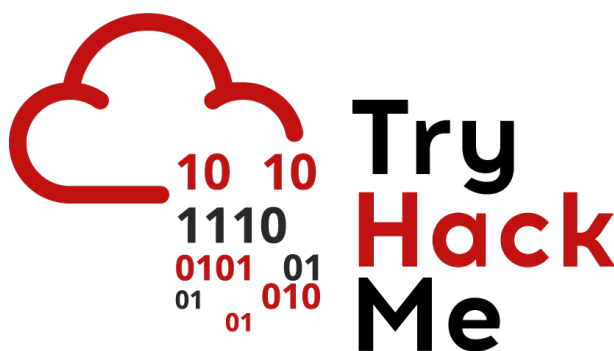


Writeup: Sala *Threat Intelligence Tools*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción	2
2. Sala	2
2.1. Tarea 1 – Esquema de la sala	2
2.2. Tarea 2 - Inteligencia de Amenazas	2
2.3. Tarea 3 - UrlScan.io	2
2.4. Tarea 4 - Abuse.ch	3
2.5. Tarea 5 - PhishTool	4
2.6. Tarea 6 - Inteligencia de Cisco Talos	9
2.7. Tarea 7 - Escenario 1	10
2.8. Tarea 8 - Escenario 2	13
2.9. Tarea 9 - Conclusion	16
3. Conclusión sobre la Sala	16

1. Introducción

En esta sala se explorarán plataformas clave como UrlScan.io, Abuse.ch, Phish-Tool y Cisco Talos, aprendiendo a recolectar, analizar y correlacionar indicadores de compromiso (IOCs). También, incluye escenarios prácticos en los que se asume el rol de un analista SOC enfrentando correos sospechosos.

2. Sala

2.1. Tarea 1 – Esquema de la sala

En esta primera tarea nos explica los conceptos que se abordarán de inteligencia de amenazas, las diversas herramientas de código abierto útiles y nos deja los objetivos de aprendizaje de la sala.

Pregunta: Read the description! Continue to the next task.

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.2. Tarea 2 - Inteligencia de Amenazas

Aprenderemos qué es la inteligencia de amenazas, la recolección y análisis de datos para detectar patrones y proteger a organizaciones de amenazas emergentes. También, conoceremos sobre cómo podemos clasificar la inteligencia de amenazas en las siguientes categorías:

- **Estratégica**
- **Técnica**
- **Táctica**
- **Operacional**

Pregunta: I've read on Threat Intel and the classifications

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.3. Tarea 3 - UrlScan.io

Aprenderemos sobre [UrlScan.io](#), una herramienta que escanea URLs y proporciona datos como IP, registros HTTP, redirecciones, frameworks utilizados y dominios vinculados.

Una vez que aprendemos sobre UrlScan.io, podemos pasar a responder las siguientes preguntas.

Pregunta: What was TryHackMe's Cisco Umbrella Rank based on the screenshot?

Respuesta: **345612**

Pregunta: How many domains did UrlScan.io identify on the screenshot?

Respuesta: **13**

Pregunta: What was the main domain registrar listed on the screenshot?

Respuesta: **NAMECHEAP INC**

Pregunta: What was the main IP address identified for TryHackMe on the screenshot?

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

2.4. Tarea 4 - Abuse.ch

Ahora, aprenderemos sobre la plataforma [Abuse.ch](#) y sus servicios como Malware Bazaar, FeodoTracker, SSL Blacklist, URLhaus y ThreatFox, cada uno dedicado a rastrear malware, botnets, SSL maliciosos, URLs peligrosas e indicadores de compromiso.

Ahora que aprendimos sobre Abuse.ch, pasamos a responder las siguientes preguntas.

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

Respuesta: **Katana**

Pregunta: Which malware is associated with the JA3 Fingerprint 51c64c77e60f3980eea90869b6 on SSL Blacklist?

Respuesta: **Dridex**

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

Respuesta: **DIGITALOCEAN-ASN**

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

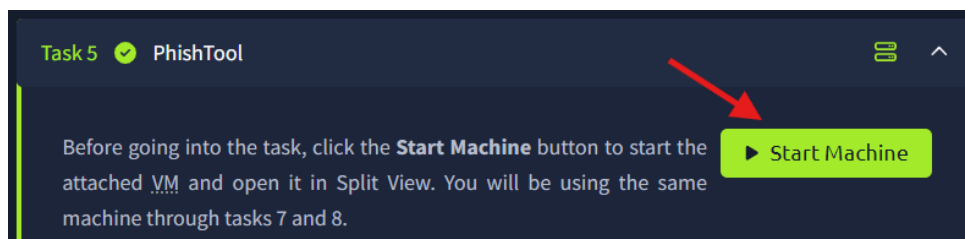
Respuesta: **Georgia**

2.5. Tarea 5 - PhishTool

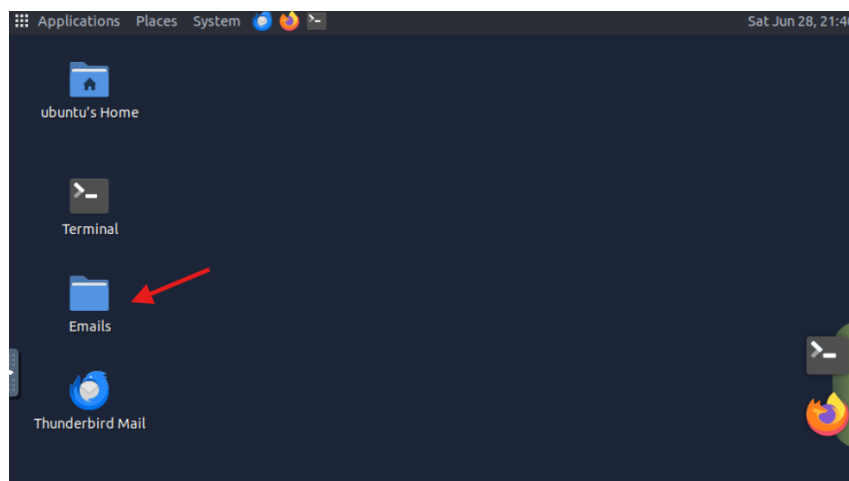
Nos introduciremos en PhishTool, una solución para analizar correos de phishing. Se revisan sus funciones clave y se aprende a cómo usarla para extraer datos relevantes (como URLs, cabeceras y malware involucrado) a partir de emails sospechosos.

