**
   345612
b. **How many domains did UrlScan.io identify on the screenshot?**
   13 domains.
c. **What was the main domain registrar listed on the screenshot?**
   NAMECHEAP INC
d. **What was the main IP address identified for TryHackMe on the screenshot?**
   2606:4700:10::ac43:1b0a

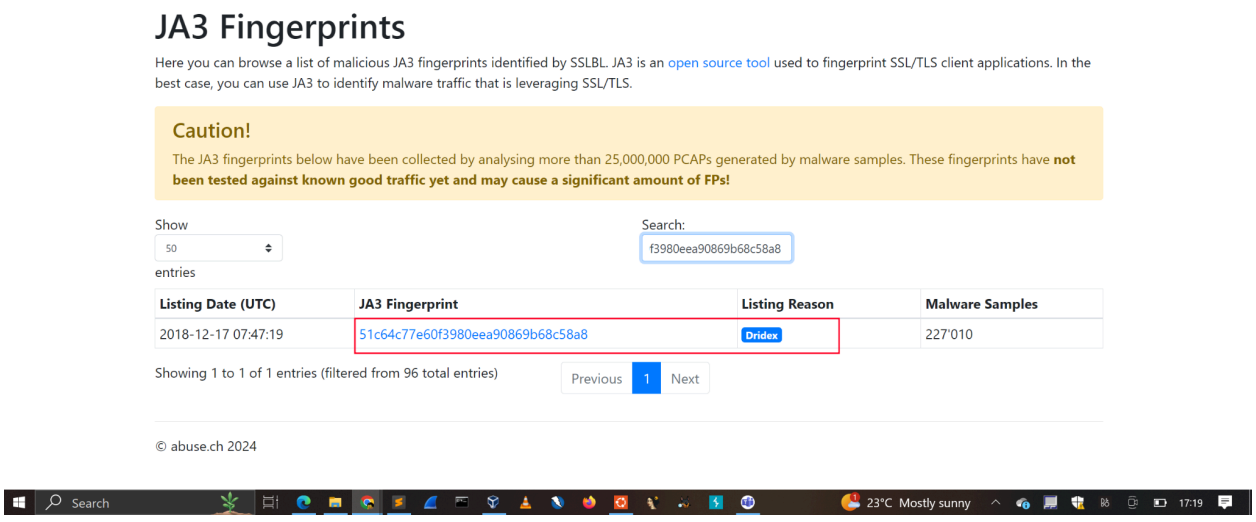
Abuse.ch

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

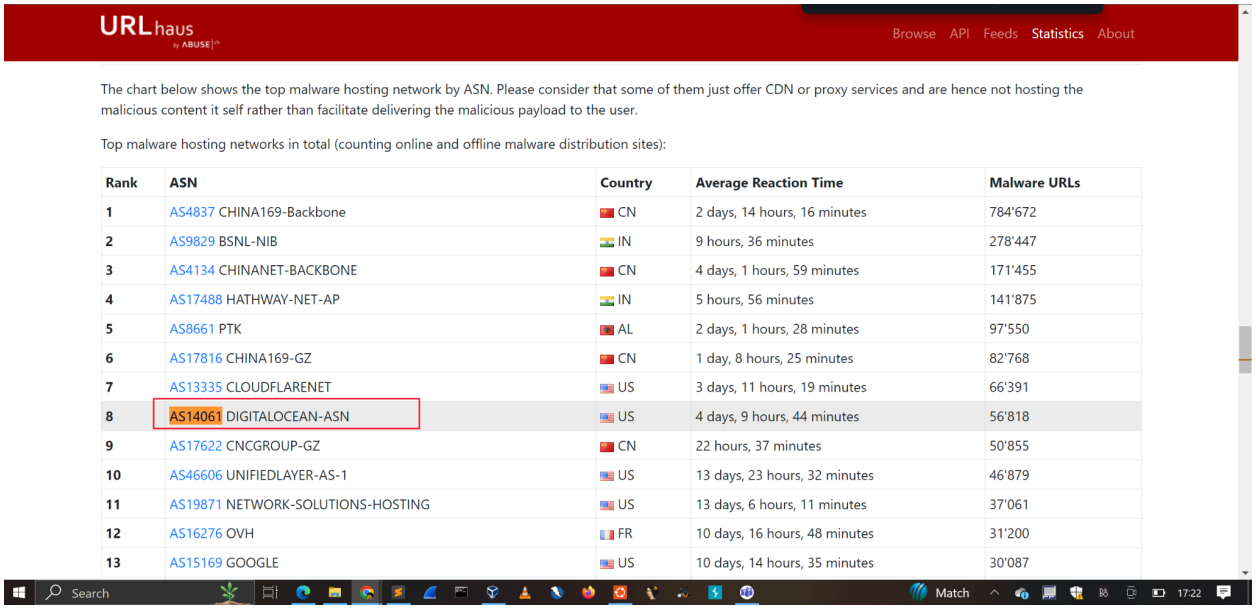
Mirai

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

