UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

TÍTULO DEL PROYECTO:
OPEN SOURCE INTELLIGENCE PARA INTELIGENCIA DE AMENAZAS DE SEGURIDAD INFORMÁTICA
Línea de Investigación:
Sistemas de Información e Informática
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor:
Ing. Eddy Javier Logroño León
Tutor:
MSc. Ing. Pablo Recalde

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, MSc. Ing. Pablo Recalde con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: **OPEN SOURCE INTELLIGENCE PARA INTELIGENCIA DE AMENAZAS DE SEGURIDAD INFORMÁTICA.**

Elaborado por: Eddy Javier Logroño León, de C.I: 1714557665, estudiante de la Maestría: Seguridad Informática, mención: Tecnologías de la Información y Comunicación de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

_____

Firma

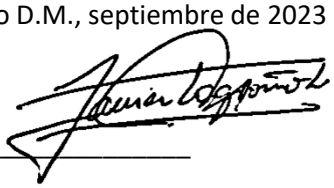
ORCID: 0000-0001-7256-2836

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Ing. Eddy Javier Logroño León con C.I: 1714557665, autor del proyecto de titulación denominado: *OPEN SOURCE INTELLIGENCE PARA INTELIGENCIA DE AMENAZAS DE SEGURIDAD INFORMÁTICA*. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2023



Firma

ORCID: 0009-0000-2388-9373

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

A medida que aumenta la complejidad de las ciberamenazas, la necesidad de conocimiento y previsión se vuelve más importante, para garantizar la seguridad de los sistemas y la protección de datos sensibles. Por esta razón, el análisis de amenazas se ha convertido en un componente importante de la seguridad de la información.

Contextualización del tema

Las amenazas cibernéticas están evolucionando y volviéndose más complejas y difíciles de identificar como resultado del desarrollo continuo de las tecnologías de la información y las comunicaciones. Los ciberdelincuentes utilizan técnicas y tácticas cada vez más avanzadas, como el phishing, el ransomware, el malware y el espionaje cibernético, para infiltrarse en sistemas y redes, robar información confidencial, causar daños y perturbar las operaciones comerciales. Por lo tanto, es de importancia contar con herramientas de investigación que permitan obtener información sobre las amenazas que se encuentran en el mundo.

Según el artículo de González, (2023) afirma que «La inteligencia de fuentes abiertas (OSINT, por sus siglas en inglés) se ha convertido en un proceso fundamental para recopilar, analizar y utilizar información de fuentes públicamente disponibles. Este tipo de inteligencia ha adquirido gran relevancia en los campos de la ciberseguridad y la inteligencia.».

En dicho contexto, se puede decir que OSINT puede ser usado para monitorear la reputación en línea de una organización y sus activos digitales, así como para identificar posibles amenazas de reputación o ataques de suplantación de identidad. Esto permite a las organizaciones proteger su imagen y reputación en línea, así como responder rápidamente a cualquier incidente que pueda afectar su reputación.

Problema de investigación

El problema de investigación radica en la necesidad de comprender y aprovechar el potencial de OSINT como una herramienta efectiva en la investigación de amenazas cibernéticas en entornos tecnológicos. Aunque OSINT ofrece una amplia gama de ventajas en la identificación, prevención y mitigación de amenazas cibernéticas, todavía hay desafíos y limitaciones que deben ser abordados en la implementación y uso de esta técnica.

El problema de investigación puede incluir los siguientes aspectos:

Aunque OSINT es una disciplina amplia y en constante evolución, puede haber una falta de conciencia y comprensión adecuada sobre su potencial y aplicaciones en el contexto de la inteligencia de amenazas de seguridad informática. Ciertos métodos y mejores prácticas para recopilar, analizar y el usar los datos pueden ser necesarios para la integración efectiva de OSINT en el proceso de inteligencia de amenazas de seguridad informática.

OSINT implica recopilar y analizar información proveniente de fuentes abiertas, lo cual puede presentar desafíos técnicos en términos de accesibilidad, confiabilidad y validez de la información. Además, la disponibilidad y eficacia de las herramientas de OSINT pueden variar, lo que puede dificultar su implementación y uso eficiente en el proceso de investigación de amenazas.

La recopilación de información de fuentes públicas también puede plantear preocupaciones legales y éticas, como la privacidad, la propiedad intelectual y el cumplimiento de las regulaciones de protección de datos. Por lo tanto, es importante abordar y mitigar estos desafíos para garantizar un uso ético y legal de la OSINT en el proceso de investigación.

¿Cómo OSINT puede integrarse de manera efectiva en los procesos de inteligencia de amenazas para fortalecer la capacidad de las organizaciones para detectar, evaluar y mitigar riesgos de seguridad de manera proactiva y eficiente?

Objetivo general

Analizar el uso de *Open-Source Intelligence* para inteligencia de amenazas como una herramienta estratégica en el proceso de investigación y detección de amenazas informáticas.

Objetivos específicos

1. Investigar los fundamentos teóricos mediante el análisis documental sobre inteligencia de amenazas y OSINT para identificar posibles amenazas en las empresas.
2. Aplicar las herramientas y técnicas de OSINT mediante los frameworks seleccionados más apropiadas para el proceso de investigación de amenazas de seguridad informática.
3. Proponer una metodología para la detección de amenazas informáticas a través del análisis de los resultados teóricos y prácticos.

Vinculación con la sociedad y beneficiarios directos:

El desarrollo de la investigación tiene como objetivo, entender qué es la inteligencia de amenazas informáticas y cuáles son los impactos, métodos y herramientas utilizadas para la inteligencia de amenazas, que brindara un apoyo a instituciones privadas y públicas que buscan mantener una postura de seguridad adecuada y responsable.

El material de estudio de este proyecto llegará a ser una guía práctica para: consultores de seguridad informática, jefes o gerentes de seguridad de la información, y personas afines a la investigación de amenazas utilizando técnicas de OSINT.

La metodología que se ha propuesto, en función del objetivo de desarrollo sostenible: Industria, innovación e infraestructura, aporta en la colaboración entre investigadores, empresas y gobiernos en esta área es crucial. Intercambio de conocimientos y colaboración técnica pueden resultar en soluciones más efectivas para combatir amenazas de seguridad informática y mejorar la seguridad digital a nivel global.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

En este capítulo se describe a los aspectos importantes que son parte del proyecto y que incluye la contextualización y conceptos de seguridad informática que se emplean.

1.1. Introducción

¿Qué es una ciber amenaza?

El instituto Nacional de Estándares y Tecnología NIST, (2023) describe a una amenaza como: "Cualquier circunstancia o suceso que podría tener un impacto negativo en las operaciones de una organización (incluyendo su misión, función, imagen o reputación), activos o propiedad personal a través de un sistema de comunicación de información mediante acceso no autorizado, destrucción, divulgación, alteración y/o negativa a proporcionar información. Trabajo. Además, la probabilidad de que el actor de la amenaza logre explotar una debilidad específica en el sistema de información".

¿Qué es Inteligencia?

Según el Departamento de Comunicaciones INSEG, (2018), menciona que «Es posible resolver problemas y tomar decisiones con la menor cantidad de incertidumbre mediante el razonamiento, la evaluación, la interpretación y la generación de información útil.»

"La política de seguridad nacional depende en gran medida de la inteligencia. En consecuencia, la mayoría de las naciones del mundo cuentan con agencias de inteligencia." (INISEG, 2018)

"La producción de inteligencia se centra en el conocimiento integral de todas las facetas de los fenómenos que plantean riesgos y amenazas a la seguridad nacional, incluidas sus posibles manifestaciones, probabilidades y efectos, así como los factores que interactúan con ellos y las conexiones que los causan." (GOBMX, 2023)

Según la Oficina de la Dirección Nacional de Inteligencia, (2023) se puede decir que "El resultado de recopilar, procesar, integrar, evaluar, analizar e interpretar información sobre enemigos, fuerzas o elementos hostiles o potencialmente hostiles, naciones extranjeras y zonas de combate reales o potenciales es inteligencia. El término también se aplica a las actividades de creación de productos y a las organizaciones que participan en dichas actividades."

¿Qué es la Ciberinteligencia?

De acuerdo al artículo de Domouso, (2018) menciona que «La ciberinteligencia no es más que la aplicación de la inteligencia en el ciberespacio. Los campos relacionados con la

tecnología, como la inteligencia de malware, la inteligencia de botnets y la inteligencia APT, están todos cubiertos por la inteligencia desde una perspectiva militar y de defensa y seguridad.»

¿Qué es Inteligencia de amenazas?

Inteligencia de Amenazas es el proceso de recopilación, análisis y uso de información relevante para identificar amenazas a la seguridad de una organización. Esta información se recopila de una variedad de fuentes, incluidos datos de eventos de seguridad, inteligencia de amenazas, análisis de malware y actividades de piratería. El análisis de estos datos puede ayudar a identificar amenazas potenciales y tomar medidas proactivas para prevenir ataques de ciberseguridad. (Sousa, 2023)

La inteligencia de amenazas a menudo se genera mediante el análisis de datos de una variedad de fuentes, que incluyen:

- Herramientas de seguridad como cortafuegos, sistemas de detección de intrusos y software antivirus.
- Información disponible públicamente, incluidos artículos de noticias, publicaciones en redes sociales y foros.
- Fuentes privadas, como proveedores de seguridad y organizaciones de inteligencia

Al recopilar información relevante, como inteligencia de amenazas y análisis de malware, las empresas pueden identificar tendencias y comportamientos sospechosos, además de anticiparse a posibles amenazas. De esta manera, es posible proteger a la institución contra amenazas conocidas y desconocidas, permitiendo medidas proactivas para mitigar los riesgos de seguridad. Además, la adopción de Inteligencia puede ayudar a mejorar la eficacia de los equipos de ciberseguridad. Esto les permite tomar decisiones mejor informadas más rápido en respuesta a las amenazas emergentes. (Sousa, 2023)

Un componente clave de la ciberseguridad contemporánea es la inteligencia sobre amenazas, que es crucial para que las organizaciones se mantengan al día sobre el panorama de amenazas en constante evolución. Al mantenerse informadas sobre amenazas potenciales, las organizaciones pueden tomar medidas proactivas para defenderse, minimizando el riesgo de ataques exitosos y protegiendo sus valiosos activos.

La idea de generar inteligencia para abordar los desafíos de seguridad informática permite mirar hacia herramientas que permitan investigar y recolectar información relevante en el proceso de investigación.

OSINT (Open Source Intelligence)

Según Fonte, (2021), indica que “OSINT es un conjunto de métodos y herramientas para recopilar información disponible públicamente, analizar los datos y compararlos, convirtiéndolos en conocimiento útil.”

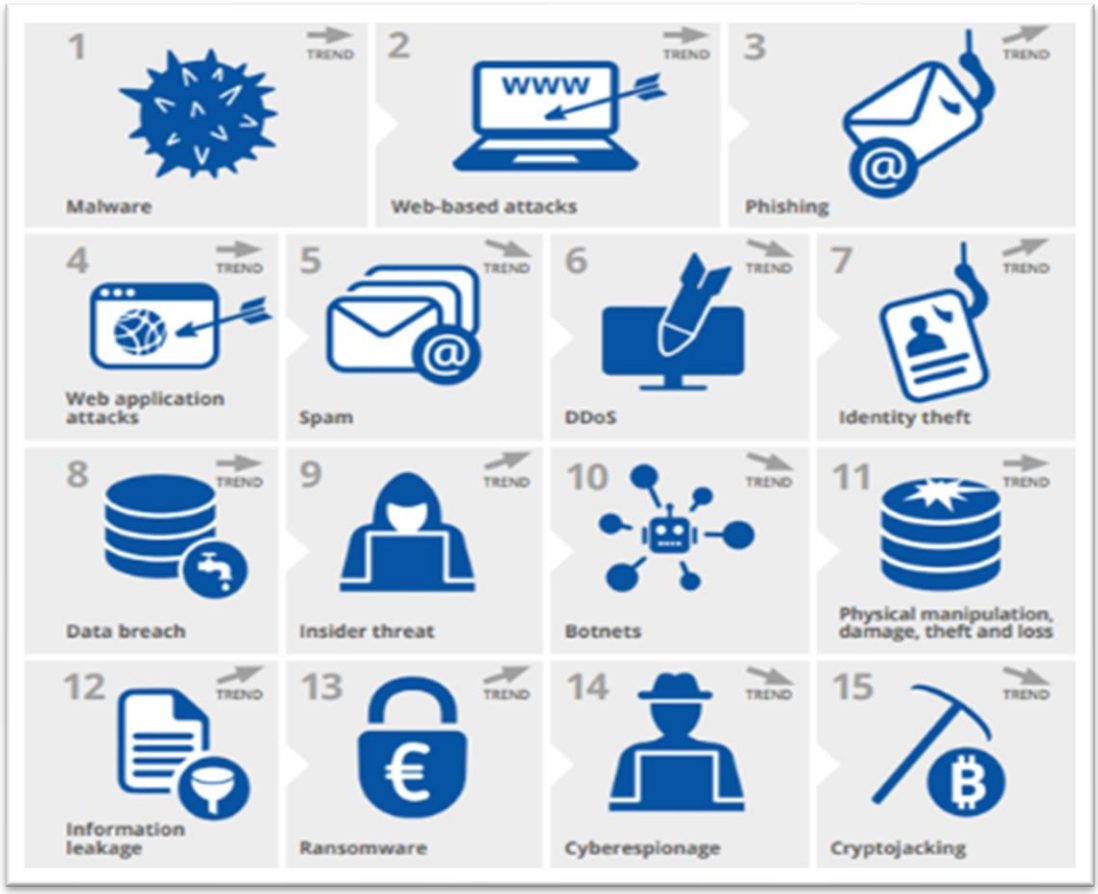
“En otras palabras, se puede decir que usamos OSINT para recopilar toda la información que podamos de cualquier fuente disponible públicamente sobre una empresa, una persona o cualquier otra cosa que queramos investigar y convertir todos los datos recopilados en inteligencia, lo que nos ayuda.” (Fonte, 2021)

La OSINT desempeña un papel fundamental en la ciberseguridad, la inteligencia y la investigación. Es una herramienta valiosa que aprovecha la disponibilidad de las fuentes de información para proteger a las organizaciones y personas de posibles amenazas. Es esencial familiarizarse con los diferentes tipos de OSINT, comprender sus usos, estar al tanto de las últimas tendencias y estar informado sobre las tecnologías emergentes. (González, 2023)

1.2. Amenazas en Ciberseguridad

Según la empresa Kriptos, (2023), «En los últimos años, la ciberseguridad ha cobrado gran importancia a nivel mundial, especialmente para las empresas que manejan información confidencial e información sensible». En este sentido, es fundamental comprender los distintos tipos de ataques, sus mecanismos y las precauciones necesarias para evitarlos.

