Threat intelligence tools: TryHackMe

Name: Daniel Mwendwa Mwithui

ADM NO. CS-SA04-23080

Program: Security Analyst

Date of submission:22nd June 2023

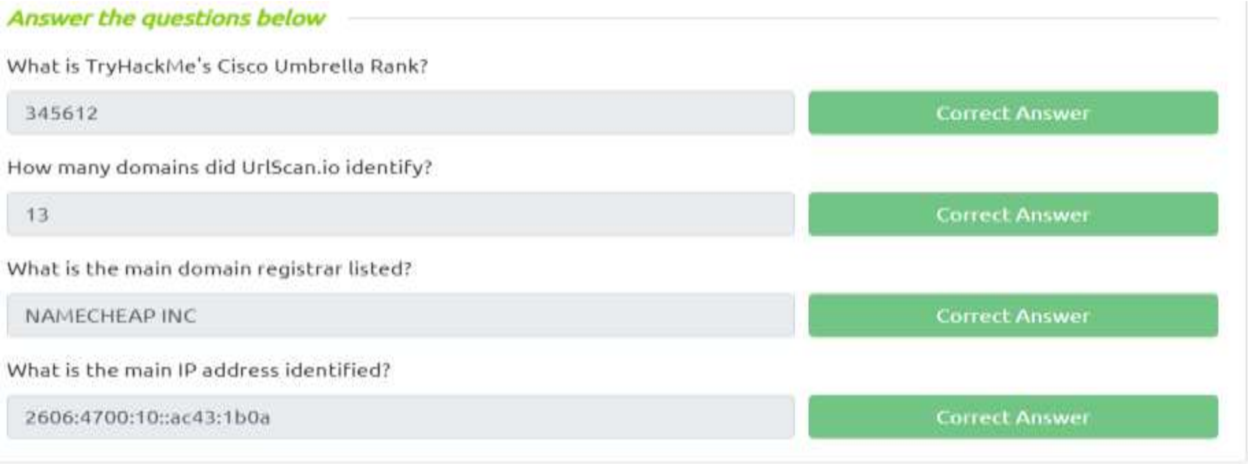
Introduction

In this assignment, we will explore the world of threat intelligence tools, focusing on two prominent platforms: URLScan.io and abuse.ch. We will begin by understanding urlscan.io, an online service that allows users to scan and analyze URLs for potential threats and malicious activities. We will delve into its functionality, how it aids in identifying and detecting suspicious websites, and the valuable information it provides for making informed security decisions. Additionally, we will explore abuse.ch, an organization dedicated to combating cybercrime and online abuse. We will discuss its operational projects, such as ZeuS Tracker and Feodo Tracker, which play a crucial role in tracking and monitoring botnets and malicious activities. Lastly, we will touch upon Malware Bazaar, an initiative by abuse.ch, serving as a platform for sharing and analyzing malware samples. Some of other tools we are going to discuss in this paper is Cisco Talo intelligence and PhishTool as important tools in threat intelligence.

Task 1: urlscan.io

Urlscan.io is an online service that scans and analyzes URLs for potential threats and malicious activities, providing users with information about the scanned URL and any identified risks or suspicious behavior. It helps in identifying harmful websites and protecting against online threats. When a user submits a URL to urlScan.io, the service retrieves the webpage content and performs various security checks and analysis. This includes examining the HTML source code, inspecting embedded scripts, evaluating network requests made by the webpage, and checking for indicators of compromise.

To complete this section, we use the urlscan for tryhackme.com provided.



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

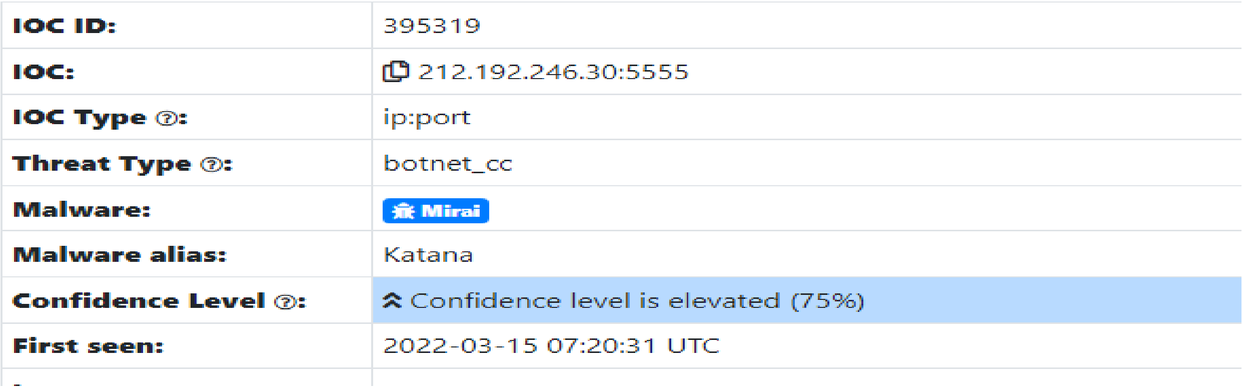
What is the main IP address identified?

2606:4700:10::ac43:1b0a

Task 2: Abuse.ch

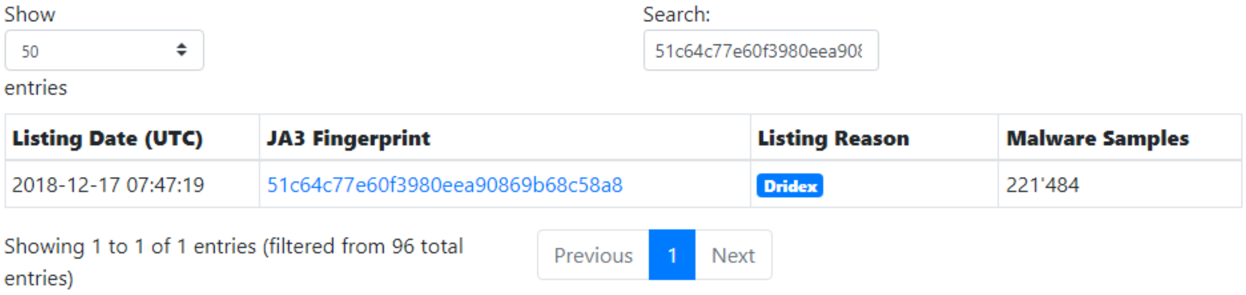
Abuse.ch is a research project that focuses on combating cybercrime and online abuse though keeping a track of malware and botnets. Its operational platform such as malware bazaar, Feodor tracker, SSL blacklist, URL Haus and Threat Fox provides real-time threat intelligence, malware tracking, and information among security professionals. It serves as a collaborative hub for reporting and monitoring malicious activities, such as botnets, malware distribution, and phishing campaigns.

