PRACTICA 1

OSINT

Ignacio Amador López

ENUNCIADO

Hemos detectado un usuario con una actividad algo inusual en sus redes sociales que necesitamos investigar. Hasta ahora la única información que tenemos es que se llama igual que el receptor de un correo de spear phishing detectado en la empresa Paterva.

Desde el centro de inteligencia nos están solicitando:
• Obtener la flag que se conoce que el usuario ha ido dejando por el camino.
• Obtener las redes sociales en las que este usuario tiene actividad.

A parte de esta información se nos aporta la configuración de la herramienta **Maltego**, mediante la cual los responsables de **Paterva** han llevado a cabo esta investigación para que nosotros podamos partir desde el mismo punto.

Dicho esto, se nos pide lo siguiente en el **primer ejercicio**:

Responde a las siguientes preguntas:
- *Cuál es la flag1:*
- *¿Qué redes sociales tiene nuestro usuario?:*

Como añadido, hemos detectado que nuestro usuario ha creado un servidor de Intercambio de ficheros al que seguro que es muy interesante poder acceder a ver si tiene información que nos pueda ser útil:

- Cuál es la flag2:

Como **segundo ejercicio** se nos solicita lo siguiente:

¿Puedes obtener información a través de OSINT de nuestro profesor Yuba Gonzalez Parrilla?

- *Realiza un apartado en tu informe final con toda la información obtenida de este usuario.*

EJERCICIO 1

Analizando el enunciado se nos pide que investiguemos el comportamiento por redes sociales de uno de los trabajadores de la empresa. A parte sabemos que este fue **receptor de un correo de spear phishing**.

Dicho esto, vamos a utilizar la herramienta **Maltego** y sus transformadas para ver la **información disponible,** tanto en fuentes públicas como privadas, de la organización Paterva y ver si podemos obtener información relevante en cuanto a lo que nos piden.

Tras aplicar la configuración dada en el enunciado, buscamos transformadas que nos puedan servir para obtener la información que nos interesa. De todas las disponibles encontramos la siguiente:

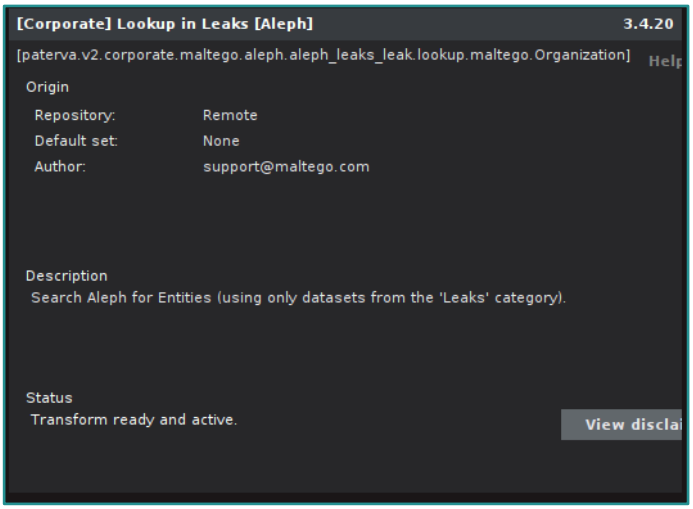

Ilustración 1- Transformada de Maltego

Esta nos permite conseguir todas las entidades las cuales contengan la categoría "Filtraciones", con la esperanza de encontrar emails o documentos que nos permitan obtener los mails de phishing mencionados. Al lanzarla obtenemos lo siguiente:

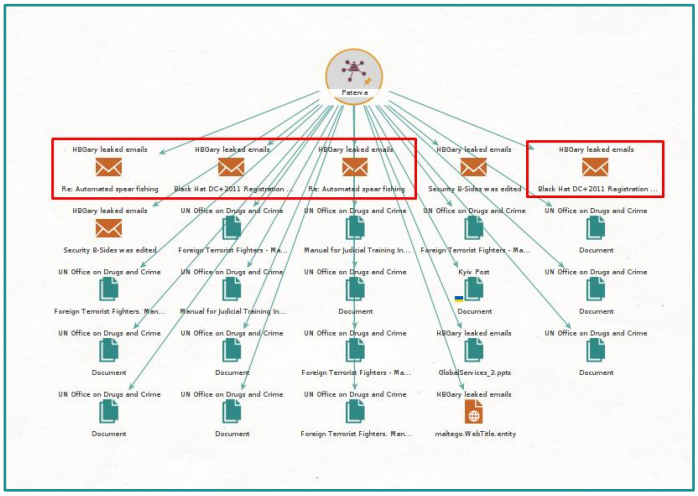

Ilustración 2 - Resultado Maltego tras transformada

Conversaciones y mails

Señalados encontramos los potenciales emails referidos al phishing mencionado. Si revisamos su contenido y conversaciones:

