Introduction:
https://tryhackme.com/p/Damiano254

Threat Intelligence is essential in cybersecurity, providing insights into emerging and active cyber threats. This report explores the key aspects of threat intelligence, focusing on its classifications and the use of various open-source tools. These tools are crucial for identifying and mitigating cyber threats, enhancing the security posture of organizations.

Task 1: Room Outline

Objective:

- Learn about Threat Intelligence and its applications.
- Explore various open-source tools for threat intelligence.

Tools and Concepts:

1. **Understanding Threat Intelligence & Classifications**
   - Basics of threat intelligence.
   - Classifications: Strategic, Technical, Tactical, Operational.
2. **UrlScan.io**
   - Tool for scanning malicious URLs.
   - Analyzes website interactions and metadata.
3. **Abuse.ch**
   - Tracks malware and botnet indicators.
4. **PhishTool**
   - Investigates phishing emails.
5. **Cisco's Talos Intelligence**
   - Platform for intelligence gathering.

Task 2: Threat Intelligence

Definition:

- Analysis of data to identify patterns and mitigate risks from threats**.**

Key Questions:

1. Who's attacking?
2. Motivation?
3. Capabilities?
4. Artefacts/Indicators of compromise?

Classifications:

1. Strategic Intel: High-level, trend-based intel.
2. Technical Intel: Evidence/artefacts of attacks.
3. Tactical Intel: Adversaries' tactics and techniques.
4. Operational Intel: Specific motives and intents.

Task 3: UrlScan.io

Functionality:

- Automates browsing and crawling to record website activities.
- Analyzes domains, IP addresses, page snapshots, and technologies used.

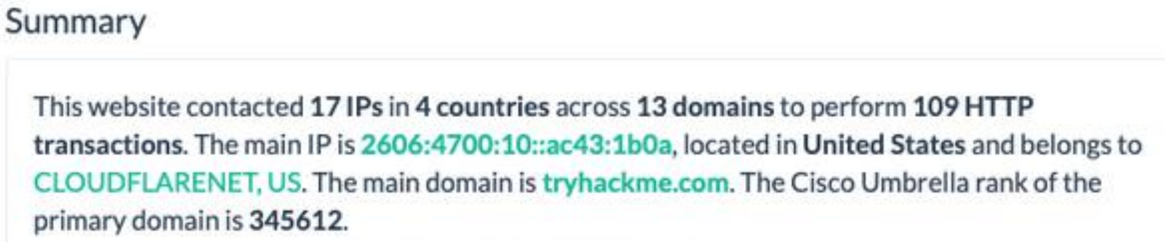
Key Aspects of Analysis:

1. Summary: IP, domain details, site screenshot.
2. HTTP: HTTP connection details.

3. Redirects: HTTP/client-side redirects.
4. Links: Outgoing links.
5. Behaviour: Site variables and cookies.
6. Indicators: IPs, domains, hashes.

Example: TryHackMe Domain Analysis

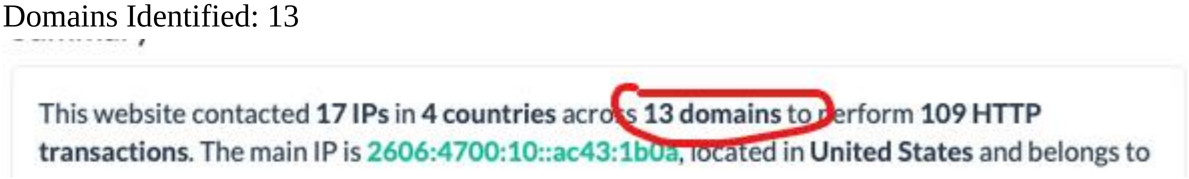
- Cisco Umbrella Rank: 345612



Summary

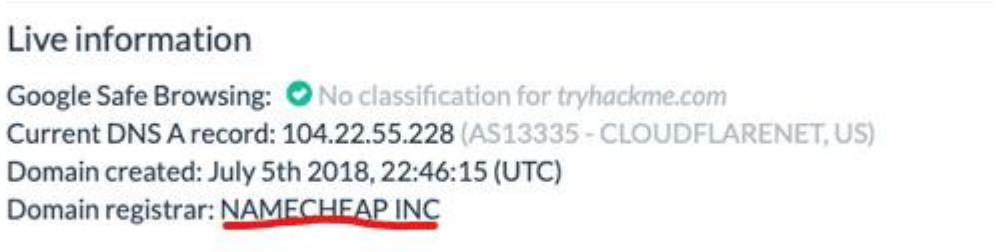
This website contacted **17 IPs** in **4 countries** across **13 domains** to perform **109 HTTP transactions**. The main IP is 2606:4700:10::ac43:1b0a, located in **United States** and belongs to CLOUDFLARENET, US. The main domain is tryhackme.com. The Cisco Umbrella rank of the primary domain is **345612**.

- Domains Identified: 13



This 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 **United States** and belongs to

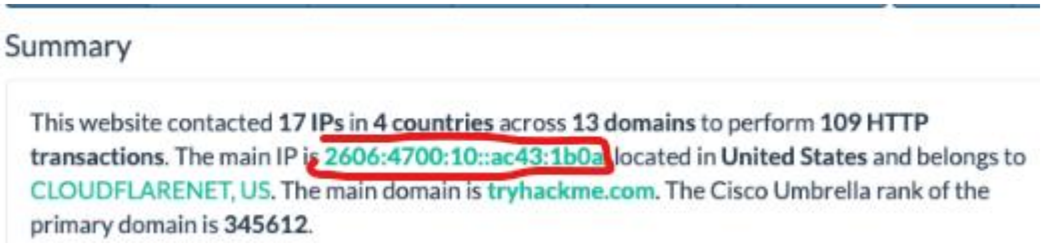
- Main Domain Registrar: NAMECHEAP INC



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

- Main IP Address: 2606:4700:10::ac43:1b0a



Summary

This 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 **United States** and belongs to CLOUDFLARENET, US. The main domain is tryhackme.com. The Cisco Umbrella rank of the primary domain is **345612**.