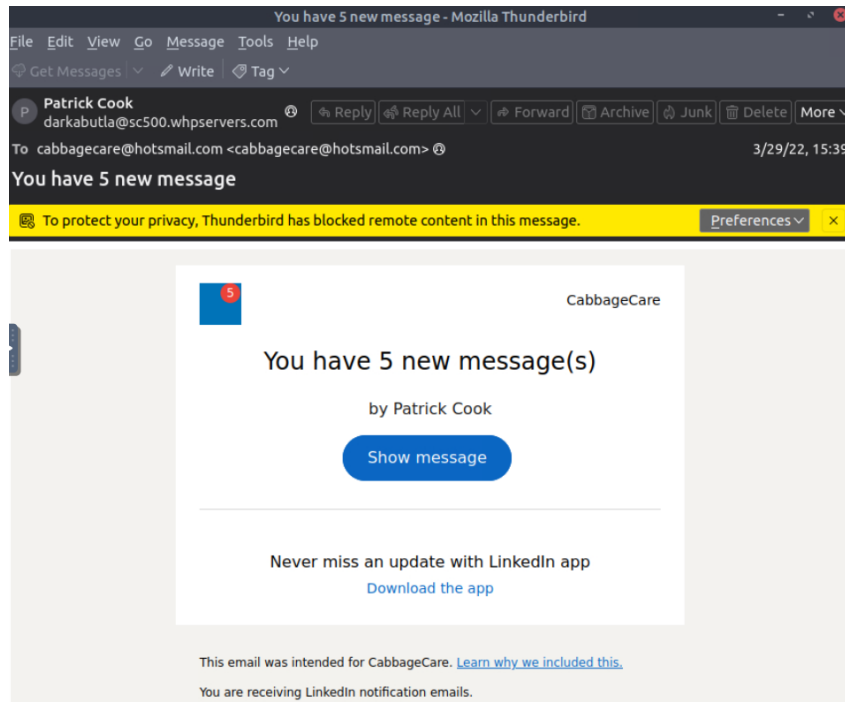
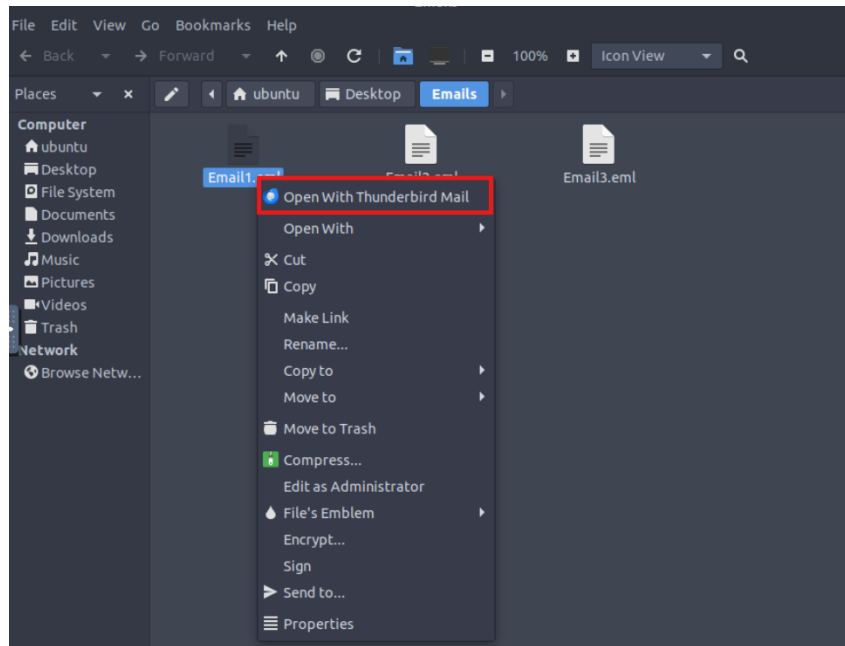
Después que logramos aprender PhishTool, debemos abrir el correo electrónico con **Thunderbird** en la máquina virtual, analízelo y responda las preguntas a continuación para completar la tarea.

Para iniciar la máquina, simplemente hacemos clic en **Start Machine** en el lado superior de la tarea.



Una vez en la máquina, abriremos la carpeta Emails y procederemos abrir el archivo **Email1.eml** con **Thunderbird**.

