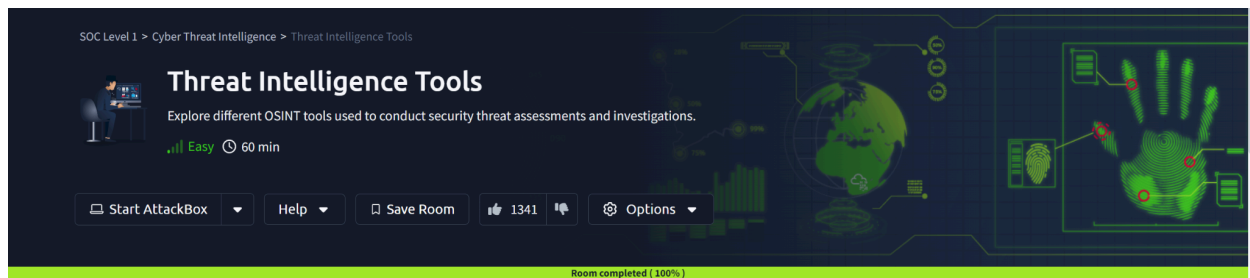


THREAT INTELLIGENCE TOOLS

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 displays the Urlscan.io analysis for the URL `http://www.tryhackme.com/`. Key information highlighted includes:

- Summary:** The 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 the United States and belongs to CLOUDFLARENET.US. The main domain is tryhackme.com. The Cisco Umbrella rank of the primary domain is 345612. The TLS certificate is issued by E1 on March 25th 2022, valid for 3 months.
- Scans:** www.tryhackme.com scanned 30 times on urlscan.io; tryhackme.com scanned 239 times on 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.
- Page URL History:** 1. `http://www.tryhackme.com/` (HTTP 301); `https://tryhackme.com/` (Page URL).
- Detected technologies:** Paths.js (JavaScript Graphics).

The screenshot above highlights the answers to the questions below:

- What was TryHackMe's Cisco Umbrella Rank based on the screenshot?**
345612
- How many domains did UrlScan.io identify on the screenshot?**
13 domains.
- What was the main domain registrar listed on the screenshot?**
NAMECHEAP INC
- 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

ThreatFox Database

Indicators of Compromise (IOCs) on ThreatFox are associated with a certain malware family. A malware sample can be associated with only one malware family. The page below gives you an overview on indicators of compromise associated with [elf.mirai](#).

You can also get this data through the [ThreatFox API](#).

Database Entry

Malware:	Mirai
Malware alias:	Katana
First seen:	2020-12-27 07:34:56 UTC
Last seen:	2024-05-31 06:25:21 UTC
Number of IOCs:	19'693
Malpedia:	https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai

of IOCs

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

Dridex

JA3 Fingerprints

Here you can browse a list of malicious JA3 fingerprints identified by SSLBL. JA3 is an [open source tool](#) used to fingerprint SSL/TLS client applications. In the best case, you can use JA3 to identify malware traffic that is leveraging SSL/TLS.

Caution!

The JA3 fingerprints below 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!**

Show: 50 entries

Search: f3980eea90869b68c58a8

Listing Date (UTC)	JA3 Fingerprint	Listing Reason	Malware Samples
2018-12-17 07:47:19	51c64c77e60f3980eea90869b68c58a8	Dridex	227'010

Showing 1 to 1 of 1 entries (filtered from 96 total entries)

Previous 1 Next

© abuse.ch 2024

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

The chart below shows the top malware hosting network by ASN. Please consider that some of them just offer CDN or proxy services and are hence not hosting the malicious content it self rather than facilitate delivering the malicious payload to the user.

Top malware hosting networks in total (counting online and offline malware distribution sites):