Solving this section involves searching through the operational platforms listed above. For the first task, search for the ioc:**212.192.246.30:5555** from the threatfox database.



IOC ID:	395319
IOC:	212.192.246.30:5555
IOC Type ⓘ:	ip:port
Threat Type ⓘ:	botnet_cc
Malware:	Mirai
Malware alias:	Katana
Confidence Level ⓘ:	Confidence level is elevated (75%)
First seen:	2022-03-15 07:20:31 UTC

Here, find the JA3 fingerprint given from the SSL blacklist.



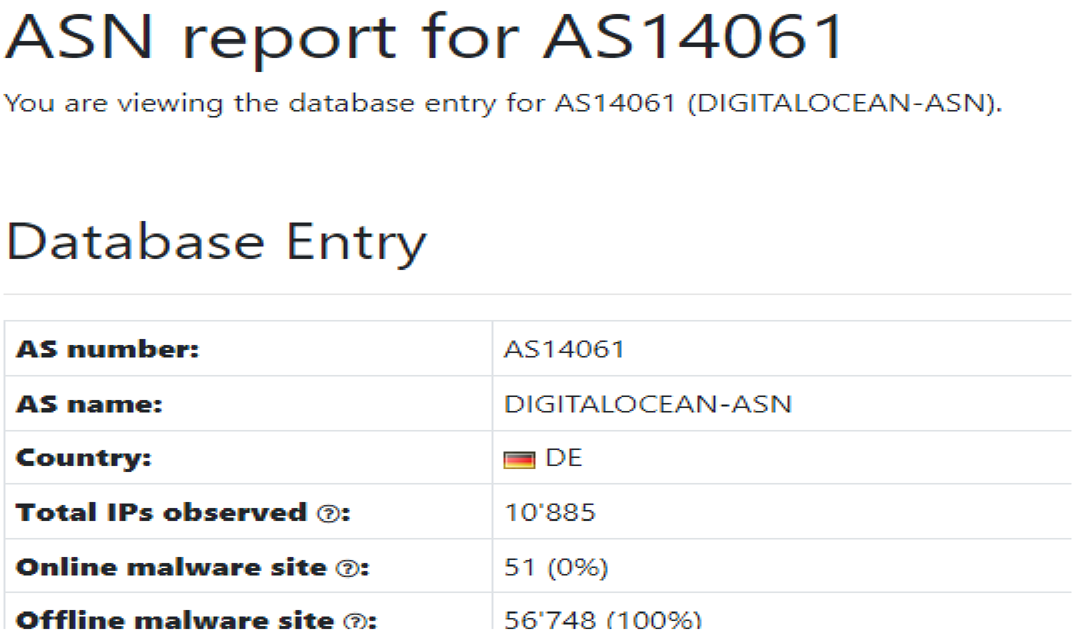
Show 50 entries

Search: 51c64c77e60f3980eea90

Listing Date (UTC)	JA3 Fingerprint	Listing Reason	Malware Samples
2018-12-17 07:47:19	51c64c77e60f3980eea90869b68c58a8	Dridex	221'484

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

Here search for AS14061 from the statistics page of urlhaus



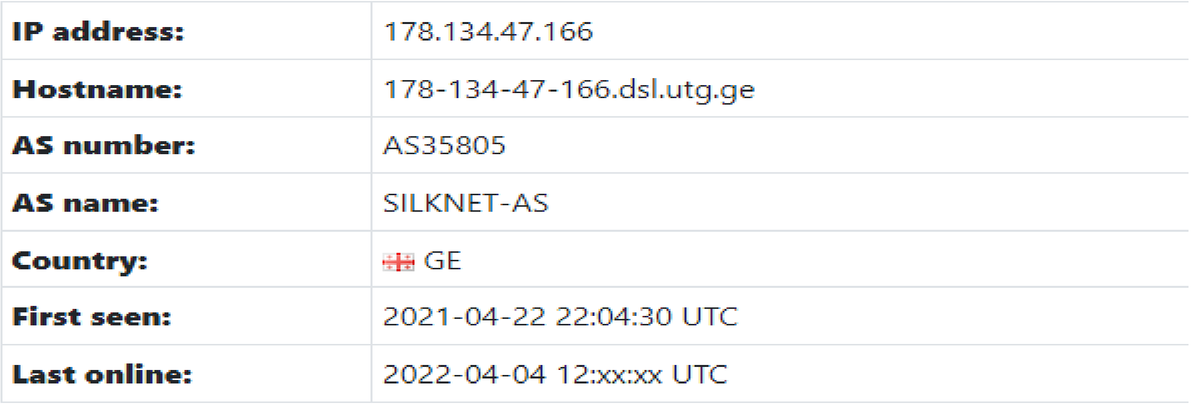
ASN report for AS14061

You are viewing the database entry for AS14061 (DIGITALOCEAN-ASN).

Database Entry

AS number:	AS14061
AS name:	DIGITALOCEAN-ASN
Country:	DE
Total IPs observed ?:	10'885
Online malware site ?:	51 (0%)
Offline malware site ?:	56'748 (100%)

In this last question for this section, search the ip address **178.134.47.166** under the botnet section on the feodo tracker site. After that I browsed online to search for a country starting with GE and with the shown flag.