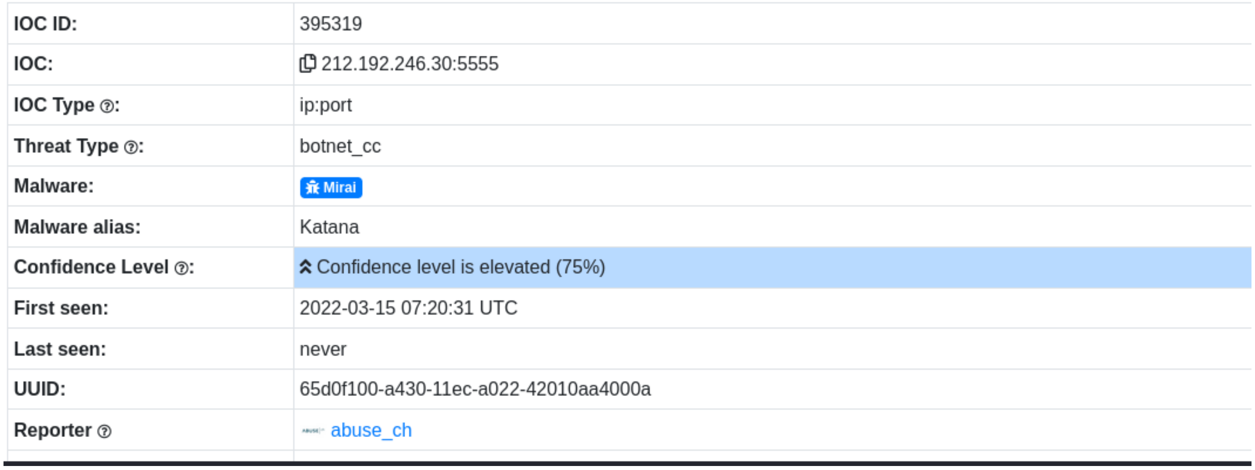
Task 4: Abuse.ch

- Purpose: Focuses on tracking and reporting malware and botnet activities.

Questions:

Q: The IOC 212.192.246.30:5555 is identified under which malware alias name on Threat Fox?

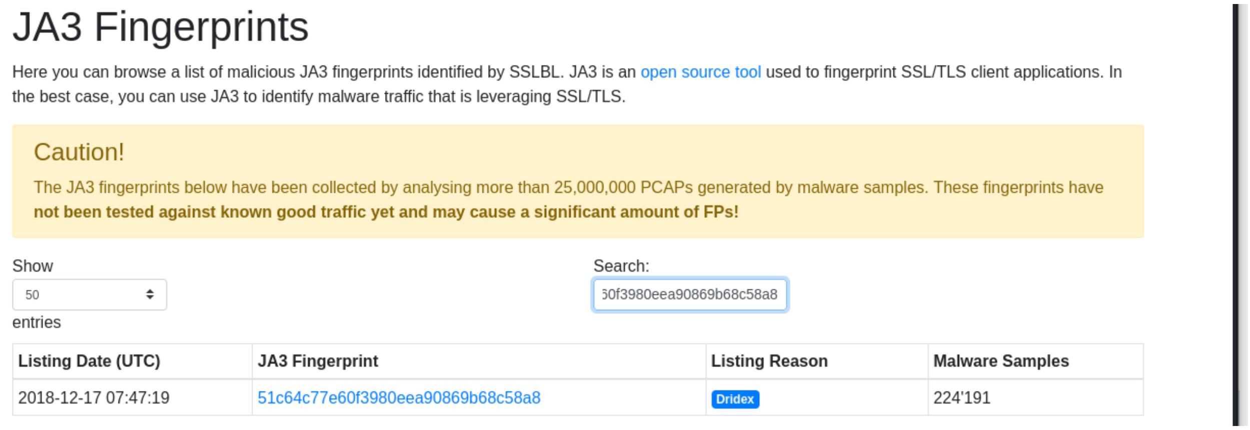
A: Katana



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
Last seen:	never
UUID:	65d0f100-a430-11ec-a022-42010aa4000a
Reporter ⓘ	abuse_ch

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

A: 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!**

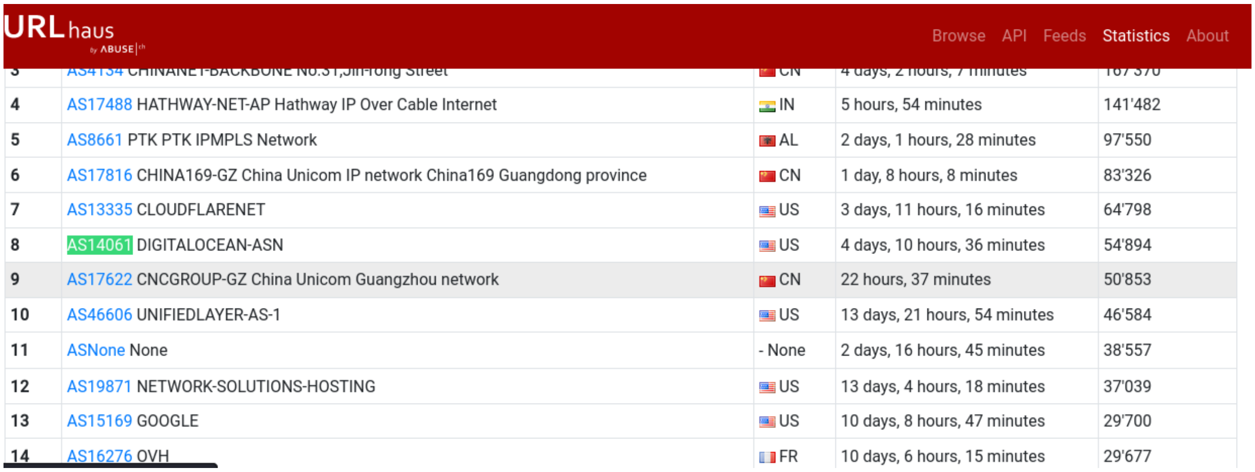
Show 50 entries

Search: 60f3980eea90869b68c58a8

Listing Date (UTC)	JA3 Fingerprint	Listing Reason	Malware Samples
2018-12-17 07:47:19	51c64c77e60f3980eea90869b68c58a8	Dridex	224'191