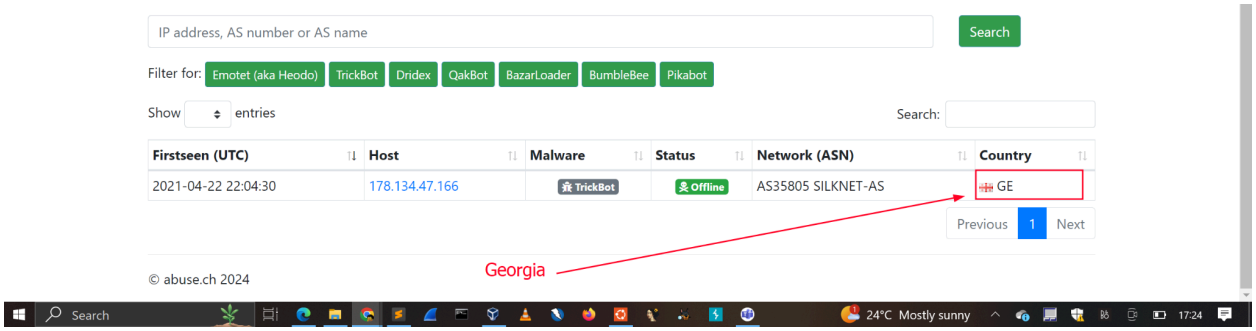
Dridex



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



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



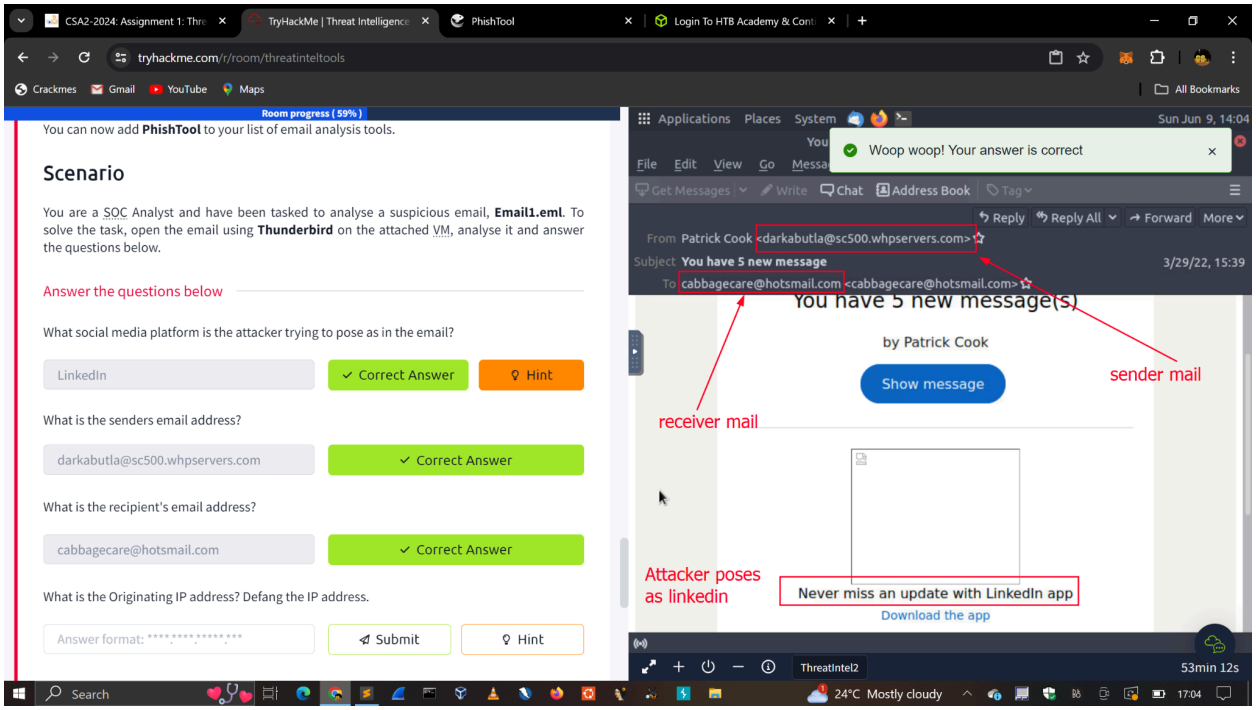
Phishtool

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

b. **What is the sender's email address?**
darkabutla@sc500.whpservers.com

c. **What is the recipient's email address?**
cabbagecare@hotsmail.com

The screenshot below showcases the answers to the questions above.

