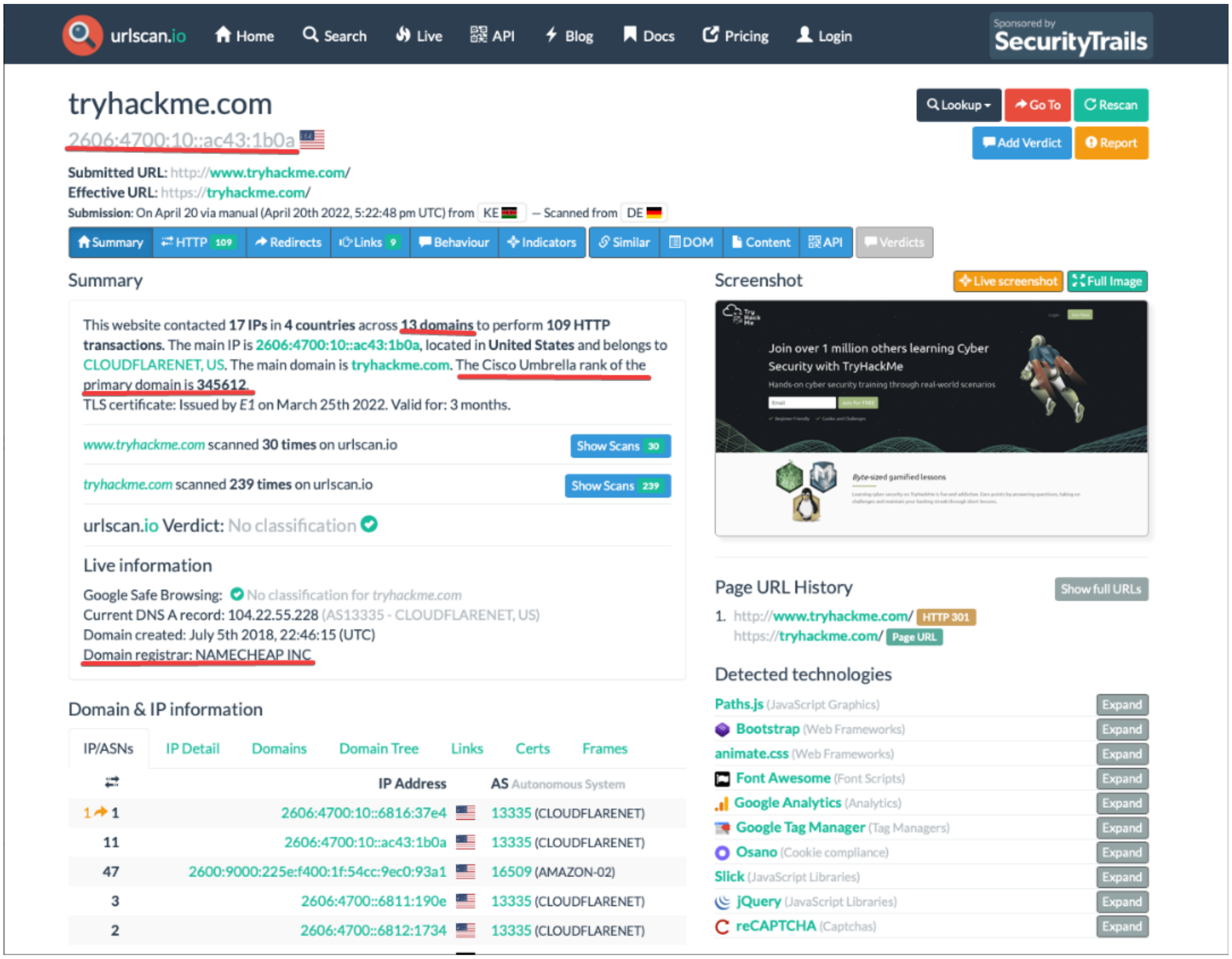
Task3: URLScan.io

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-



tryhackme.com

2606:4700:10::ac43:1b0a

Submitted URL: http://www.tryhackme.com/
Effective URL: https://tryhackme.com/
Submission: On April 20 via manual (April 20th 2022, 5:22:48 pm UTC) from KE — Scanned from DE

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.**
TLS certificate: Issued by *E1* on March 25th 2022. Valid for: 3 months.

www.tryhackme.com scanned **30 times** on urlscan.io — Show Scans 30

tryhackme.com scanned **239 times** on urlscan.io — Show Scans 239

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

Domain & IP information

IP/ASNs | IP Detail | Domains | Domain Tree | Links | Certs | Frames

⇄	IP Address	AS Autonomous System
1 → 1	2606:4700:10::6816:37e4	13335 (CLOUDFLARENET)
11	2606:4700:10::ac43:1b0a	13335 (CLOUDFLARENET)
47	2600:9000:225e:f400:1f:54cc:9ec0:93a1	16509 (AMAZON-02)
3	2606:4700::6811:190e	13335 (CLOUDFLARENET)
2	2606:4700::6812:1734	13335 (CLOUDFLARENET)

Screenshot

Page URL History

1. http://www.tryhackme.com/ HTTP 301
https://tryhackme.com/ Page URL

Detected technologies

Paths.js (JavaScript Graphics)	Expand
Bootstrap (Web Frameworks)	Expand
animate.css (Web Frameworks)	Expand
Font Awesome (Font Scripts)	Expand
Google Analytics (Analytics)	Expand
Google Tag Manager (Tag Managers)	Expand
Osano (Cookie compliance)	Expand
Slick (JavaScript Libraries)	Expand
jQuery (JavaScript Libraries)	Expand
reCAPTCHA (Captchas)	Expand

Q: What is TryHackMe’s Cisco Umbrella Rank?

A: *345612*

Q: How many domains did UrlScan.io identify?

A: *13*

Q: What is the main domain registrar listed?

A: *NAMECHEAP INC*

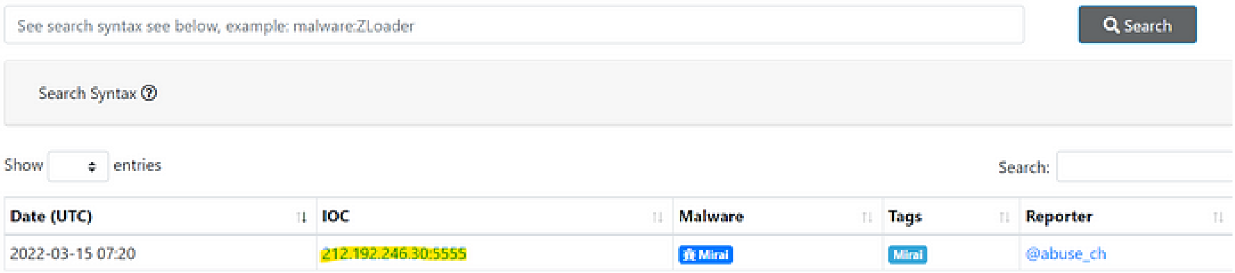
Q: What is the main IP address identified?