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

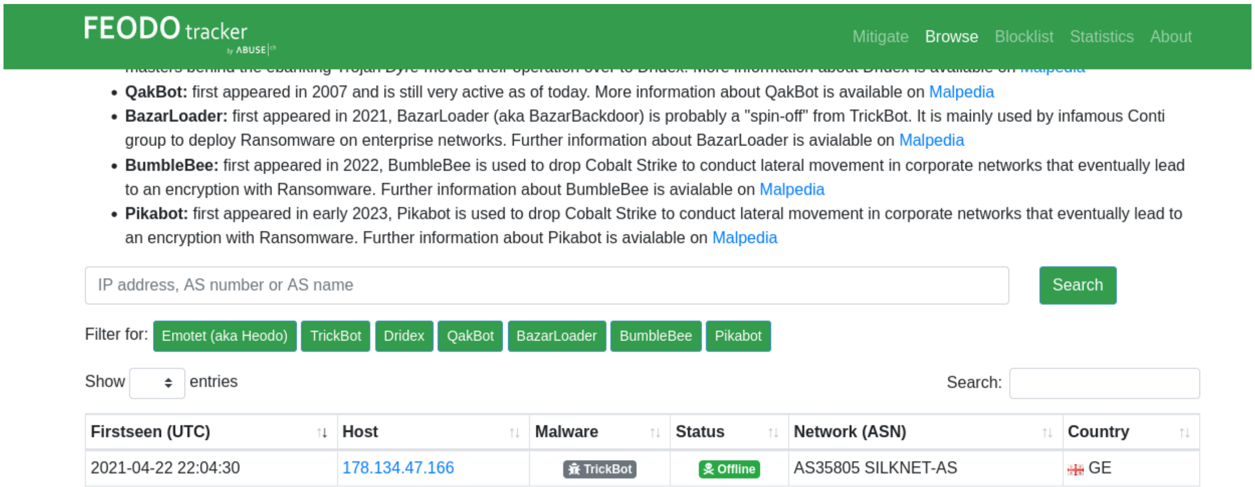
A: **DIGITALOCEAN-ASN**



3	AS4134 CHINANET-BACKBONE No.31,Jin-rong Street	CN	4 days, 2 hours, 7 minutes	167'370
4	AS17488 HATHWAY-NET-AP Hathway IP Over Cable Internet	IN	5 hours, 54 minutes	141'482
5	AS8661 PTK PTK IPMPLS Network	AL	2 days, 1 hours, 28 minutes	97'550
6	AS17816 CHINA169-GZ China Unicom IP network China169 Guangdong province	CN	1 day, 8 hours, 8 minutes	83'326
7	AS13335 CLOUDFLARENET	US	3 days, 11 hours, 16 minutes	64'798
8	AS14061 DIGITALOCEAN-ASN	US	4 days, 10 hours, 36 minutes	54'894
9	AS17622 CNCGROUP-GZ China Unicom Guangzhou network	CN	22 hours, 37 minutes	50'853
10	AS46606 UNIFIEDLAYER-AS-1	US	13 days, 21 hours, 54 minutes	46'584
11	ASNone None	- None	2 days, 16 hours, 45 minutes	38'557
12	AS19871 NETWORK-SOLUTIONS-HOSTING	US	13 days, 4 hours, 18 minutes	37'039
13	AS15169 GOOGLE	US	10 days, 8 hours, 47 minutes	29'700
14	AS16276 OVH	FR	10 days, 6 hours, 15 minutes	29'677

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

A: Georgia



masters behind the ebanking Trojan Dyre moved their operation over to Dridex. More information about Dridex is available on Malpedia

- **QakBot:** first appeared in 2007 and is still very active as of today. More information about QakBot is available on Malpedia
- **BazarLoader:** first appeared in 2021, BazarLoader (aka BazarBackdoor) is probably a "spin-off" from TrickBot. It is mainly used by infamous Conti group to deploy Ransomware on enterprise networks. Further information about BazarLoader is avialable on Malpedia
- **BumbleBee:** first appeared in 2022, BumbleBee is used to drop Cobalt Strike to conduct lateral movement in corporate networks that eventually lead to an encryption with Ransomware. Further information about BumbleBee is avialable on Malpedia
- **Pikabot:** first appeared in early 2023, Pikabot is used to drop Cobalt Strike to conduct lateral movement in corporate networks that eventually lead to an encryption with Ransomware. Further information about Pikabot is avialable on Malpedia

IP address, AS number or AS name

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

Task 5: PhishTool

PhishTool Overview:

- Analyzes phishing emails to identify threats.
- Versions: Community and Enterprise.

Core Features:

1. Email Analysis: Metadata retrieval and analysis.
2. Heuristic Intelligence: OSINT for attack insights.
3. Classification and Reporting: Email classifications and forensic reports**.**

Enterprise Features:

- Manage user-reported phishing.
- Integrate with Microsoft 365 and Google Workspace.

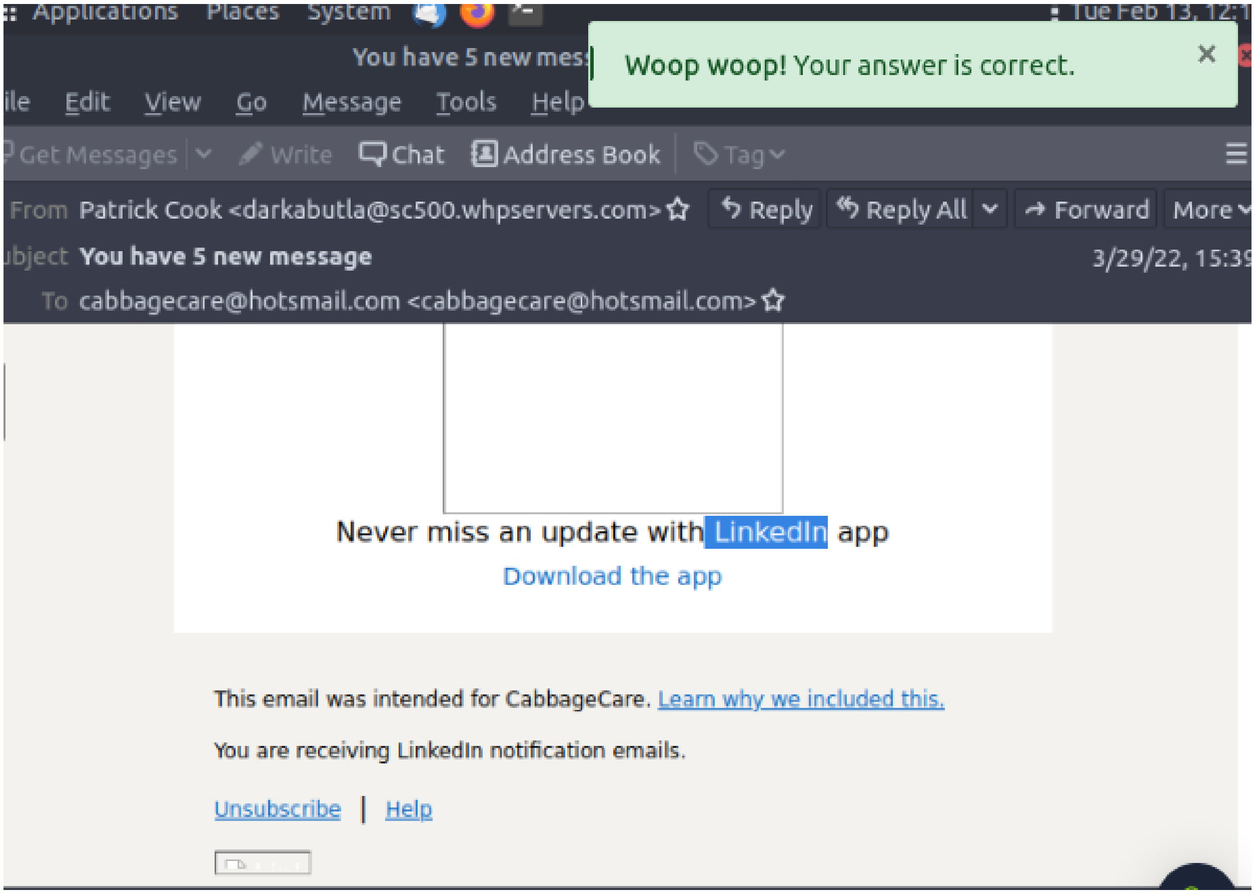
Analysis Process:

