Cyber Mission #3: investigación de fuentes abiertas

Una investigación internacional ha permitido detectar la posible existencia de una **red criminal transnacional vinculada a la trata de seres humanos**, con presencia y actividad en distintos países.

La organización no parece operar mediante una única estructura visible. Por el contrario, utiliza diferentes empresas, páginas web, perfiles digitales, intermediarios y servicios financieros para facilitar sus actividades, captar potenciales víctimas, mover fondos y dificultar la identificación de sus miembros.

Los primeros indicios apuntan a que parte de la infraestructura utilizada por la red estaría relacionada con **operaciones de blanqueo de capitales**, mientras que otras ramas se dedicarían al **reclutamiento fraudulento de personas mediante falsas ofertas de empleo**. Paralelamente, determinadas operaciones financieras y actividades detectadas en redes sociales podrían estar vinculadas con la **explotación sexual de víctimas en distintos países**.

La información disponible se encuentra fragmentada.

Dominios que ya no están operativos, perfiles en redes sociales, anuncios, documentos, transacciones financieras y diferentes huellas digitales contienen piezas de una misma investigación. Algunas de ellas pueden parecer independientes a primera vista, pero su análisis permitirá comprender cómo una organización criminal puede utilizar Internet para desarrollar distintas fases de su actividad.

Como analista de ciberinteligencia, tu misión será explotar la información disponible mediante técnicas de **WEBINT, OSINT, SOCMINT, análisis de fuentes digitales y correlación de inteligencia**.

La investigación se divide en tres misiones de dificultad progresiva.

En la primera deberás recuperar información vinculada a una infraestructura web utilizada por la organización para canalizar fondos.

En la segunda investigarás una posible rama de captación de víctimas mediante falsas ofertas de empleo.

Finalmente, la tercera misión te situará ante una investigación compleja derivada de un informe de inteligencia financiera, desde el que tendrás que identificar potenciales víctimas, asociados y miembros de la organización, así como reconstruir parte de su actividad y área de operaciones.

Cada dato puede convertirse en un selector.

Cada selector puede abrir una nueva línea de investigación.

Y cada hallazgo puede acercarte un paso más a comprender la estructura de la red.

MISIÓN 1. Nivel: básico — WEBINT (2 PUNTOS)

Durante la investigación relacionada con una **red criminal vinculada a la trata de seres humanos**, los analistas han identificado varias páginas web presuntamente utilizadas para canalizar y blanquear parte de los beneficios obtenidos por la organización.

Una de las infraestructuras detectadas corresponde al dominio **aix-trader.com**. Actualmente, la página ya no se encuentra accesible, por lo que será necesario recurrir a técnicas de **WEBINT** y consultar versiones históricas del sitio para recuperar información de interés.

A partir de la información disponible en fuentes abiertas, responde a las siguientes preguntas:

1. ¿Cuál era el precio del plan "Gold", señalado por los investigadores como uno de los productos utilizados para canalizar cantidades elevadas de dinero?

Respuesta: _____
_____

2. ¿Qué dirección física completa figuraba públicamente vinculada a la plataforma?

Respuesta: _____
_____

3. ¿Qué dirección de correo electrónico aparecía como contacto principal de la plataforma?

Respuesta: _____
_____

4. La Financial Market Authority (FMA) de Austria publicó información relacionada con esta entidad. ¿Qué dirección de correo electrónico alternativa aparece asociada a un supuesto contacto de la plataforma?

Respuesta: _____
_____

MISIÓN 2. Nivel: intermedio — SOCMINT / WEBINT (3 PUNTOS)

Durante el análisis de la infraestructura utilizada por la organización criminal, los investigadores han identificado una posible **rama dedicada al reclutamiento fraudulento de trabajadores en Chipre**.

La empresa utiliza el nombre **Asteria Jobs International** y promociona ofertas de empleo con condiciones especialmente atractivas, incluyendo salarios elevados, alojamiento y otros beneficios.

Los investigadores sospechan que estas ofertas podrían estar siendo utilizadas para **captar potenciales víctimas y facilitar su posterior explotación**.

Como punto de partida dispones únicamente del **logotipo de Asteria Jobs International** y de la información de que la organización mantiene presencia en **Facebook**.

Tu objetivo será localizar la infraestructura digital utilizada por la falsa agencia de contratación, identificar al supuesto reclutador y analizar las evidencias publicadas para determinar quién se encuentra realmente detrás de las ofertas.

A partir de la información disponible en fuentes abiertas, responde a las siguientes preguntas:

1. ¿Cuál es el identificador numérico del perfil de Facebook que administra el grupo de Asteria Jobs International?