A: *2606:4700:10::ac43:1b0a*

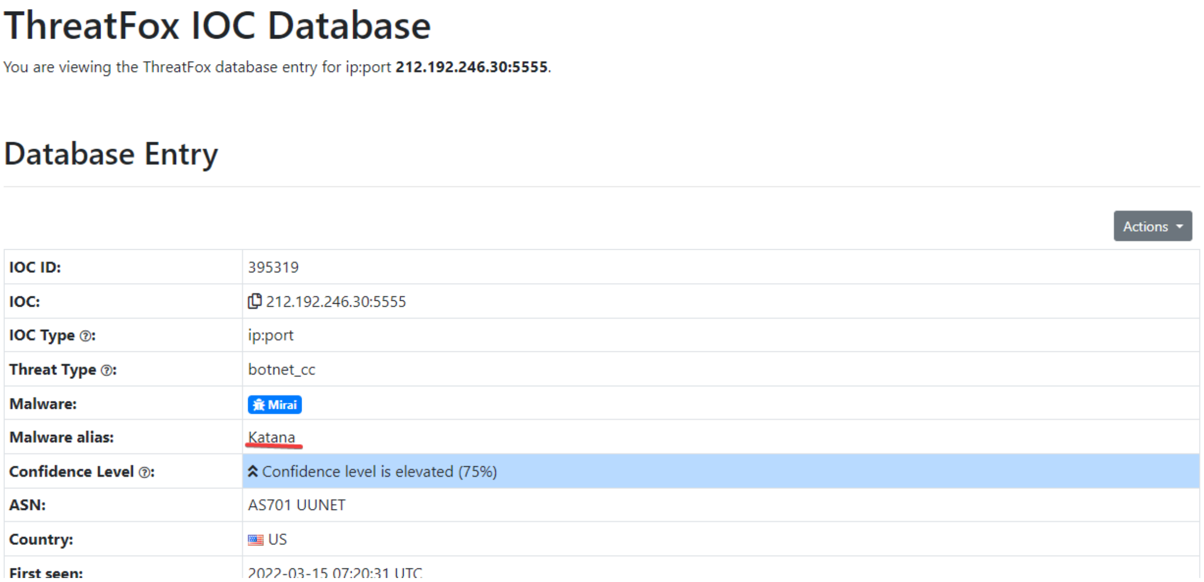
Task4: Abuse.ch

Q: The IOC *212.192.246.30:5555* is linked to which malware on ThreatFox?

Type **ioc:212.192.246.30:5555** in the search box



Date (UTC)	IOC	Malware	Tags	Reporter
2022-03-15 07:20	212.192.246.30:5555	Mirai	Mirai	@abuse_ch



ThreatFox IOC Database

You are viewing the ThreatFox database entry for ip:port **212.192.246.30:5555**.

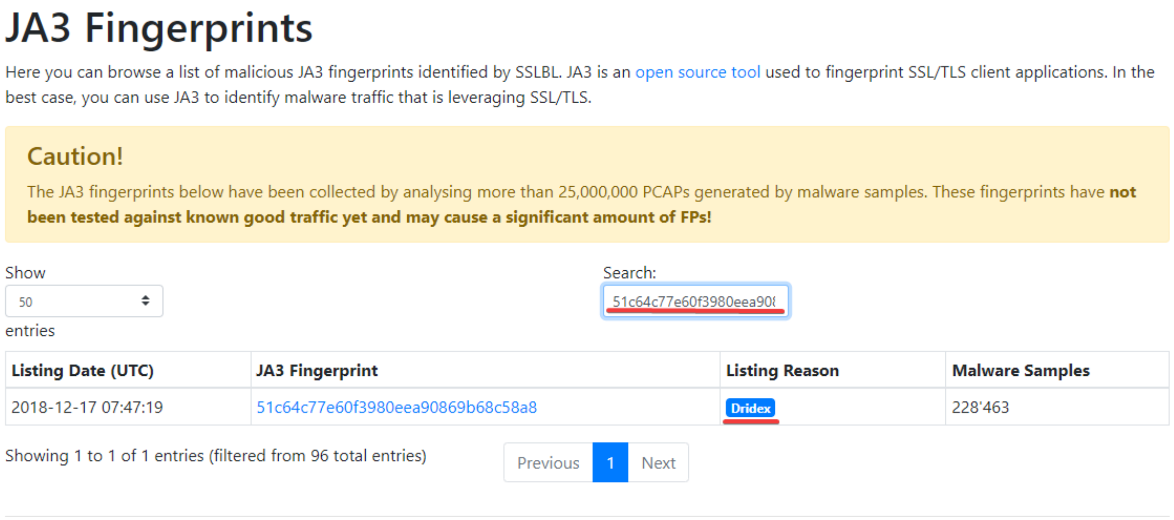
Database Entry

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%)
ASN:	AS701 UUNET
Country:	US
First seen:	2022-03-15 07:20:31 UTC

A: Katana

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

Goto SSl blacklist, and click on the ja3 fingerprints tab. In the search bar put the fingerprint and look it up:



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: 51c64c77e60f3980eea90

Listing Date (UTC)	JA3 Fingerprint	Listing Reason	Malware Samples
2018-12-17 07:47:19	51c64c77e60f3980eea90869b68c58a8	Dridex	228'463