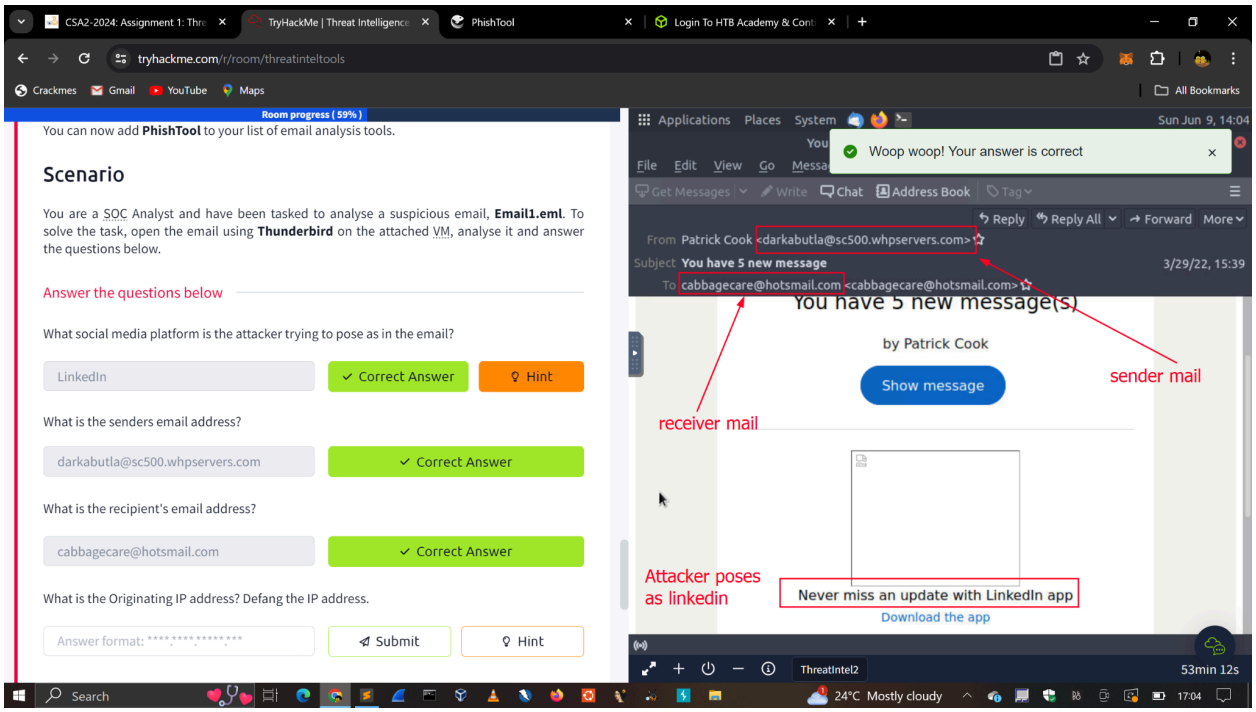


d. What is the Originating IP address? Defang the IP address.

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