Figura 1.
Top 15 de amenazas en 2020



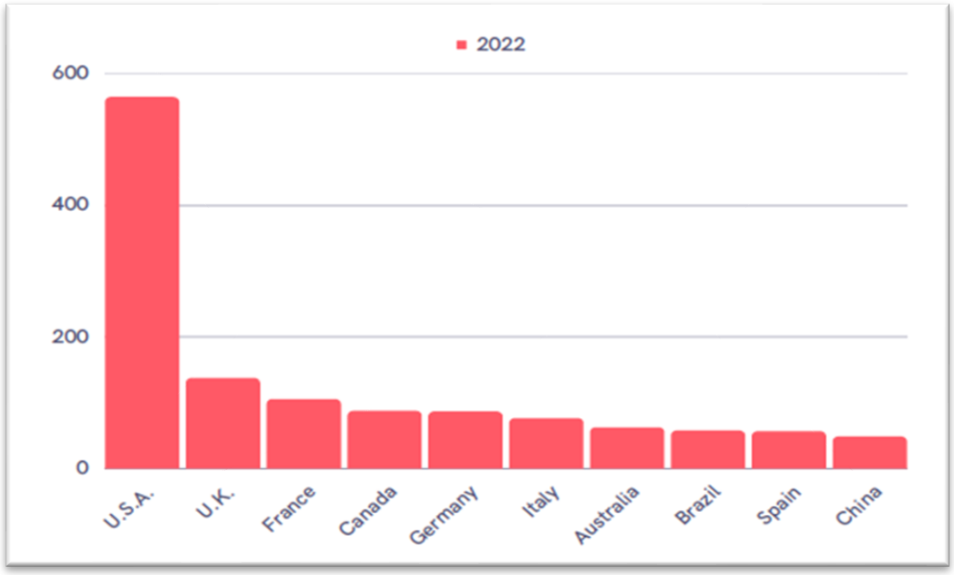
Nota: Imagen tomada de Instituto Nacional de Ciberseguridad (España, 2020)

En la figura 1, se representan los principales tipos de amenazas a los que las organizaciones se ven expuestas. El Instituto Nacional de Ciberseguridad pretende dar una visión global de las ciber amenazas existentes y que actualmente son de mayor representación. (INCIBE, 2021)

A continuación, se describen las amenazas más comunes, que una empresa puede ser víctima en el mundo digital:

- **Ransomware**: Es un tipo de software que se distribuye a través de archivos adjuntos enviados por correo electrónico maliciosos, sitios web dudosos, aplicaciones poco confiables y dispositivos de almacenamiento infectados con virus para cifrar e interceptar datos en la computadora de un usuario.

Figura 2.
Países objetivos para ataques Ransomware en 2022

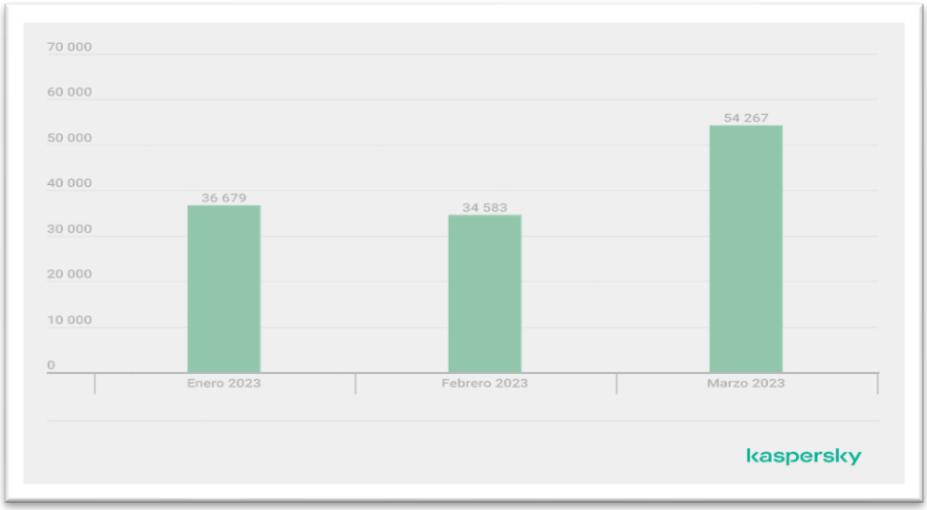


Nota: Imagen tomada del reporte Global Ransomware 2022, SOCRadar

En la figura 2, se muestra los países que tuvieron una gran cantidad de ataques en el año 2022. El tamaño de la población de los Estados Unidos, el exceso de empresas y el hecho que las sedes de muchas empresas a nivel mundial estén en Estados Unidos son factores fundamentales. Además, los grupos de ransomware que normalmente se encuentran en Rusia son otra razón para apuntar a empresas estadounidenses. (SOCRadar, 2022)

- **Malware**: software malicioso que tiene que objetivo atacar los sistemas, los datos y la red de una organización.

Figura 3.
Ataques malware financiero, primer trimestre de 2023

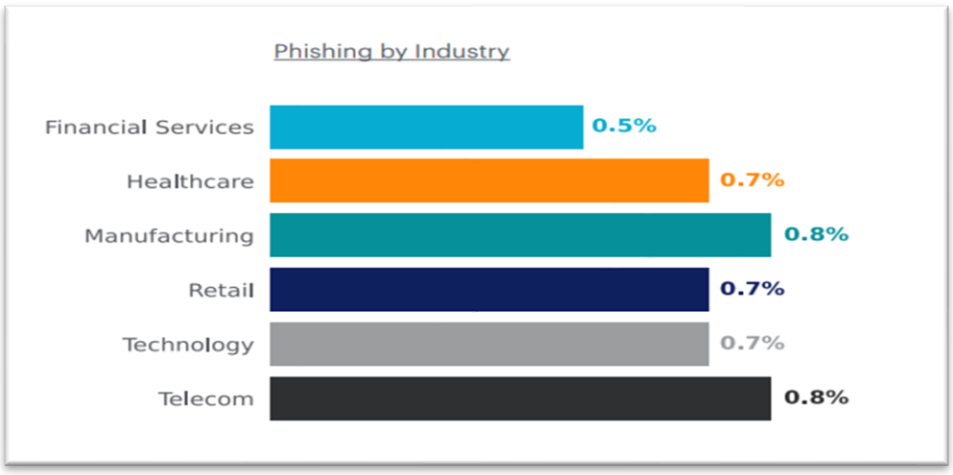


Nota: Imagen tomada del Informe sobre Malware, SecureList (Kaspersky, 2023)

En la figura 3, se muestra que, en el primer trimestre de 2023, existieron miles de ejecuciones de uno o más programas maliciosos diseñados con la finalidad de robar dinero de cuentas bancarias. (Kaspersky, 2023)

- **Phishing**: Técnica de ingeniería social diseñada para engañar y confundir a los usuarios para que faciliten información confidencial; los ciberdelincuentes suelen enviar correos electrónicos falsos que se supone provienen de fuentes legítimas.

Figura 4.
Phishing por Industrias en el Q4 de 2022

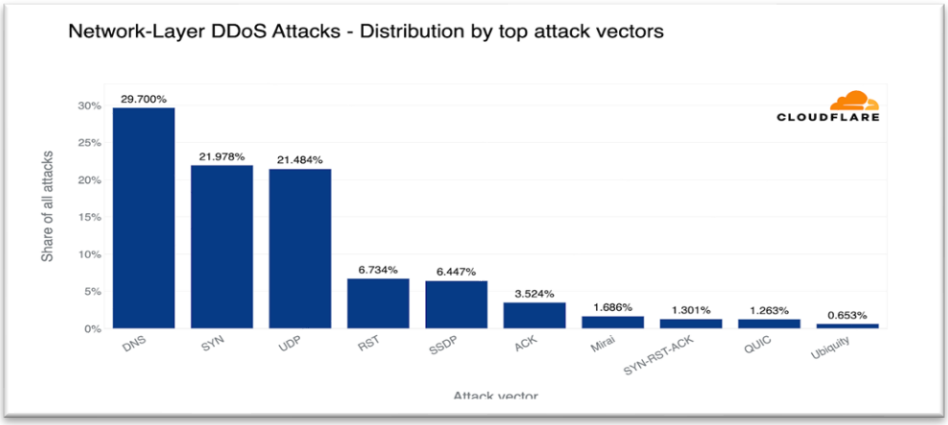


Nota: Imagen tomada del Informe de nube y amenazas: phishing, (NetsKope, 2022)

En la figura 4, se muestra que El Grupo de Trabajo Anti-Phishing (APWG) informa que los ataques de phishing continúan aumentando a niveles récord, con instituciones financieras, aplicaciones en la nube y redes sociales que representan más de la mitad de todos los objetivos de phishing. Este informe sobre la nube y las amenazas explora los ataques de phishing que están llegando con éxito a los usuarios empresariales. En el tercer trimestre de 2022, 8 de cada 1000 usuarios empresariales hicieron clic en un enlace de phishing o intentaron acceder a contenido de phishing. (Netskope, 2022)

- **Ataques distribuidos de denegación de servicio (DDoS):** diferentes equipos infectados y comprometidos, atacan a un objetivo (un servidor, un sitio web o cualquier otro recurso informático en la red) que hace que el servicio se vea afectado.

Figura 5.
Distribución por vector de ataques, ataques DDoS en la capa de aplicación

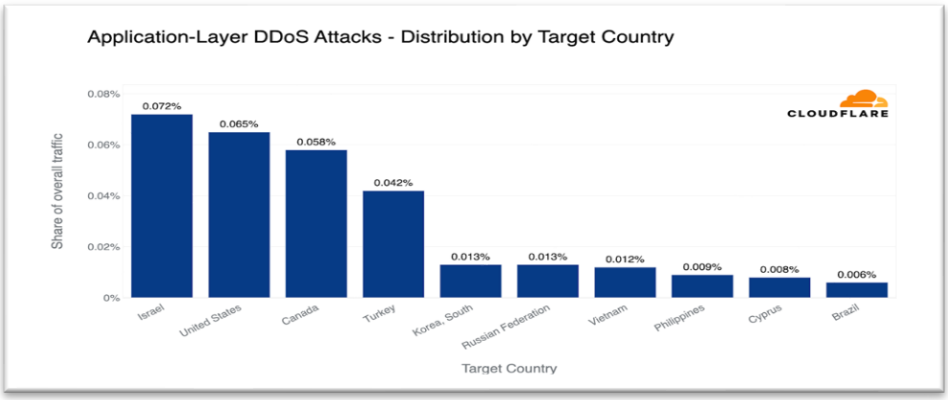


Nota: Imagen tomada del Reporte de amenazas DDoS 2023 Q1, (CloudFlare, 2023)

En la figura 5, "se pueden observar cambios significativos en el primer trimestre. SYN Floods cayó al segundo lugar con un 22%, convirtiendo a los ataques DDoS basados en DNS en el método de ataque más común (30%). Un tercio de todos los ataques DDoS de Capa 3 y Capa 4 están basados en DNS: ataques de desbordamiento de DNS o ataques de amplificación de DNS. Los ataques a través de UDP ocuparan el tercer lugar con un 21%." (CloudFlare, 2023)

- **Redes de bots:** Dispositivos conectados a Internet infectados y controlados remotamente por un tipo específico de malware.

Figura 6**.**
Distribución por países, objetivos sobre ataques DDoS en la capa de aplicación



Nota: Imagen tomada del Reporte de amenazas DDoS 2023 Q1, (CloudFlare, 2023)

En la figura 6, se muestra que “Israel encabezó la lista de naciones afectadas por la mayor cantidad de tráfico HTTP DDoS en el primer trimestre, superando a Estados Unidos. Esto puede deberse a reformas judiciales, protestas de la oposición o tensiones actuales en Cisjordania, se trata de una cifra asombrosa. Los ataques HTTP DDoS contra sitios web israelíes representaron menos del 1% del tráfico HTTP total manejado por Cloudflare en el primer trimestre del año. Estados Unidos no se quedó atrás, le siguieron de cerca Estados Unidos, Canadá y Turquía.”(CloudFlare, 2023)

1.3. Tácticas, técnicas y procedimientos (TTP) para emulación de adversarios

“La capacidad de una organización para reconocer, reaccionar, recuperarse y mitigar un ataque público se prueba mediante el uso de simulación de atacante, un tipo de ejercicio de seguridad de ataque que simula las tácticas de un atacante o adversario en particular.” (Raggi, 2021)

Fragmento de la obra “El Arte de la Guerra” de Sun-Tzu

> “*Si conoces a tu enemigo y te conoces a ti mismo, no debes temer el resultado de cien batallas. Si te conoces a ti mismo, pero no conoces a tu enemigo, por cada victoria obtenida también sufrirás una derrota. Si no conoces a tu enemigo ni a ti mismo, caerás en cada batalla*”

Basado en el artículo de Raggi, (2021) «Estos ejercicios crean un escenario basado en una técnica o estructura organizacional específica que luego será utilizada por el equipo atacante (Equipo Rojo/*Red Team*) en la organización, permitiéndonos comprender cómo los defensores (Equipo Azul/*Blue Team*) pueden contrarrestarlo. Como resultado de este tipo de ejercicio conjunto entre el *Red Team* y el *Blue Team*, se crea un equipo virtual denominado Equipo Púrpura/*Purple Team*»

En resumen, este tipo de ejercicios mejoran así la capacidad de evaluar y mejorar diversos procedimientos y funciones de seguridad dentro de la organización, como la función SOC (Analista de seguridad, Analista de seguridad o Respuesta a incidentes, Cazador de amenazas), TI y Administrador del sistema, directivos y personas interesadas. Su objetivo es algo más que una simple evaluación técnica de las medidas preventivas y de seguridad.

1.4. Framework utilizado para la emulación de adversario

MITRE ATT&CK es una organización que ha creado una base de conocimientos que contiene información sobre tácticas, técnicas y procedimientos; con una metodología de clasificación para describir y categorizar el comportamiento de los actores de amenazas.

Figura 7.
Mitre Att&ck Framework

Nota: imagen tomada de Hyper, Moffatt, 2021

En la figura 7, se muestra la matriz de MITRE ATT&CK, la cual está conformada por 14 tácticas y 224 técnicas con sus respectivos procedimientos o sub técnicas agrupados de manera que se pueden identificar las actividades de intrusión y el software utilizados por actores de maliciosos. Para el efecto de este estudio, tomaremos como referencia las tácticas TA0043 que son parte del apartado de Reconocimiento, que usa herramientas de OSINT para el proceso de investigación.

Figura 8.
Matriz empresarial MITRE ATT&CK

Nota: Ver Anexo 4, fuente: NetGain Systems, 2021

1.5. Contextualización general del estado del arte

La inteligencia de fuentes abiertas, conocida como OSINT, ha adquirido una importancia significativa debido a la abundante cantidad de datos personales y organizacionales expuestos en Internet. Su versatilidad permite su aplicación en diversos ámbitos y con distintos propósitos. Por ejemplo, los cuerpos policiales utilizan OSINT para evaluar posibles conexiones entre individuos bajo investigación, mientras que el periodismo de investigación puede aprovecharlo para encontrar información complementaria que ha quedado al descubierto por descuido y está al alcance de todos.

En el campo de la seguridad de la información, OSINT es una temática de gran actualidad que se utiliza tanto en el ámbito ofensivo como defensivo con el objetivo de salvaguardar la seguridad de personas y organizaciones.

En la actualidad, las técnicas, métodos y herramientas de OSINT siguen evolucionando constantemente. Es fundamental contar con el conocimiento adecuado sobre las distintas herramientas y métodos para lograr resultados óptimos al aplicar OSINT. La habilidad para realizar búsquedas y vinculaciones de información se vuelve crucial para las organizaciones, lo cual afecta directamente a la necesidad de contar con profesionales especializados en OSINT que sean capaces de analizar grandes volúmenes de información de manera efectiva.