- Email headers, security policies, attachments, URLs analysis.
- Resolution: Classifying emails, flagging artefacts.

Example: Email Analysis

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

A: LinkedIn.



You have 5 new mes

Woop woop! Your answer is correct.

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

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

To cabbagecare@hotsmail.com <cabbagecare@hotsmail.com>

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

Q: What is the senders email address?

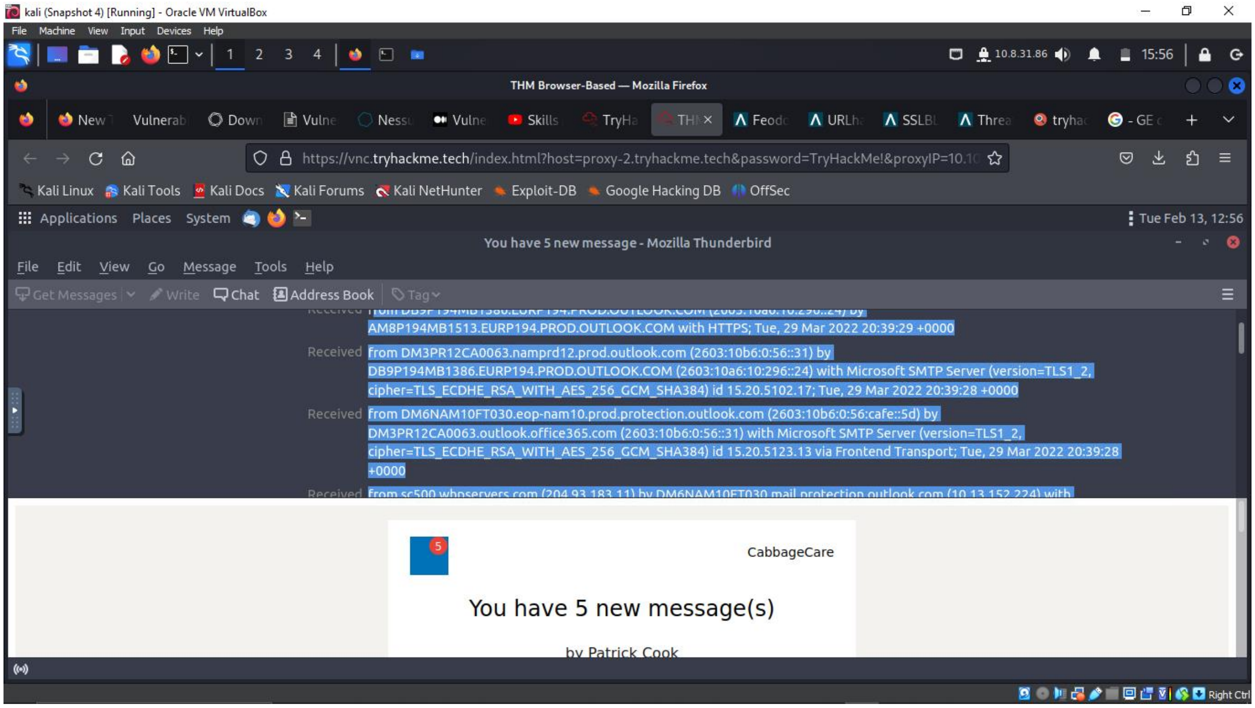
A: darkabutla@sc500.whpservers.com

Q: What is the recipient's email address**?**

A: cabbagecare@hotsmail.com

Q: What is the Originating IP address? Defang the IP address.: 204[.]93[.]183[.]11

A: Email Hops: 4



kali (Snapshot 4) [Running] - Oracle VM VirtualBox

THM Browser-Based — Mozilla Firefox

https://vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=TryHackMe!&proxyIP=10.1

You have 5 new message - Mozilla Thunderbird

```
Received  from DB9P194MB1386.EURP194.PROD.OUTLOOK.COM (2603:10a6:10:296::24) by
          AM8P194MB1513.EURP194.PROD.OUTLOOK.COM with HTTPS; Tue, 29 Mar 2022 20:39:29 +0000
Received  from DM3PR12CA0063.namprd12.prod.outlook.com (2603:10b6:0:56::31) by
          DB9P194MB1386.EURP194.PROD.OUTLOOK.COM (2603:10a6:10:296::24) with Microsoft SMTP Server (version=TLS1_2,
          cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5102.17; 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
```

CabbageCare

You have 5 new message(s)

by Patrick Cook

File Machine View Input Devices Help
1 2 3 4
10.8.31.86
15:56
New Vulnerab Down Vulne Nessu Vulne Skills TryHa THM Feod URLh SSLBl Threa tryhac - GE
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Applications Places System
Tue Feb 13, 12:56
File Edit View Go Message Tools Help
Get Messages Write Chat Address Book Tag
Right Ctrl

Task 6: Cisco Talos Intelligence

Components:

1. Threat Intelligence & Interdiction
2. Detection Research
3. Engineering & Development
4. Vulnerability Research & Discovery
5. Communities
6. Global Outreach