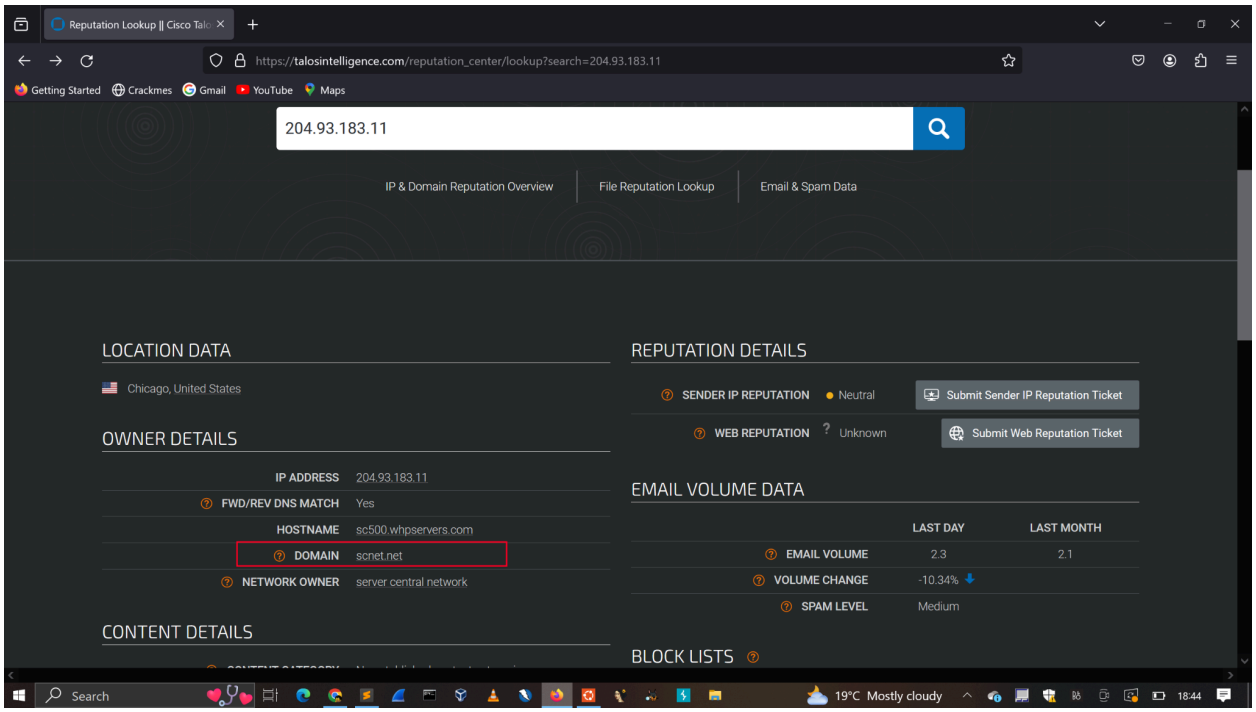
e. How many hops did the email go through to get to the recipient?