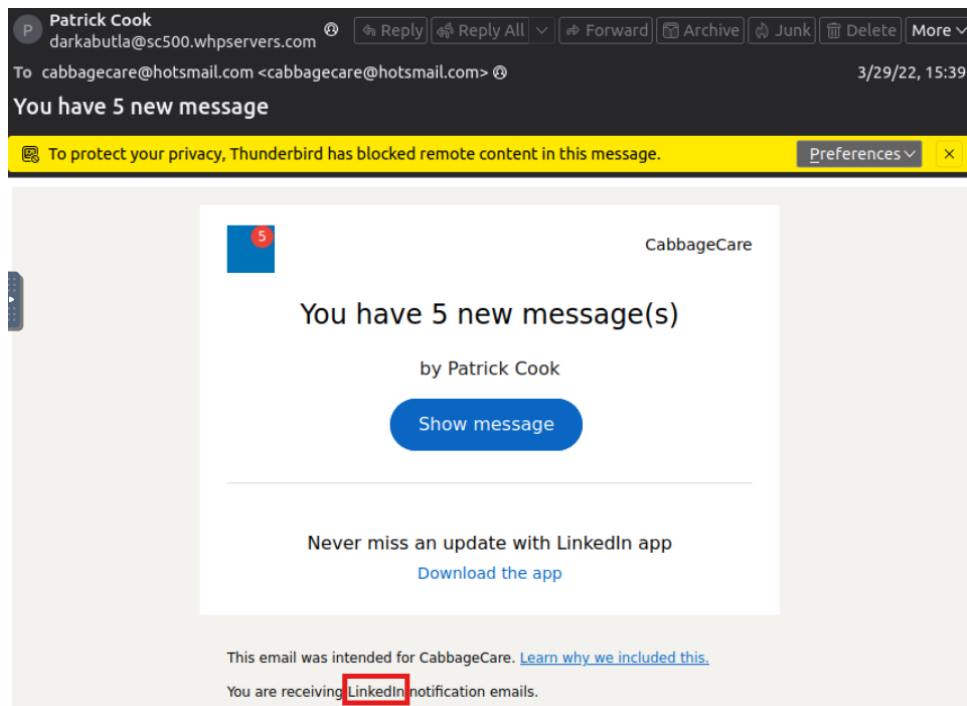




Ahora que abrimos el Email con Thunderbird, podemos pasar a responder las siguientes preguntas.

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

Para encontrar la respuesta a la pregunta, debemos analizar y leer bien el correo electrónico. Encontraremos un mensaje debajo que esta notificación es recibida desde LinkedIn



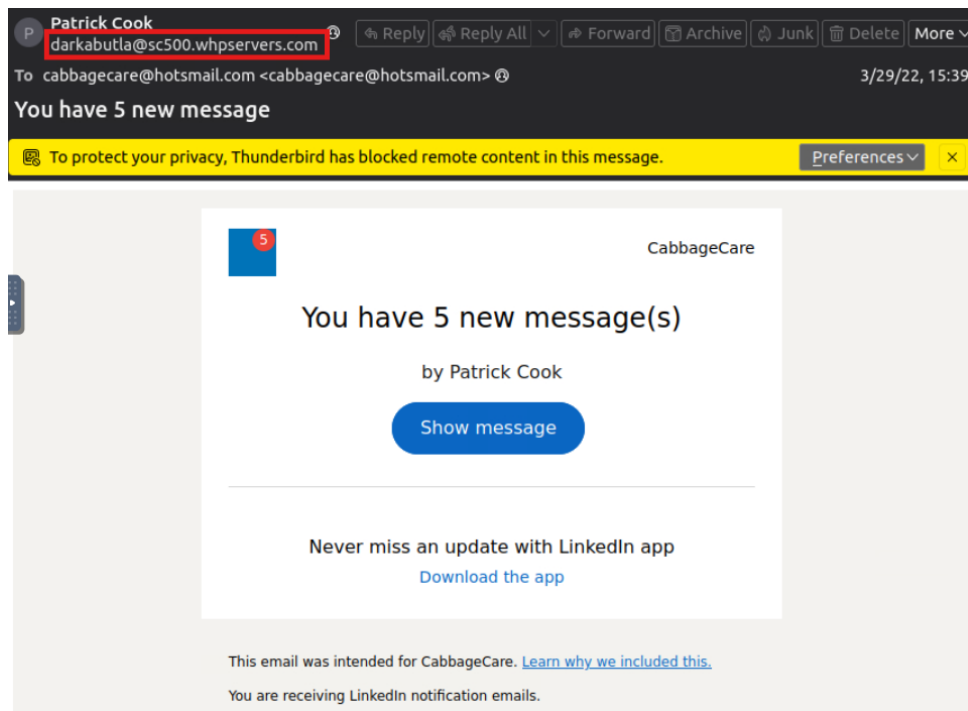
Para estar aún más seguros y realizar un análisis más profundo, podemos ir al lado superior en la sección **More** y abrir el código fuente del sitio, encontraremos en el apartado **List-Unsubscribe** que la red social es LinkedIn.

```
Require-Recipient-Valid-Since: cabbagecare@hotmail.com; Tue, 29 Mar 2022 15:39:22  
List-Unsubscribe: <https://www.linkedin.com/e/v2?e=22d94b7e8b-b231791&t=lun&midTok  
feedback-id: email_notification_single_search_appearance_05:linkedin
```

Respuesta: **LinkedIn**

Pregunta: What is the senders email address?

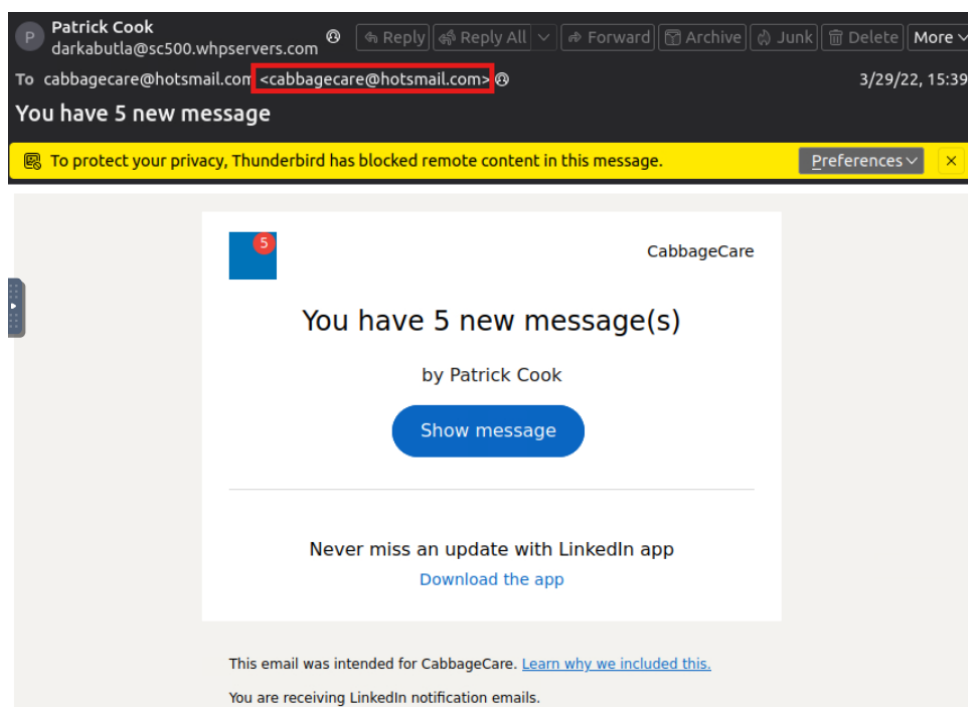
La respuesta a la pregunta es sencilla, simplemente analizamos el encabezado del email y encontraremos el correo del usuario.