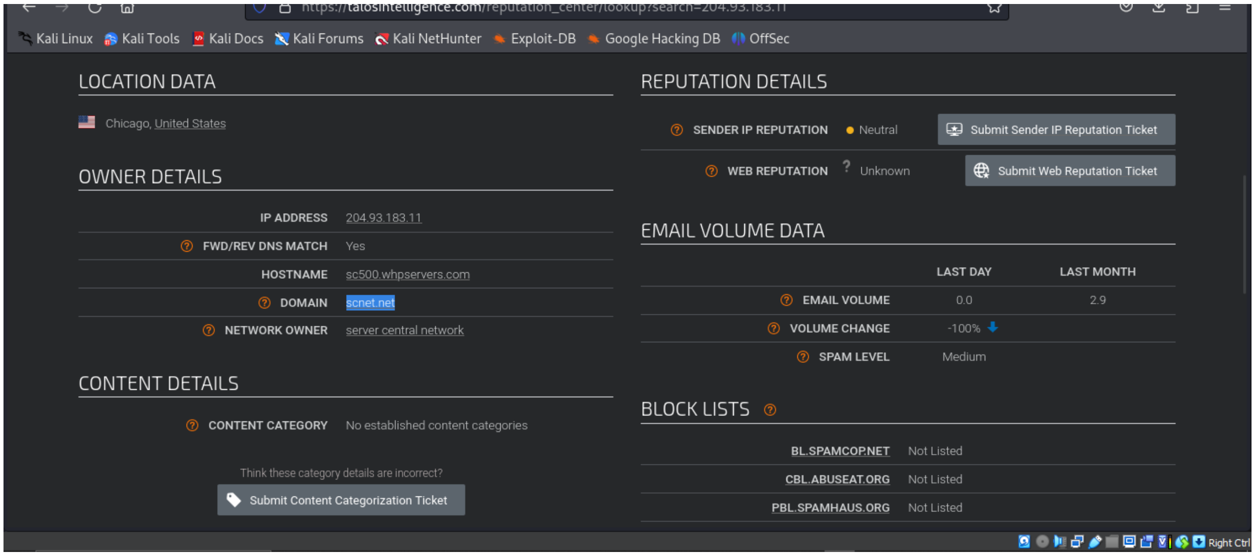
Features:

- Reputation lookup dashboard.
- Vulnerability Information.
- Reputation Center.

Task Application:

Q: What is the listed domain of the IP address from the previous task? (204[.]93[.]183[.]11):

A: scnet.net



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 server central network

CONTENT DETAILS

CONTENT CATEGORY No established content categories

Think these category details are incorrect?

Submit Content Categorization Ticket

REPUTATION DETAILS

SENDER IP REPUTATION ● Neutral — Submit Sender IP Reputation Ticket
WEB REPUTATION ? Unknown — Submit Web Reputation Ticket

EMAIL VOLUME DATA

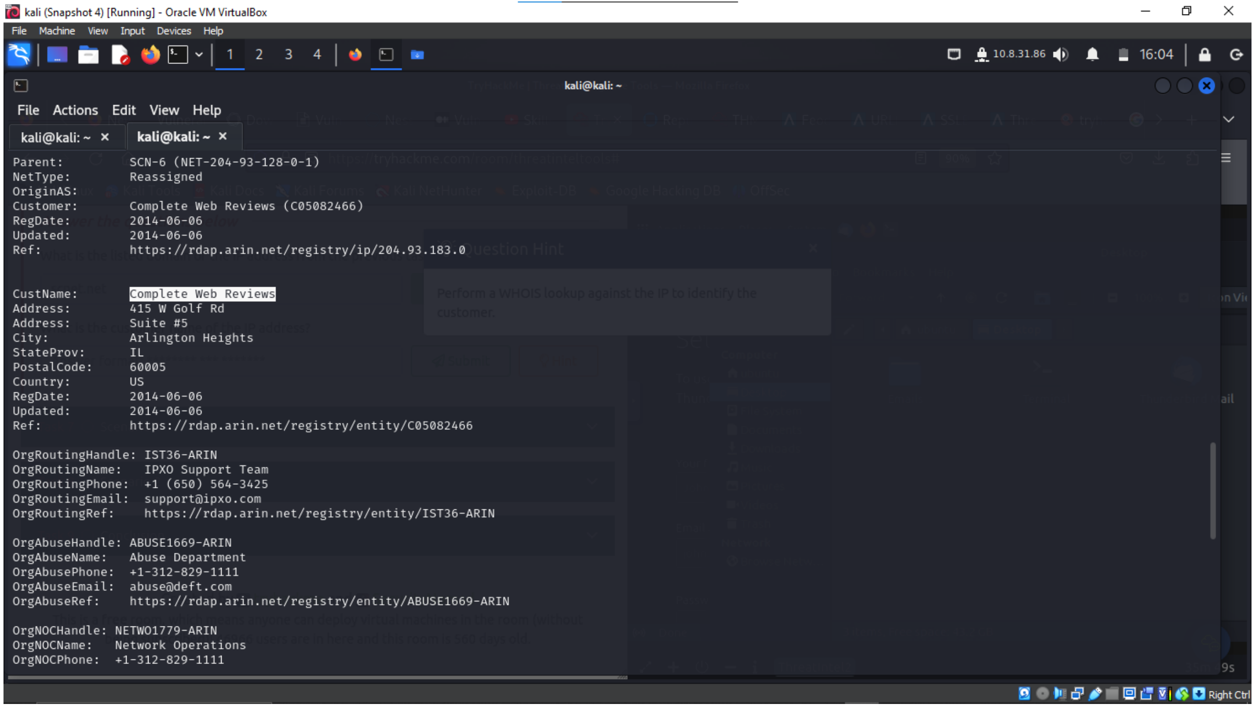
	LAST DAY	LAST MONTH
EMAIL VOLUME	0.0	2.9
VOLUME CHANGE	-100%	
SPAM LEVEL	Medium	

BLOCK LISTS

BL.SPAMCOP.NET Not Listed
CBL.ABUSEAT.ORG Not Listed
PBL.SPAMHAUS.ORG Not Listed

Q: What is the customer's name of the IP address?