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



Cisco Talos Intelligence

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



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

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

Scenario 1

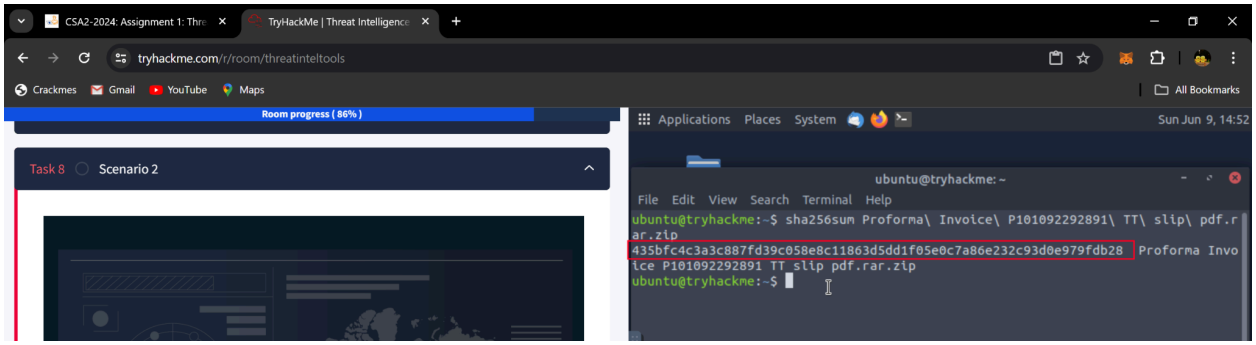
You are a SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email to triage the incidents reported.

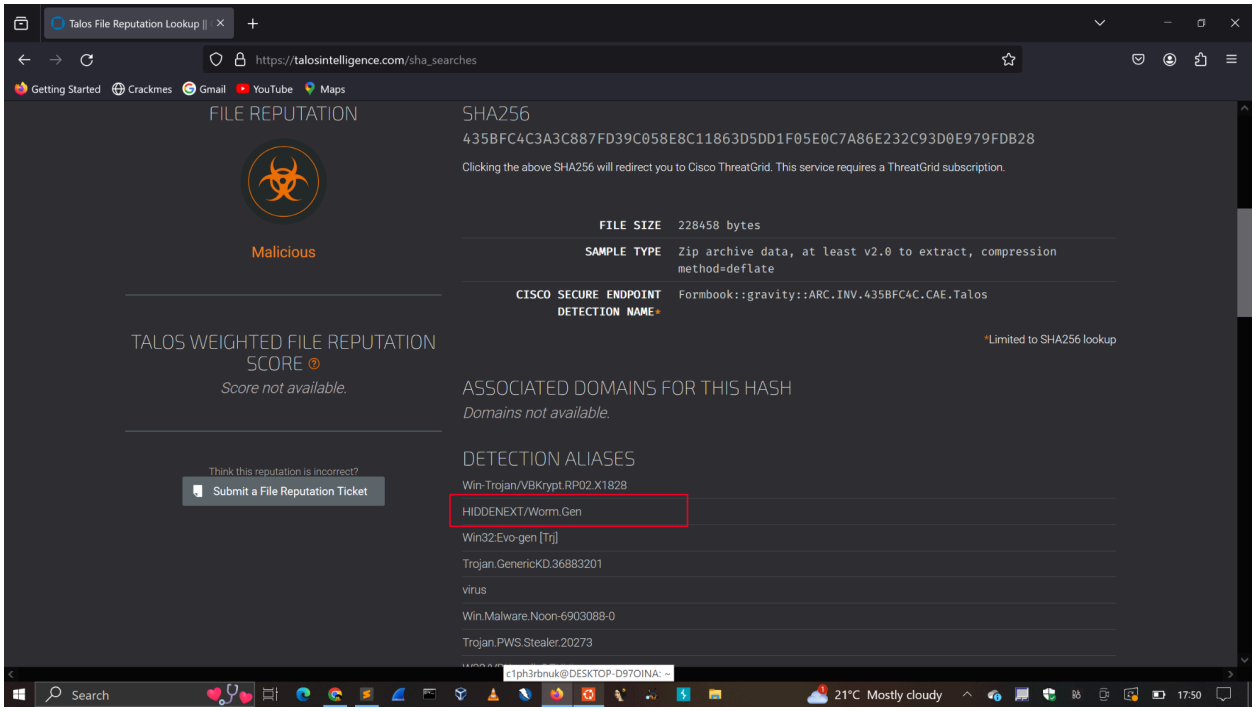
Task: Use the tools and knowledge discussed throughout this room (or use your resources) to help you analyze **Email2.eml** found on the VM attached to **Task 5** and use the information to answer the questions.