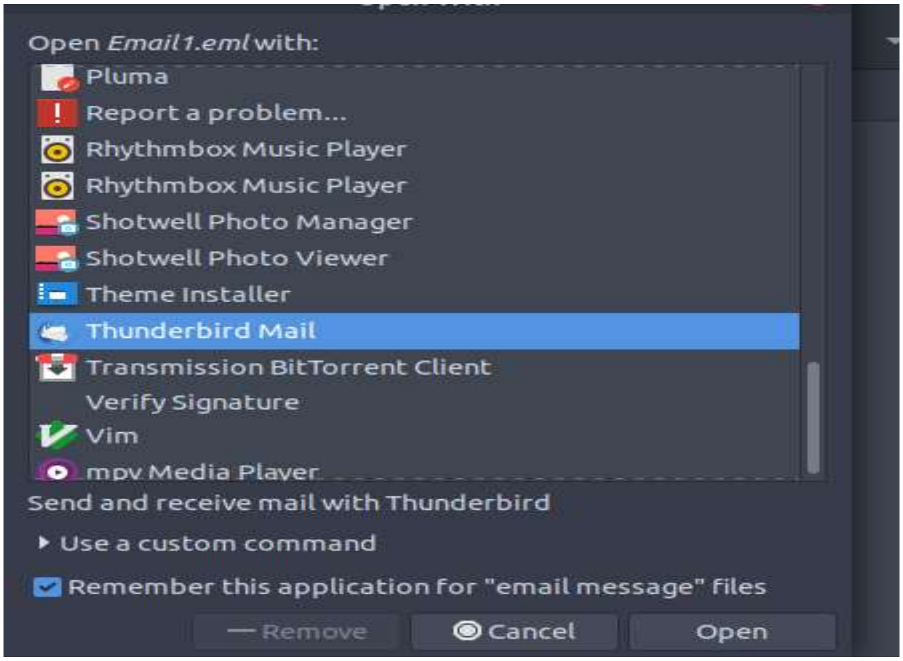


IP address:	178.134.47.166
Hostname:	178-134-47-166.dsl.utg.ge
AS number:	AS35805
AS name:	SILKNET-AS
Country:	GE
First seen:	2021-04-22 22:04:30 UTC
Last online:	2022-04-04 12:xx:xx UTC

Task 3: PhishTool

PhishTool is designed to assist in detecting and mitigating phishing attacks via email. It typically provides functionalities such as analyzing suspicious emails, URLs, and attachments to identify signs of phishing attempts. PhishTool may include features like link scanning, email header analysis, blacklisting, and reporting mechanisms to help individuals and organizations in protecting against phishing threats. Its primary goal is to enhance security and help users avoid falling victim to phishing scams by identifying and raising awareness about potentially fraudulent activities.

To complete this section here is a step-by-step guide. For question 1, opened the email from the machine provided. See the screenshot below.

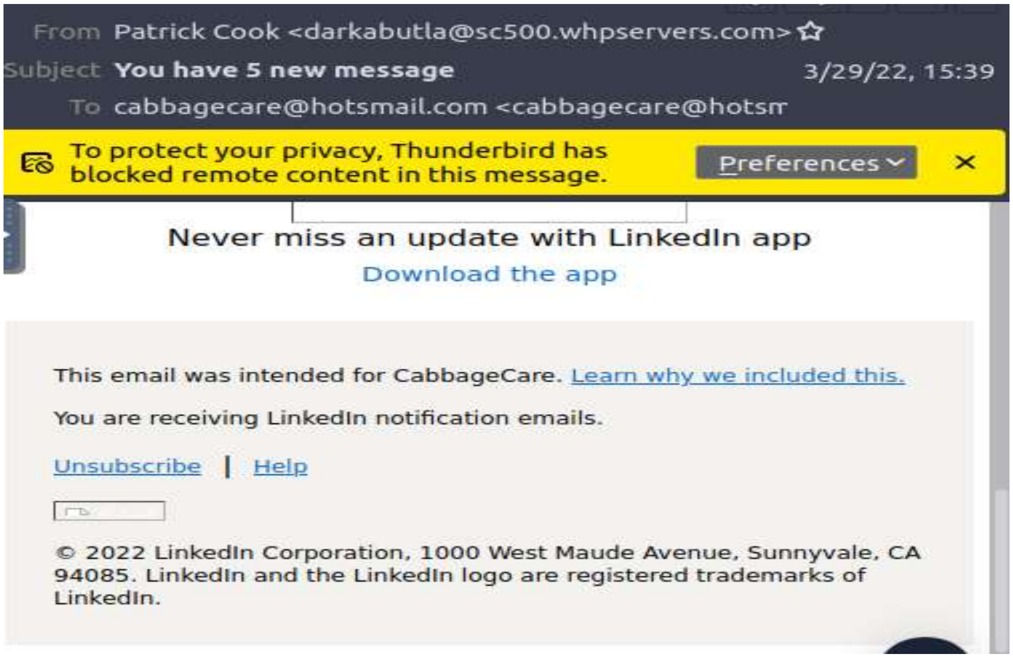


Open *Email1.eml* with:

Send and receive mail with Thunderbird

☑ Remember this application for "email message" files

The screenshot below shows both the social media platform attacker is posing, the senders and recipient’s email.



From Patrick Cook <darkabutla@sc500.whpservers.com>

Subject You have 5 new message 3/29/22, 15:39

To cabbagecare@hotsmail.com <cabbagecare@hotsm

To protect your privacy, Thunderbird has blocked remote content in this message.

Never miss an update with LinkedIn app

Download the app

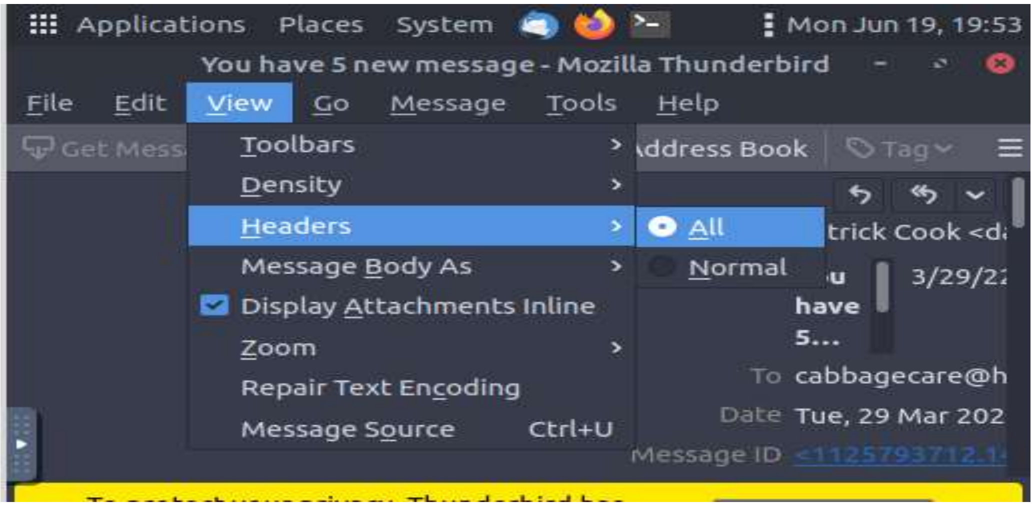
This email was intended for CabbageCare. Learn why we included this.