Rank	ASN	Country	Average Reaction Time	Malware URLs
1	AS4837 CHINA169-Backbone	CN	2 days, 14 hours, 16 minutes	784'672
2	AS9829 BSNL-NIB	IN	9 hours, 36 minutes	278'447
3	AS4134 CHINANET-BACKBONE	CN	4 days, 1 hours, 59 minutes	171'455
4	AS17488 HATHWAY-NET-AP	IN	5 hours, 56 minutes	141'875
5	AS8661 PTK	AL	2 days, 1 hours, 28 minutes	97'550
6	AS17816 CHINA169-GZ	CN	1 day, 8 hours, 25 minutes	82'768
7	AS13335 CLOUDFLARENET	US	3 days, 11 hours, 19 minutes	66'391
8	AS14061 DIGITALOCEAN-ASN	US	4 days, 9 hours, 44 minutes	56'818
9	AS17622 CNCGROUP-GZ	CN	22 hours, 37 minutes	50'855
10	AS46606 UNIFIEDLAYER-AS-1	US	13 days, 23 hours, 32 minutes	46'879
11	AS19871 NETWORK-SOLUTIONS-HOSTING	US	13 days, 6 hours, 11 minutes	37'061
12	AS16276 OVH	FR	10 days, 16 hours, 48 minutes	31'200
13	AS15169 GOOGLE	US	10 days, 14 hours, 35 minutes	30'087

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

IP address, AS number or AS name

Filter for: Emotet (aka Heodo) TrickBot Dridex QakBot BazarLoader BumbleBee Pikabot

Show 1 entries

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

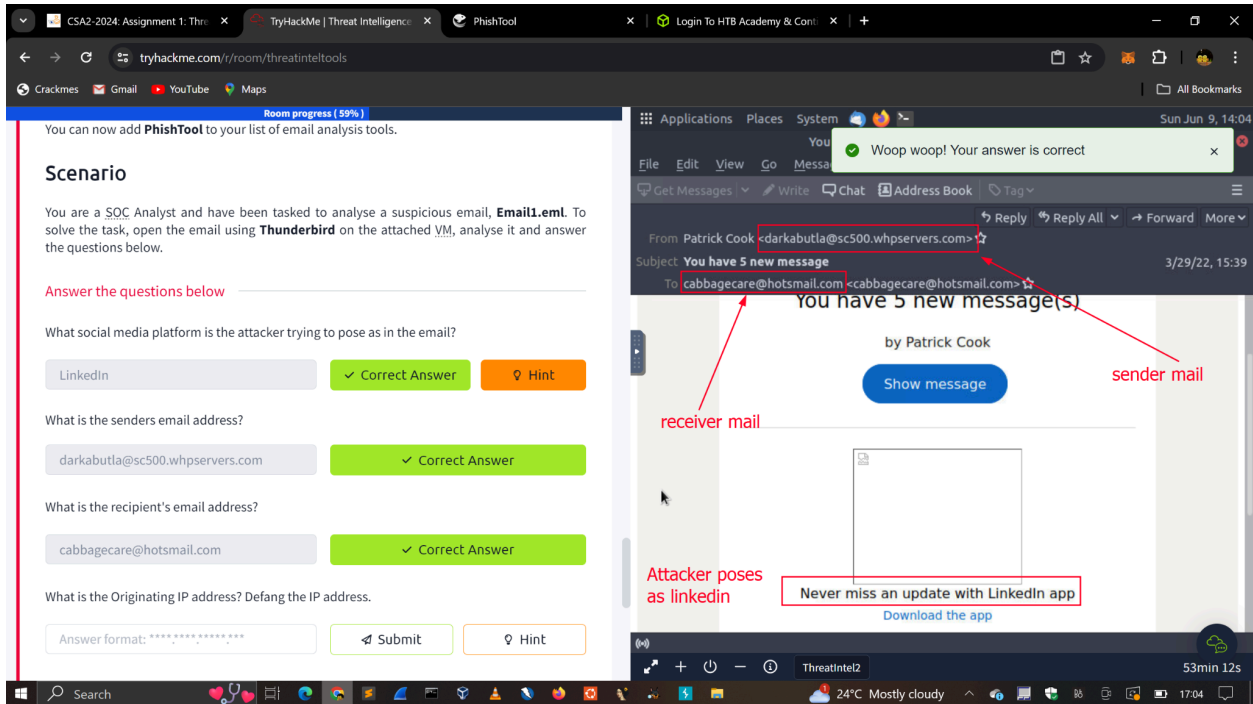
© abuse.ch 2024

Georgia

Phishtool

- What social media platform is the attacker trying to pose as in the email?
Linkedin
- What is the sender's email address?
darkabutla@sc500.whpservers.com
- What is the recipient's email address?
cabbagecare@hotmail.com

The screenshot below showcases the answers to the questions above.