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

chris.lyons@supercarcenterdetroit.com

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



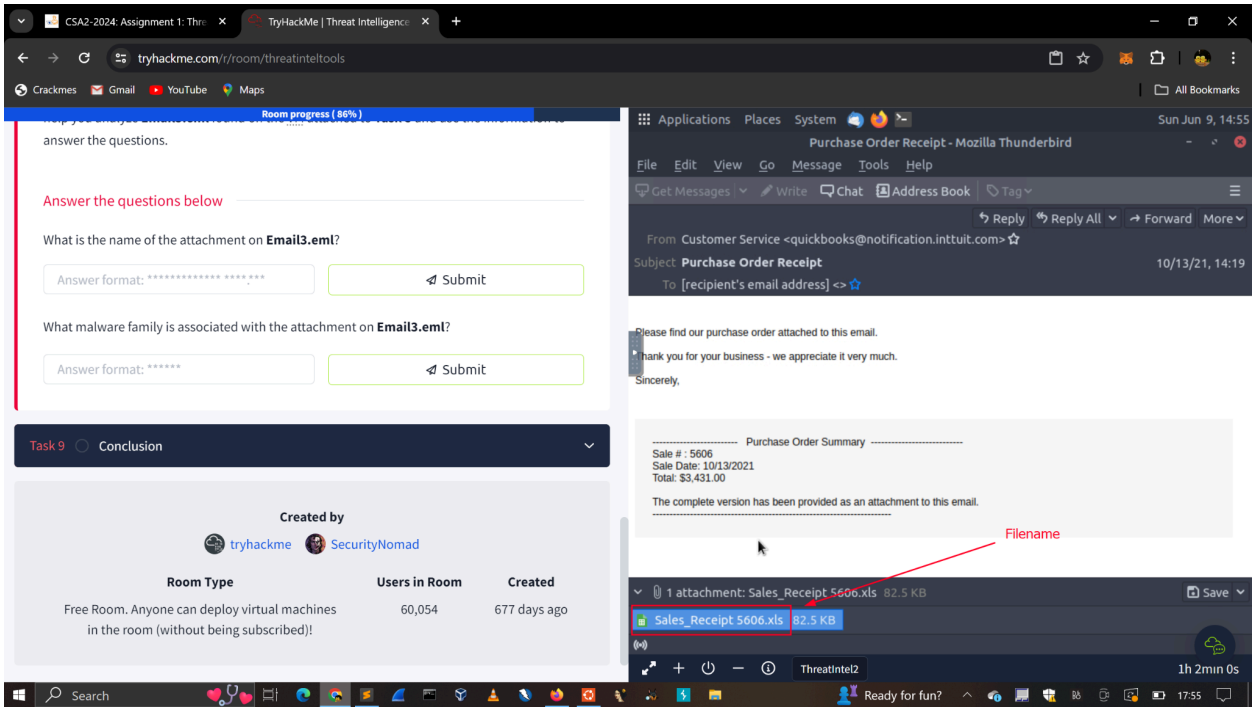


Scenario 2

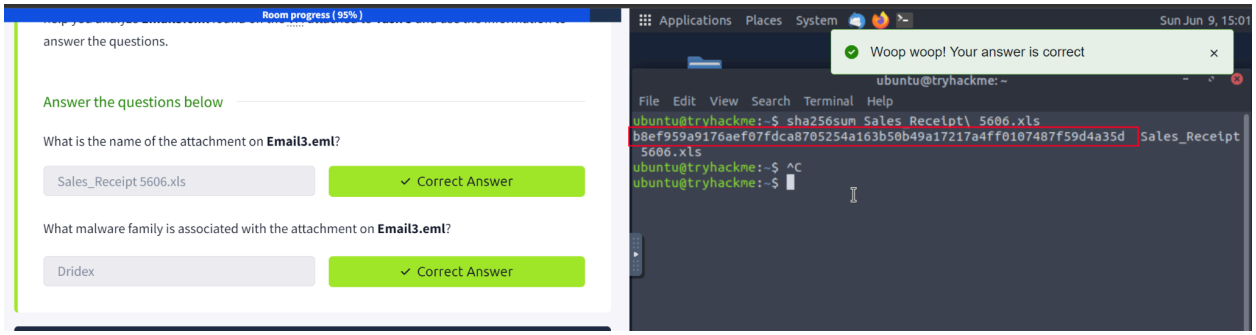
You are a SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email