- **A: Complete Web Reviews**



kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.8.31.86
16:04
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
Right Ctrl

```
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
Country:        US
RegDate:        2014-06-06
Updated:        2014-06-06
Ref:            https://rdap.arin.net/registry/entity/C05082466

OrgRoutingHandle: IST36-ARIN
OrgRoutingName:   IPXO Support Team
OrgRoutingPhone:  +1 (650) 564-3425
OrgRoutingEmail:  support@ipxo.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/IST36-ARIN

OrgAbuseHandle: ABUSE1669-ARIN
OrgAbuseName:   Abuse Department
OrgAbusePhone:  +1-312-829-1111
OrgAbuseEmail:  abuse@deft.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE1669-ARIN

OrgNOCHandle: NETWO1779-ARIN
OrgNOCName:   Network Operations
OrgNOCPhone:  +1-312-829-1111
```

-

Task 8: Scenario 1

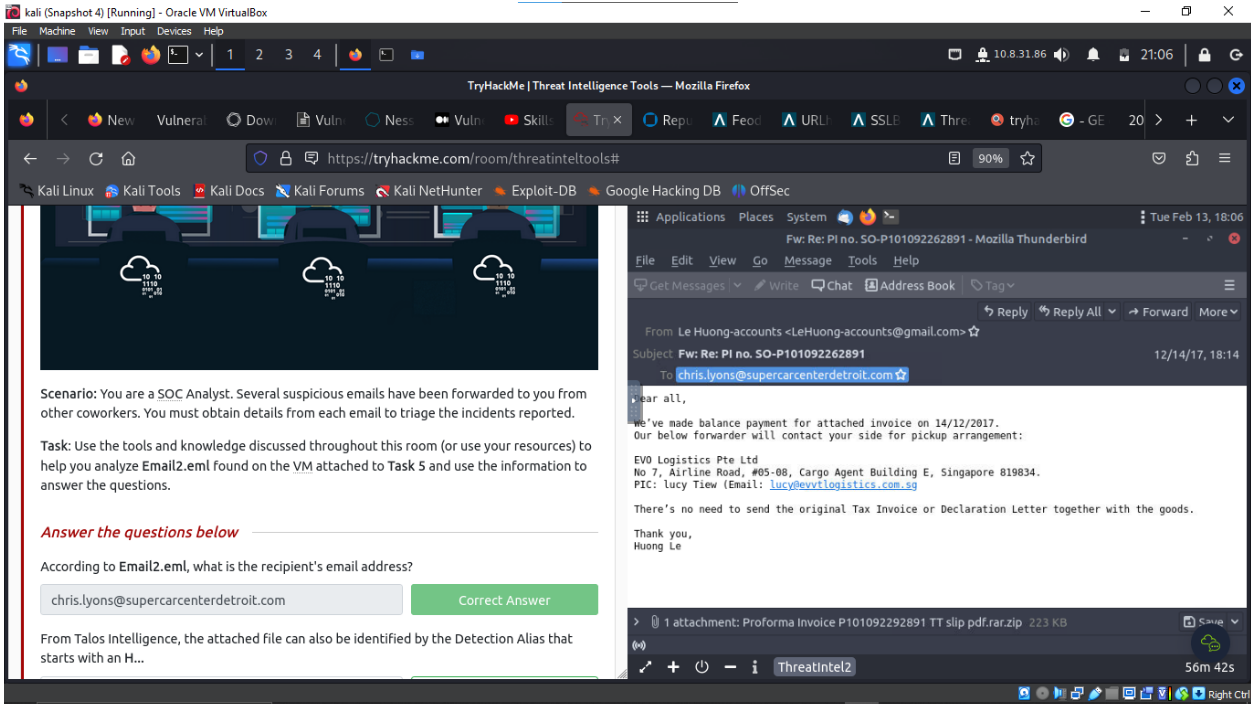
Scenario Analysis:

- Analyze suspicious emails using learned tools and techniques.

Examples:

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

A: **chris.lyons@supercarcenterdetroit.com**



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?

chris.lyons@supercarcenterdetroit.com — Correct Answer

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

Fw: Re: PI no. SO-P101092262891 - Mozilla Thunderbird

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

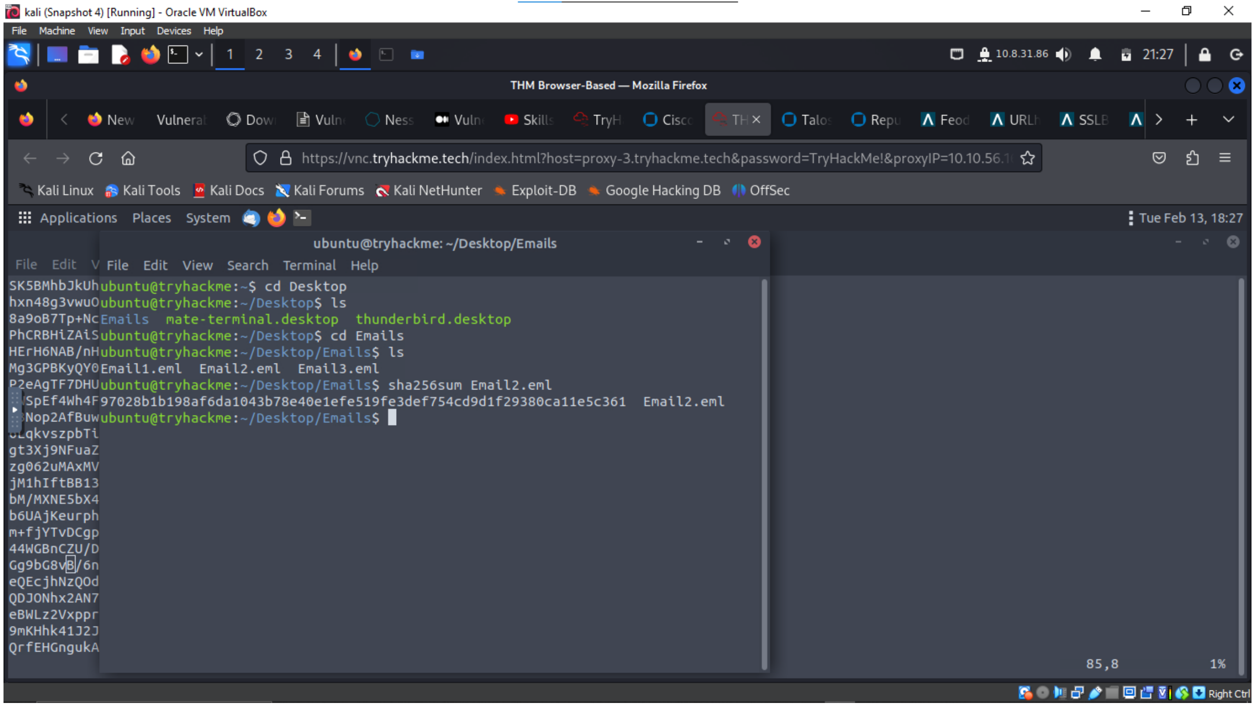
```
Dear all,

We've made balance payment for attached invoice on 14/12/2017.
Our below forwarder will contact your side for pickup arrangement:

EVO Logistics Pte Ltd
No 7, Airline Road, #05-08, Cargo Agent Building E, Singapore 819834.
PIC: lucy Tiew (Email: lucy@evvtlogistics.com.sg

There's no need to send the original Tax Invoice or Declaration Letter together with the goods.

Thank you,
Huong Le
```