Respuesta: darkabutla@sc500.whpservers.com

Pregunta: What is the recipient's email address?

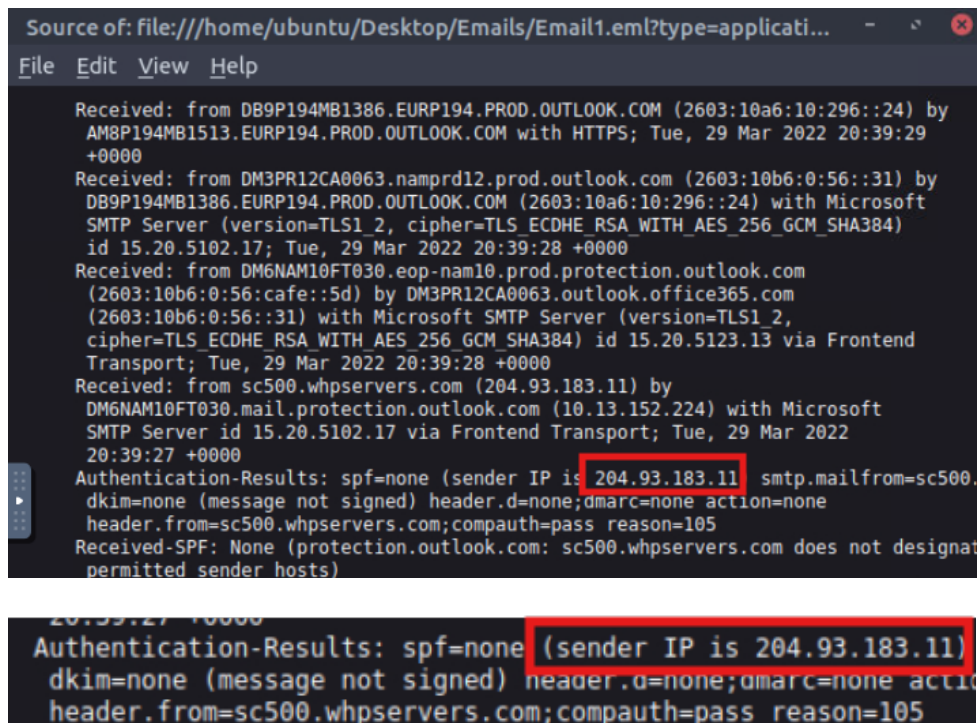
Analizamos otra vez el encabezado y en el apartado de **To** vamos a encontrar el correo electrónico.



Respuesta: cabbagecare@hotmail.com

Pregunta: What is the Originating IP address? Defang the IP address.

Para encontrar la dirección IP, debemos realizar un análisis profundo revisando el código fuente, para ello, iremos al código fuente abierto previamente y en la sección **Authentication-Results** vamos a encontrar la IP de origen.



```
Source of: file:///home/ubuntu/Desktop/Emails/Email1.eml?type=applicati...
File Edit View Help

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.
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 designat
permitted sender hosts)
```

Respuesta: 204.[.]93.[.]183.[.]11

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

Para encontrar la cantidad de saltos que dio el correo hasta llegar a destino, debemos analizar el código fuente nuevamente y contar las veces que se recibió.


```
Source of: file:///home/ubuntu/Desktop/Emails/Email1.eml?type=applicati...
File Edit View Help
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.v
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:33F38BD05032233B02515107520BE45CC841D08
Require-Recipient-Valid-Since: cabbagecare@hotmail.com; Tue, 29 Mar 2022 15:39:22
List-Unsubscribe: <https://www.linkedin.com/e/v2?e=22d94b7e8b-b231791&t=lun&midTok
Feedback-ID: email_notification_single_search_appearance_05:linkedin
To: "cabbagecare@hotmail.com" <cabbagecare@hotmail.com>
Date: Tue, 29 Mar 2022 15:39:22 +0000 (UTC)
Hapless-Filipinos-Mortimer: 2E1150BE361
Subject: You have 5 new message
Bala-Cybergraphis-Berlin-ctrooled
```

Respuesta: 4

2.6. Tarea 6 - Inteligencia de Cisco Talos

Conoceremos sobre la plataforma **Talos de Cisco** y sus seis equipos:

- Inteligencia
- Investigación
- Ingeniería
- Vulnerabilidades
- Comunidad
- Alcance Global

Además, veremos su panel de reputación, búsqueda de IOCs y datos de WHOIS y CVE.

Una vez aprendimos un poco sobre **Talos de Cisco**, procederemos a responder las siguientes preguntas.