E-Mail #1	
Título	
Black Hat DC+2011 Registration Is Open	
Emisor	**Receptor**
Black Hat DC <email@blackhat.messages4.com>	aaron@hbgary.com
En copia	
Nadie	
Resúmen	
El correo anuncia el evento enfocado en técnicas ofensivas de ciberseguridad, con cursos técnicos y oportunidades de capacitación. Ofrece descuentos por registro anticipado, grupal y académico, e invita a presentar ponencias antes del 1 de diciembre. Incluye una lista de cursos destacados impartidos por expertos reconocidos en la comunidad de seguridad informática.	

Revisando el contenido encontramos enlaces los cuales usan ciertos enlaces para dar acceso al registro para el evento, usando el siguiente dominio: **http://links.covertchannel.blackhat.com/**

Resulta un tanto extraño el dominio usado, por eso podemos corroborar la autenticidad del mismo con diferentes herramientas. Vamos a usar **Whois**:

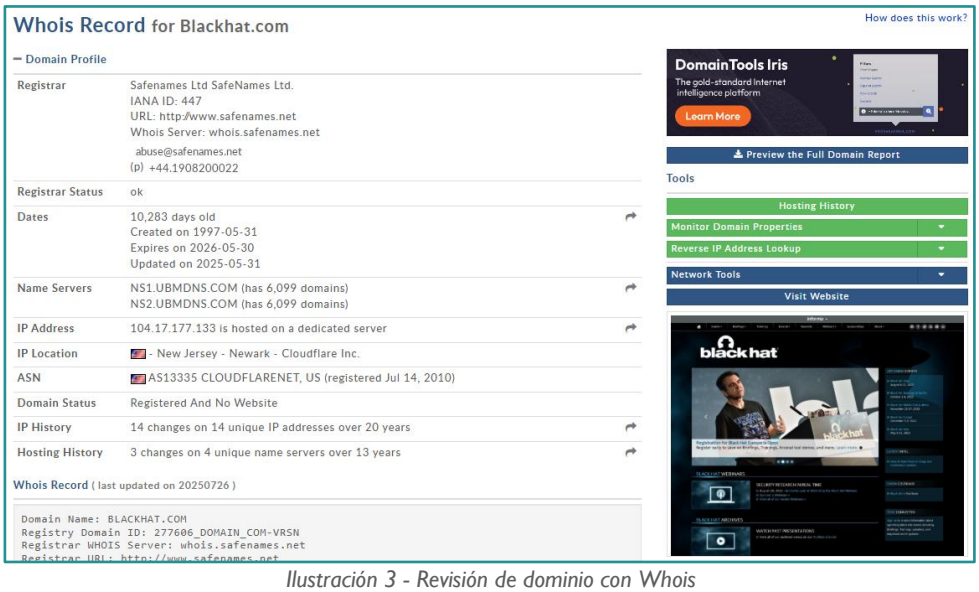

Ilustración 3 - Revisión de dominio con Whois

Revisando el resultado vemos que no parece un dominio malicioso, por lo que podemos descartar por el momento este email y a su receptor para el ejercicio.