You are receiving LinkedIn notification emails.

Unsubscribe | Help

© 2022 LinkedIn Corporation, 1000 West Maude Avenue, Sunnyvale, CA 94085. LinkedIn and the LinkedIn logo are registered trademarks of LinkedIn.

The next question, go to view>header then set it to all. It gives more details. This allows us to view the email address. To defang ip address, put [] for every”.” as [.]. See the screenshot below.



trick Cook <d

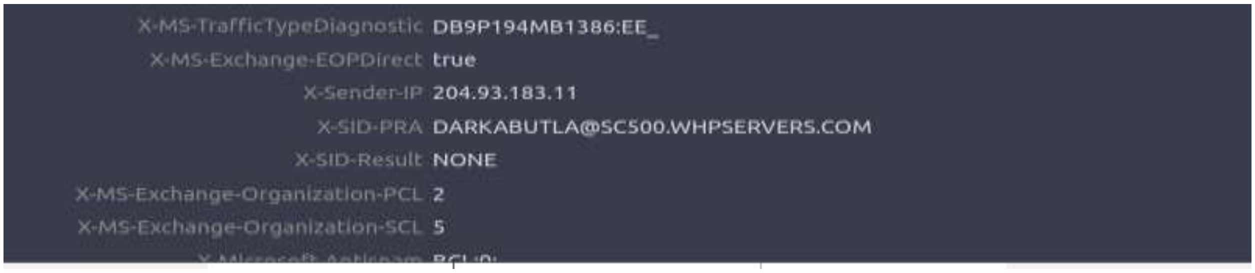
u have 5...

3/29/2

To cabbagecare@h

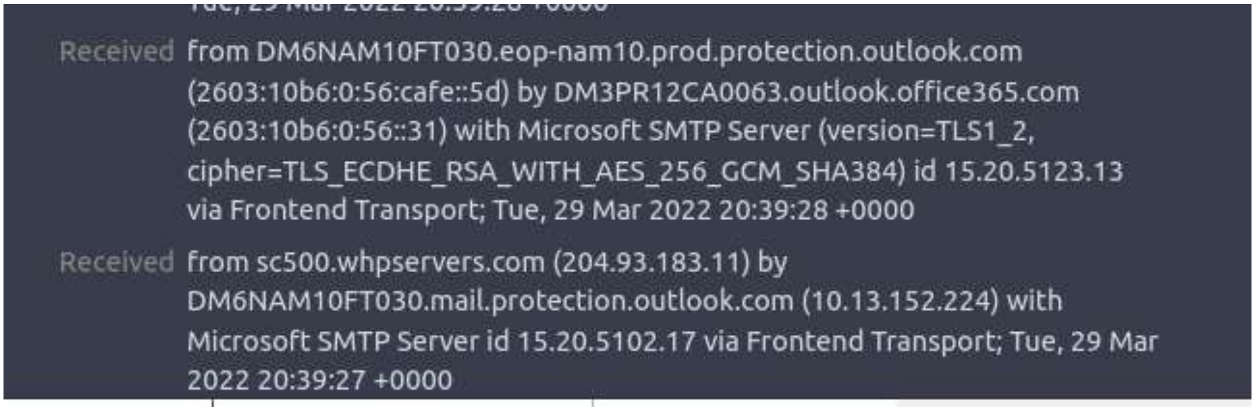
Date Tue, 29 Mar 202

Message ID <1125793712.1



```
X-MS-TrafficTypeDiagnostic DB9P194MB1386:EE_
    X-MS-Exchange-EOPDirect true
                X-Sender-IP 204.93.183.11
                 X-SID-PRA DARKABUTLA@SC500.WHPSERVERS.COM
              X-SID-Result NONE
X-MS-Exchange-Organization-PCL 2
X-MS-Exchange-Organization-SCL 5
   X-Microsoft-Antispam BCL:0;
```

To know how many hops the email went through, look at how many times the email shows received from the view all panel. See the screenshot below.

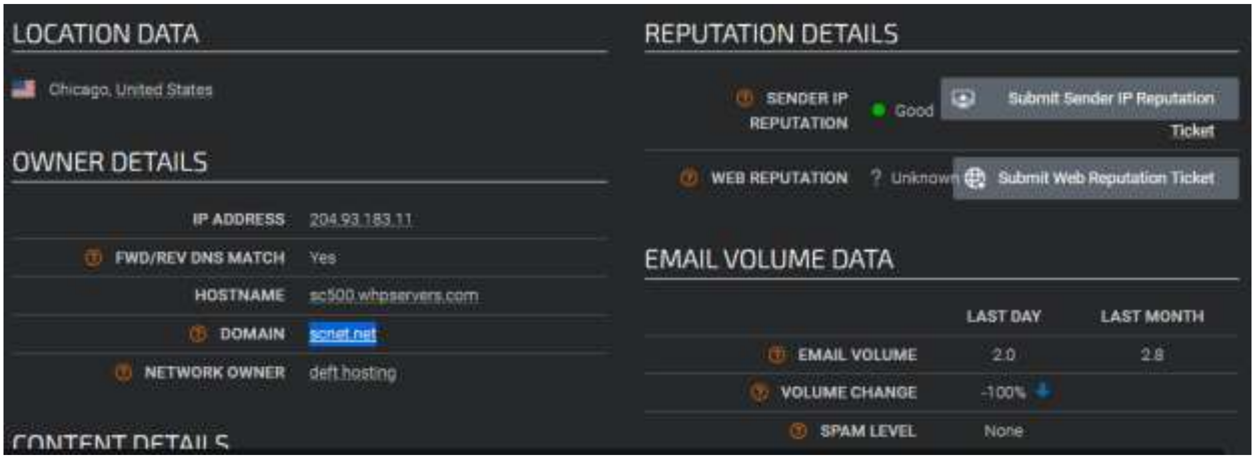


```
         Tue, 29 Mar 2022 20:39:28 +0000
Received from DM6NAM10FT030.eop-nam10.prod.protection.outlook.com
         (2603:10b6:0:56:cafe::5d) by DM3PR12CA0063.outlook.office365.com
         (2603:10b6:0:56::31) with Microsoft SMTP Server (version=TLS1_2,
         cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5123.13
         via Frontend Transport; Tue, 29 Mar 2022 20:39:28 +0000
Received from sc500.whpservers.com (204.93.183.11) by
         DM6NAM10FT030.mail.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
```

Task 4: Cisco Talos intelligence

Cisco Talos Intelligence is a cybersecurity research group assembled by Cisco that provides threat intelligence, research, and analysis to help organizations identify and defend against advanced cyber threats. They specialize in researching and tracking emerging threats, vulnerabilities, malware, and cybercriminal activities. Talos Intelligence offers valuable insights, security updates, and actionable recommendations to enhance the overall security posture of businesses and individuals.