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

Respuesta: **scnet.net**

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

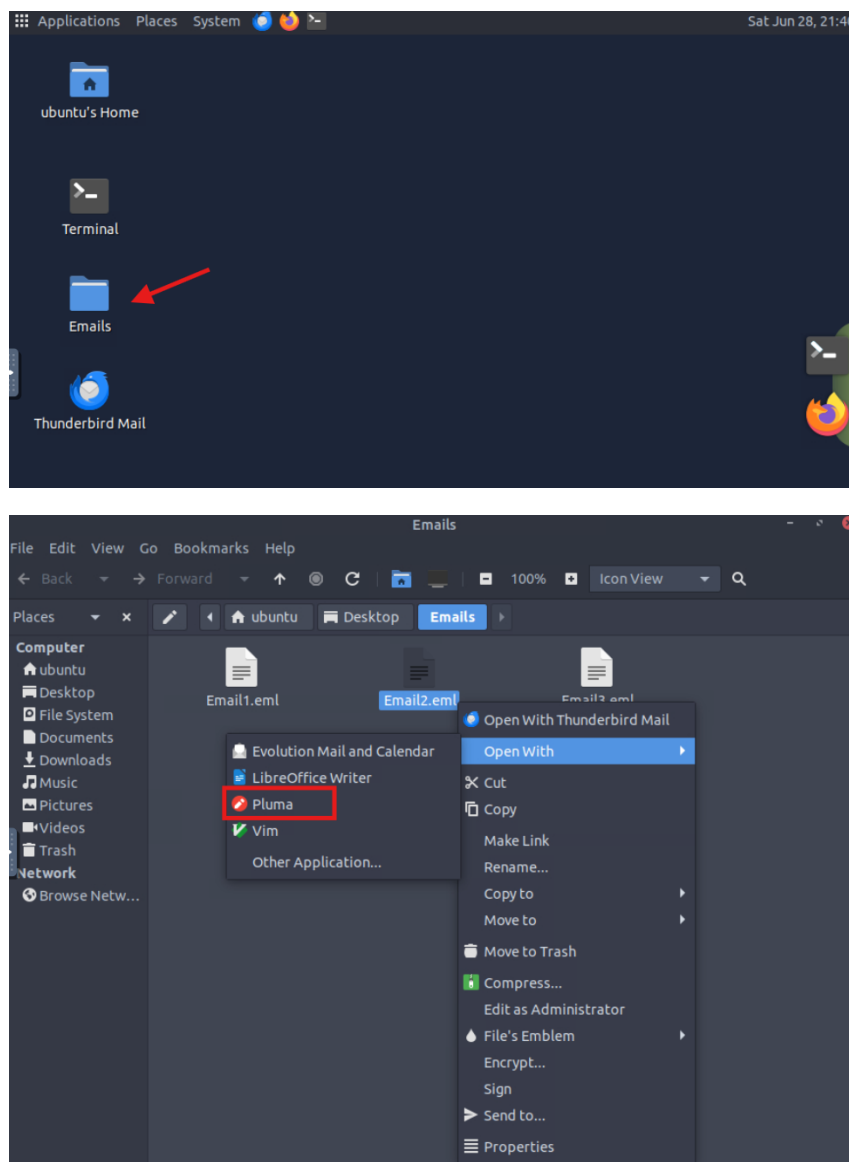
Respuesta: **Complete Web Reviews**

2.7. Tarea 7 - Escenario 1

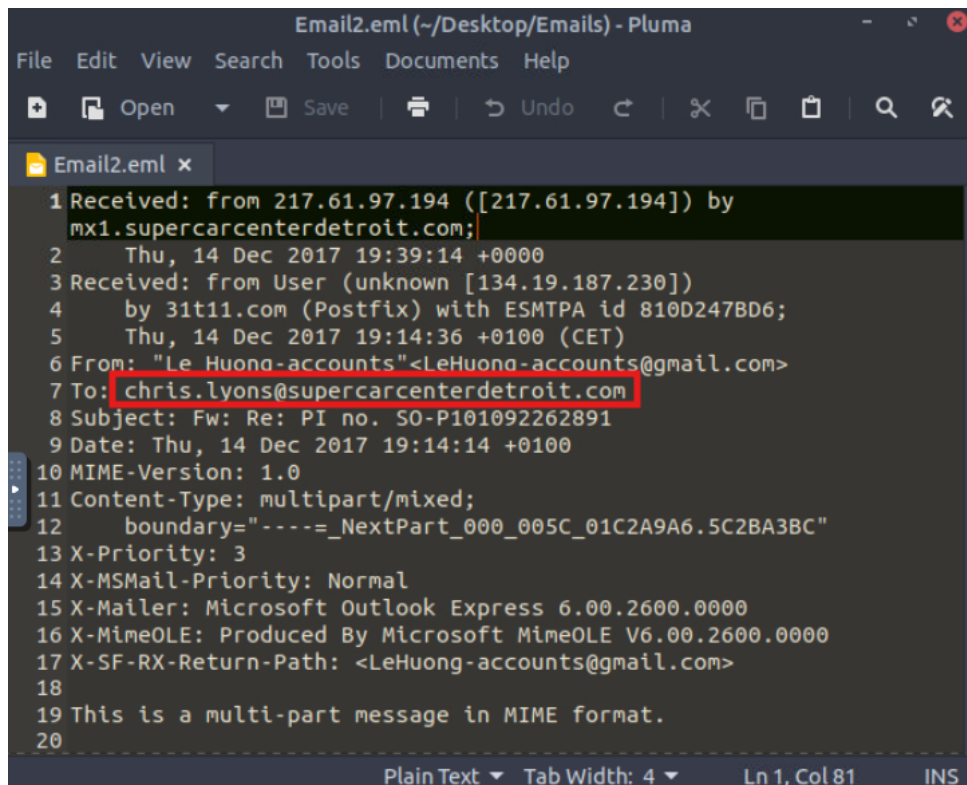
En esta tarea debemos utilizar las herramientas y los conocimientos analizados en esta sala para analizar el correo **Email2.eml** que se encuentra en la máquina virtual (Tarea 5) y utilice la información para responder las preguntas.