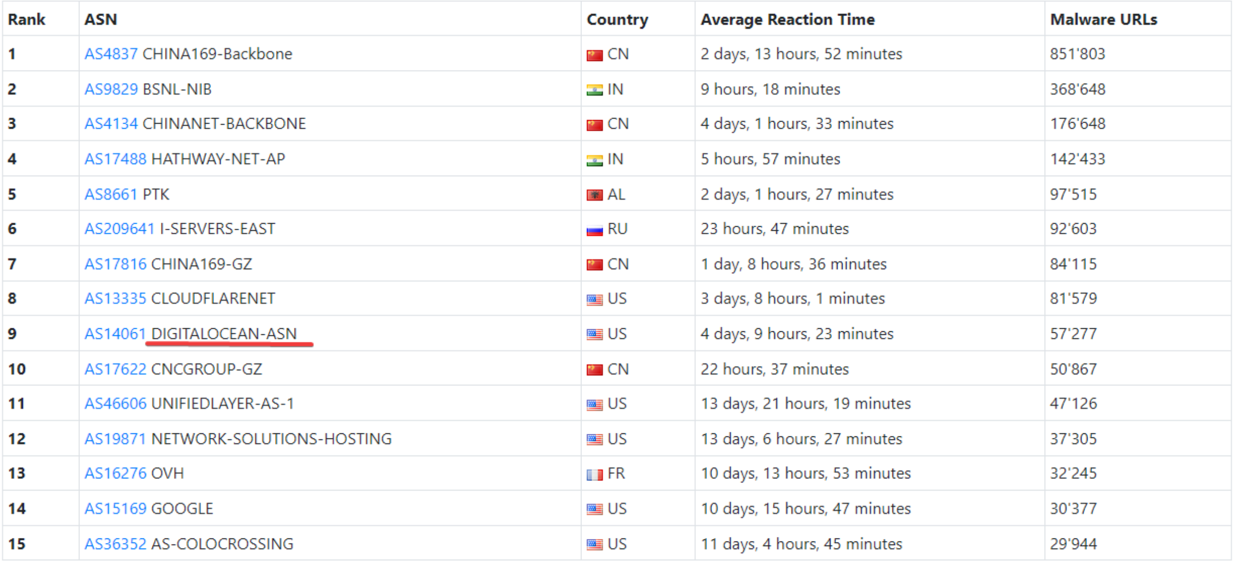
Showing 1 to 1 of 1 entries (filtered from 96 total entries)

A: Dridex

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

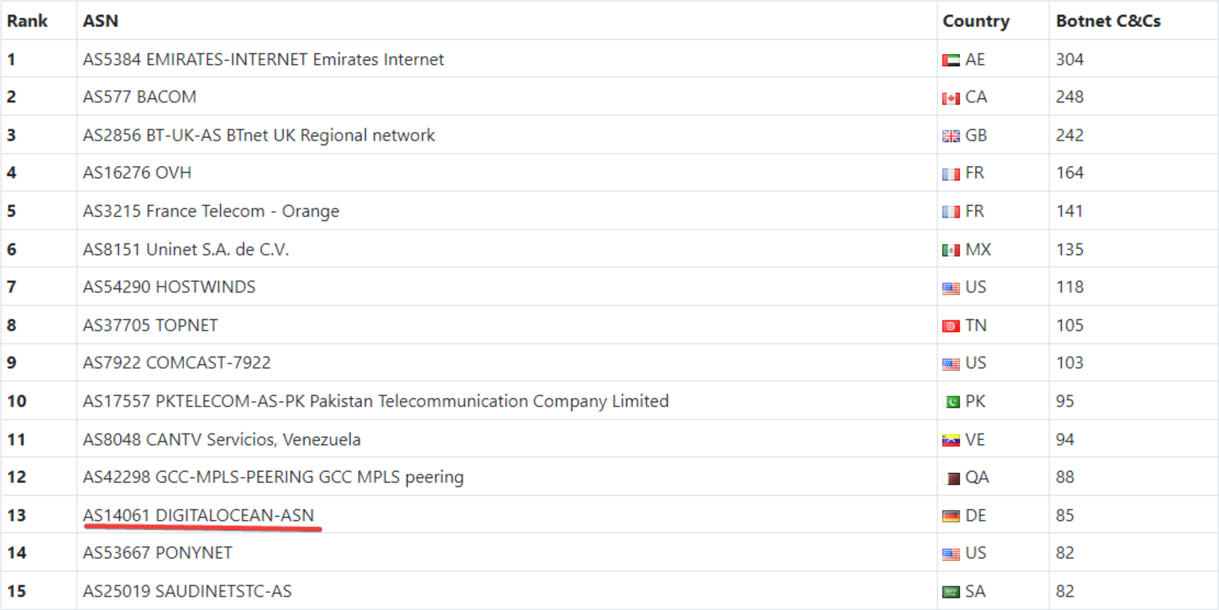
Using URLHaus —

Go to https://urlhaus.abuse.ch/statistics/ and scroll down :



Rank	ASN	Country	Average Reaction Time	Malware URLs
1	AS4837 CHINA169-Backbone	CN	2 days, 13 hours, 52 minutes	851'803
2	AS9829 BSNL-NIB	IN	9 hours, 18 minutes	368'648
3	AS4134 CHINANET-BACKBONE	CN	4 days, 1 hours, 33 minutes	176'648
4	AS17488 HATHWAY-NET-AP	IN	5 hours, 57 minutes	142'433
5	AS8661 PTK	AL	2 days, 1 hours, 27 minutes	97'515
6	AS209641 I-SERVERS-EAST	RU	23 hours, 47 minutes	92'603
7	AS17816 CHINA169-GZ	CN	1 day, 8 hours, 36 minutes	84'115
8	AS13335 CLOUDFLARENET	US	3 days, 8 hours, 1 minutes	81'579
9	AS14061 DIGITALOCEAN-ASN	US	4 days, 9 hours, 23 minutes	57'277
10	AS17622 CNCGROUP-GZ	CN	22 hours, 37 minutes	50'867
11	AS46606 UNIFIEDLAYER-AS-1	US	13 days, 21 hours, 19 minutes	47'126
12	AS19871 NETWORK-SOLUTIONS-HOSTING	US	13 days, 6 hours, 27 minutes	37'305
13	AS16276 OVH	FR	10 days, 13 hours, 53 minutes	32'245
14	AS15169 GOOGLE	US	10 days, 15 hours, 47 minutes	30'377
15	AS36352 AS-COLOCROSSING	US	11 days, 4 hours, 45 minutes	29'944

We can also get the details using FeodoTracker :

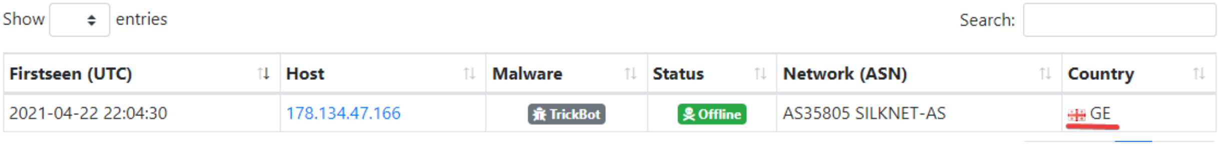


Rank	ASN	Country	Botnet C&Cs
1	AS5384 EMIRATES-INTERNET Emirates Internet	AE	304
2	AS577 BACOM	CA	248
3	AS2856 BT-UK-AS BTnet UK Regional network	GB	242
4	AS16276 OVH	FR	164
5	AS3215 France Telecom - Orange	FR	141
6	AS8151 Uninet S.A. de C.V.	MX	135
7	AS54290 HOSTWINDS	US	118
8	AS37705 TOPNET	TN	105
9	AS7922 COMCAST-7922	US	103
10	AS17557 PKTELECOM-AS-PK Pakistan Telecommunication Company Limited	PK	95
11	AS8048 CANTV Servicios, Venezuela	VE	94
12	AS42298 GCC-MPLS-PEERING GCC MPLS peering	QA	88
13	AS14061 DIGITALOCEAN-ASN	DE	85
14	AS53667 PONYNET	US	82
15	AS25019 SAUDINETSTC-AS	SA	82