This section is completed from the https://talosintelligence.com/ site. Search for the ip address from the previous section to get its domain.



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

NETWORK OWNER deft hosting

CONTENT DETAILS

REPUTATION DETAILS

SENDER IP REPUTATION ● Good

Submit Sender IP Reputation Ticket

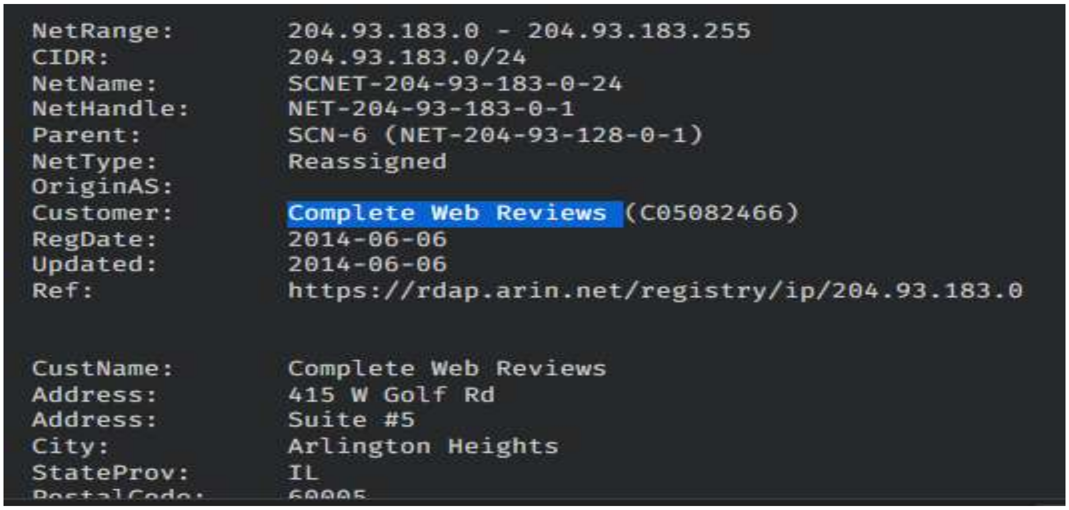
WEB REPUTATION ? Unknown

Submit Web Reputation Ticket

EMAIL VOLUME DATA

	LAST DAY	LAST MONTH
EMAIL VOLUME	2.0	2.8
VOLUME CHANGE	-100%	
SPAM LEVEL	None	

From the whois section, you can find the customer's name of the ip addr;ess.



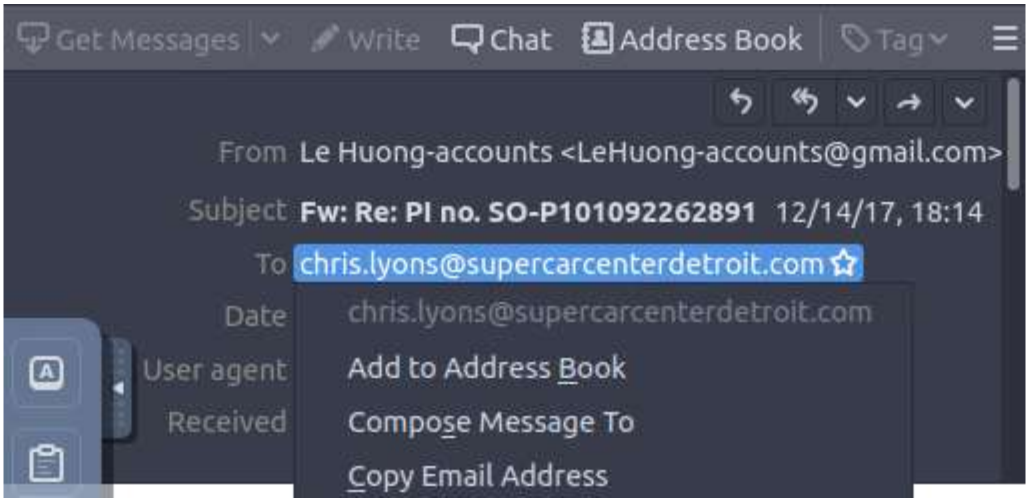
```
NetRange:       204.93.183.0 - 204.93.183.255
CIDR:           204.93.183.0/24
NetName:        SCNET-204-93-183-0-24
NetHandle:      NET-204-93-183-0-1
Parent:         SCN-6 (NET-204-93-128-0-1)
NetType:        Reassigned
OriginAS:
Customer:       Complete Web Reviews (C05082466)
RegDate:        2014-06-06
Updated:        2014-06-06
Ref:            https://rdap.arin.net/registry/ip/204.93.183.0


CustName:       Complete Web Reviews
Address:        415 W Golf Rd
Address:        Suite #5
City:           Arlington Heights
StateProv:      IL
PostalCode:     60005
```

.

Task 5: Scenario

In this section, we are going to apply the knowledge learned in this module to solve the given scenario. Opening the email2.eml with Thunderbird Mail shows the recipient's email address.