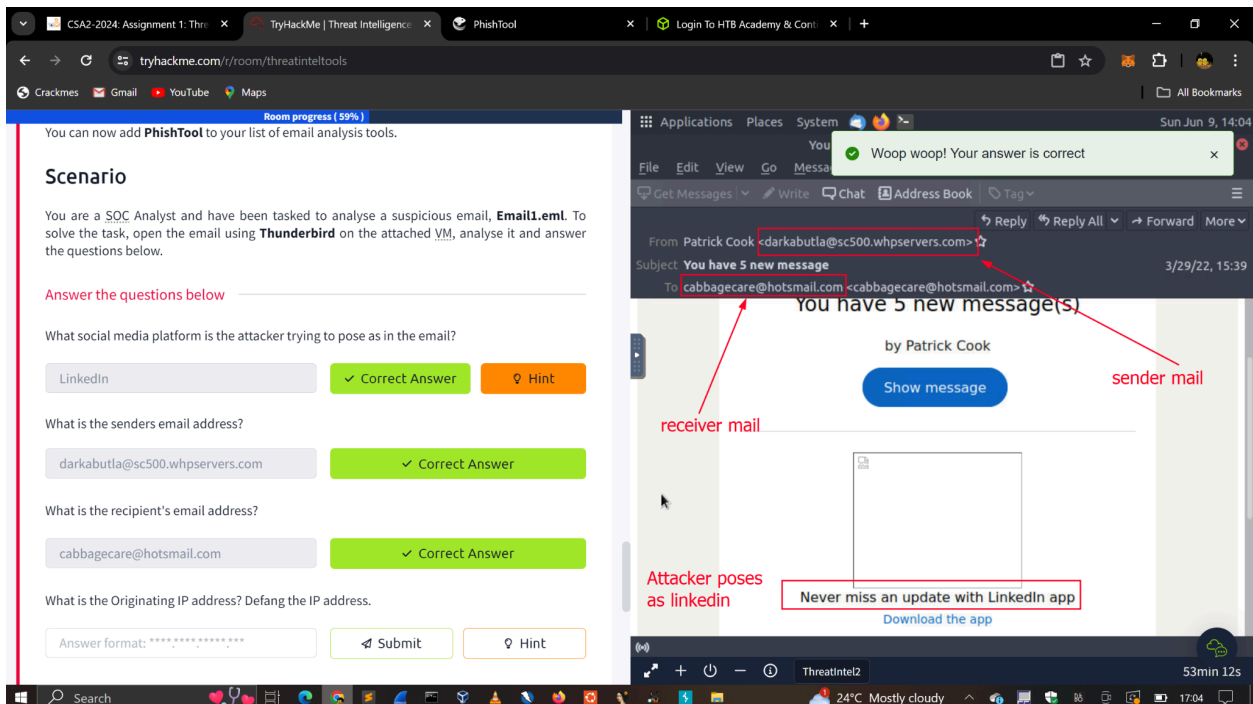


d. What is the Originating IP address? Defang the IP address.

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

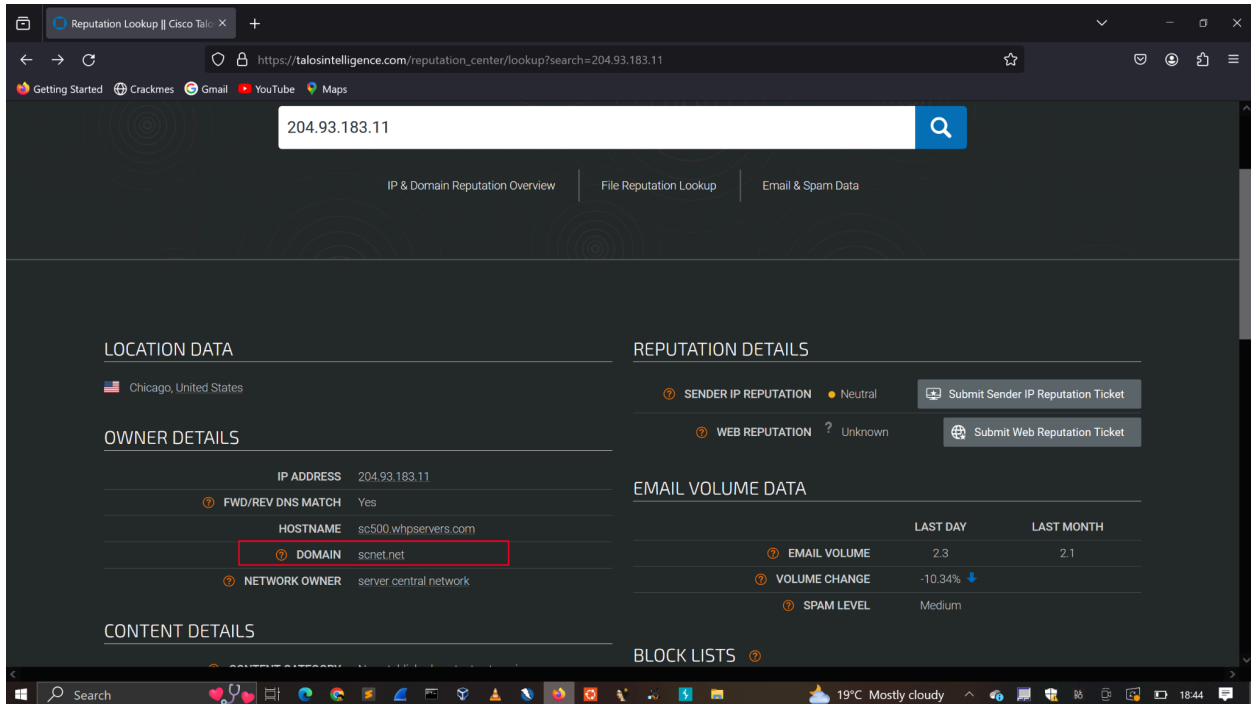
e. How many hops did the email go through to get to the recipient?