A: DIGITALOCEAN-ASN

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

Type in the ip address in the search bar and you will see it immediately

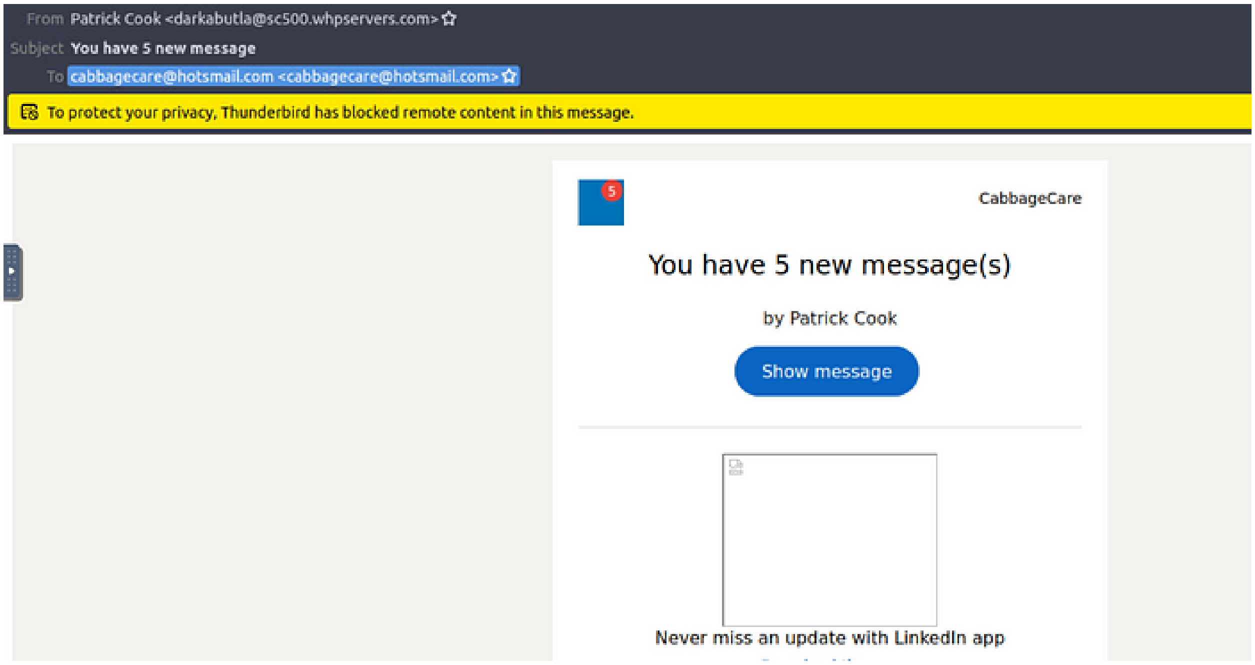


Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Country
2021-04-22 22:04:30	178.134.47.166	TrickBot	Offline	AS35805 SILKNET-AS	GE

A: Georgia

Task 5: PhishTool

You are a SOC Analyst and have been tasked to analyze a suspicious email **Email1.eml**. Use the tool and skills learnt on this task to answer the questions.



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

Subject You have 5 new message

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

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

CabbageCare

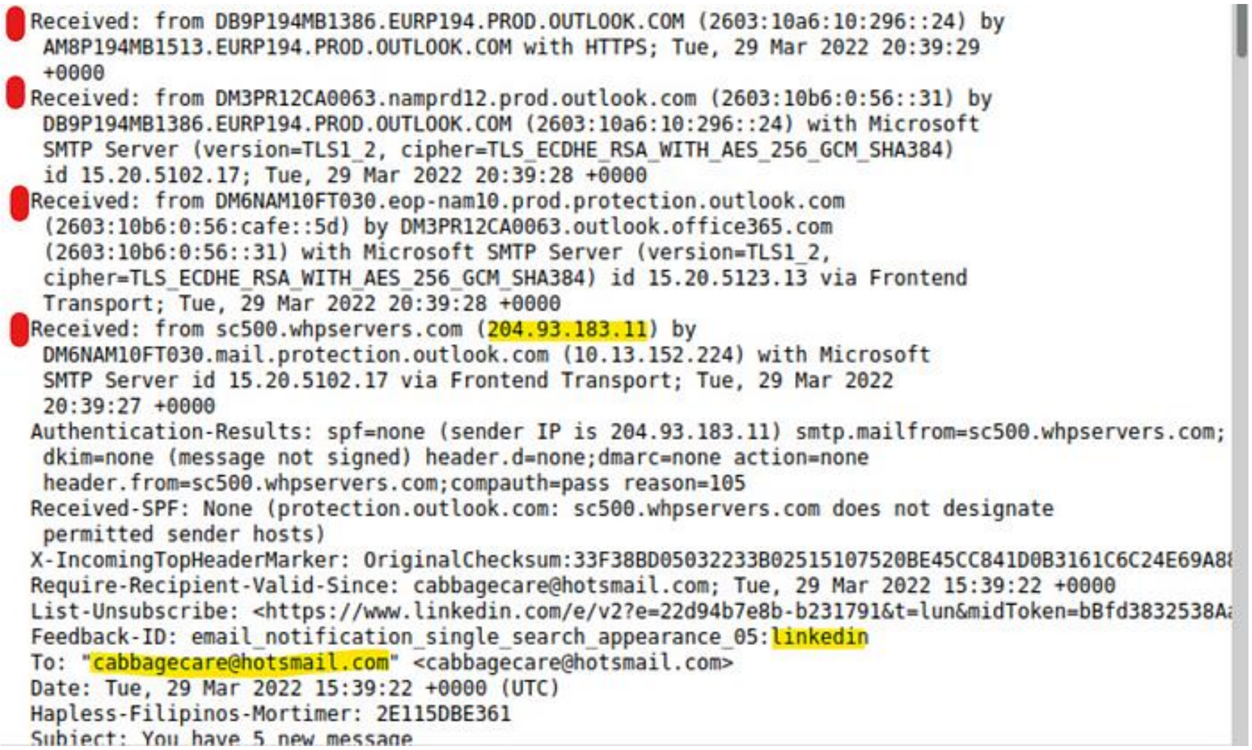
You have 5 new message(s)