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

Subject **Fw: Re: PI no. SO-P101092262891** 12/14/17, 18:14

To chris.lyons@supercarcenterdetroit.com

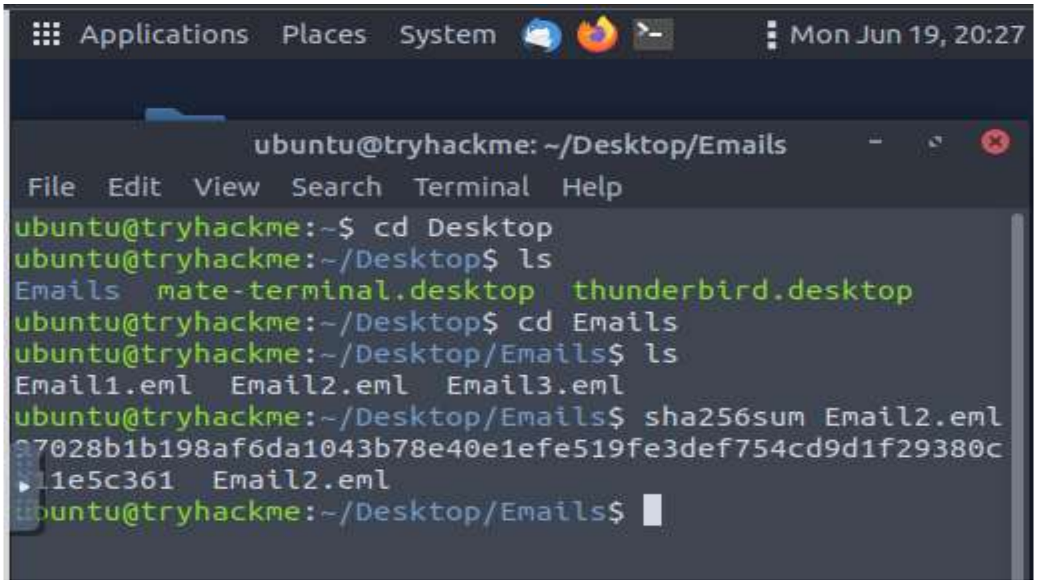
chris.lyons@supercarcenterdetroit.com

Date

User agent

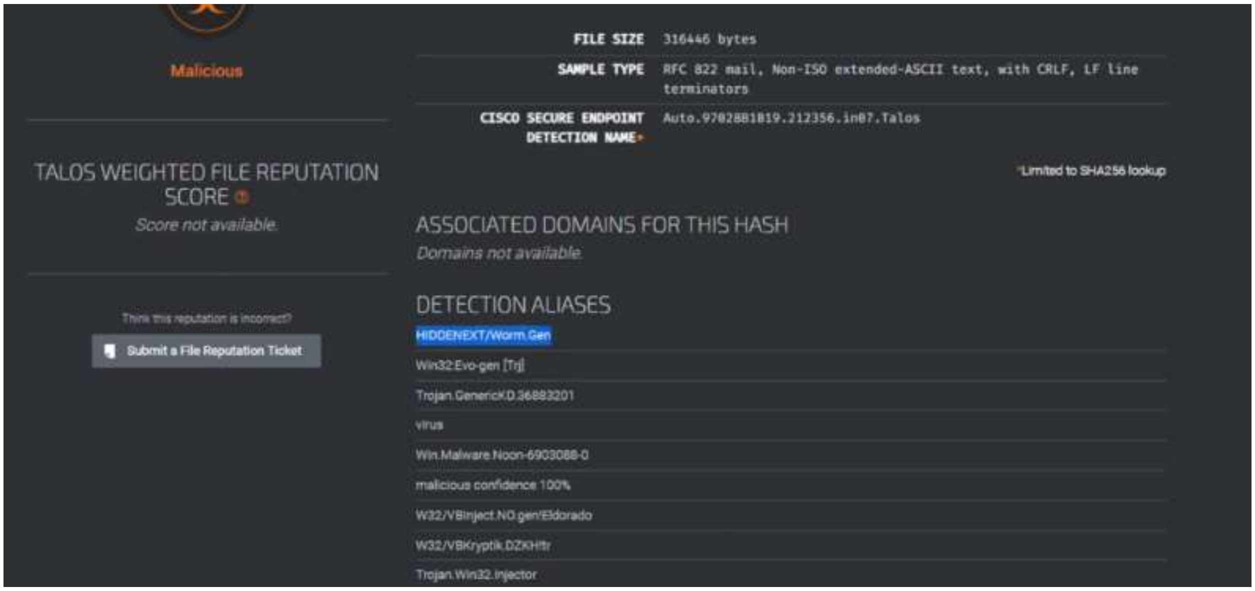
Received

In the second question, do the sha256sum to get the hash value of the email2.eml. see the screenshot below.



```
ubuntu@tryhackme:~$ cd Desktop
ubuntu@tryhackme:~/Desktop$ ls
Emails  mate-terminal.desktop  thunderbird.desktop
ubuntu@tryhackme:~/Desktop$ cd Emails
ubuntu@tryhackme:~/Desktop/Emails$ ls
Email1.eml  Email2.eml  Email3.eml
ubuntu@tryhackme:~/Desktop/Emails$ sha256sum Email2.eml
7028b1b198af6da1043b78e40e1efe519fe3def754cd9d1f29380c
1e5c361  Email2.eml
untu@tryhackme:~/Desktop/Emails$
```

Search the hash value from the talos intelligence site.



Malicious

TALOS WEIGHTED FILE REPUTATION SCORE

Score not available.

Think this reputation is incorrect?

Submit a File Reputation Ticket

FILE SIZE	316446 bytes
SAMPLE TYPE	RFC 822 mail, Non-ISO extended-ASCII text, with CRLF, LF line terminators
CISCO SECURE ENDPOINT DETECTION NAME*	Auto.9702881819.212356.in07.Talos

*Limited to SHA256 lookup

ASSOCIATED DOMAINS FOR THIS HASH

Domains not available.

DETECTION ALIASES

HIDDENEXT/Worm.Gen

Win32:Evo-gen [Trj]