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

Para encontrar el correo del destinatario, debemos ir a la carpeta Emails y abrir el archivo **Email2.eml** con la herramienta **Pluma**.



Una vez abierto, procederemos a leerlo y analizarlo hasta encontrar en el apartado **To** el correo del destinatario.



```
1 Received: from 217.61.97.194 ([217.61.97.194]) by
2   mx1.supercarcenterdetroit.com;
3   Thu, 14 Dec 2017 19:39:14 +0000
4 Received: from User (unknown [134.19.187.230])
5   by 31t11.com (Postfix) with ESMTPA id 810D247BD6;
6   Thu, 14 Dec 2017 19:14:36 +0100 (CET)
7 From: "Le Huong-accounts"<LeHuong-accounts@gmail.com>
8 To: chris.lyons@supercarcenterdetroit.com
9 Subject: Fw: Re: PI no. SO-P101092262891
10 Date: Thu, 14 Dec 2017 19:14:14 +0100
11 MIME-Version: 1.0
12 Content-Type: multipart/mixed;
13   boundary="-----_NextPart_000_005C_01C2A9A6.5C2BA3BC"
14 X-Priority: 3
15 X-MSMail-Priority: Normal
16 X-Mailer: Microsoft Outlook Express 6.00.2600.0000
17 X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
18 X-SF-RX-Return-Path: <LeHuong-accounts@gmail.com>
19 This is a multi-part message in MIME format.
20
```

Respuesta: chris.lyons@supercarcenterdetroit.com

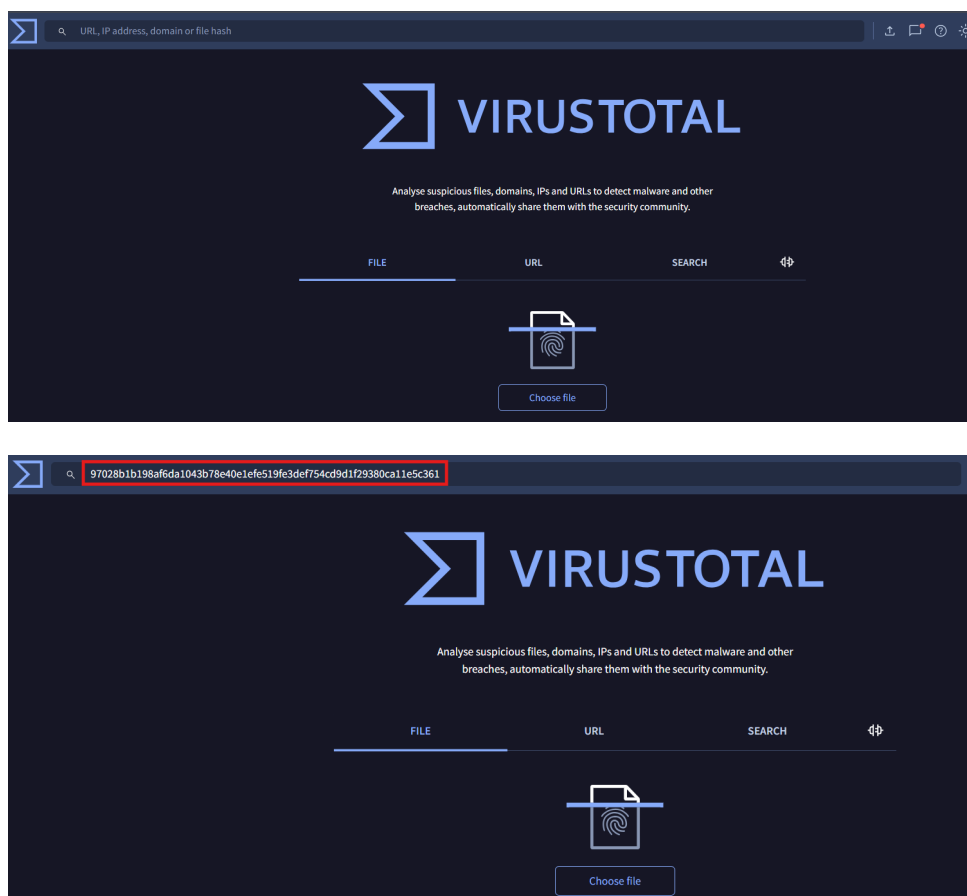
Pregunta: On VirusTotal, the attached file can also be identified by a Detection Alias, which starts with an H.

Para encontrar la respuesta a esta pregunta debemos realizar una serie de pasos. Lo primero será abrir la terminal y procederemos a ejecutar los siguientes comandos:

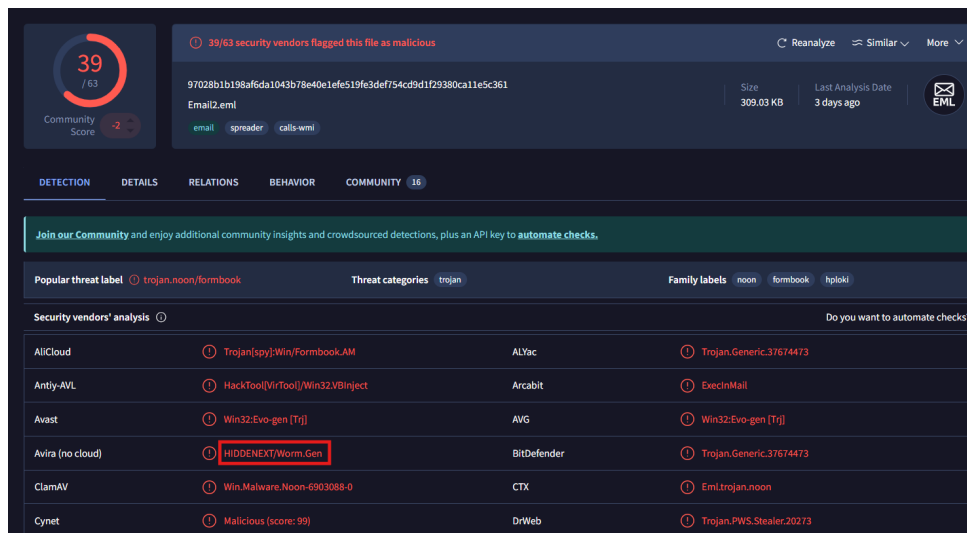
- **ls**
- **cd Desktop**
- **ls**
- **cd Emails**
- **ls**
- **sha256sum Email2.eml**

```
ubuntu@tryhackme: ~/Desktop/Emails
File Edit View Search Terminal Help
ubuntu@tryhackme:~$ ls
Desktop  Downloads  Pictures  Templates  go          outgoingsmtp.json
Documents Music      Public   Videos    msfinstall setoolkit
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$
```