1 attachment: Proforma Invoice P101092292891 TT slip pdf.rar.zip 223 KB

kali (Snapshot 4) [Running] - Oracle VM VirtualBox
TryHackMe | Threat Intelligence Tools — Mozilla Firefox
https://tryhackme.com/room/threatinteltools#
Applications Places System
Tue Feb 13, 18:06
ThreatIntel2
56m 42s

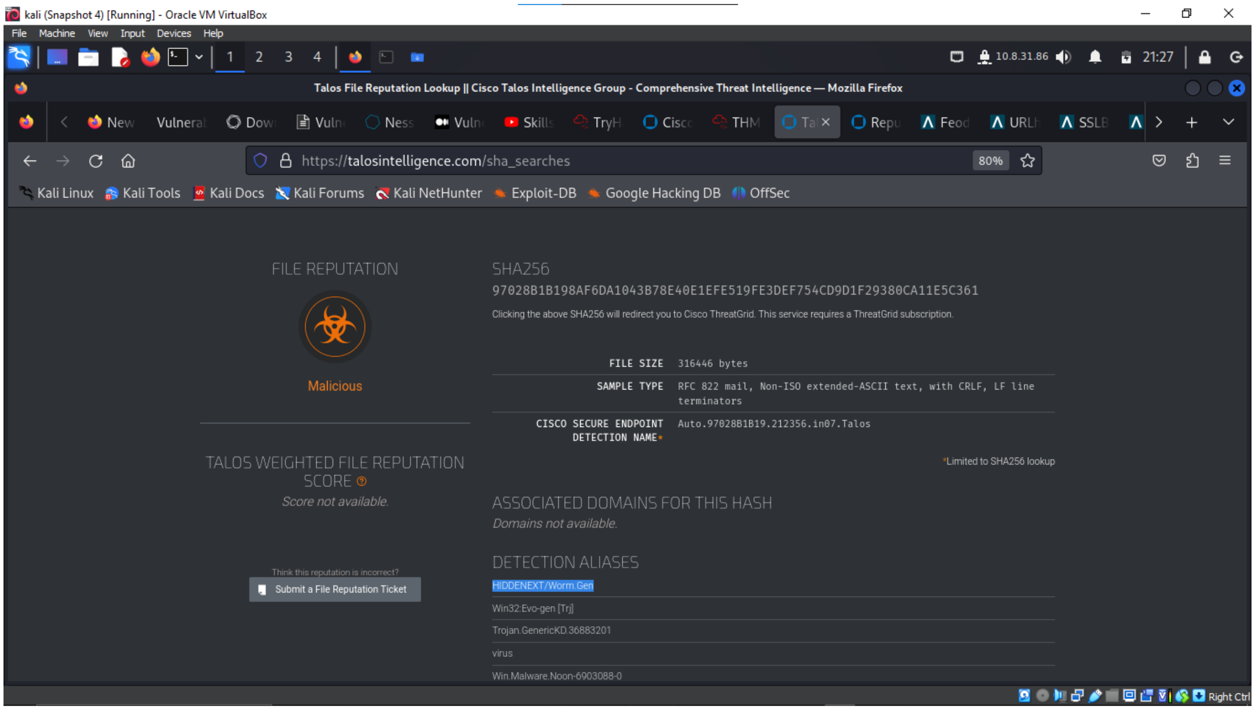
Q: From Talos Intelligence, the attached file can also be identified by the Detection Alias that starts with an H...

A: **HIDDENEXT/Worm.Gen**



```
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
97028b1b198af6da1043b78e40e1efe519fe3def754cd9d1f29380ca11e5c361  Email2.eml
ubuntu@tryhackme:~/Desktop/Emails$ 
```

kali (Snapshot 4) [Running] - Oracle VM VirtualBox
THM Browser-Based — Mozilla Firefox
https://vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=TryHackMe!&proxyIP=10.10.56.1
ubuntu@tryhackme: ~/Desktop/Emails
Tue Feb 13, 18:27
85,8 1%


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.31.86 21:27
Talos File Reputation Lookup || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence — Mozilla Firefox
https://talosintelligence.com/sha_searches
80%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Right Ctrl

FILE REPUTATION

Malicious

SHA256

97028B1B198AF6DA1043B78E40E1EFE519FE3DEF754CD9D1F29380CA11E5C361

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

```
                 FILE SIZE  316446 bytes
               SAMPLE TYPE  RFC 822 mail, Non-ISO extended-ASCII text, with CRLF, LF line
                            terminators
    CISCO SECURE ENDPOINT   Auto.97028B1B19.212356.in07.Talos
          DETECTION NAME*
```

*Limited to SHA256 lookup

TALOS WEIGHTED FILE REPUTATION SCORE

Score not available.

Think this reputation is incorrect?

Submit a File Reputation Ticket

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

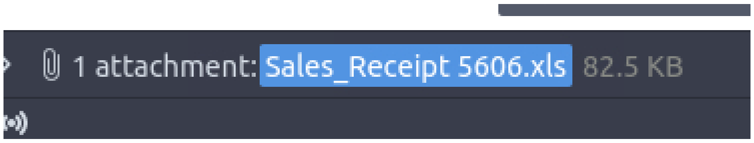
Task 8: Scenario 2

Scenario Analysis:

- Analyze suspicious emails using learned tools and techniques.