by Patrick Cook

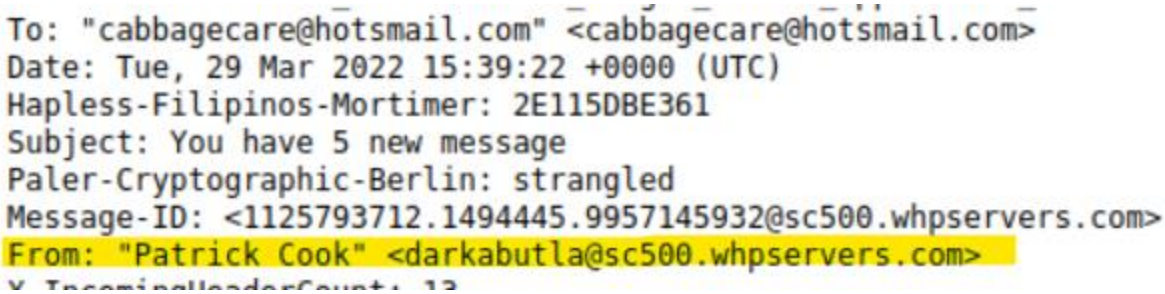
Never miss an update with LinkedIn app

email1.eml

I will show you how to get these details using headers of the mail. You can use phishtool and Talos too for the analysis part. If you just open this email with a text editor, you will see the header. And find all the information in it



```
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 Microsoft
 SMTP Server id 15.20.5102.17 via Frontend Transport; Tue, 29 Mar 2022
 20:39:27 +0000
Authentication-Results: spf=none (sender IP is 204.93.183.11) smtp.mailfrom=sc500.whpservers.com;
 dkim=none (message not signed) header.d=none;dmarc=none action=none
 header.from=sc500.whpservers.com;compauth=pass reason=105
Received-SPF: None (protection.outlook.com: sc500.whpservers.com does not designate
 permitted sender hosts)
X-IncomingTopHeaderMarker: OriginalChecksum:33F38BD05032233B02515107520BE45CC841D0B3161C6C24E69A8
Require-Recipient-Valid-Since: cabbagecare@hotsmail.com; Tue, 29 Mar 2022 15:39:22 +0000
List-Unsubscribe: <https://www.linkedin.com/e/v2?e=22d94b7e8b-b231791&t=lun&midToken=bBfd3832538A
Feedback-ID: email_notification_single_search_appearance_05:linkedin
To: "cabbagecare@hotsmail.com" <cabbagecare@hotsmail.com>
Date: Tue, 29 Mar 2022 15:39:22 +0000 (UTC)
Hapless-Filipinos-Mortimer: 2E115DBE361
Subject: You have 5 new message
```



```
To: "cabbagecare@hotsmail.com" <cabbagecare@hotsmail.com>
Date: Tue, 29 Mar 2022 15:39:22 +0000 (UTC)
Hapless-Filipinos-Mortimer: 2E115DBE361
Subject: You have 5 new message
Paler-Cryptographic-Berlin: strangled
Message-ID: <1125793712.1494445.9957145932@sc500.whpservers.com>
From: "Patrick Cook" <darkabutla@sc500.whpservers.com>
X-IncomingHeaderCount: 13
```

Q: What organization is the attacker trying to pose as in the email?

A: *LinkedIn*

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.

A: *204[.]93[.]183[.]11*

Q: How many hops did the email go through to get to the recipient?