De esta manera, lograremos generar un hash SHA-256 único para Email2.eml, posterior a eso, copiaremos el hash e iremos al sitio oficial de [VirusTotal](#) y pegaremos en su buscador el hash generado.



Comenzará a realizar la búsqueda y nos saltará diversa información sobre el archivo y leyendo cuidadosamente encontraremos el alias.



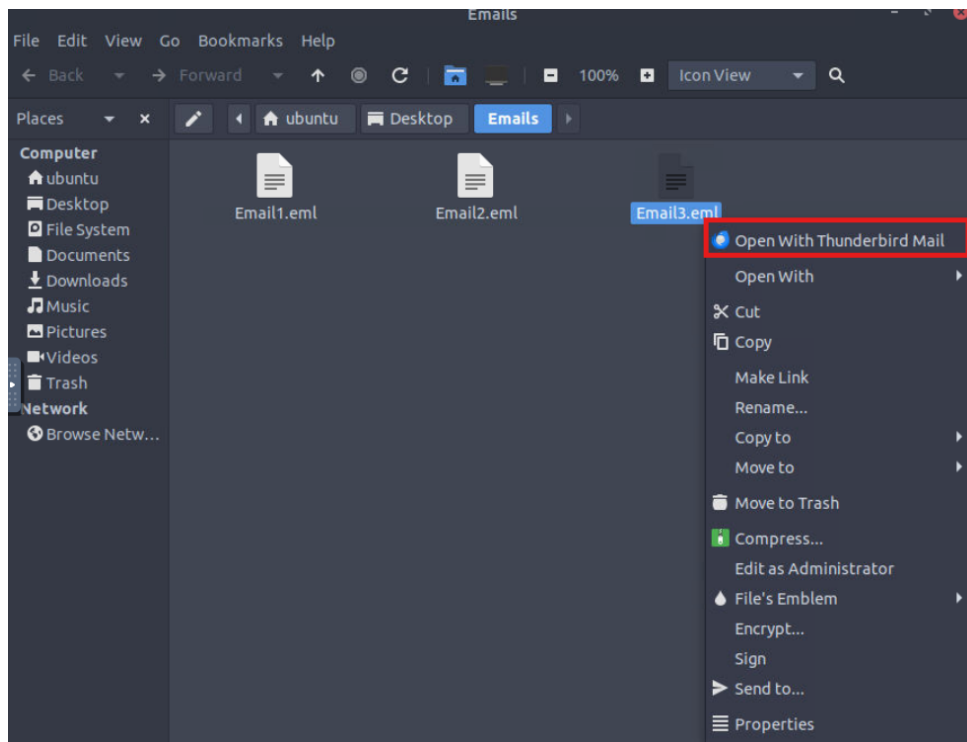
Respuesta: **HIDDENEXT/Worm.Gen**

2.8. Tarea 8 - Escenario 2

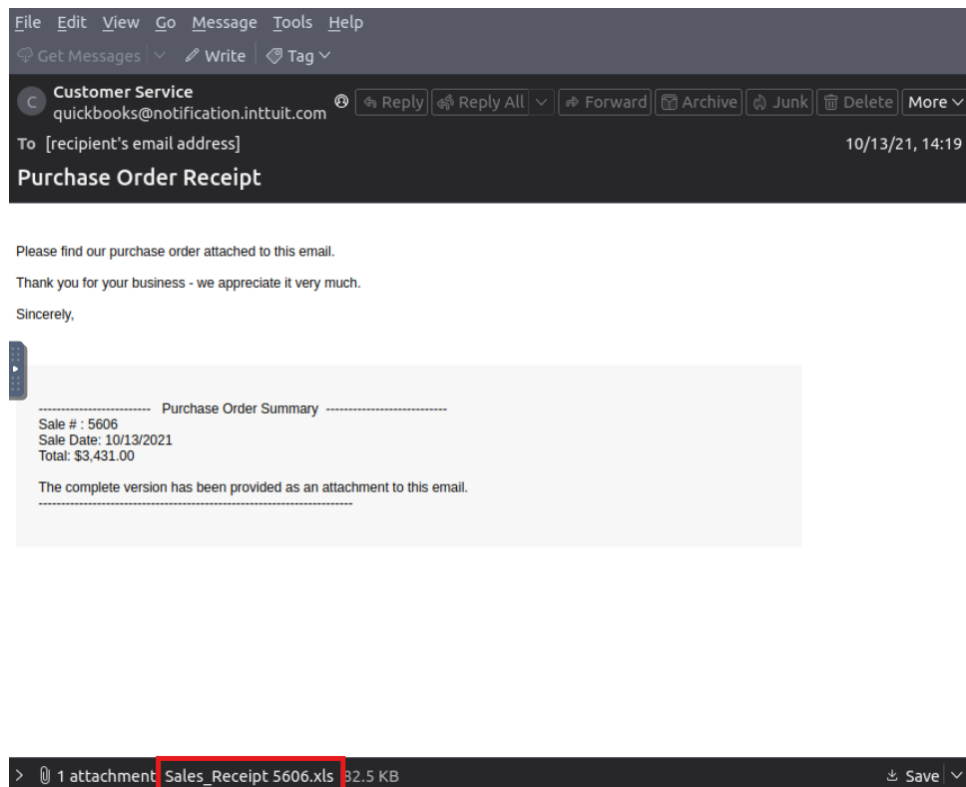
En este segundo escenario práctico es similar al anterior, realizaremos los mismos pasos para encontrar las respuestas a las siguientes preguntas.