Trojan.GenericKD.36883201

virus

Win.Malware.Noon-6903088-0

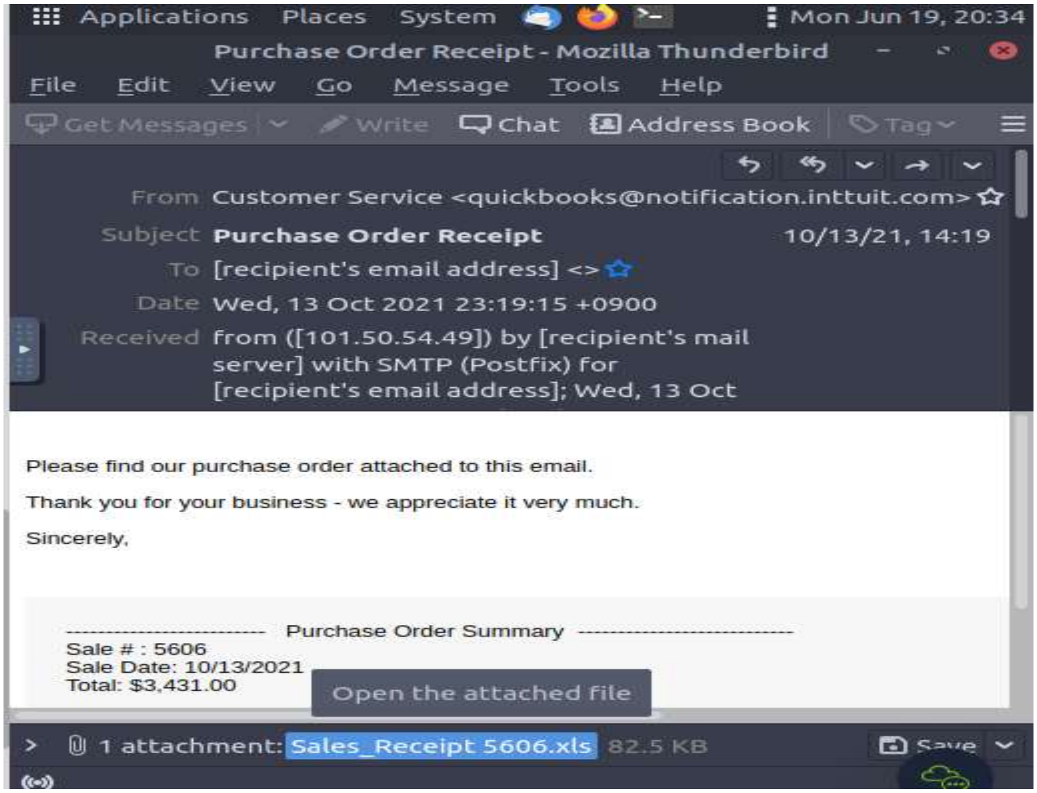
malicious confidence 100%

W32/VBinject.NO.gen!Eldorado

W32/VBKryptik.DZKHftr

Trojan.Win32.Injector

In this next scenario, we weork with email3.eml. open the email again with Thunderbird mail.



Applications Places System
Mon Jun 19, 20:34
Purchase Order Receipt - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages Write Chat Address Book Tag

From Customer Service <quickbooks@notification.inttuit.com>

Subject **Purchase Order Receipt** 10/13/21, 14:19

To [recipient's email address] <>

Date Wed, 13 Oct 2021 23:19:15 +0900

Received from ([101.50.54.49]) by [recipient's mail server] with SMTP (Postfix) for [recipient's email address]; Wed, 13 Oct

Please find our purchase order attached to this email.

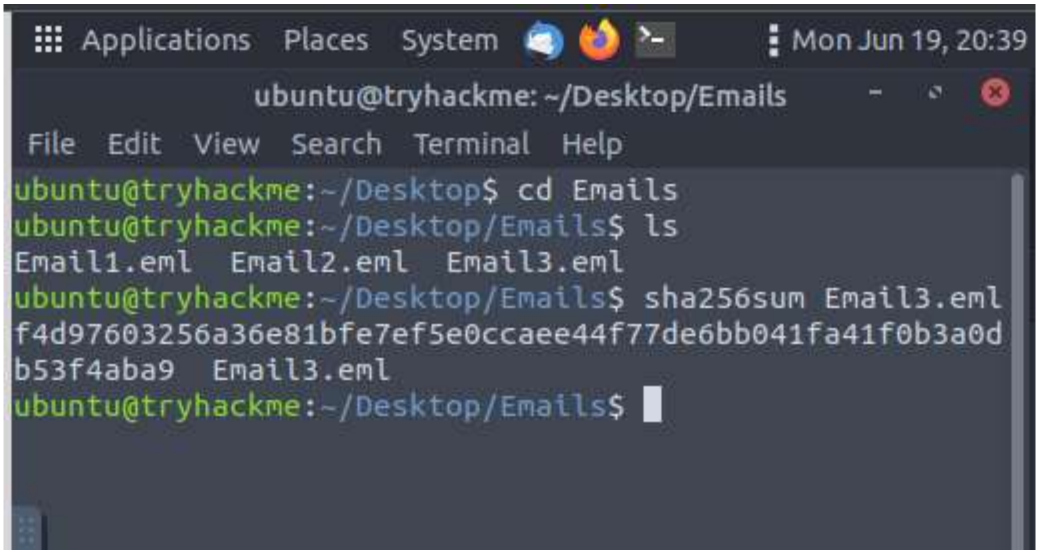
Thank you for your business - we appreciate it very much.

Sincerely,

```
------------------------- Purchase Order Summary ---------------------------
Sale # : 5606
Sale Date: 10/13/2021
Total: $3,431.00
```

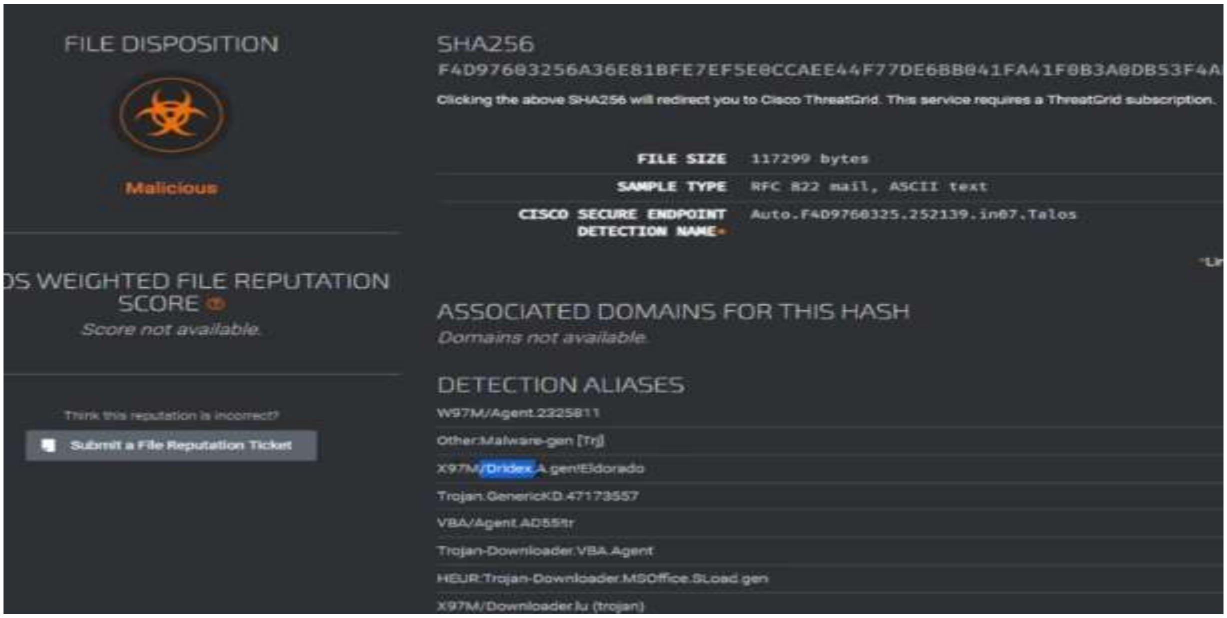
1 attachment: Sales_Receipt 5606.xls 82.5 KB