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.



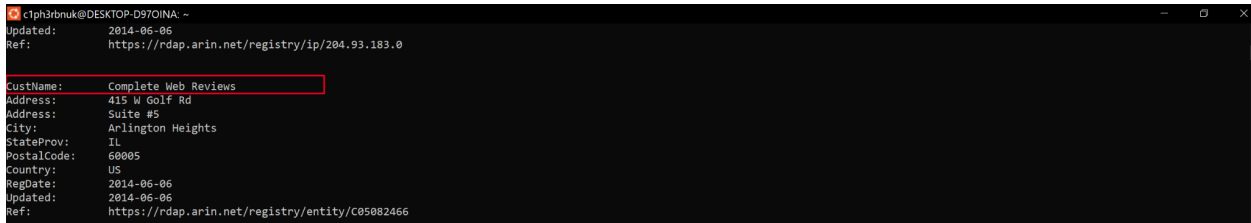
Cisco Talos Intelligence

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

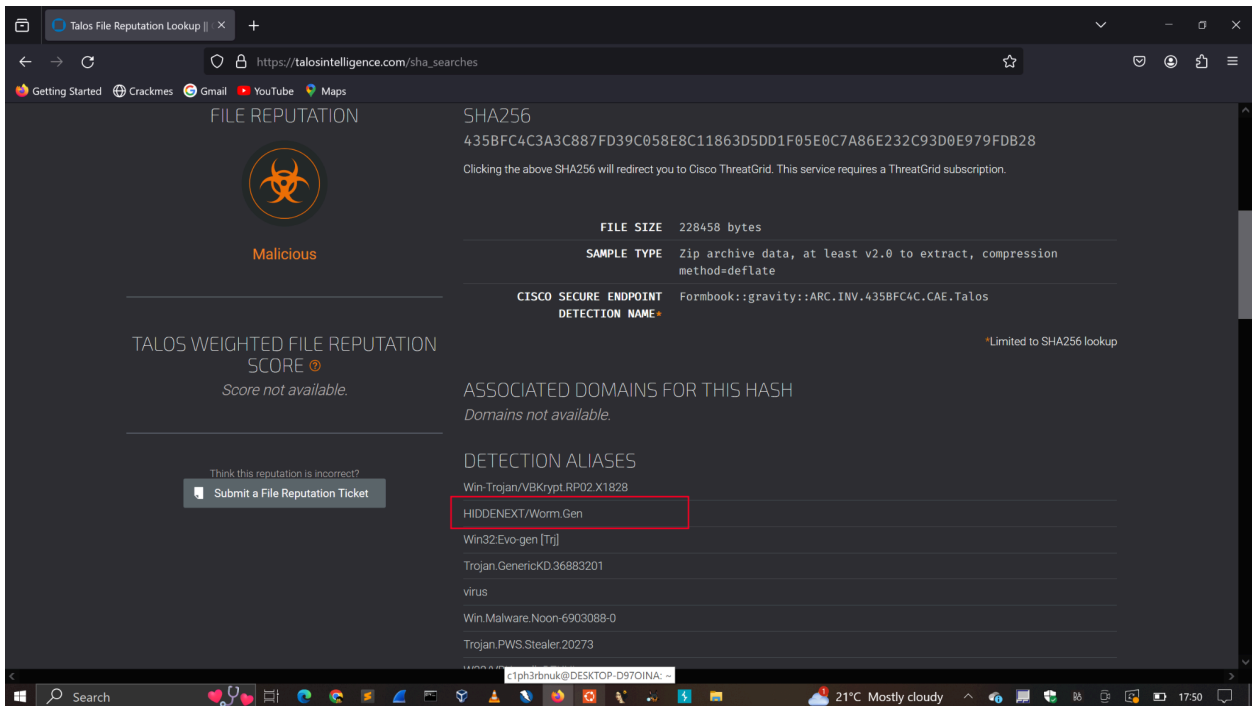
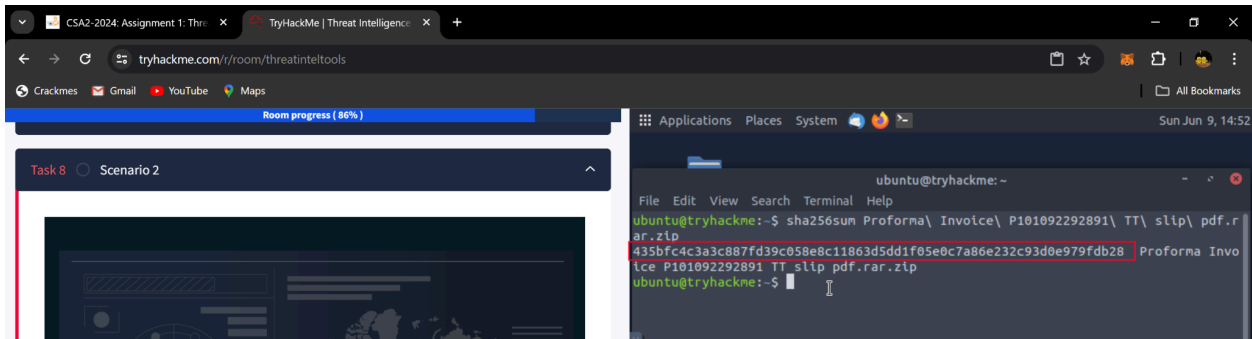
You are a SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email to triage the incidents reported.

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...