El Departamento de Defensa (DoD) de los Estados Unidos define OSINT como:

> *"La Inteligencia de fuentes abiertas (OSINT) es una inteligencia que se produce partiendo de información pública disponible y es obtenida, utilizada y difundida a tiempo a una audiencia adecuada con la finalidad de responder a una petición específica de inteligencia*"

"Obtener inteligencia sobre amenazas basada en evidencia, incluida información sobre los recursos, la infraestructura, las motivaciones y las capacidades de los atacantes. Como resultado, CTI permite la detección de indicadores de ciberamenazas, la extracción de información sobre técnicas de ataque, la identificación de amenazas a la seguridad y la toma temprana de decisiones necesarias para responder con precisión y decisión a posibles ataques." (Portillo, 2023)

"La inteligencia sobre amenazas es creada por analistas de seguridad que recopilan datos no procesados sobre amenazas a la seguridad de diversas fuentes, los compilan y luego analizan los números para encontrar tendencias, patrones y conexiones que indiquen amenazas reales o potenciales." (IBM, 2023)

"Para gestionar las amenazas, es fundamental tener una visión integral y completa de los activos. Para tomar decisiones informadas y proteger su empresa, necesita un software que pueda monitorear la actividad, detectar problemas y entregar datos precisos." (Kaspersky, 2023)

"Esta información será aclarada un poco más por Open Source Intelligence. En cierto modo, se podría decir que su objetivo es identificar los datos apropiados en todas estas combinaciones y luego transformarlos en información que sea útil para un propósito particular". (ThinkBig, 2022)

“Las partes interesadas evalúan los hallazgos, toman decisiones importantes y ofrecen comentarios para mejorar los esfuerzos de inteligencia después de recibir la inteligencia final. La eficacia y la velocidad de las operaciones de inteligencia, así como los plazos de entrega, son con frecuencia el foco de las mejoras en esta área de operaciones.” (OSTEC, 2022)

La inteligencia de amenazas basada en OSINT ha evolucionado de ser un enfoque complementario a ser una pieza central en la estrategia de ciberseguridad de muchas organizaciones. Al aprovechar datos de fuentes abiertas, las empresas pueden anticipar y responder de manera proactiva a las amenazas cibernéticas, mejorando su resiliencia y protección de activos críticos. (Romero, 2018)

“OSINT se basa en buscar y analizar información disponible en la web, como sitios web, redes sociales, fuentes de noticias, blogs y otros medios públicos de Internet. Esta información se recopila, clasifica y analiza para proporcionar información útil y valiosa que puede usarse para identificar tendencias, oportunidades y problemas potenciales.” (Arimetrics, 2023)

“En otras palabras, podemos decir que usamos OSINT para recopilar todos los datos sobre una empresa, una persona o cualquier otra cosa que queramos investigar de cualquier fuente pública y transformar cantidades masivas de datos en inteligencia, para que podamos producir resultados más eficazmente.” (Fonte, 2021)

“El mundo está ahora más interconectado que nunca gracias a la tecnología digital, pero esta mayor conectividad también aumenta el riesgo de ciberataques como malware, robo de datos y violaciones de seguridad. Un componente esencial de la ciberseguridad es la inteligencia sobre amenazas”. (Kaspersky, 2023)

“Según Seisdedos, el método OSINT ofrece información detallada sobre el objetivo de la prueba o el activo que necesita ser protegido para el investigador de ciberseguridad o analista de seguridad de la información. Cuanto más conocimiento tenga sobre su objetivo, por ejemplo, mayores serán sus posibilidades de éxito en las pruebas de penetración o en los servicios de ingeniería social.” (ThinkBig, 2022)

1.6. Proceso investigativo metodológico

El proyecto de investigación «Uso de *Open-Source Intelligence(OSINT)* para inteligencia de amenazas en el proceso de investigación de amenazas informáticas» se enfoca en el uso de fuentes de información de acceso público para recopilar datos y analizarlos en el contexto de la seguridad informática. En cuanto al tipo de investigación, se utilizará una investigación de tipo exploratorio-descriptivo, ya que se busca identificar y describir los aspectos relevantes del uso

de OSINT en el proceso de inteligencia de amenazas, con el fin de establecer una base teórica y metodológica que permitiera su aplicación práctica.

En cuanto a los métodos teóricos y prácticos que se aplican, se llevará a cabo una revisión bibliográfica exhaustiva para recopilar información relevante y actualizada sobre el tema. Además, se realizaron entrevistas a expertos en ciberseguridad y se utilizaron herramientas de OSINT para recolectar información sobre casos de estudio relevantes.

La metodología de trabajo utilizada para desarrollar el proyecto incluye las siguientes etapas: revisión bibliográfica, análisis de datos y resultados, y elaboración de conclusiones y recomendaciones. Para garantizar la validez, y fiabilidad de los resultados obtenidos, cada uno de estos pasos se realiza de forma sistemática y minuciosa utilizando las herramientas y métodos adecuados.

CAPÍTULO II: PROPUESTA

En este capítulo, se presenta la propuesta de investigación que busca explorar y analizar el uso de OSINT en el ámbito de la inteligencia de amenazas informáticas.

2.1 Inteligencia de fuentes abiertas: O*SINT*

Introducción

"Los datos en el mundo digital se consideran como el mayor riesgo que las empresas deben abordar y que deben mantenerse a salvo de personal no autorizado. Con la ayuda de Internet podemos realizar casi cualquier tarea desde la comodidad de nuestros hogares o desde cualquier parte del mundo. Estos riesgos están presentes a pesar de la facilidad de acceso. Entre ellos se encuentran el robo de identidad y la piratería informática." (Ramírez, 2023)

En este contexto, se requieren soluciones confiables y seguras para superar los problemas asociados con la confiabilidad de las fuentes y la forma que se presentan los datos y como se acceden a ellos. El uso de datos impulsa la toma de decisiones convirtiéndose en una oportunidad de interés tanto para las empresas públicas y privadas, así como para los gobiernos.

Algunos datos están protegidos de forma privada, pero un gran porcentaje de los datos está disponible públicamente. Los datos públicos (o datos de "fuente abierta") están ahí para que cualquiera los use, pero puede ser difícil identificar la información relevante en el momento adecuado. OSINT es la aplicación de procesos dirigidos por inteligencia para transformarlos en información procesable.

De acuerdo con lo expuesto por Marugán, (2023) «OSINT es un término de inteligencia militar y sigue siendo una técnica básica en las investigaciones contra el terrorismo, la contrainteligencia y el crimen organizado». Sin embargo, podemos decir que la naturaleza potencial y de amplio alcance de OSINT ha impulsado una expansión de las aplicaciones militares y gubernamentales hacia el sector privado.

Con un mayor enfoque en el análisis de datos inteligente (alineado con las tendencias de Big Data en general), OSINT está transformando las mejores prácticas de investigación. y creando resultados mucho más sólidos en otros casos de uso e industrias, que incluyen:

1. Investigaciones de fraude
2. Protección de marca
3. Identificación de amenazas internas
4. Investigaciones de comercio ilícito
5. Diligencia debida

Su ventaja frente a otros métodos de obtención de información es que no requiere permisos de seguridad especiales, por lo que no es necesario pertenecer a un organismo público para utilizarla. (Marugán, 2022)

2.2 Naturaleza de la información

Con el propósito de diferenciar los simples datos de inteligencia es posible describir la naturaleza de la información, la cual tiene como propósito detallar los aspectos y características que componen cada uno de los elementos de la llamada «pirámide de la información», estos elementos se definen de la siguiente forma:

- **Datos:** corresponde a la más mínima unidad de información, la cual por si sola es irrelevante para toma de decisiones ya que carece de un orden lógico y contexto.
- **Información:** corresponde a datos que se encuentran clasificados y en un formato que facilita su análisis. Estos datos poseen relevancia, propósito y contexto, relacionándolos también a la generación de conocimiento. En resumen, la información es equivalente a datos que poseen un contexto y utilidad.
- **Inteligencia:** corresponde a información que ha sido procesada mediante técnicas de análisis, obteniendo de estas conclusiones que permiten apoyar la toma de decisiones.

2.3 Aplicando el Ciclo de Inteligencia a OSINT

La transformación de los datos a inteligencia requiere de un proceso estructurado y estratégico esencial para recopilar, analizar y utilizar información de fuentes abiertas con el propósito de detectar, prevenir y mitigar amenazas cibernéticas. que permita mantener enfocado los resultados relevantes. Uno de esos procesos que vale la pena examinar en detalle es el ciclo de inteligencia. (BlackDot, 2021)

El uso del ciclo de inteligencia puede ayudar a comprender lo que significa cada etapa del ciclo para la investigación OSINT que seguirá. El ciclo de inteligencia sigue una serie de etapas interconectadas que permiten a los investigadores obtener una comprensión completa del panorama de amenazas y tomar decisiones informadas. (BlackDot, 2021)

Figura 9.
Ciclo de Inteligencias de OSINT

Nota: Elaboración propia basado en ODINT.net, 2023

En la figura 9, se muestra el ciclo de vida de inteligencia OSINT. A continuación, se describe algunas etapas del Ciclo de Inteligencia de OSINT que se aplicara a esta propuesta de investigación:

1. **Preparación y Dirección Estratégica:** Define los objetivos de la investigación y se determina qué información es relevante para la organización. Se establecen las metas específicas, los recursos necesarios y los criterios de éxito para guiar el proceso de obtención y análisis de datos.
2. **Recolección de Datos:** Busca recopilar información de fuentes abiertas, como sitios web, noticias, redes sociales, foros y otras fuentes públicas. Los equipos pueden recopilar estos datos utilizando herramientas y metodologías de su preferencia para filtrar la información para obtener lo más relevante.
3. **Procesamiento:** Procesa y organiza la información recopilada, lo que ayuda a comprender la intención y el comportamiento de los actores maliciosos y a evaluar la magnitud de las amenazas.
4. **Análisis:** En esta etapa, se produce Inteligencia ya que se generan informes estructurados para ser comprensibles y entendibles para las partes interesadas.

Este es un paso importante en el ciclo OSINT, ya que permite que sus equipos comprendan y anticipen eventos utilizando los datos que han recopilado.

5. **Entrega o Distribución:** Los informes y análisis generados se distribuyen a las partes interesadas de la organización. Los responsables de tomar decisiones estratégicas de ciberseguridad a este respecto incluyen la gerencia, el equipo de seguridad y otros.

2.4 Tipos de Fuentes de Información *OSINT*

"Las fuentes abiertas no sólo están disponibles en línea hoy, en la era de las tecnologías de la información y la comunicación, aunque la mayoría de nosotros podemos acceder a ellas a través de Internet." (Domouso, 2018)

A continuación, se mencionan algunas fuentes de inteligencia OSINT:

- Publicaciones en papel: como artículos de autor, piezas analíticas, tesis doctorales y publicaciones en ciencias y medios, etc.
- Medios de comunicación y fuentes de información convencionales: incluidos libros, periódicos, revistas, radio, sistemas de megafonía, televisión y radio.
- Imágenes públicas, vídeos y metadatos relacionados, lo que resulta especialmente útil si están georreferenciados y son actuales.
- Las imágenes y videos capturados por drones, satélites u otras aeronaves mientras se encuentran en el aire o en el espacio se denominan información geoespacial pública.
- La web profunda, la web oscura e Internet: estas son las principales fuentes de información. (LISA, 2023)

2.5 Herramientas y técnicas de *OSINT*

Al realizar una investigación OSINT, hay muchas herramientas disponibles que pueden ser muy beneficiosas y brindar una variedad de opciones. A continuación, se mencionan algunas:

Google Dorks

En su blog Keepcoding, (2022) dice que “El término "Google Dork" proviene de la palabra "dork", que significa "idiota" en inglés. Así que fue Google Dork el que dejó información sensible y desprotegida en Internet." "Google Hacking o Google Dorking es uno de los métodos de inteligencia OSINT o de código abierto (osint google dorks) más famosos.”

Figura 10.
Operadores para Google Dorks

Operadores avanzados de búsqueda en Google

Operador	Ejemplo	Detalles
intitle:	intitle:estadísticas twitter""	Devuelve páginas con la frase exacta en el título.
allintitle:	intitle:estadísticas twitter facebook	Devuelve páginas con cualquiera de las palabras especificadas
inurl:	inurl:estadísticas facebook""	Devuelve páginas con la frase exacta en la URL.
allinurl:	allinurl:instagram youtube	Incluye páginas con cualquiera de las palabras especificadas
intext:	intext:historia de facebook""	Devuelve páginas con la frase exacta en el texto o en el cuerpo de la página.
allintext:	allintext:historia facebook	Devuelve páginas con cualquiera de las palabras especificadas en el texto o cuerpo

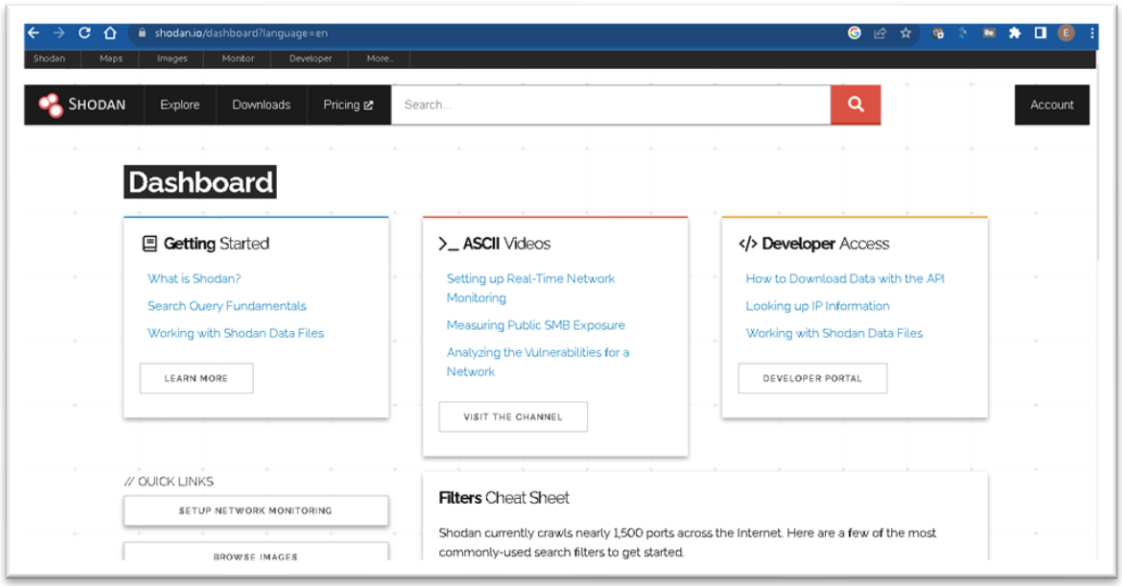
Nota: Imagen tomada desde la fuente: (Boyd, 2023)

En la figura 10, se muestran algunas opciones de operadores avanzados para Google Dorks, que permite realizar búsquedas personalizadas y dirigidas.

Shodan

Es un motor de búsqueda que permite encontrar dispositivos conectados a Internet. Conocido como "truco de Google", se utiliza para encontrar dispositivos personales, servidores, dispositivos de comunicación como enrutadores, conmutadores, así como cámaras web, dispositivos IOT, etc.