E-Mail #2	
Título	
Black Hat DC+2011 Registration Is Open	
Emisor	**Receptor**
Greg Hoglund greg@hbgary.com Aaron Barr aaron@hbgary.com	Aaron Barr aaron@hbgary.com Greg Hoglund greg@hbgary.com
En copia	
Ted Vera ted@hbgary.com Rich Cummings rich@hbgary.com	
Resúmen	
Aaron Barr (HBGary Federal) y Greg Hoglund (HBGary) discuten sobre la automatización de ataques de *spear phishing* utilizando datos recolectados desde redes sociales. Aaron plantea cómo es posible llegar a un objetivo pasando por contactos cercanos y sugiere automatizar ese proceso. Greg responde que ya vio un sistema funcional, desarrollado por el fundador de Paterva (creadores de Maltego), que automatizaba todo el ciclo del ataque. Dicho sistema incluía exploits cliente, capacidades de gusano para moverse lateralmente, y recopilación automática de correos desde fuentes abiertas. Se mencionan los correos de Aaron y Greg, y se referencia a un blanco de prueba llamado Dave Luber.	

Visto el contenido del correo, hay uno de los correos de la conversación el cual dice:

Aaron,

Yes I have seen a very effective automated spearfishing system. I got a demo of it about 7 years ago. The developer is actually the same guy who went on to found Paterva, the creators of Maltego. The automated system was fully weaponized with client-side exploits for iexplore and outlook, including a worm package for lateral movement once inside an Enterprise, it launched attackes/ran from a server platform with a web front end, and would automatically find email addresses for a given corporation, country domain, or government target. For any target it could find hundreds of valid email addresses by combing open sources and using intelligent email-address patterns. Attached is a whitepaper and some screenshots. At the time this was clearly able to take out any target without exception, given that a small percentage of email targets would end up clicking on the package, and all it takes is a handful to victims to get the worming package inside the network.

-Greg

Por lo que entendemos que el usuario **Greg Hoglund** es quien recibió, al menos una demo, del spear phishing, por lo que vamos a investigar al usuario que se llama de esta manera.

Investigación de usuario

Hemos decidido entonces investigar al trabajador que se llama **Greg Hoglund**. habiéndonos pedido que investiguemos las redes sociales del mismo, vamos a revisar inicialmente las principales: **Instagram, Twitter (X) y LinkedIn.**

LinkedIn

En lo referente a esta red social no encontramos ningún perfil más allá de los perfiles verificados y sin ninguna actividad sospechosa relevante

Twitter (X)

De igual manera no encontramos información relevante tras buscar en los perfiles coincidentes con el nombre, por lo que descartamos esta red social por el momento.

Instagram

Realizamos de igual manera la búsqueda por nombre de perfiles y encontramos múltiples, donde tras revisarlos encontramos el siguiente:

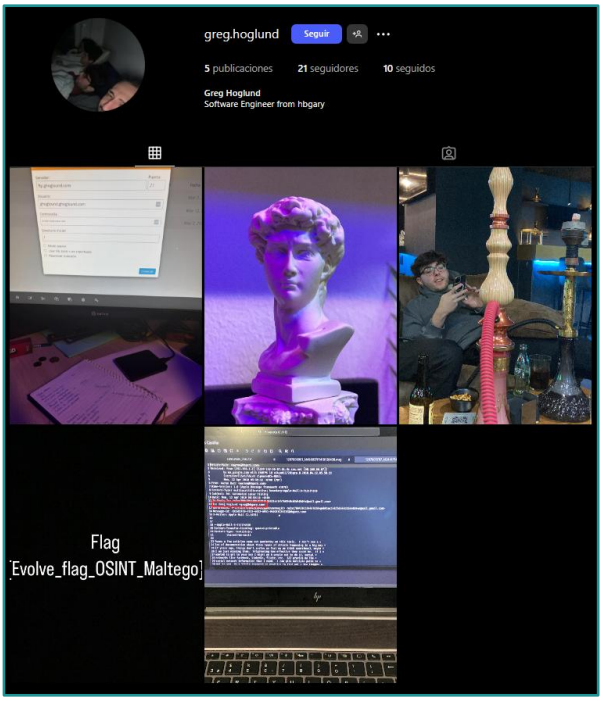

Ilustración 4 - Perfil Instagram Greg Hoglund

Revisando las publicaciones encontramos la **Flag#1: {Evolve_flag_OSINT_Maltego}**

Búsqueda de perfiles en redes sociales

Una vez hemos logrado la primera flag vamos a continuar con la segunda pregunta de la primera parte la cual es: **¿Qué redes sociales tiene nuestro usuario?**

Una vez tenemos el usuario de nuestro objetivo (**greg.hoglund**) podemos utilizar diferentes herramientas para la búsqueda de perfiles en base al mismo. Detallamos entonces la ejecución de las herramientas y el análisis de los resultados obtenidos.

sherlock

https://github.com/sherlock-project/sherlock.git

Una vez hemos logrado la primera flag vamos a continuar con la segunda pregunta de la primera parte la cual es: **¿Qué redes sociales tiene nuestro usuario?**

Una vez tenemos el usuario de nuestro objetivo (**greg.hoglund**) podemos utilizar diferentes herramientas para la búsqueda de perfiles en base al mismo. Detallamos entonces la ejecución de las herramientas y el análisis de los resultados obtenidos.