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

Para encontrar el nombre del archivo, debemos dirigirnos a la carpeta Emails y abrir el archivo **Email3.eml** con la herramienta **Thunderbird**



Una vez abierto el archivo, debajo del todo nos aparecera el nombre del archivo.



Respuesta: **Sales_Receipt 5606.xls**

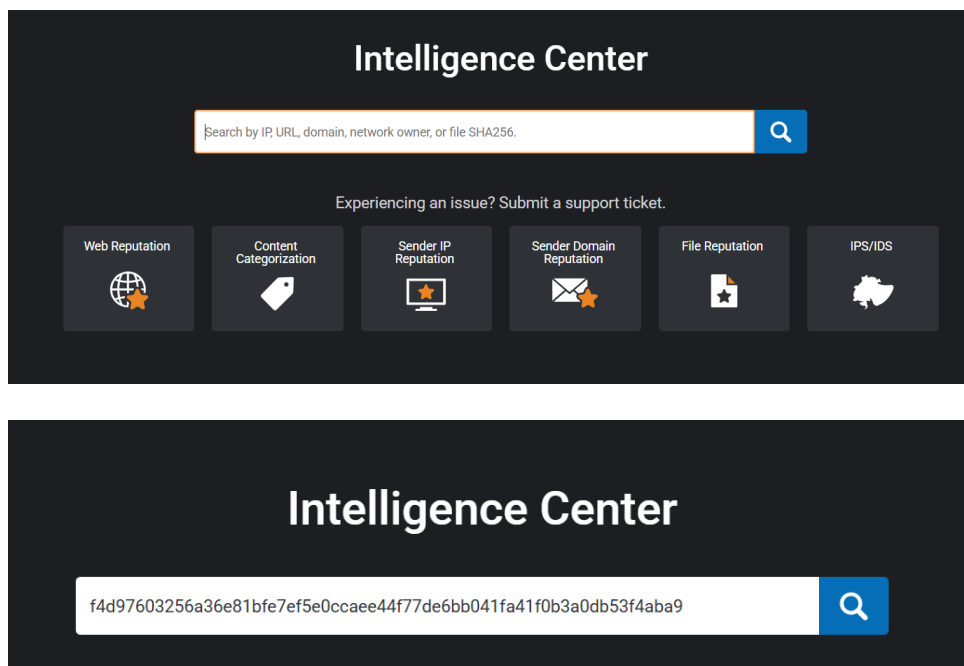
Pregunta: What malware family is associated with the attachment on Email3.eml?

Ahora, para encontrar la respuesta a esta pregunta debemos abrir la Terminal y ejecutar los siguientes comandos:

- **ls**
- **cd Desktop**
- **ls**
- **cd Emails**
- **ls**
- **sha256sum Email3.eml**


```
ubuntu@tryhackme: ~/Desktop/Emails
File Edit View Search Terminal Help
ubuntu@tryhackme:~$ ls
Desktop  Downloads  Pictures  Templates  go          outgoingsmtp.json
Documents Music      Public    Videos    msfinstall  setoolkit
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 Email3.eml
f4d97603256a36e81bfe7ef5e0ccae44f77de6bb041fa41f0b3a0db53f4aba9  Email3.eml
ubuntu@tryhackme:~/Desktop/Emails$
```

De esta manera, lograremos generar un hash SHA-256 único para Email3.eml, posterior a eso, copiaremos el hash e iremos al sitio oficial de **Cisco Talos** y pegaremos en su buscador el hash generado



Nos saltará una diversa información sobre el archivo, analizaremos bien la información proporcionada y encontraremos la respuesta.

FILE REPUTATION


Malicious

TALOS WEIGHTED FILE REPUTATION SCORE
Score not available.

Think this reputation is incorrect?
[Submit a File Reputation Ticket](#)

SHA256
F4D97603256A36E81BFE7EF5E0CCAE44F77DE6BB041FA41F0B3A0DB53F4ABA9
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.F4D9760325.252139.1n07.Talos

*Limited to SHA256 lookup

ASSOCIATED DOMAINS FOR THIS HASH
Domains not available.

DETECTION ALIASES

detected

VBA:Dropper-GX [Trj]

virus

VB:Trojan.Valyria.5569

VBA/Agent.AD55tr

Trojan-Downloader.VBA.Agent

X97M/Downloader.lu (trojan)

TrojanDownloader.D97M/Dridex.PKIMTB

X97M.Downloader.44710

Downloader.AgentB.823

Troj/DocBl-AEMO

W97M.Downloader

TROJ_FRS.ONA103UE21

X97M/Dridex.AgentEldorado

Other/Malware.gen [Trj]

Respuesta: Dridex

2.9. Tarea 9 - Conclusion

En esta última tarea explica que el contenido aprendido es solo el principio y que podemos visitar otras salas para profundizar en la inteligencia de amenazas.

Pregunta: Read the above and completed the room

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

3. Conclusión sobre la Sala

Al finalizar la sala hemos logrado aprender a identificar URLs maliciosas, analizar cabeceras de correos, detectar malware a través de bases de datos colaborativas y consultar plataformas como Cisco Talos para obtener información detallada sobre amenazas.