Figura 11.
Shodan como herramienta de búsqueda de información



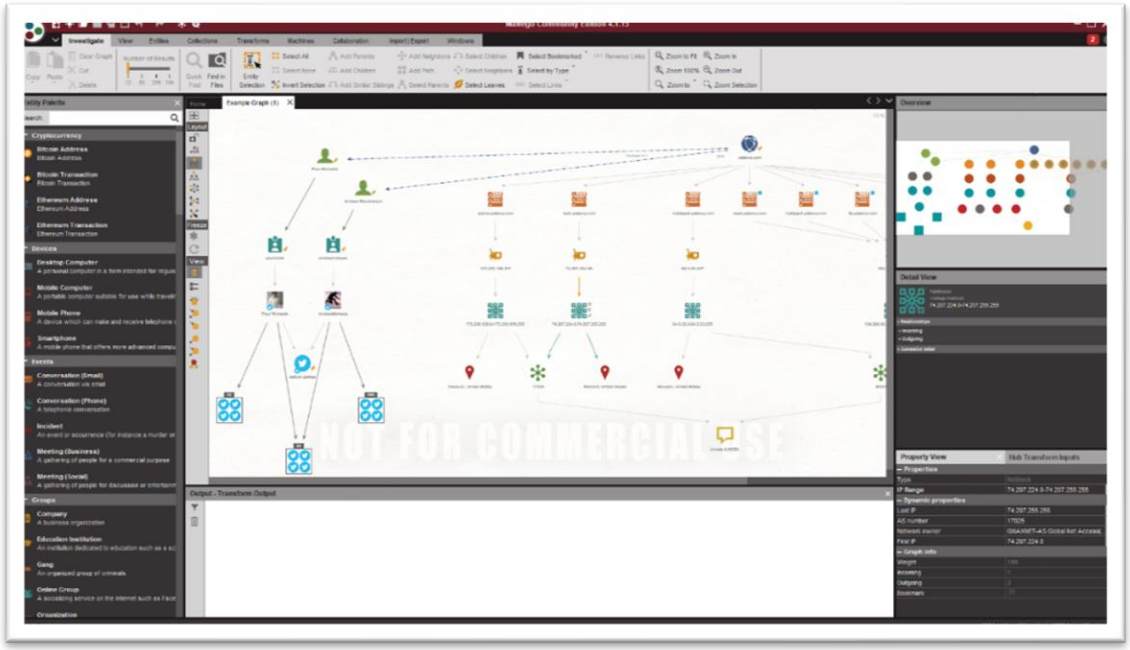
Nota: Imagen tomada desde Shodan, cuenta personal

En la figura 11, se muestra la herramienta Shodan con su página inicial, donde se observa algunas opciones con las que se puede empezar con las búsquedas.

Maltego

Esta herramienta muy poderosa, recopila información de un objetivo específico, y proporciona una infografía de los resultados, facilitando el análisis de los datos.

Figura 12.
Maltego como herramienta de búsqueda de información



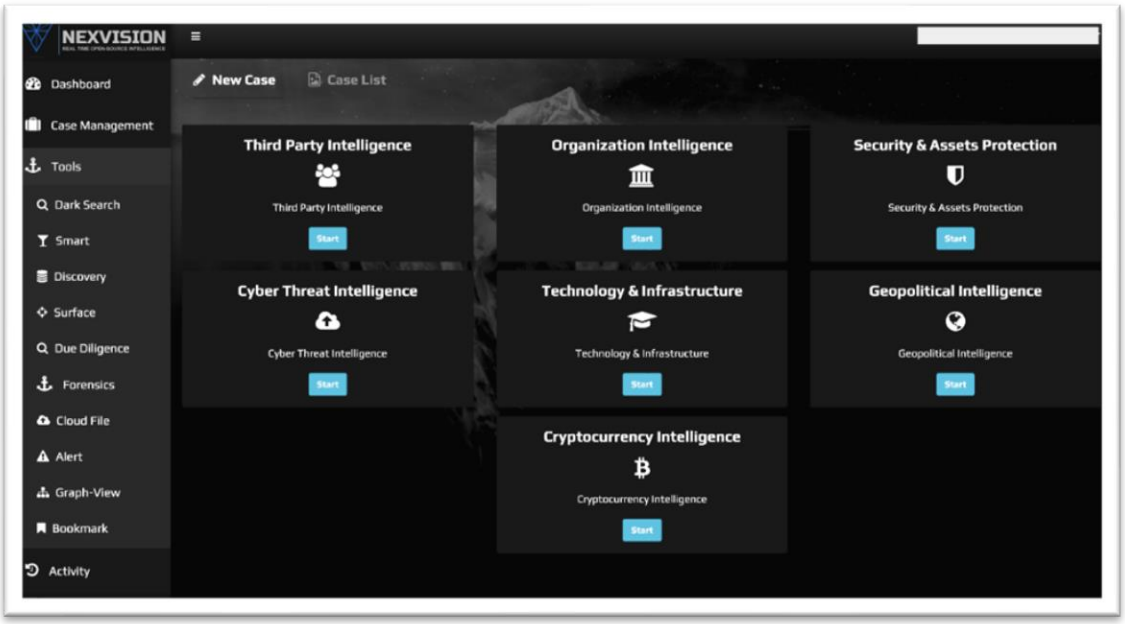
Nota: Imagen tomada desde el portal de Maltego, 2023

En la figura 12, se muestra la herramienta Maltego, donde se puede observar el árbol de información que se puede obtener en base a las búsquedas que se personalicen.

NexVision

Es una herramienta que utiliza inteligencia artificial para entregar información actual de búsquedas en la web oscura y otros sitios web.

Figura 13.
NexVision Engine



Nota: Imagen tomada desde SoftwareAdvice, 2023

En la figura 13, se muestra la herramienta NexVision y las opciones que presta para la búsqueda de información.

Social Links

Permite extraer, analizar y visualizar datos de fuentes abiertas, como redes sociales, noticias, la Dark Web y más, la herramienta también utiliza inteligencia artificial.

Figura 14.
Inteligencia en redes sociales

Nota: Imagen tomada desde la página oficial de Twitter

En la figura 14, se muestra que a través de fuentes de redes sociales se puede obtener información pública de un objetivo.

2.6 Validación de la propuesta

En el mundo de la ciberseguridad, la primera fase de un ataque es el reconocimiento y recolección de información de un objetivo. Los actores maliciosos ejecutan técnicas para recopilar información relevante, que permita conocer cuál será su siguiente paso al momento y que herramientas utilizará para continuar con el ciclo del ataque.

Para esta propuesta, se utilizará tácticas, técnicas y procedimientos que permitirán generar inteligencia con OSINT y el paso a paso en el proceso de investigación. Lo que permitirá identificar información importante que aporte en la fase de reconocimiento y el ciclo de ejecución de OSINT.

Primera fase: Preparación

Para esta fase se ha determinado que los actores de amenazas están en constante evolución sobre las técnicas y tácticas a la hora de empezar un ataque. Se ha tomado como referencia a la institución financiera Diners Club del Ecuador, por ser una de las empresas de mayor renombre en Ecuador, y que será el objetivo de análisis de este estudio.

Se toma como punto inicial la información sensible que esta institución procesa y protege. Puesto que, al ser una institución financiera, es propensa a recibir ataques de diversas formas. Por lo tanto, se ejecutará esta fase para comenzar con el estudio considerando la criticidad de los activos que maneja.

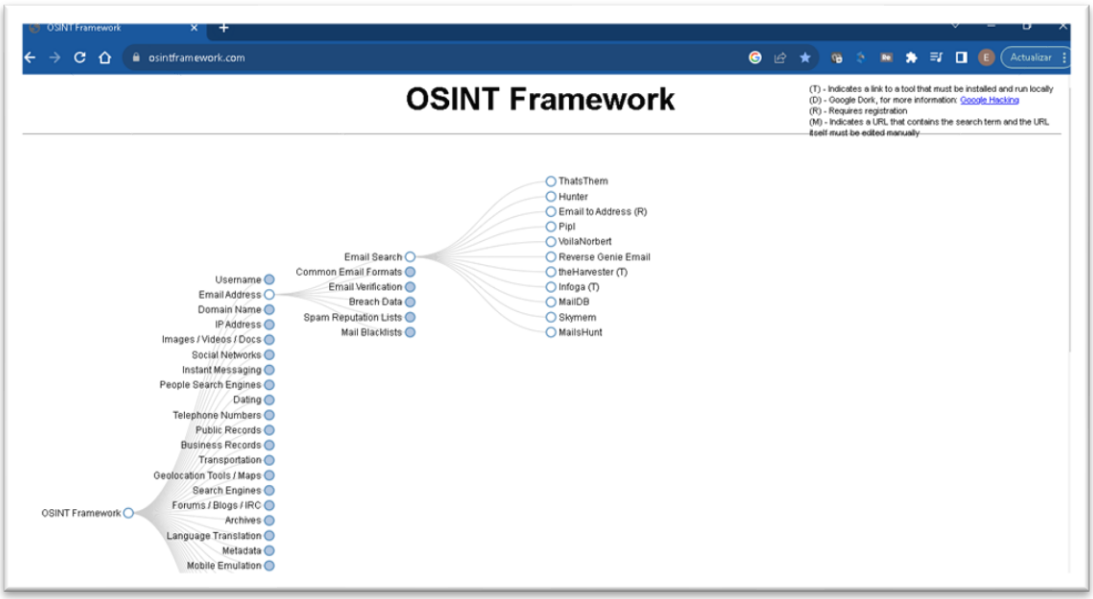
Segunda Fase: Reconocimiento

Para esta fase, se utilizará el Framework de MITRE ATT&CK, específicamente la táctica T0043 que comprende la fase de reconocimiento. Las técnicas que se usará en este proyecto serán: T1589, T1590, T1591 y 1593.

Técnica T1589: Recopilar información de identidad de la víctima.

Los atacantes pueden conocer la identidad de la víctima y luego utilizarla para rastrearla. Se pueden incluir numerosos tipos de información, incluida información personal (como nombres de empleados, direcciones de correo electrónico, etc.).

Figura 15.
OSINT Framework



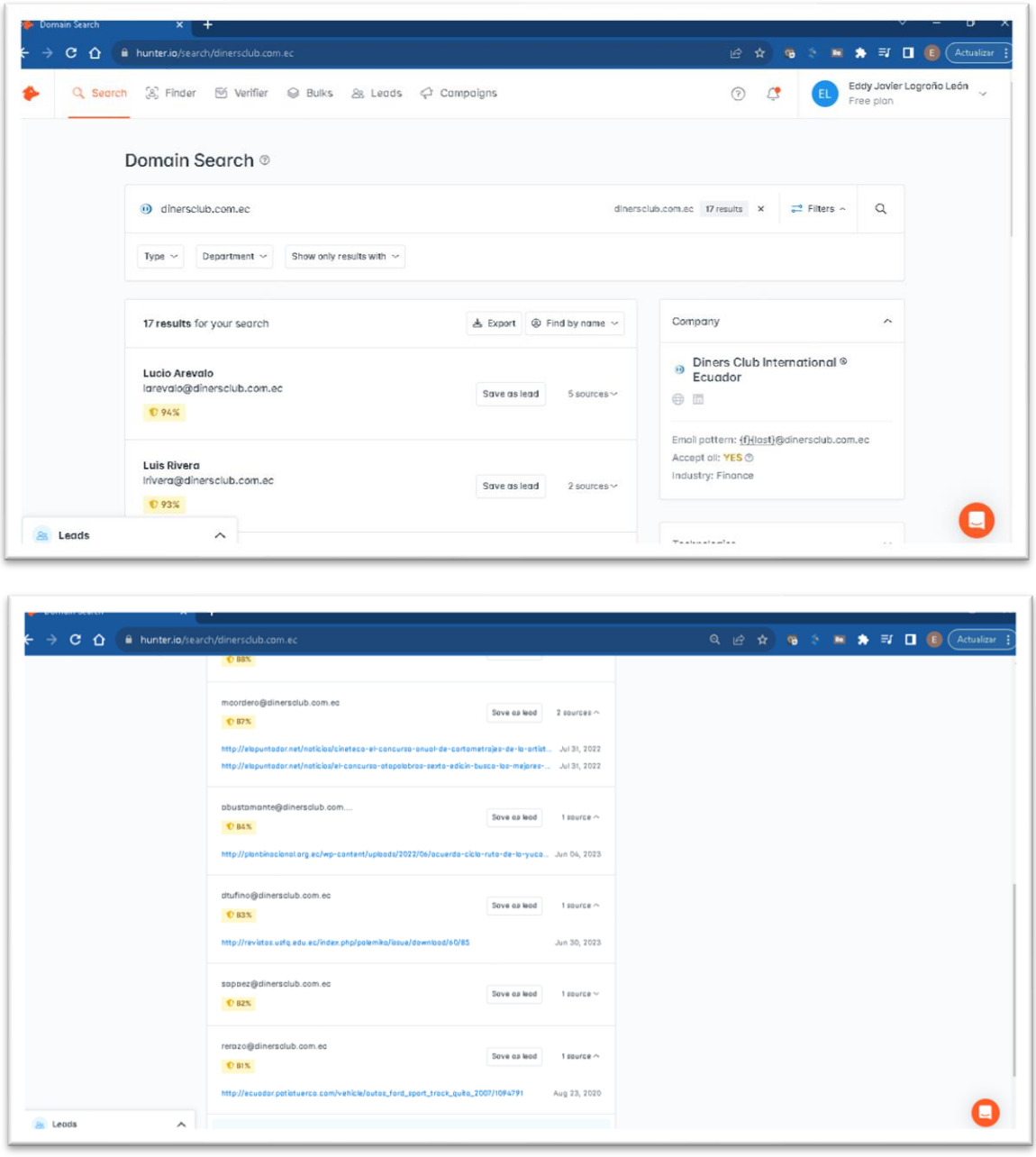
Nota: Imagen tomada desde el portal de OSINT Framework

En la figura 15, se muestran las herramientas del Framework de OSINT para la búsqueda de información sobre direcciones de correo, se utilizan herramientas gratuitas y de acceso público.

Sub Técnica T1589.002: Direcciones de correo

Hunter.io, Con solo ingresar al sitio web o dominio web de una empresa, podrá utilizar el portal en línea Hunter.io para buscar correos electrónicos de personas que trabajan allí.

Figura 16.
Búsqueda de información por dominio Diners Club del Ecuador



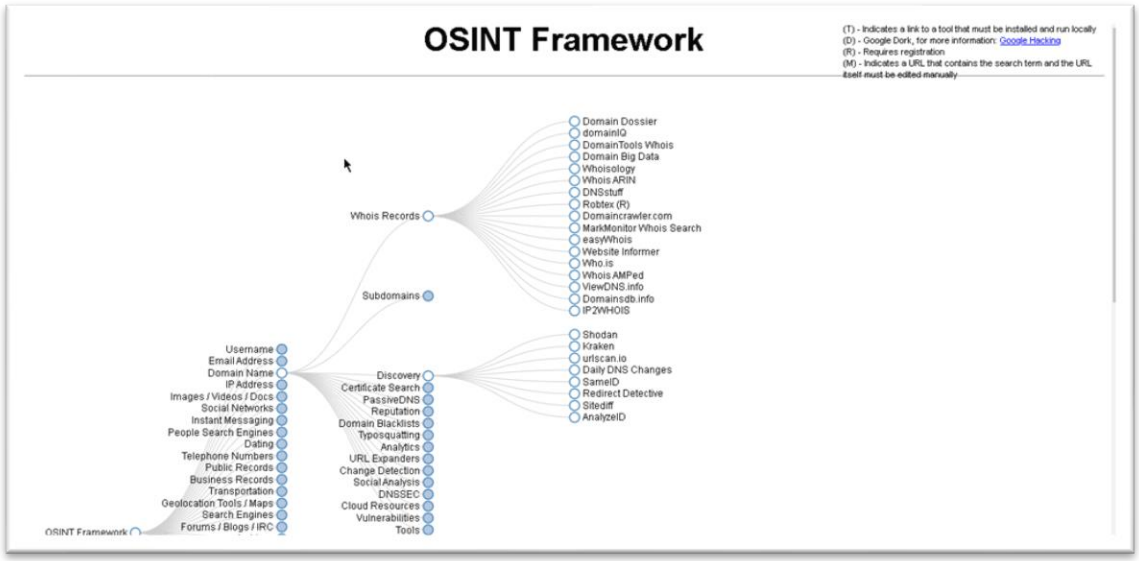
Nota: Imágenes tomadas desde el portal de búsquedas Hunter.io

En la figura 16, se muestra como usuarios de la empresa Diners Club del Ecuador, están registrados en algunos portales de noticias, revistas y sitios de intereses.