Do the sha256sum to generate the hash value of the file.



```
ubuntu@tryhackme:~/Desktop$ cd Emails
ubuntu@tryhackme:~/Desktop/Emails$ ls
Email1.eml  Email2.eml  Email3.eml
ubuntu@tryhackme:~/Desktop/Emails$ sha256sum Email3.eml
f4d97603256a36e81bfe7ef5e0ccaee44f77de6bb041fa41f0b3a0d
b53f4aba9  Email3.eml
ubuntu@tryhackme:~/Desktop/Emails$ 
```

Search the hash on talos intelligence


FILE DISPOSITION
Malicious
DS WEIGHTED FILE REPUTATION SCORE
Submit a File Reputation Ticket

Score not available.

Think this reputation is incorrect?

SHA256

F4D97603256A36E81BFE7EF5E0CCAEE44F77DE6BB041FA41F0B3A0DB53F4A

Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

FILE SIZE 117299 bytes

SAMPLE TYPE RFC 822 mail, ASCII text

CISCO SECURE ENDPOINT DETECTION NAME Auto.F4D9760325.252139.in07.Talos

ASSOCIATED DOMAINS FOR THIS HASH

Domains not available.

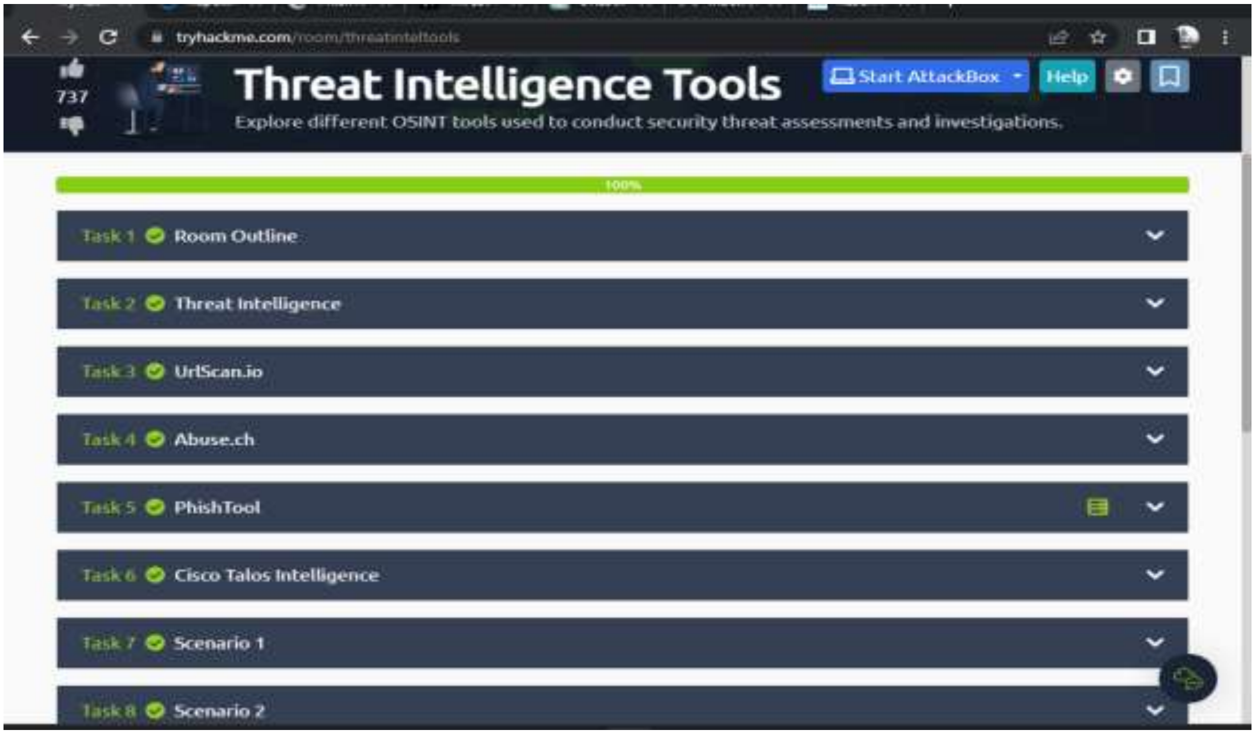
DETECTION ALIASES

W97M/Agent.2225811
Other:Malware-gen [Trj]
X97M/Dridex.A.gen!Eldorado
Trojan.GenericKD.47173557
VBA/Agent.AD55!tr
Trojan-Downloader.VBA.Agent
HEUR:Trojan-Downloader.MSOffice.SLoad.gen
X97M/Downloader.lu (trojan)

Here is the completion for this module and the link:

Link: https://tryhackme.com/room/threatinteltools

Link to public profile: https://tryhackme.com/p/Daniel.Mwendwa



Threat Intelligence Tools

Explore different OSINT tools used to conduct security threat assessments and investigations.

Task 1 Room Outline

Task 2 Threat Intelligence

Task 3 UrlScan.io

Task 4 Abuse.ch

Task 5 PhishTool

Task 6 Cisco Talos Intelligence

Task 7 Scenario 1

Task 8 Scenario 2

Conclusion

Through our exploration of threat intelligence tools, particularly urlscan.io, abuse.ch, PhishTool and Cisco Talo intelligence, we have gained insights into the critical role these tools play in enhancing cybersecurity. We have learned how URLScan.io assists in identifying potential threats and providing valuable information about scanned URLs, aiding in informed decision-making to protect against online dangers. Furthermore, we have seen the significant impact of abuse.ch's operational projects, tracking and monitoring malicious activities, and contributing to the collaborative effort of combating cybercrime. The existence of platforms like Malware Bazaar highlights the importance of sharing malware samples for research and analysis, enabling the cybersecurity community to stay vigilant against emerging threats. Overall, this journey has highlighted the value and effectiveness of threat intelligence tools in mitigating risks and reinforcing the security landscape.