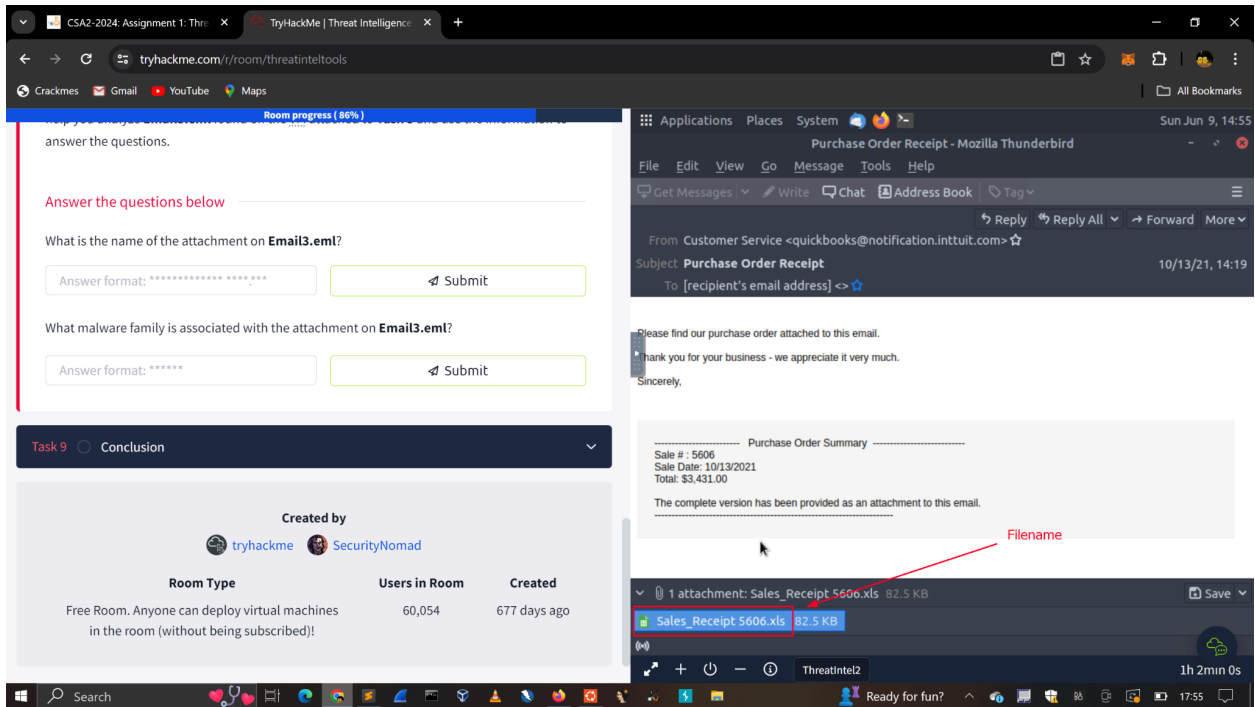


Scenario 2

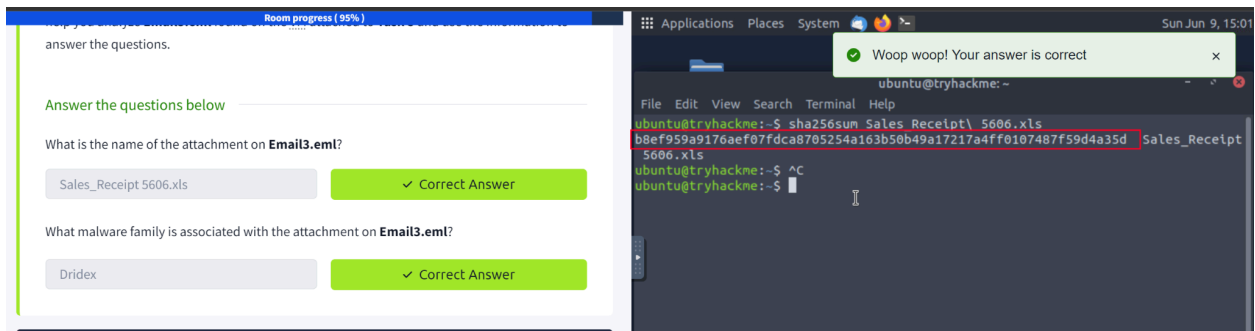
You are a SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email to triage the incidents reported.

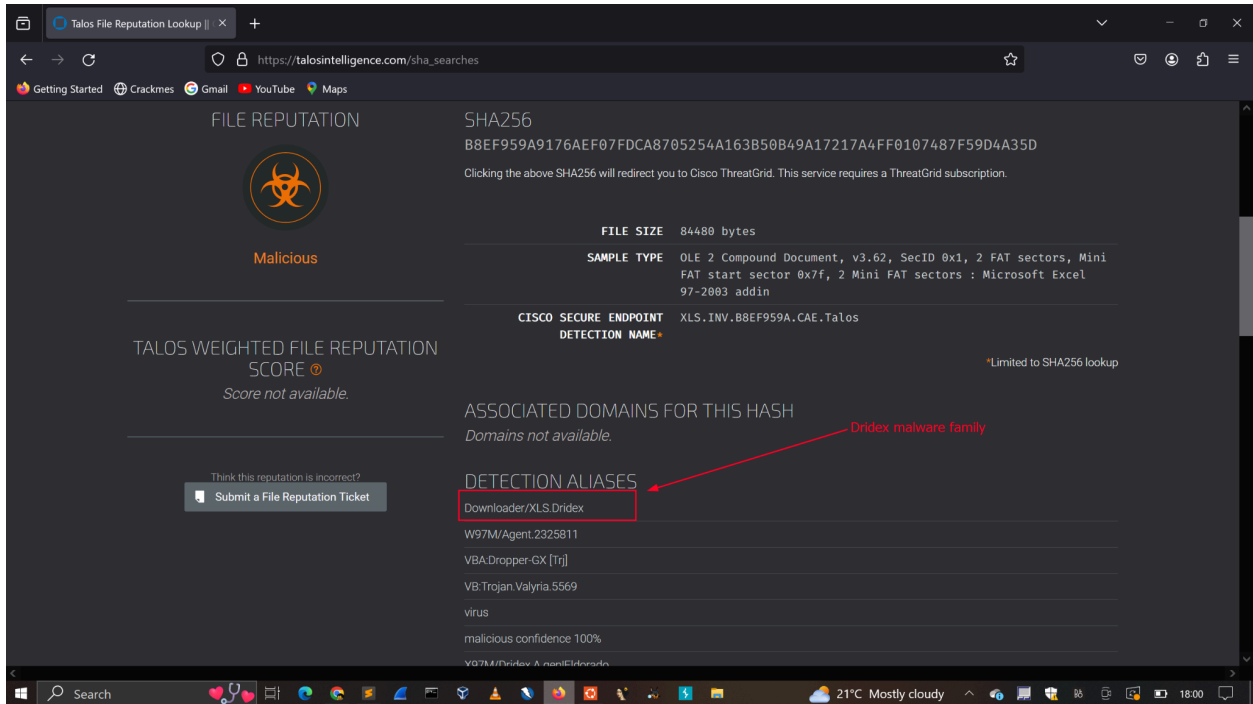
Task: Use the tools and knowledge discussed throughout this room (or use your resources) to help you analyze Email3.eml found on the VM attached to Task 5 and use the information to answer the questions.