Técnica T1590: Recopilar información de la red de víctimas

Los atacantes pueden recopilar información sobre la red de la víctima para utilizarla en ataques. La información de la red puede incluir una variedad de información, incluidos datos administrativos (como rangos de direcciones IP, nombres de dominio, etc.), así como detalles sobre su topología y operaciones.

Figura 17.
OSINT Framework. Obtención de información de red



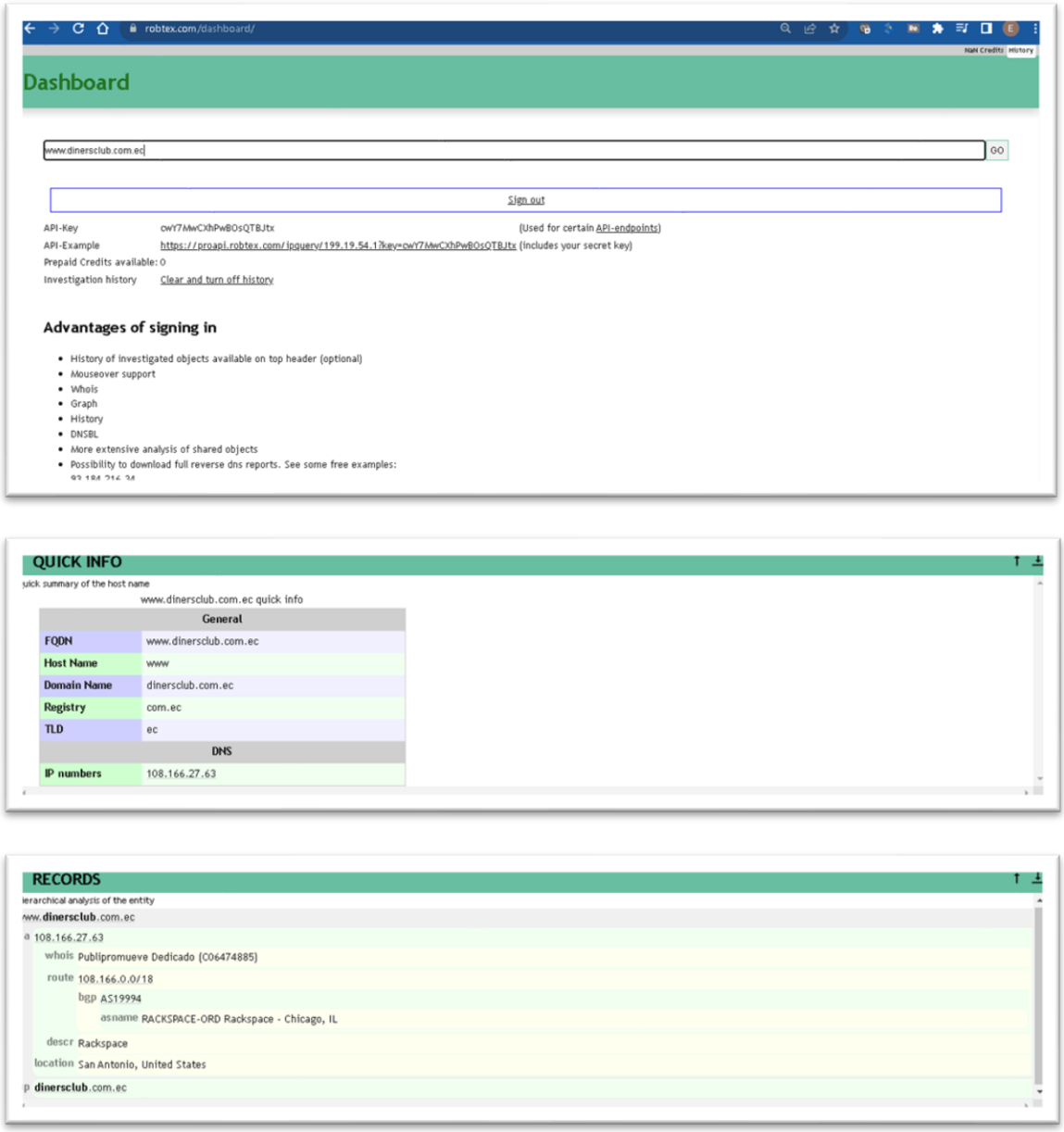
Nota: Imagen tomada desde el portal de OSINT Framework

En la figura 17, se muestra las herramientas utilizadas para conocer los registros y datos adicionales de un dominio, inclusive su topología.

Sub Técnica T1590.001: Propiedades del dominio, T1590.002 - DNS

Robtex, nos permite conocer información relevante sobre el dominio de una organización. En este caso vamos a buscar información de la empresa: Diners Club del Ecuador.

Figura 18.
Búsqueda de información con Robtex



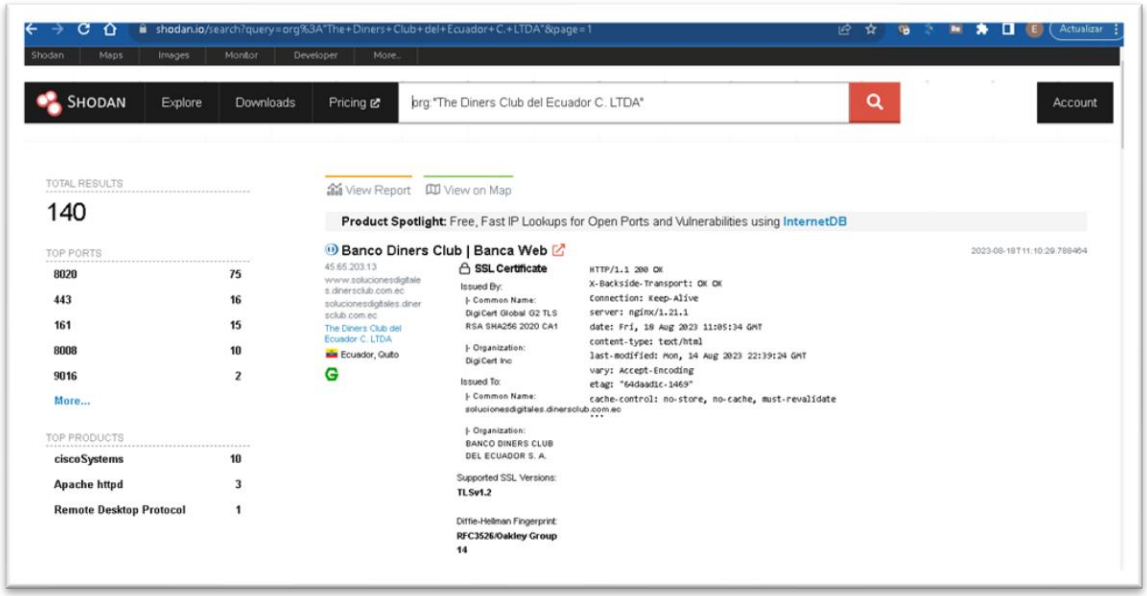
Nota: imágenes tomadas desde Robtex, fragmentos del resultado

En la figura 18, se muestra la información obtenida desde la búsqueda de un dominio en específico y las propiedades que entrega en la respuesta.

Sub Técnica T1590.005: Direcciones IP, T1590.006: Equipos de comunicaciones

Shodan, es un motor de búsqueda de dispositivos conectados a Internet. Los motores de búsqueda web, como Google y Bing, son excelentes para encontrar sitios web.

Figura 19.
Búsqueda de información desde Shodain.io



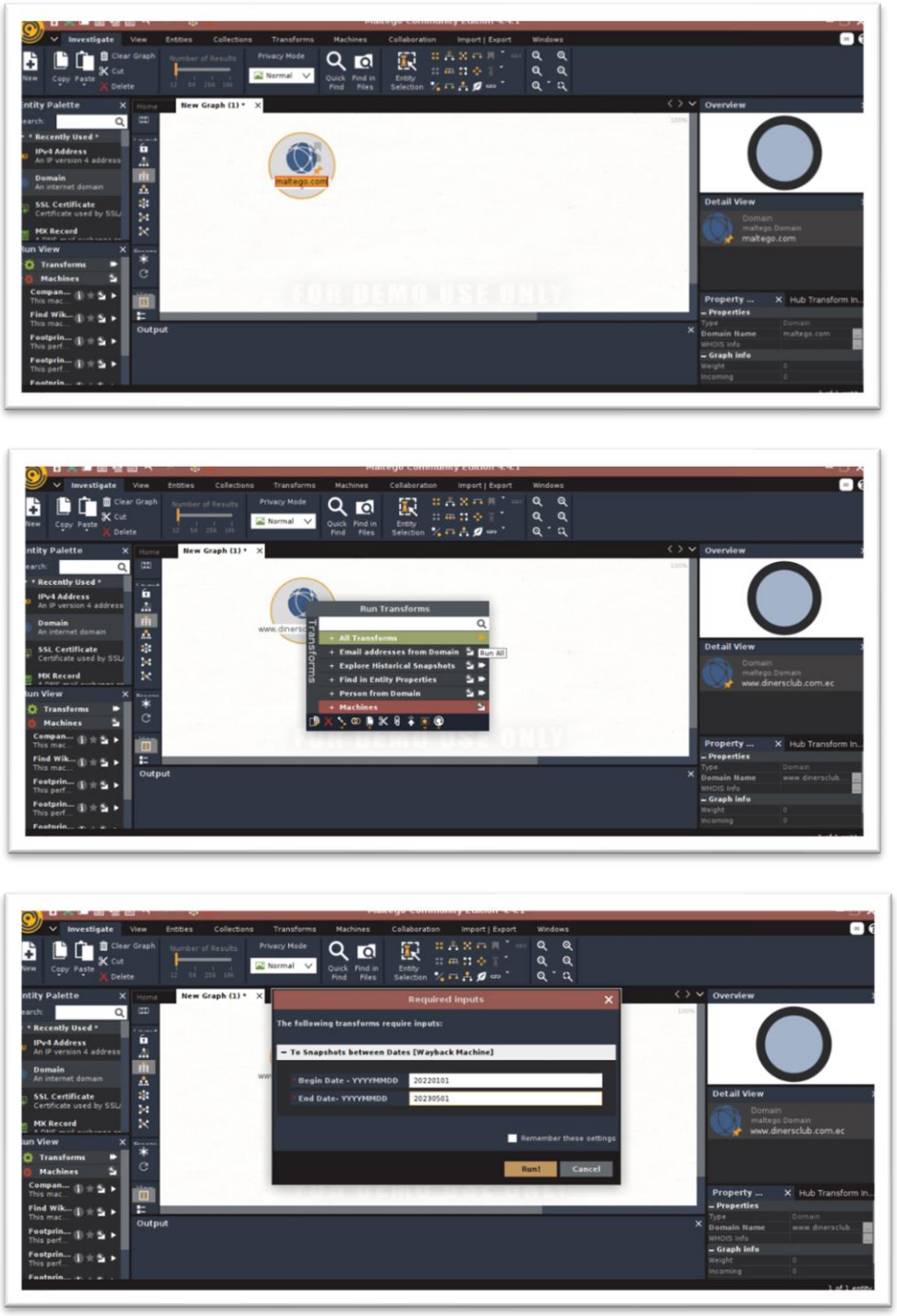
Nota: Imagen tomada desde la búsqueda de Shodan.io

En la figura 19, podemos observar que la herramienta permite capturar información pública de los recursos tecnológicos que cuenta la empresa Diners Club del Ecuador.

Sub Técnica T1590.004: Topología de red

Maltego, es un software utilizado para la Inteligencia de fuentes abiertas y forensia.

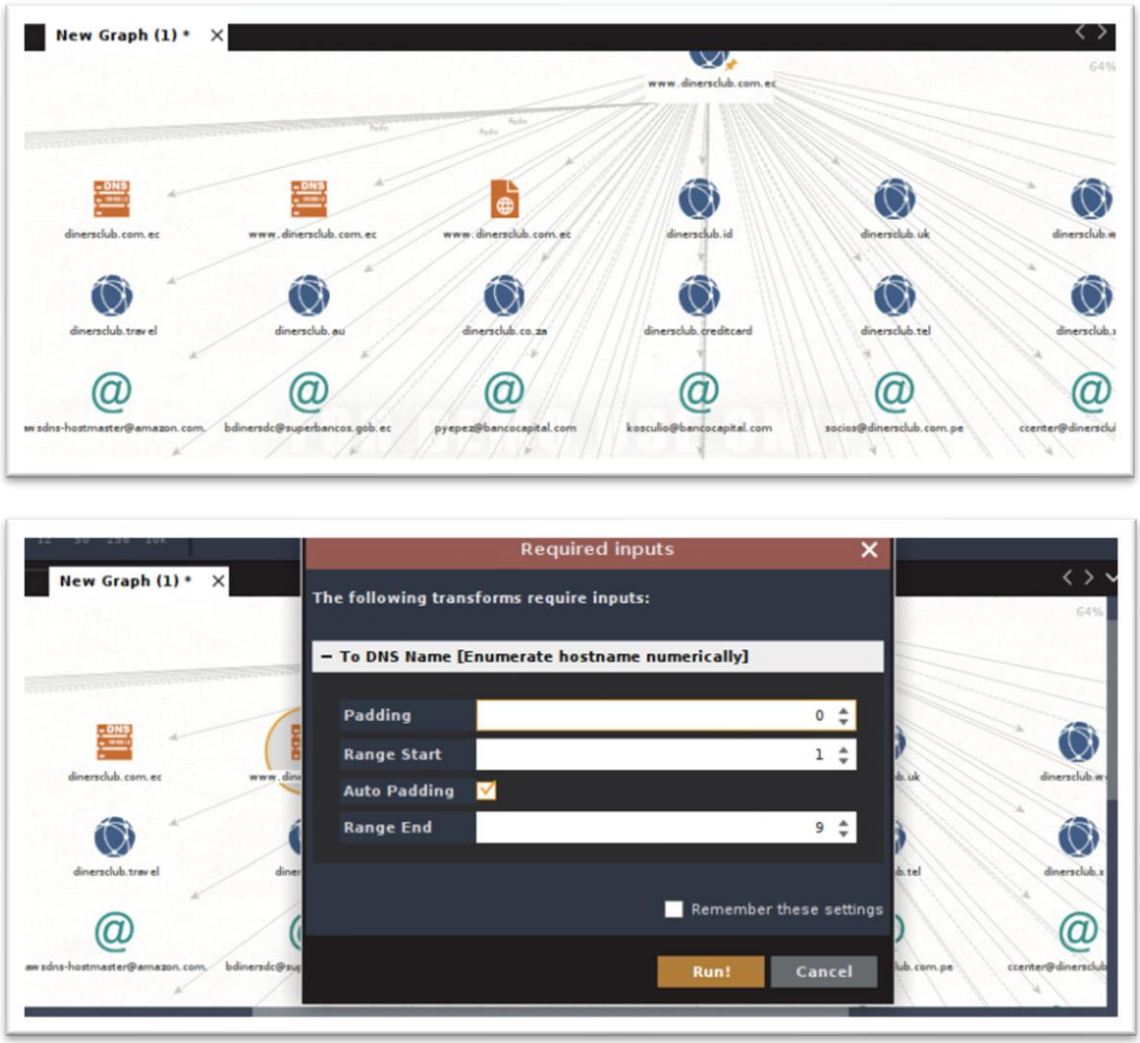
Figura 20.
Búsqueda de información desde Maltego



Nota: Imágenes de resultados desde la herramienta Maltego

En la figura 20, se configura a Maltego para realizar una búsqueda y escaneo del dominio: www.dinersclub.com.ec

Figura 21.
Topología de la empresa desde el dominio con Maltego



Nota: Imágenes de resultados desde la herramienta Maltego

En la figura 21, se obtiene resultados de la enumeración con nombre de DNS desde Maltego.