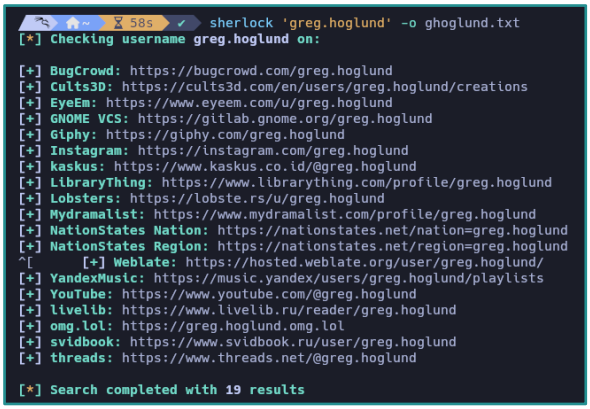

Ilustración 5 - Ejecución de sherlock

Pero ninguna de estas redes sociales nos reporta información relevante.

WhatsMyName

https://whatsmyname.app/

Ilustración 6 - Ejecución WhatsMyName

De igual manera ninguno de los perfiles encontrados aporta información relevante, además de que alguno de los encontrados se encuentra duplicados en concordancia con la anterior herramienta.

Determinamos entonces que, a la gran cantidad de falsos positivos, por el momento, que no cuenta con más redes sociales a parte de **Instagram**.

Revisión de perfil

Si revisamos las publicaciones presentes en Instagram, vemos la siguiente:

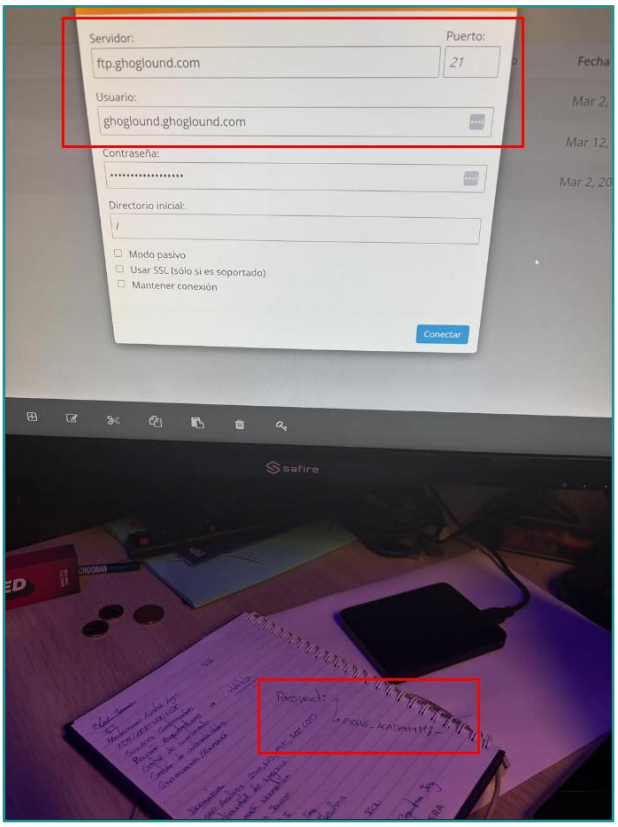

Ilustración 7 - Publicación Instagram

Que si transcribimos la imagen tenemos:

- **Servidor**: ftp.ghoglound.com:21
- **Usuario**: ghoglound.ghoglound.com
- **Contraseña**: EVOLVE_ACADEMY17?_

Lo que son sin ninguna duda unas credenciales para un servidor de ftp, que si revisamos el enunciado:

> *Como añadido, hemos detectado que nuestro usuario ha creado un servidor de Intercambio de ficheros al que seguro que es muy interesante poder acceder a ver si tiene información que nos pueda ser útil:*
>
> *- Cuál es la flag2:*

Por lo que vamos a revisar el servidor.