to triage the incidents reported.

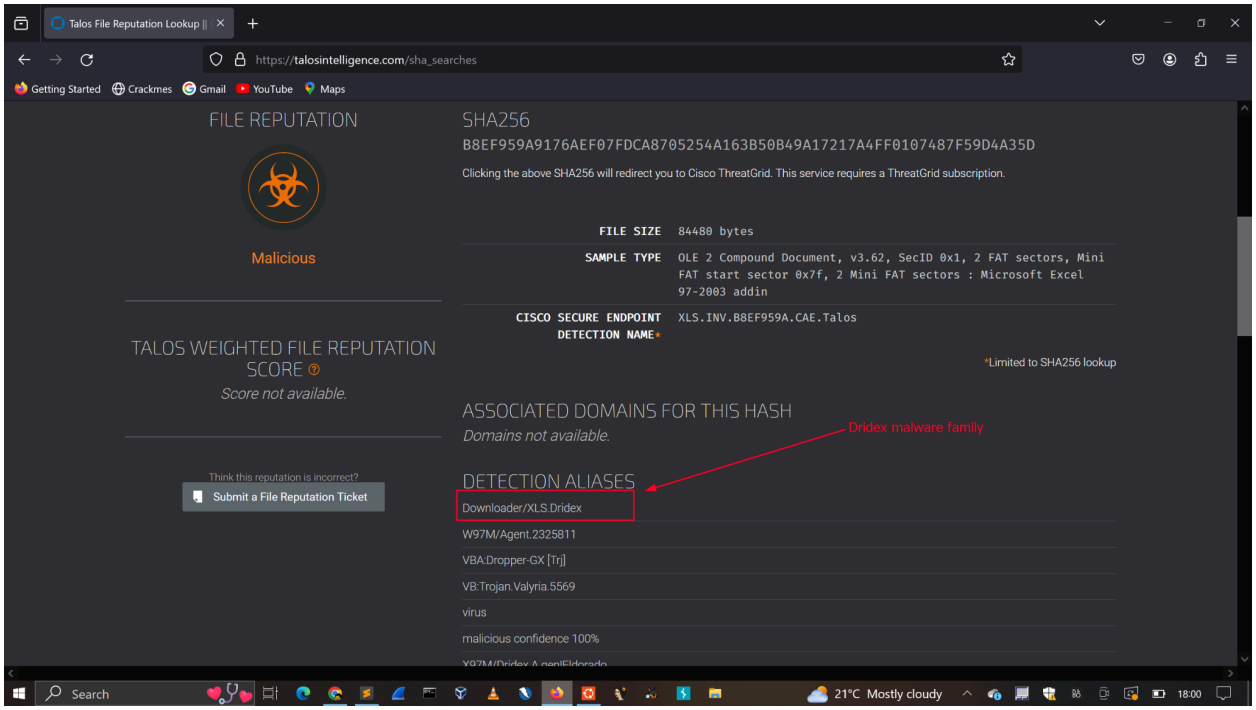
Task: Use the tools and knowledge discussed throughout this room (or use your resources) to help you analyze Email3.eml found on the VM attached to Task 5 and use the information to answer the questions.