Figura 22.

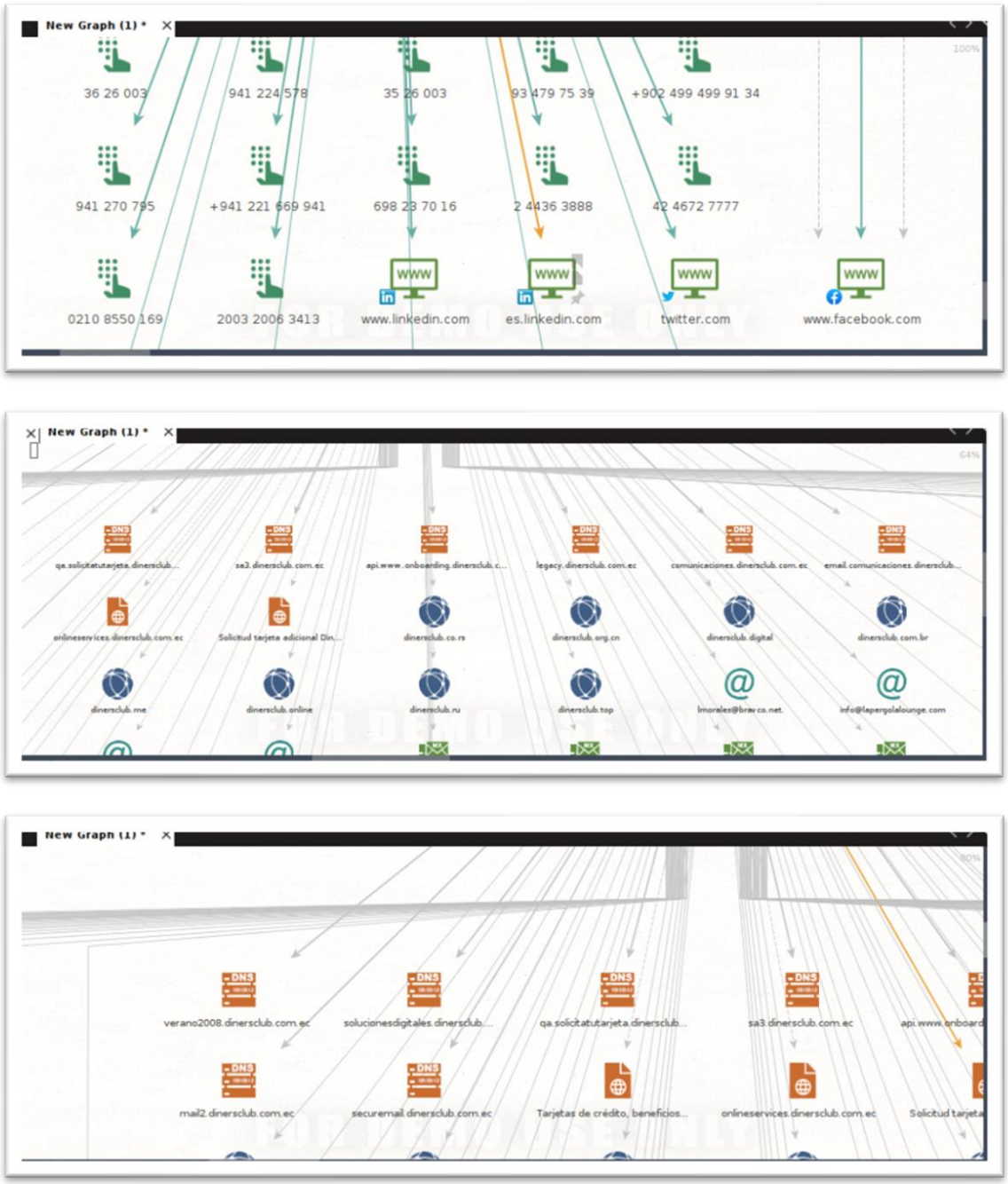
Búsqueda información adicional el dominio con Maltego

Nota: Imágenes desde Maltego, sobre enumeración de correos electrónicos

En la figura 22, se ha identificado una persona de la empresa, realizando una búsqueda a nivel de correo, relacionando el dominio: dinersclub.com.ec

Figura 23.

Búsqueda información adicional el dominio con Maltego, redes sociales



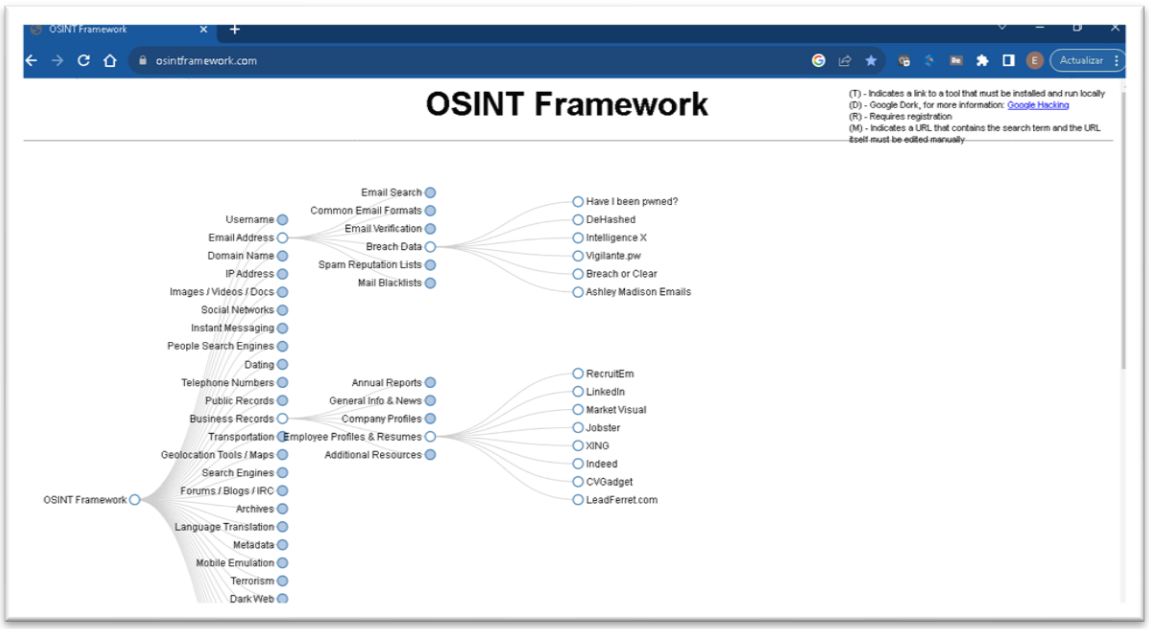
Nota: Imágenes desde Maltego, sobre enumeración de redes sociales

En la figura 23, podemos observar algunas cuentas de usuarios están asociados a redes sociales como: LinkedIn, Twitter y Facebook. Además, el resultado ha mostrado algunos subdominios bajo el dominio principal.

Técnica T1591: Recopilar información de la organización de la víctima

Los atacantes pueden recopilar información sobre la organización de una víctima para utilizarla en un ataque. La información de empresas puede incluir una variedad de detalles, como nombre del departamento, detalles de operaciones comerciales, funciones y responsabilidades de empleado.

Figura 24.
OSINT Framework. Obtención de información de usuarios del negocio



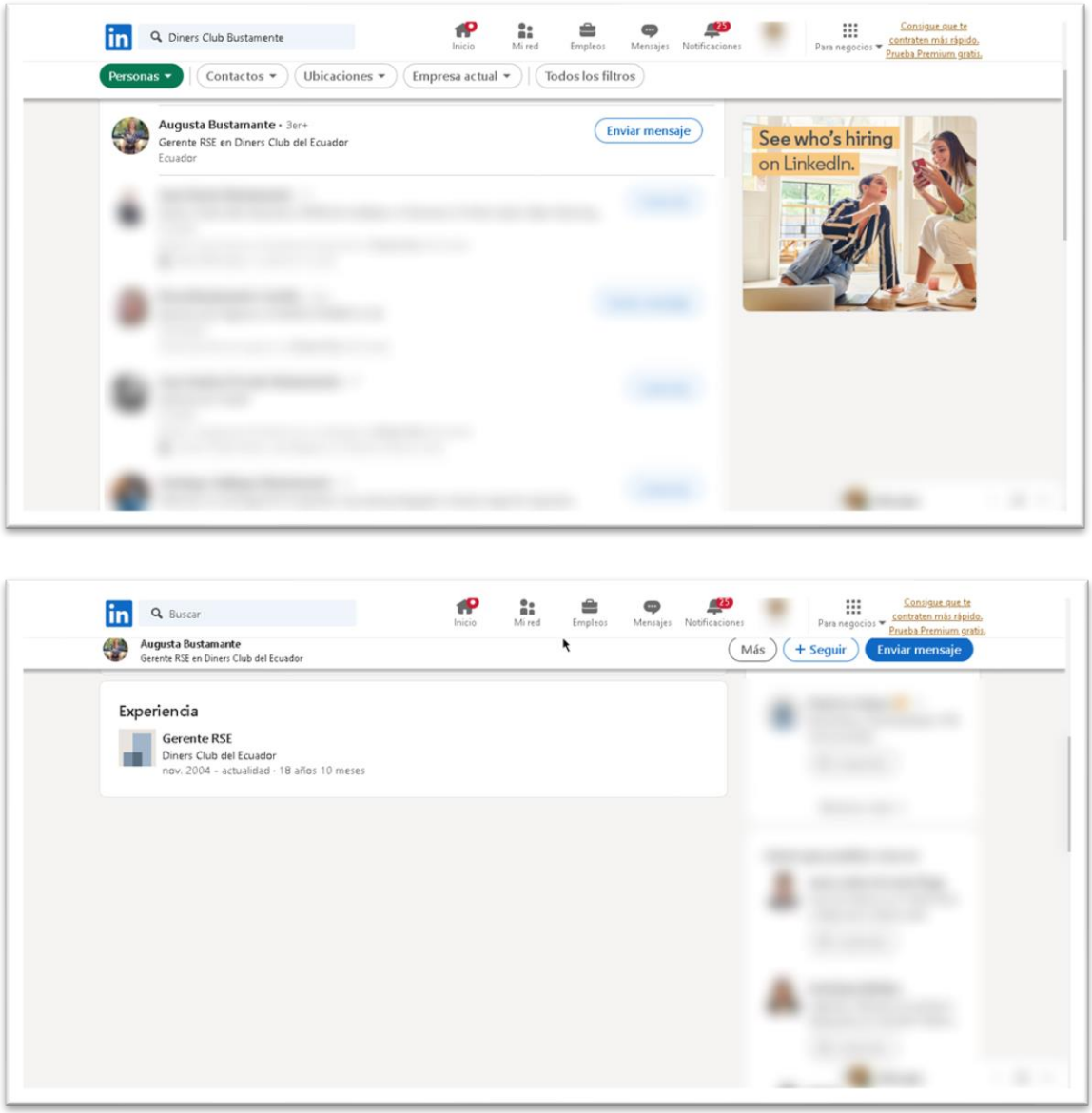
Nota: Imagen tomada desde el portal de OSINT Framework

En la figura 24, se muestran las herramientas del Framework de OSINT para la búsqueda de información recopilando información de usuarios de la empresa.

Sub Técnica T1591.004: Identificar roles

LinkedIn, es una red colaborativa donde se pueden conectar profesionales de cualquier área. Es una herramienta que permite interactuar entre profesionales y compartir ideas, además de empleos y mucho más.

Figura 25.
Búsqueda de información de personas mediante LinkedIn



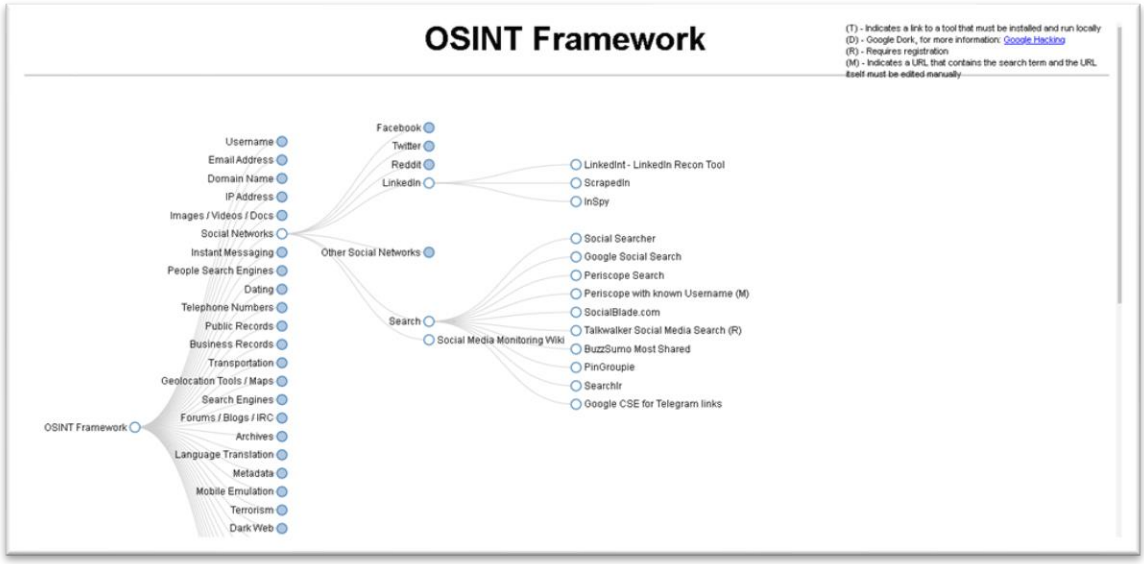
Nota: Imágenes tomadas desde la búsqueda de información en LinkedIn

En la figura 25, se muestra los resultados de la búsqueda mediante LinkedIn. Obteniendo información relevante sobre el rol de un colaborador de la empresa Diners Club.

Técnica T1593: Recopilar información de identidad de la víctima.

Los atacantes pueden buscar sitios web y/o dominios disponibles públicamente la información de las víctimas. La información de las víctimas puede estar disponible en varios sitios web, como redes sociales, sitios web nuevos o sitios web que publican información sobre transacciones comerciales, como contratos de trabajo o comisiones/salarios.