A: 4

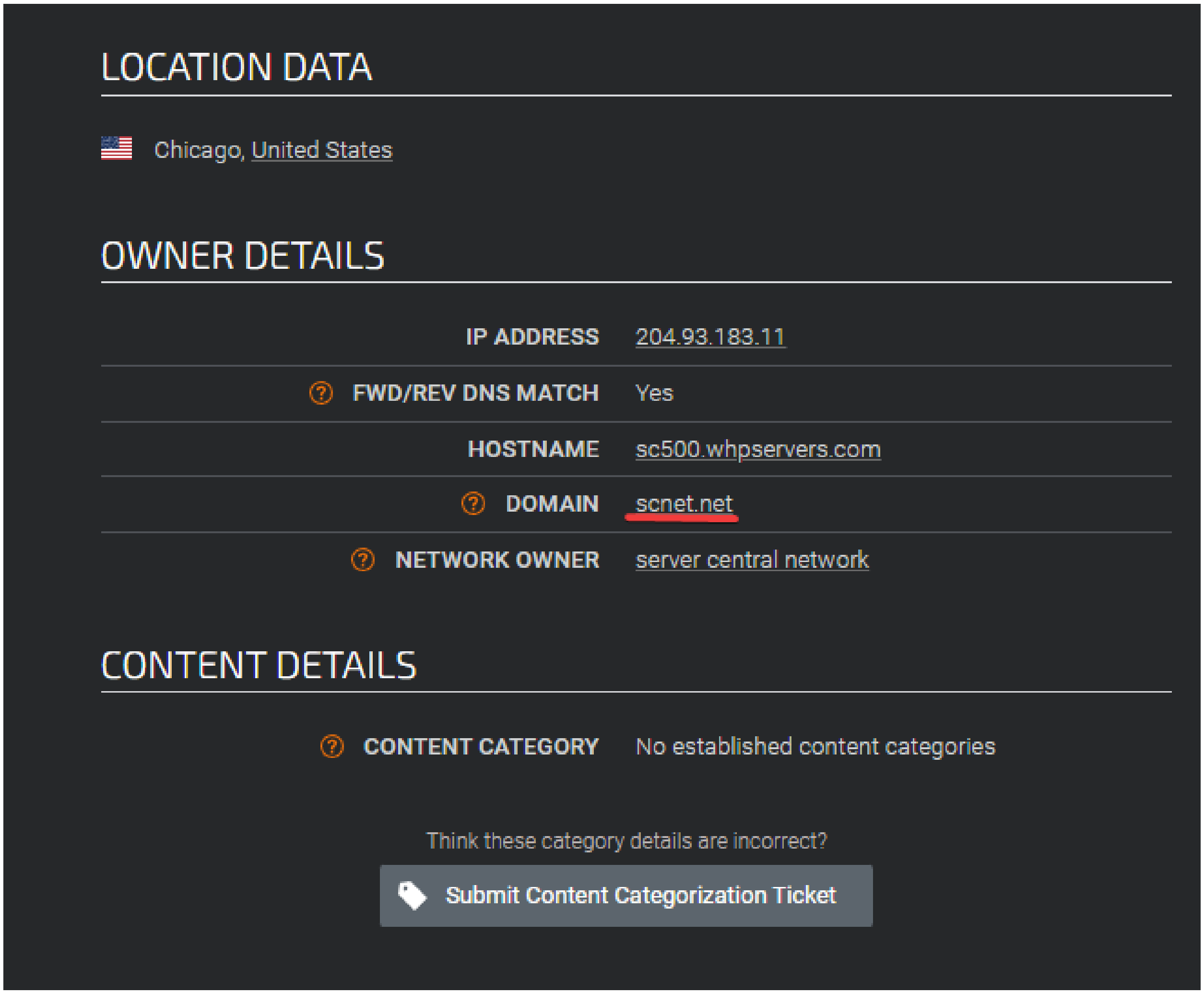
Task6: Cisco Talos Intelligence

Use the .eml file you've downloaded in the previous task, PhishTool, to answer the following questions.

Answer the questions below

Here, I used Whois.com and AbuseIPDB for getting the details of the IP. Like this, you can use multiple open source tools for the analysis..

Q: What is the listed domain of the IP address from the previous task?



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

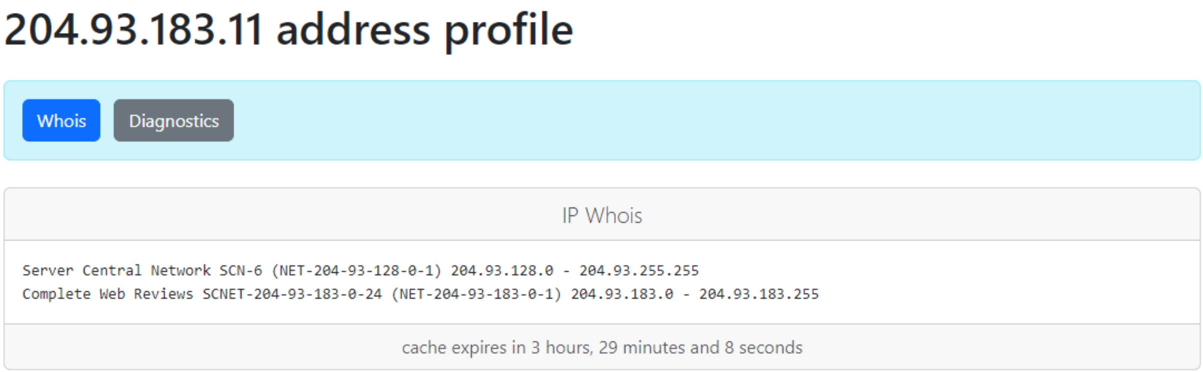
CONTENT CATEGORY	No established content categories

Think these category details are incorrect?

A: *scnet.net*

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

Using who.is we can lookup the ip and find this:



204.93.183.11 address profile

IP Whois

```
Server Central Network SCN-6 (NET-204-93-128-0-1) 204.93.128.0 - 204.93.255.255
Complete Web Reviews SCNET-204-93-183-0-24 (NET-204-93-183-0-1) 204.93.183.0 - 204.93.183.255
```

cache expires in 3 hours, 29 minutes and 8 seconds

A: *Complete Web Reviews*

Task 7 : 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 discussed throughout this room (or use your resources) to help you analyze **Email2.eml** and use the information to answer the questions.

Download the task files first —

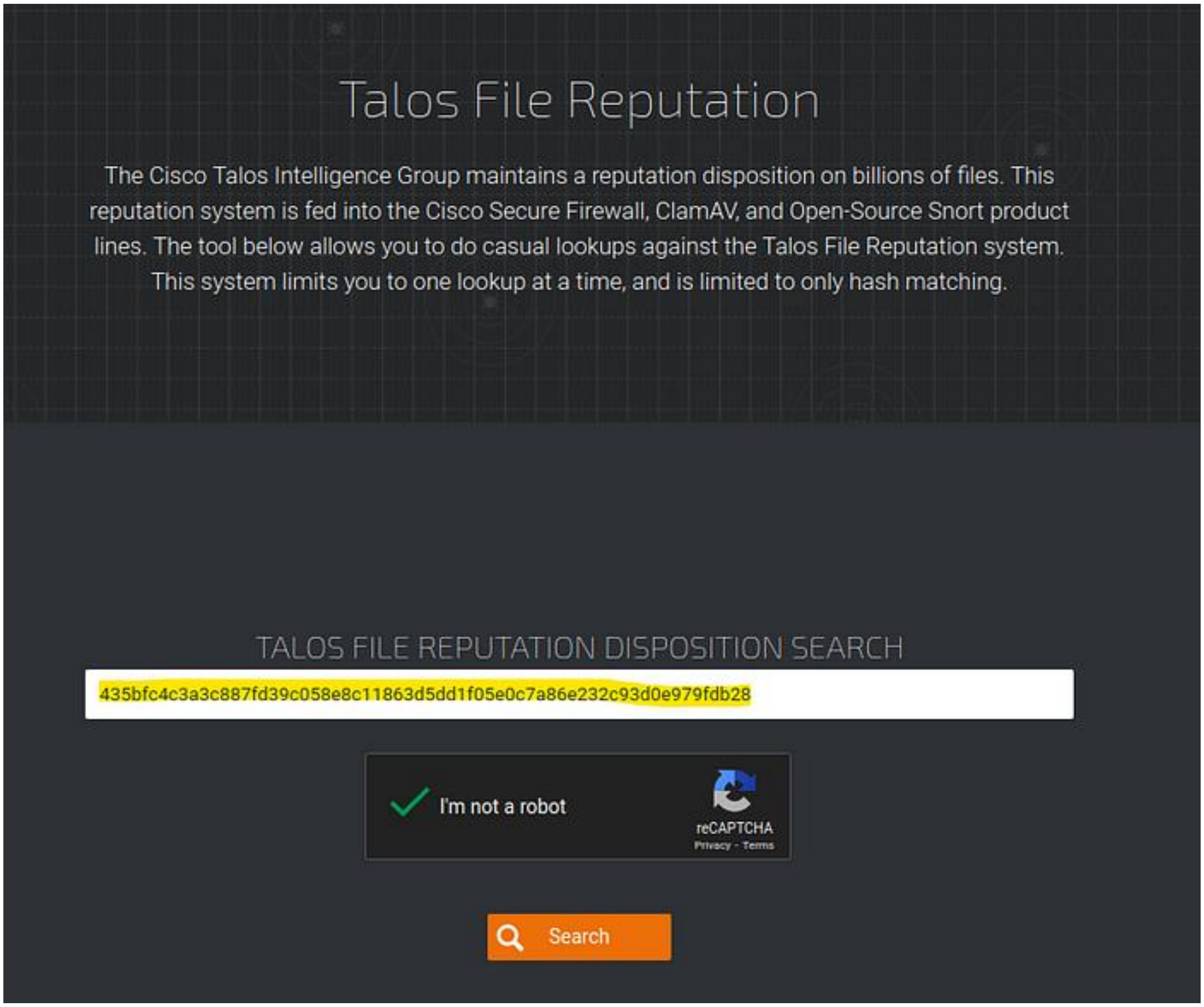
Q: According to Email2.eml, what is the recipient's email address?