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



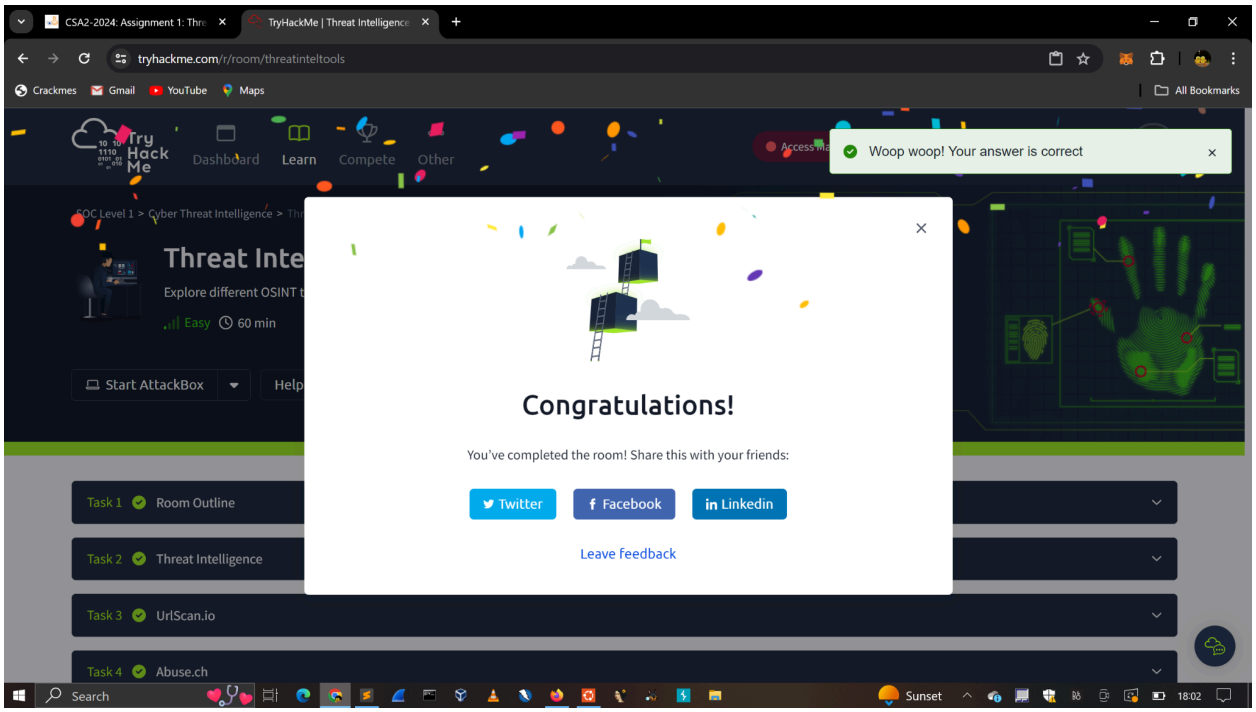
b. What malware family is associated with the attachment on Email3.eml?





3. MODULE COMPLETION

https://tryhackme.com/p/c1ph3rbnuk



4. CONCLUSION

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