Figura 26.
OSINT Framework. Identificación de la víctima



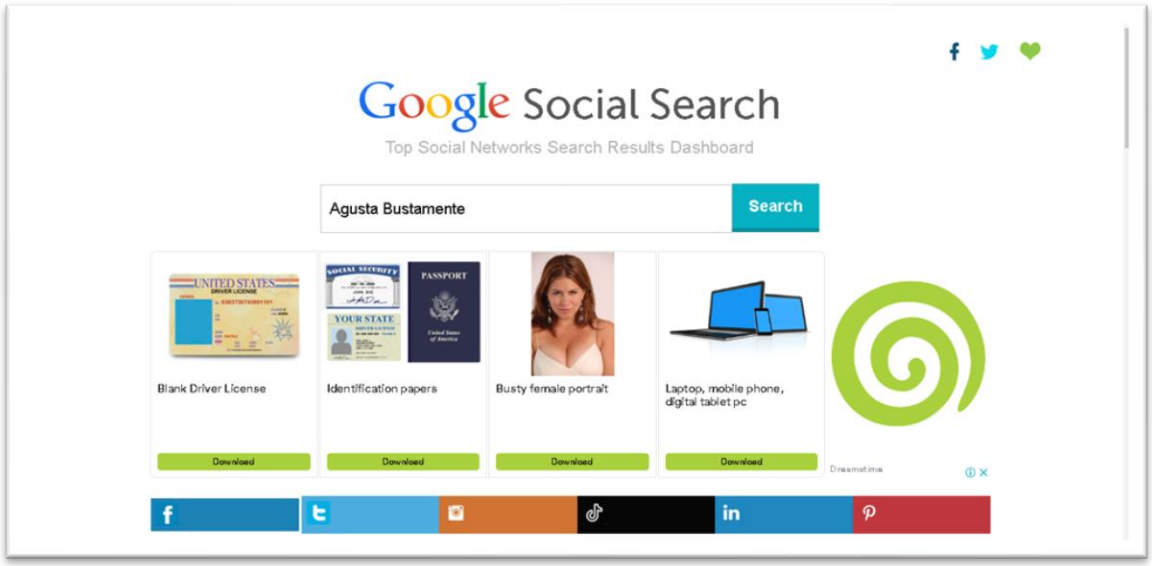
Nota: Imagen tomada desde el portal de OSINT Framework

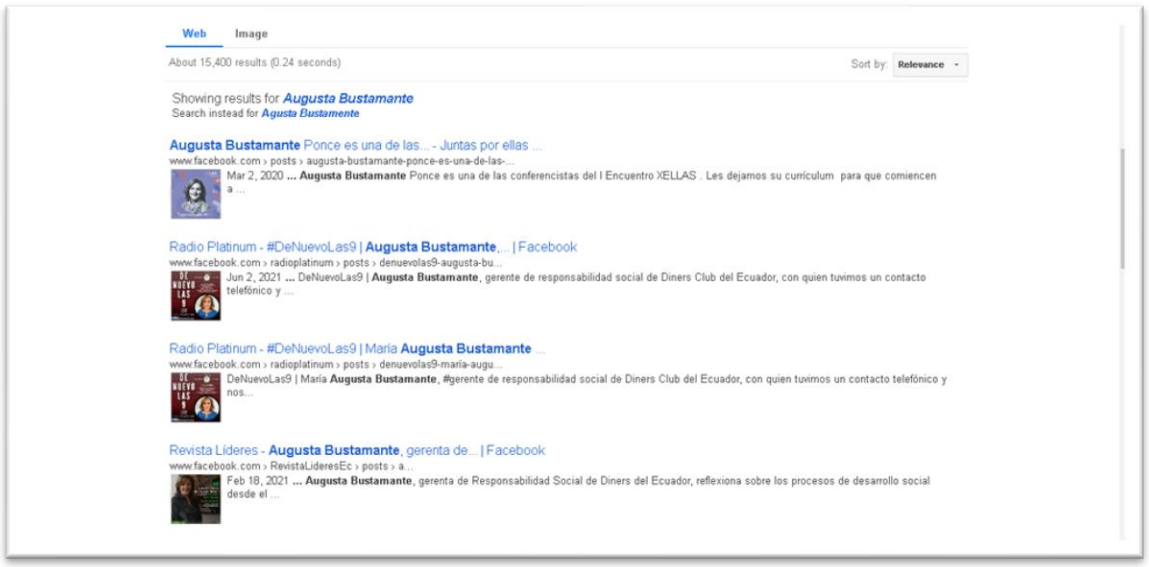
En la figura 26, se muestran las herramientas del Framework de OSINT para la búsqueda e identificación de la víctima.

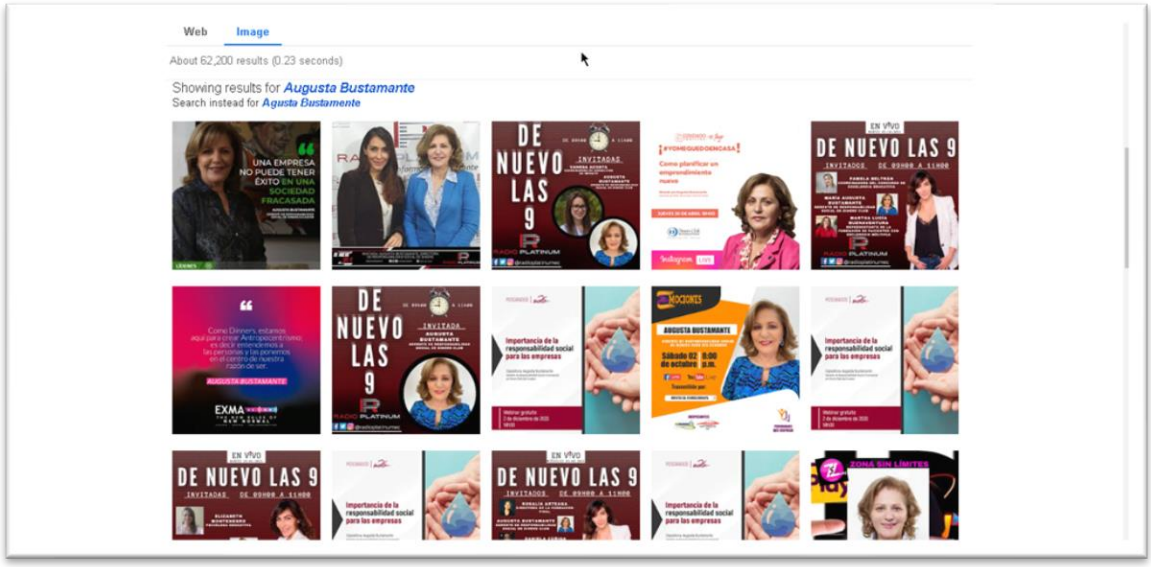
Sub Técnica T1593.001: Medios Sociales

Google Social Search, es un motor de búsqueda desarrollado por Google que presenta contenido generado por contactos y amigos, y de los círculos sociales.

Figura 27.
Búsqueda de información desde Google Social Search







Nota: Imágenes tomadas desde la búsqueda de información en LinkedIn

En la figura 27, se muestra los resultados de la búsqueda mediante Google Social Search. Obteniendo información que permite identificar a la víctima, donde se la puede encontrar en algunos medios de comunicación y redes sociales.

Twitter advanced search. Permite personalizar los resultados de la búsqueda según criterios especificos que se pretende encontrar.

Figura 28.
Búsqueda de información desde Twitter advanced search

Nota: Imágenes tomadas desde la búsqueda de información avanzada en Twitter.

En la figura 28, se muestra los resultados de la búsqueda mediante Twitter advanced Search. Obteniendo información que permite identificar a la víctima, donde se la puede corroborar su rol en la empresa Diners Club.

Tercera Fase: Procesamiento

A continuación, los hallazgos recopilados luego de la ejecución de las técnicas de reconocimiento utilizadas con MITRE ATT&CK Framework.

- **Información recopilada: Sub Técnica T1589.002 – Direcciones de correo**

Tabla 1.
Información obtenida desde Hunter.io

Indicador	Información	Interpretación de los datos
Empresa	Diners Club del Ecuador	El nombre de la empresa es el objetivo
Dominio	www.dinersclub.com.ec	Dominio para búsqueda de información
Cuentas de Email	mandrade@dinersclub.com.ec mcordero@dinersclub.com.ec abustamante@dinersclub.com.ec dtufino@dinersclub.com.ec sapaez@dinersclub.com.ec rerazo@dinersclub.com.ec	6 cuentas de correo, que se identificaron que están enlazadas con sitios que no son parte de la empresa Diners Club del Ecuador
Intereses	Revistas universidades Compra y venta de autos Noticas Publicaciones de empleos	Se ha identificado a una persona que es parte del área de recursos humanos de la empresa Diners Club del Ecuador: mandrade@dinersclub.com.ec

Nota: Resultados obtenidos por medio de la herramienta Hunter.io

En la tabla 1, se ha recopilado datos sobre la empresa Diners Club, utilizando la Sub Técnica T1589.002 – Direcciones de correo, donde se ha obtenido información de usuarios, como: cuentas de do correos y donde estas cuentas están siendo utilizadas.

- **Información recopilada: Sub Técnica T1590.001 – Propiedades de dominio, T1590.002 – DNS**

Tabla 2.
Información obtenida desde Robtex

Indicador	Información	Interpretación de los datos
Empresa	Diners Club del Ecuador	El nombre de la empresa es el objetivo
FQDN	www.dinersclub.com.ec	El FQDN nos muestra la información de la dirección completa y única necesaria para tener presencia en Internet.
Dominio	dinersclub.com.ec	El dominio de la empresa es dinersclub.com.ec
IP	108.166.27.63	La IP asociada el dominio es 108.166.27.63
Whois	Publipromueve Dedicado (C06474885) RACKSPACE-ORD	El dominio de la empresa Diners Club, se encuentra en administración de la empresa Publipromueve
As name	Rackspace - Chicago, IL	El servidor web se encuentra en RACKSPACE
Localidad	San Antonio, United States	El servidor web se encuentra en San Antonio, USA

Nota: Resultados obtenidos por medio de la herramienta Robtex

En la tabla 2, se ha recopilado datos sobre la empresa Diners Club, utilizando la Sub Técnica T1590.001 – Domain properties y T1590.002 – DNS, donde se ha obtenido información importante de la empresa, como: la IP pública del dominio www.dinersclub.com.ec, a nombre de quien está registrado el dominio, en qué localidad se encuentra el servidor web, y cuál es la empresa hosting del dominio.

- **Información recopilada: Sub Técnica T1590.005 – Direcciones IP, T1590.006 – Equipos de comunicaciones**

Tabla 3.
Información obtenida desde Shodan

Indicador	Información	Interpretación de los datos
Puertos	443, 8020, 8008, 9016 y más	Puertos encontrados
Dominios	solucionesdigitales.dinersclub.com.ec webservicios.dinersclub.com.ec mdco.dinersclub.com.ec www.optar.com.ec servicios.interdin.com.ec www3.optar.ec s3.dinersclub.com.ec www4.optar.ec payclubmovil.dinersclub.com.ec	Dominios asociados con Diners Club del Ecuador
Productos	Sistemas Cisco Apache httpd Remote Desktop protocol	Productos encontrados, y que son usados por parte de la empresa
IP	45.65.203.16 45.65.203.12 45.65.203.16 45.65.203.4 45.65.203.111 45.65.203.180 45.65.203.129 190.216.104.18	La Ips asociadas a los servicios publicados

Nota: Resultados obtenidos por medio de la herramienta Shodan

En la tabla 3, se ha recopilado datos sobre la empresa Diners Club, utilizando la Sub Técnica T1590.005 – Direcciones IP, T1590.006 – Equipos de comunicaciones, donde se ha obtenido información importante de la empresa, como: Ip's publicas asociadas a servicios expuestos a internet, así mismo los nombres de subdominios asociados a dichos servicios. También se puede observar que a nivel publico hay puertos utilizados por estos servicios, así como también equipos de comunicaciones con el que cuenta la empresa.

Tabla 4.
Información obtenida desde Maltego

Indicador	Información	Interpretación de los datos
Empresa	Diners Club del Ecuador	El nombre de la empresa es el objetivo
Mail server	mail.dinersclub.com.ec mail2.dinersclub.com.ec mail90.dinersclub.com.ec mx60.dinersclub.com.ec securemail.dinersclub.com.ec	En el análisis, se identifican servidores de correos
Dominio	solucionesdigitales.dinersclub.com.ec qa.solicitatutarjeta.dinersclub.com.ec s3.dinersclub.com.ec api.www.onboarding.dinersclub.com.ec payclubmovil.dinersclub.com.ec	Dominios asociados con Diners Club del Ecuador

Nota: Resultados obtenidos por medio de la herramienta Maltego

En la tabla 4, se ha recopilado datos sobre la empresa Diners Club, utilizando la Sub Técnica T1590.005 – Direcciones IP, T1590.006 – Equipos de comunicaciones, donde se ha obtenido información importante de la empresa, como: nombres de dominios de servidores de correo, además de subdominios de servicios públicos de la empresa Diners Club.

- **Información recopilada: Sub Técnica T1591.004 – Identificar roles**

Tabla 5.
Información obtenida desde LinkedIn

Indicador	Información	Interpretación de los datos
Empresa	Diners Club del Ecuador	El nombre de la empresa es el objetivo
Persona identificada	Agusta Bustamante	Se realiza la búsqueda de información de Agusta Bustamante, a partir de la identificación del correo electrónico: abustamante@dinersclub.com.ec
Rol identificado	Gerente de Responsabilidad Social	Se identifica el rol dentro de la empresa Diners Club, de la persona Agusta Bustamante

Nota: Resultados obtenidos por medio de LinkedIn

En la tabla 5, se ha recopilado datos sobre la empresa Diners Club, utilizando la Sub Técnica T1591.004 – Identificar roles, donde se ha obtenido información importante de la empresa, como: Se identifico que en la empresa Diners Club, Agusta Bustamante es Gerente de Responsabilidad Social.

- **Información recopilada: Sub Técnica T1593.001 – Medios Sociales**

Tabla 6.
Información obtenida desde Google Social Search y Twitter advanced search.

Indicador	Información	interpretación de los datos
Empresa	Diners Club del Ecuador	El nombre de la empresa es el objetivo
Nombre de persona	María Augusta Bustamante	Nombre de la persona para la búsqueda
Redes Sociales y otros medios	Revista Lideres Radio Platinum Facebook Linkedin	Se identifica que María Agusta Bustamante es Gerente de Responsabilidad Social en Diners Club, y que se la puede encontrar en algunas redes y medios sociales

Nota: Resultados obtenidos por medios sociales

En la tabla 6, se ha recopilado datos sobre la empresa Diners Club, utilizando la Sub Técnica T1593.001 – Medios Sociales, donde se ha obtenido información importante de la empresa, como: Agusta Bustamante, Gerente de Responsabilidad Social de la empresa Diners Club se la puede encontrar en redes sociales y en medios de comunicación, por lo que se confirma que además es un personaje de conocimiento público.

Cuarta y quinta Fase: Análisis y entrega de resultados

A partir de la información recopilada utilizando la técnica de reconocimiento del Framework MITRE ATT&CK, se ha podido identificar ciertos aspectos importantes que se han convertido en inteligencia de amenazas que la empresa debe tomar en consideración, para evitar posibles brechas de seguridad.

1. Información de usuarios. Luego del análisis de la información recopilada y procesada, se confirma que existe información pública de usuarios de la empresa Diners Club del Ecuador, ya que se encontraron cuentas de correo organizacional que son utilizadas en sitios públicos, para intereses personales.

   Este hallazgo identifica una falencia y posible vulnerabilidad, ya que al conocer cuentas de correos validas se puede aplicar técnicas de phishing para obtener más información de los usuarios, o peor aún llegar a comprometer los sistemas internos por medio de malware o ransomware inyectado desde correo electrónicos no deseados.

   Las cuentas de correo organizacional deben ser utilizadas únicamente para actividades relacionadas con su rol interno y funciones específicas que demande la empresa.
2. Información de la empresa. La información obtenida y procesada, permite reconocer información relevante de la empresa Diners Club del Ecuador, mediante la búsqueda de

información por consultas DNS.

Este hallazgo puede permite que los atacantes conozcan la localización de la empresa y donde posiblemente se encuentran los servidores web, así utilizar técnicas de ataque phishing que permitan suplantar los sistemas web en internet.

Es importante analizar estos tipos de ataques, y considerar herramienta de antiphishing para servidores web, donde se autentique que las páginas web son de propiedad de la empresa, caso contrario sean reportados en las diferentes empresas que publican información de listas negras.

3. Información de topología de red y sistemas de comunicación. La información recopilada y procesada permitió conocer una gran cantidad de direcciones ip públicas que se asocian a diferentes servicios de la empresa Diners Club del Ecuador. Estas ip's publicas esta relacionadas con servicios web, a los que se identificaron los dominios y subdominios públicos. Se identificaron servidores de correo electrónico perteneciente a la empresa, así como también algunos puertos expuestos a internet por parte de los servicios web de la empresa.