Respuesta: _____
_____

2. ¿Cuál es el nombre del supuesto reclutador que administra la presencia de Asteria Jobs International en Facebook y cuál es su fecha de nacimiento?

Respuesta: _____
_____

3. ¿Qué número de teléfono aparece publicado como contacto de Asteria Jobs International?

Respuesta: _____
_____

4. ¿Qué dirección física completa aparece asociada públicamente a la supuesta empresa de contratación?

Respuesta: _____
_____

5. Una de las ofertas de empleo publicadas por la organización ofrece alojamiento en un hotel situado en una zona de Chipre con unas circunstancias históricas muy particulares. ¿Cuál es el nombre del distrito donde se encuentra el hotel y cuál es su situación actual?

Respuesta: _____
_____

6. La identidad observada en Facebook parece ser únicamente la utilizada públicamente para captar a potenciales víctimas. Continúa la investigación y determina el nombre completo de la persona que realmente se encuentra detrás de las falsas ofertas de empleo.

Respuesta: _____
_____

MISIÓN 3. Nivel: difícil — OSINT / SOCMINT / FININT (5 PUNTOS)

En el marco de la investigación contra la **red criminal transnacional dedicada a la trata de seres humanos con fines de explotación sexual**, una Unidad de Inteligencia Financiera (FIU) ha remitido un informe sobre una serie de operaciones sospechosas detectadas en una cuenta vinculada a uno de los posibles miembros de la organización.

El análisis financiero revela transferencias recurrentes procedentes de varias mujeres, pagos relacionados con plataformas de anuncios de servicios para adultos y diferentes referencias que podrían permitir identificar tanto a **potenciales víctimas** como a las personas encargadas de su explotación y control.

Como analista de ciberinteligencia, recibirás una versión resumida del informe financiero. A partir de los selectores contenidos en él deberás **pivotar entre fuentes abiertas, plataformas web y redes sociales**, correlacionar la información obtenida y reconstruir progresivamente la estructura de la red.

Tu investigación deberá permitir identificar a varias de las potenciales víctimas, localizar sus perfiles digitales y obtener información relevante sobre su actividad y entorno.

Documento de apoyo: FIU_ORION_Mision_3_LISA_Challenge.pdf. Utiliza los selectores contenidos en el informe como punto de partida para la investigación.

A partir de la información disponible, responde a las siguientes preguntas:

1. Utiliza la información contenida en el informe financiero para identificar el anuncio relevante publicado en la plataforma de servicios para adultos. Sigue el contacto disponible en redes sociales e identifica el nombre completo de la potencial víctima de nacionalidad filipina.

Respuesta: _____
_____

2. Utiliza los selectores y el contenido disponible en el perfil de Facebook de la víctima filipina para identificar su cuenta asociada de Instagram. ¿Cuál es su nombre de usuario?

Respuesta: _____
_____

3. Analiza la actividad publicada por la víctima filipina en sus redes sociales y determina el distrito de El Cairo en el que aparentemente reside.

Respuesta: _____
_____

4. Regresa a la plataforma de servicios para adultos e identifica a la potencial víctima de nacionalidad camboyana asociada al anuncio relevante. Sigue el contacto disponible en redes sociales y determina su nombre completo.

Respuesta: _____
_____

5. Analiza el perfil y la actividad pública de la víctima camboyana en Facebook y determina su fecha completa de nacimiento.

Respuesta: _____
_____

6. Utiliza los selectores y el contenido compartido en el perfil de Facebook de la víctima camboyana para identificar su cuenta asociada de TikTok. ¿Cuál es su nombre de usuario?

Respuesta: _____
_____

7. Utiliza los selectores KYC contenidos en el informe FIU para localizar la presencia digital pública del titular de la cuenta investigada. ¿Cuál es la ID del perfil de Facebook de Fadi Mahmoud El-Hadidi?

Respuesta: _____
_____

8. Algunos de los contactos que aparecen en los movimientos de la cuenta también pueden identificarse a través de la actividad del posible perpetrador en redes sociales. Determina la identidad completa de ambos.

Respuesta: _____
_____

9. ¿Cuál es el nombre de la empresa administrada por Fadi Mahmoud El-Hadidi que desarrolla actividad tanto en El Cairo como en Atenas?

Respuesta: _____
_____

10. Correlaciona las fotografías y vídeos publicados del posible perpetrador de la red en redes sociales con los gastos relevantes reflejados en su cuenta de Velora Finance para determinar cuál es su distrito operativo más probable en Atenas.

Respuesta: _____
_____