If you open the email in a text editor, you will find the email address in the header:

A: chris.lyons@supercarcenterdetroit.com

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

Go to attachments and copy the SHA-256 hash. Open Cisco Talos and check the reputation of the file. You will get the alias name. (hint given : starts with H)



Talos File Reputation

The Cisco Talos Intelligence Group maintains a reputation disposition on billions of files. This reputation system is fed into the Cisco Secure Firewall, ClamAV, and Open-Source Snort product lines. The tool below allows you to do casual lookups against the Talos File Reputation system. This system limits you to one lookup at a time, and is limited to only hash matching.

TALOS FILE REPUTATION DISPOSITION SEARCH

435bfc4c3a3c887fd39c058e8c11863d5dd1f05e0c7a86e232c93d0e979fdb28

A: HIDDENEXT/Worm.Gen

————————————————————————————————

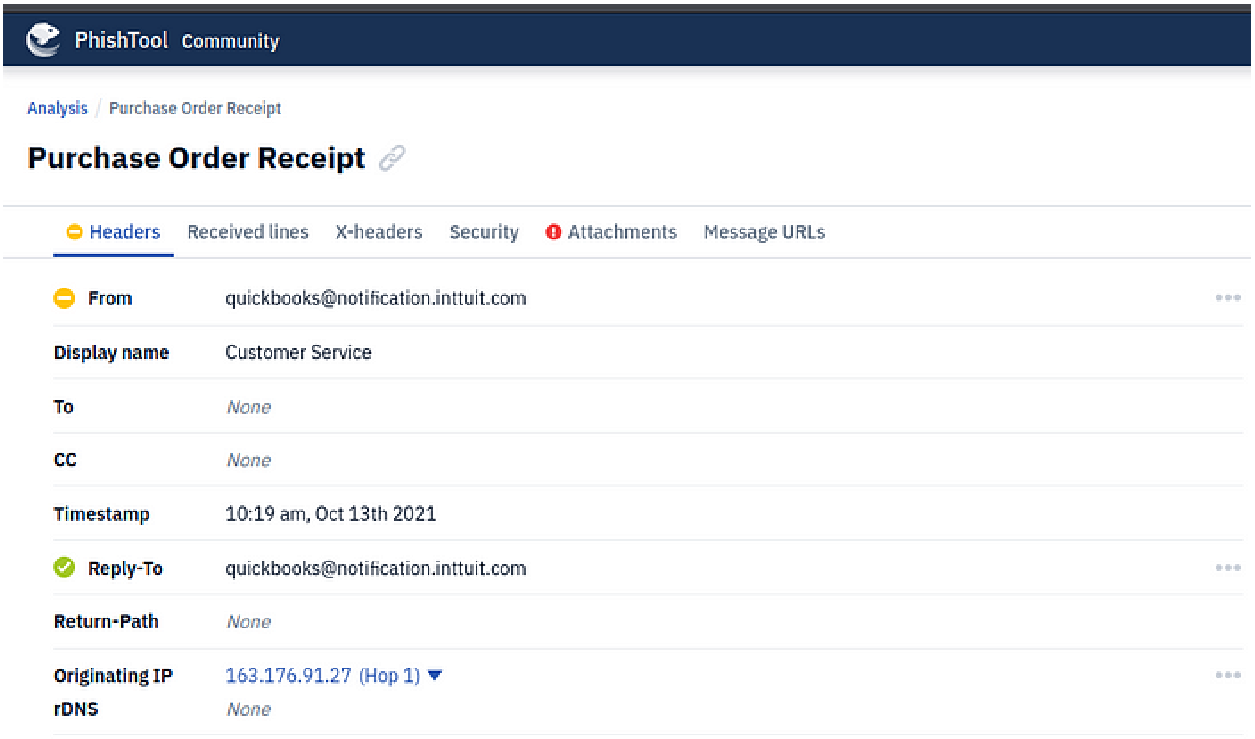
Task 8 : Scenario

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 discussed throughout this room (or use your resources) to help you analyze **Email3.eml** and use the information to answer the questions.

Download the task files first..