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



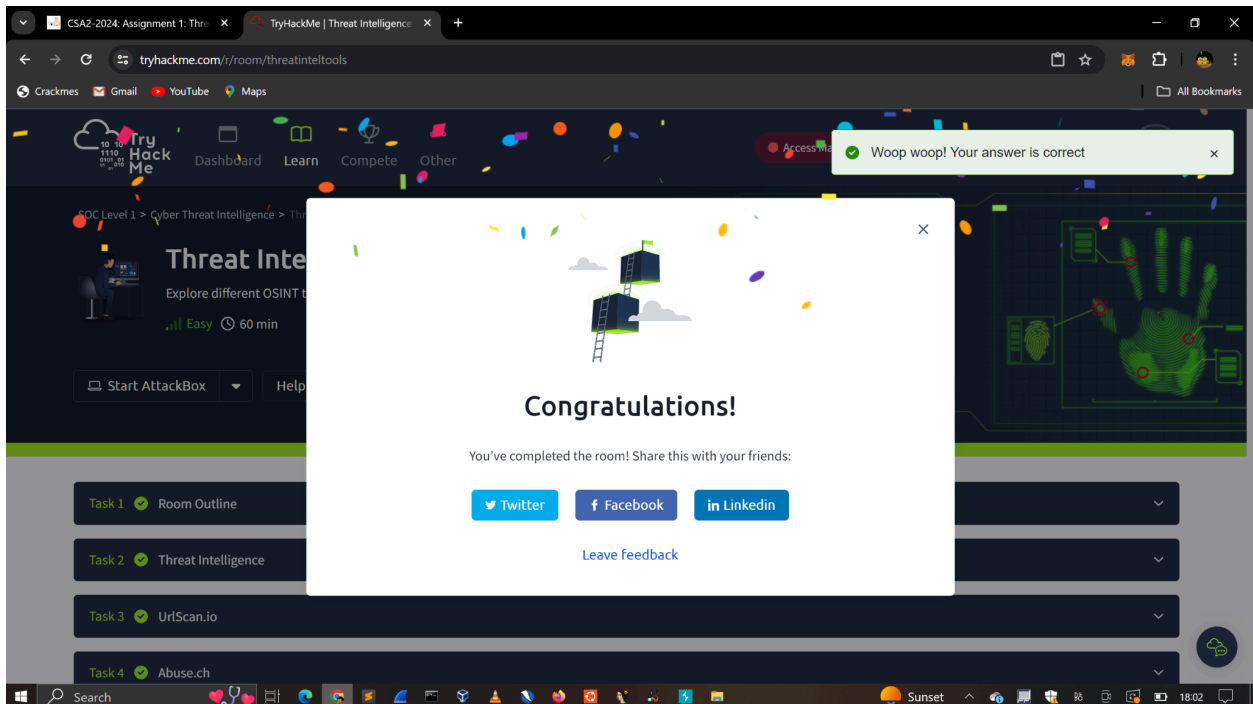
b. What malware family is associated with the attachment on Email3.eml?





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.