Servidor FTP

Si accedemos con las credenciales que hemos encontrado obtenemos acceso al servidor, donde encontramos lo siguiente:

```
ftp ftp.ghoglound.com
Connected to ftp-server-00.dondominio.net.
220-
220-
220-
220-
220-
220-
220-
220-                                          DonDominio.com - Servidor FTP
220 This is a private system - No anonymous login
Name (ftp.ghoglound.com:iamadorl): ghoglound.ghoglound.com
331 User ghoglound.ghoglound.com OK. Password required
Password:
230 OK. Current restricted directory is /
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (31,214,178,122,173,134)
150 Accepted data connection
drwxr-xr-x    5 1060102    1060102           113 Jul  8 17:46 .
drwxr-xr-x    5 1060102    1060102           113 Jul  8 17:46 ..
-rw-rw-r--    1 1060102    1060102         33669 Jul  8 17:46 Flag 2.jpg
-rw-rw-r--    1 1060102    1060102         78543 Jul  8 17:44 Metadata - CTF Handbook.html
drwxr-xr-x    9 1060102    1060102          4096 Mar  2 20:13 wp-admin
drwxr-xr-x    5 1060102    1060102            67 Mar 12 21:20 wp-content
drwxr-xr-x   30 1060102    1060102         12288 Mar  2 20:13 wp-includes
226-Options: -a -l
226 7 matches total
ftp>
```

Ilustración 8 - Servidor FTP

Encontramos un archivo JPG con el nombre de 'Flag 2.jpg'. Si descargamos el archivo para visualizarlo:

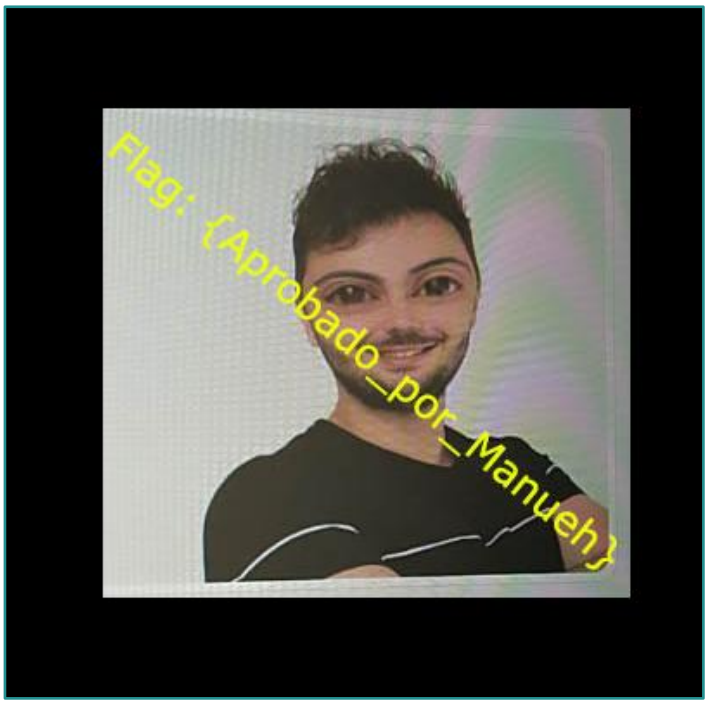

Ilustración 9 - Visualización de 'Flag 2.jpg' con eog

Por lo que obtenemos la **Flag#2**: **{Aprobado_por_Manueh}**

Si realizamos una comprobación de los metadatos también podríamos obtener la flag:

```
exiftool Flag2.jpg | grep Text
Text Layer Name                 : Flag: {Aprobado_por_Manueh}
Text Layer Text                 : Flag: {Aprobado_por_Manueh}
```

Ilustración 10 - Metadatos de 'Flag 2.jpg' con exiftool

Respuestas Ejercicio 1

- **Flag#1:** {Evolve_flag_OSINT_Maltego}
- **Redes sociales:** Instagram
- **Flag#2:** {Aprobado_por_Manueh}