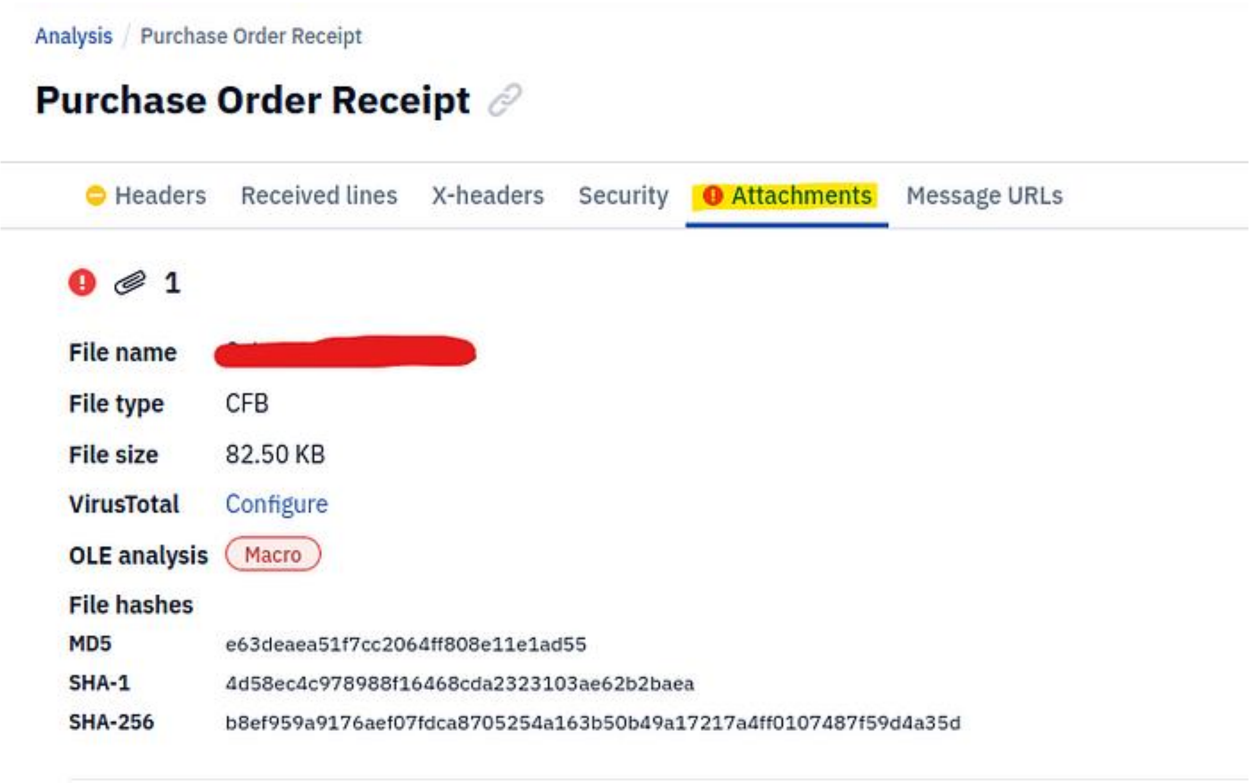
Q: What is the name of the attachment on Email3.eml?



Purchase Order Receipt

From	quickbooks@notification.inttuit.com
Display name	Customer Service
To	*None*
CC	*None*
Timestamp	10:19 am, Oct 13th 2021
Reply-To	quickbooks@notification.inttuit.com
Return-Path	*None*
Originating IP	163.176.91.27 (Hop 1)
rDNS	*None*

Go to Attachments option



Purchase Order Receipt

File name	[redacted]
File type	CFB
File size	82.50 KB
VirusTotal	Configure
OLE analysis	Macro

File hashes

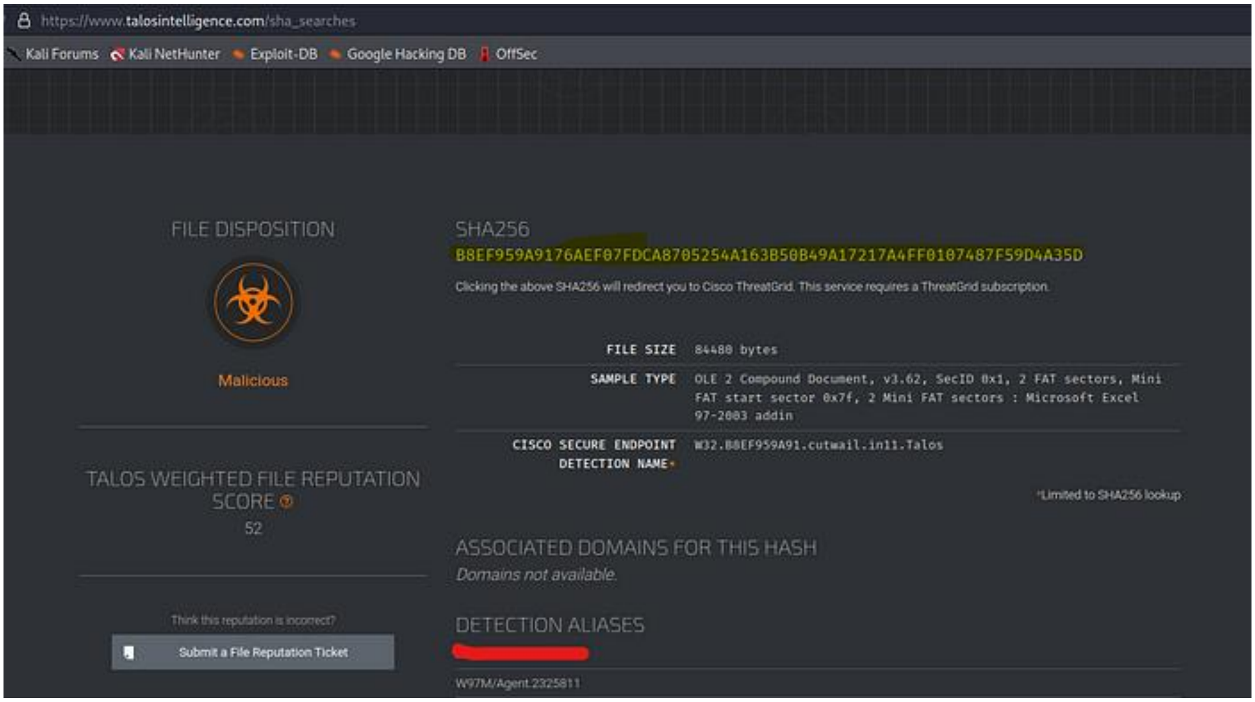
MD5	e63deaea51f7cc2064ff808e11e1ad55
SHA-1	4d58ec4c978988f16468cda2323103ae62b2baea
SHA-256	b8ef959a9176aef07fdca8705254a163b50b49a17217a4ff0107487f59d4a35d

A: Sales_Receipt 5606.xls

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

A: Dridex

Copy the SHA-256 hash and open Cisco Talos and check the reputation of the file. You will find the malware family here.



https://www.talosintelligence.com/sha_searches
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

FILE DISPOSITION

Malicious

TALOS WEIGHTED FILE REPUTATION SCORE

52

Think this reputation is incorrect?

Submit a File Reputation Ticket

SHA256

B8EF959A9176AEF07FDCA8705254A163B50B49A17217A4FF0107487F59D4A35D

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

```
                 FILE SIZE  84480 bytes
               SAMPLE TYPE  OLE 2 Compound Document, v3.62, SecID 0x1, 2 FAT sectors, Mini
                            FAT start sector 0x7f, 2 Mini FAT sectors : Microsoft Excel
                            97-2003 addin
   CISCO SECURE ENDPOINT    W32.B8EF959A91.cutwail.in11.Talos
           DETECTION NAME*
```

*Limited to SHA256 lookup

ASSOCIATED DOMAINS FOR THIS HASH

Domains not available.

DETECTION ALIASES

[redacted]

W97M/Agent.2325811