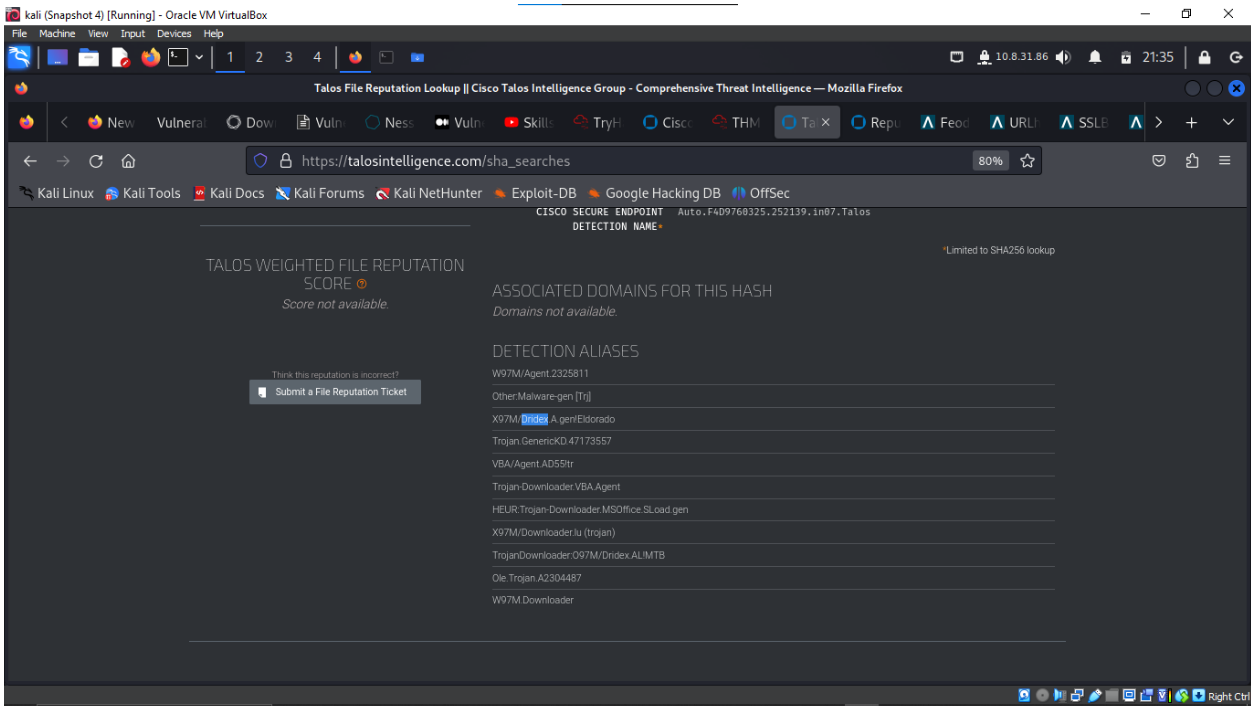
Example: Email3.eml Analysis

- Attachment Name: **Sales_Receipt 5606.xls**



1 attachment: Sales_Receipt 5606.xls 82.5 KB

-
- Associated Malware: **Dridex**


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.31.86 21:35
Talos File Reputation Lookup || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence — Mozilla Firefox
https://talosintelligence.com/sha_searches
80%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Right Ctrl

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

*Limited to SHA256 lookup

TALOS WEIGHTED FILE REPUTATION SCORE

Score not available.

Think this reputation is incorrect?

Submit a File Reputation Ticket

ASSOCIATED DOMAINS FOR THIS HASH

Domains not available.

DETECTION ALIASES

W97M/Agent.2325811

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)

TrojanDownloader:O97M/Dridex.AL!MTB

Ole.Trojan.A2304487

W97M.Downloader

Task 9: Conclusion

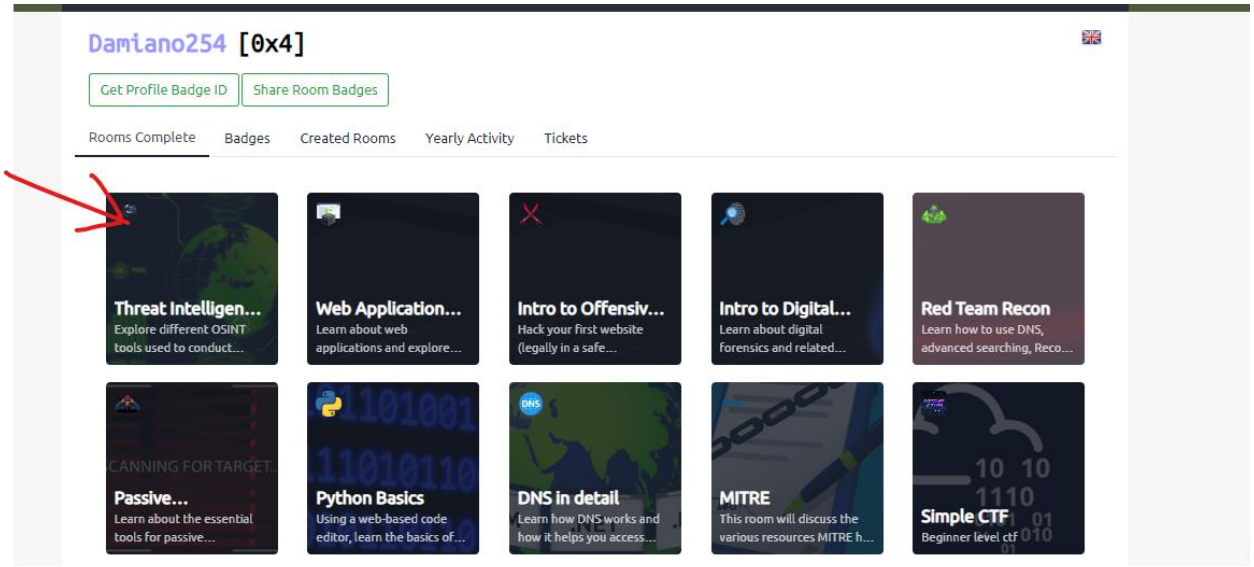
Key Takeaway:

- The discussed tools represent a fraction of available open-source threat intelligence resources.

- Further exploration recommended in Yara, MISP, Red Team Threat Intel.

Conclusion

In summary, the effective use of threat intelligence tools like UrlScan.io, Abuse.ch, PhishTool, and Cisco Talos Intelligence is vital in modern cybersecurity. They offer critical insights for understanding and combating cyber threats, thus playing a significant role in protecting digital infrastructures.



Threat Intelligen...
Explore different OSINT tools used to conduct...

Web Application...
Learn about web applications and explore...

Intro to Offensiv...
Hack your first website (legally in a safe...

Intro to Digital...
Learn about digital forensics and related...

Red Team Recon
Learn how to use DNS, advanced searching, Reco...

Passive...
Learn about the essential tools for passive...

Python Basics
Using a web-based code editor, learn the basics of...

DNS in detail
Learn how DNS works and how it helps you access...

MITRE
This room will discuss the various resources MITRE h...

Simple CTF
Beginner level ctf