   Este hallazgo identifica que al publicar servicios web al internet, es importante contar con herramienta de seguridad perimetral que permitan proteger los sistemas y la infraestructura de la empresa Diners Club del Ecuador. Si bien la información a nivel de DNS es pública, esto permite que actores maliciosos puedan realizar escaneos y ataques dirigidos a los dominios, ip's públicas y puertos de los servicios expuestos.

   Es primordial analizar la infraestructura expuesta y proponer la adquisición o renovación de nuevas tecnologías que aporten a la seguridad perimetral de la empresa. También se puede analizar el consumo de estos servicios con tecnología punto a punto, como túneles VPN, así aislar las comunicaciones entre origen y destino.

4. Información proporcionada por medios sociales. Los datos recopilados por medio de herramientas de búsqueda por medios sociales entregaron información relevante de un usuario en particular perteneciente a una Gerencia de la empresa Diners Club del Ecuador, en este caso a la Gerente de Responsabilidad Social.

   Exponer datos como roles y responsabilidades de una persona de manera pública puede permitir conocer las preferencias de su vida profesional y social. Los atacantes pueden preparar ataques dirigidos contra estas personas de alta gerencia, estos pueden ser: ataques phishing, ingeniería social y ataques personales en redes sociales para desprestigio.

   A pesar de que hay información que se necesita ser publicada en redes sociales y medios de comunicación como parte de estrategias de marketing y noticias representativas de

la empresa, esto puede permitir que hacktivistas u otro tipo de actor malicioso que intente buscar la manera de explotar o desprestigiar a las personas objetivo.

Las altas gerencias deben contar con la debida preparación y capacitación sobre la seguridad de la información, para estar al tanto de las amenazas que existen en internet y en el mundo comercial.

2.7 Propuesta metodológica para la aplicación de OSINT

La siguiente propuesta metodológica tiene como objetivo proporcionar una guia en el proceso de aplicación de OSINT en la inteligencia de amenazas de seguridad informática. Para asegurar la eficacia y validez de esta propuesta, se propone la validación de expertos en seguridad informática a través de encuestas y entrevistas.

- **Paso 1: Definición de Objetivos de Investigación**

  Identificar claramente los objetivos de la investigación de amenazas informáticas que se abordarán utilizando tecnicas y herramientas de OSINT.

- **Paso 2: Identificación de Fuentes de Información**

  Identificar fuentes abiertas relevantes para la investigación, como sitios web, foros, redes sociales, repositorios públicos y bases de datos en línea.

- **Paso 3: Selección de Herramientas y Técnicas de OSINT**

  Elegir las herramientas y técnicas de OSINT adecuadas para la recopilación, análisis y visualización de datos. Esto podría incluir motores de búsqueda especializados, rastreadores, herramientas de análisis de redes sociales, entre otros. Existen herramientas gratuitas dentro de OSINT Frameawork, también se pueden usar herramientas de pago.

- **Paso 4: Recopilación de Datos**

  Utilizar las herramientas seleccionadas para recopilar datos relevantes de las fuentes identificadas en el Paso 2.

- **Paso 5: Filtrado y Análisis de Datos**

  Filtrar y analizar los datos recopilados para identificar patrones, relaciones y posibles amenazas informáticas. Utilizar técnicas de análisis como la minería de datos y la visualización de información.

- **Paso 6: Validación de Resultados**

  Realizar una validación interna de los resultados obtenidos para asegurarse de que sean coherentes y precisos.

La propuesta metodológica expuesta para la aplicación de OSINT en la inteligencia de amenazas de seguridad informática fortalece la capacidad de las entidades financieras para detectar y mitigar de manera eficiente y proactiva las amenazas informáticas que puedan afectar sus sistemas y la seguridad de la

información. Para lo cual se mencionan algunos logros que se obtienen con la metodología a continuación:

- **Detección Temprana de Amenazas:** La metodología permite una detección temprana de amenazas cibernéticas al aprovechar fuentes abiertas de información en línea. Esto ayuda a las entidades financieras a identificar signos de actividad maliciosa en etapas tempranas, permitiendo una respuesta más rápida y efectiva.
- **Identificación de Tendencias:** La recopilación y análisis de datos mediante OSINT permite a las entidades financieras identificar tendencias emergentes en el panorama de amenazas. Esto les ayuda a anticipar los posibles vectores de ataque y adaptar sus estrategias de seguridad en consecuencia.
- **Caracterización de Actores Maliciosos:** La metodología proporciona información valiosa sobre los actores maliciosos, sus métodos y motivaciones. Esto permite a las entidades financieras comprender mejor las amenazas y ajustar sus sistemas de seguridad para contrarrestarlos de manera efectiva.
- **Optimización de Recursos:** La aplicación de herramientas y técnicas OSINT permite optimizar los recursos de las entidades financieras al enfocarse en fuentes abiertas y gratuitas de información. Esto puede resultar en ahorros significativos en comparación con soluciones de seguridad más costosas.

A continuacion se mencionan algunas ventajas y utilidades sobre entidades financieras:

- **Mejora de la Resiliencia:** Al anticipar y responder rápidamente a las amenazas, las entidades financieras mejoran su resiliencia cibernética. Esto ayuda a mantener la continuidad de las operaciones y la confianza de los clientes.
- **Protección de Datos Sensibles:** La metodología contribuye a la protección de los datos sensibles y confidenciales que manejan las entidades financieras. La detección temprana de amenazas evita posibles brechas de seguridad y fugas de información.
- **Cumplimiento Normativo:** La detección proactiva de amenazas y la adopción de medidas de seguridad adecuadas ayudan a las entidades financieras a cumplir con las regulaciones y estándares de seguridad cibernética.
- **Fortalecimiento de la Imagen:** La implementación de una metodología proactiva para la gestión de amenazas cibernéticas puede mejorar la imagen y

la reputación de una entidad financiera, demostrando su compromiso con la seguridad de los clientes.

- **Alineación con Objetivos Estratégicos:** La metodología se alinea con los objetivos estratégicos de las entidades financieras en términos de gestión de riesgos y seguridad de la información. Contribuye a la sostenibilidad y el crecimiento a largo plazo.

Valoración de Expertos

Esta propuesta metodológica fue sometida a la valoración de expertos en seguridad informática a través de un cuestionario de preguntas sobre la metodología propuesta (ver Anexo 1) y una encuestas sobre la percepción de expertos sobre la metodología (ver Anexo 2). Los resultados de esta validación son cruciales para ajustar y perfeccionar la metodología, asegurando que sea efectiva y práctica en la aplicación de OSINT en la inteligencia de amenazas de seguridad informáticas.

La valoración de expertos fue llevada a cabo por dos profesionales Gerentes de Ciberaseguridad de entidades financieras, que para mantener el sigilo de la privacidad no se mencionaran los nombres de las instituciones.

- Expero #1. Andres Montenegro, Gerente de Conrol Interno de TI y Ciberseguridad
- Experto #2. Eduardo Alvarado, Gerente de Seguridad Información y Ciberseguridad

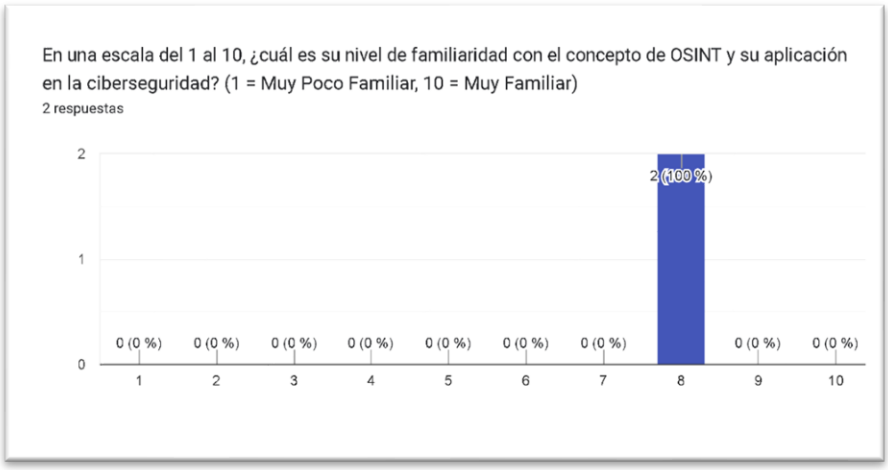
Análisis de la Validación

1. Analizar los resultados de las encuestas y entrevistas para identificar patrones y tendencias en las respuestas de los expertos.

CUESTIONARIO

Pregunta #1. Tiene como finalidad obtener el grado de comprensión de los expertos sobre la investigación y los conceptos que engloban en el contexto de la seguridad informática. Se obtiene un resultado del 80% de conocimiento de los conceptos sobre OSINT y su aplicación en la Ciberseguridad por parte de los expertos.

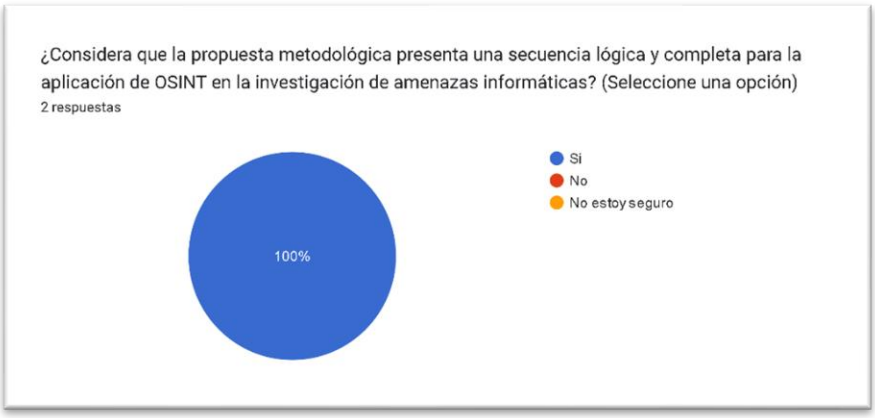
Figura 29. *Pregunta # 1, valoración de la propuesta*



Nota: Resultado pregunta #1. Generado desde Formularios de Google

Pregunta #2. Tiene como finalidad obtener la aceptación de la metodología por parte de los expertos sobre la investigacion, luego del análisis de la investigación y la estructura plasmada en ella. Se obtiene un resultado del 100% para la respuesta SI, donde se comprueba que la metodología tiene una secuencia lógica y completa sobre la aplicación de OSINT en la investigación de amenazas informáticas.

Figura 30. *Pregunta # 2, valoración de la propuesta*



Nota: Resultado pregunta #2. Generado desde Formularios de Google

Pregunta #3. Tiene como finalidad obtener el criterio de los expertos basado en los pasos seleccionados para la aplicación de la metodología propuesta.

- Experto #1. Agregaria la fase de ejecución de pruebas de alguna explotación para validar su veracidad.
- Experto #2 . Es un metodología por lo tal es una forma de organizar el trabajo, adicional también pueden apoyarse a otras metodología para complementar inclusive la inteligencia de amenazas.

Pregunta #4. Tiene como finalidad conocer si el uso de encuestas y entrevistas pueden medir la efectiviad y aplicacbiliad de la metodología propuesta.

- Experto #1. Los expertos que deben validar deben ser de tipo Ethical Hackers.
- Experto #2. Las encuestas si están definidas para profesionales en seguridad puede ser más acertada, pero eso dependerá de a que público se orienta la encuesta y sobre todo del contenido, sea digerible si no es técnico y si es técnico sea certero en las preguntas para obtener de esa respuesta un mayor conocimiento por que eso puede apoyar al especialista de ciberseguridad o al responsable de realizar la investigación.

Pregunta #5. Tiene como finalidad de conocer si la aplicación de la metodología puede aportar de manera efectiva en la detección y análisis de amenazas informáticas. Se obtiene un resultado del 100% para la respuesta SI aportaría efectivamentea sobre el análisis de amenazas de seguridad informáticas.

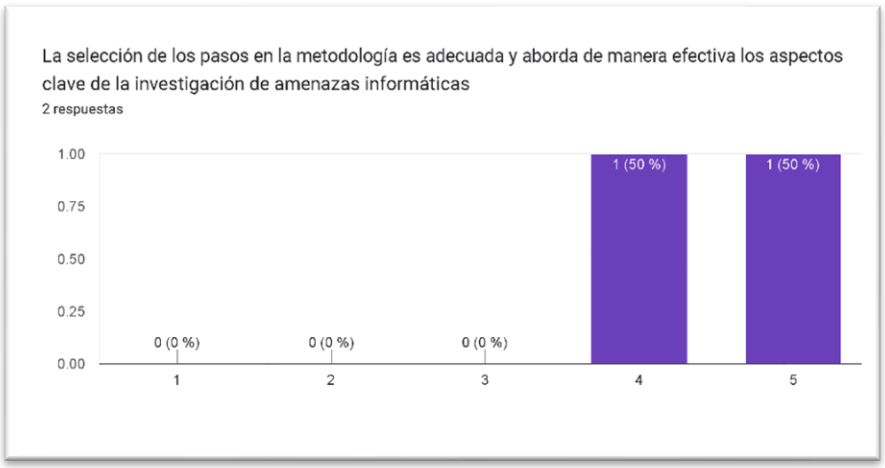
Figura 31. *Pregunta # 5, valoración de la propuesta*

Nota: Resultado pregunta #5. Generado desde Formularios de Google

ENCUESTA

Pregunta #1. Tiene como finalidad obtener la comprensión de los pasos de la metodología y como esta aborda de manera efectiva sobre la investigación de amenazas de seguridad informáticas. Se obtiene un resultado de 5 en la escala de 5 para el experto #1, y un 4 en la escala de 5 para el experto #2. Lo que quiere decir se obtiene un 90% de aceptación sobre la metodología propuesta y su efectividad en la investigación de amenazas informáticas.

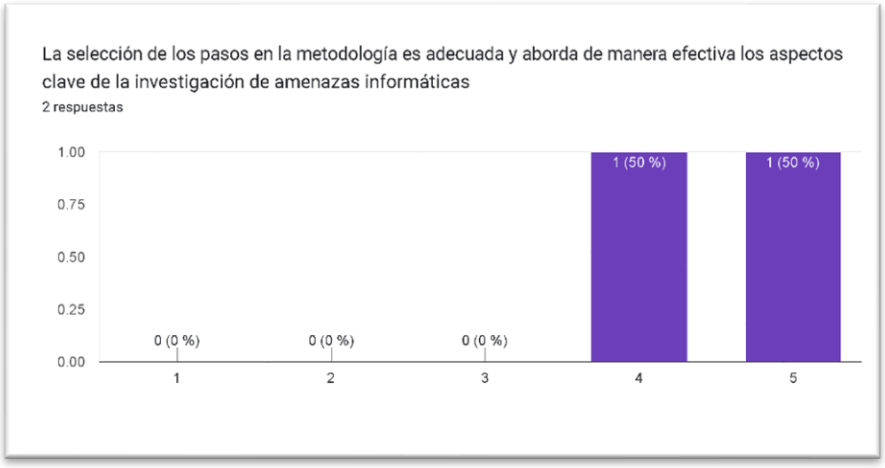
Figura 32. *Pregunta # 1, encuesta sobre la metodología*



Nota: Resultado pregunta #1. Generado desde Formularios de Google

Pregunta #2. Tiene como finalidad obtener la comprensión de la secuencia lógica de la aplicación de OSINT en la inteligencia de amenazas de seguridad informáticas. Se obtiene un resultado de 5 en la escala de 5 para el experto #1, y un 4 en la escala de 5 para el experto #2. Lo que quiere decir se obtiene un 90% de aceptación sobre la secuencia lógica de la aplicación de OSINT con la metodología propuesta.

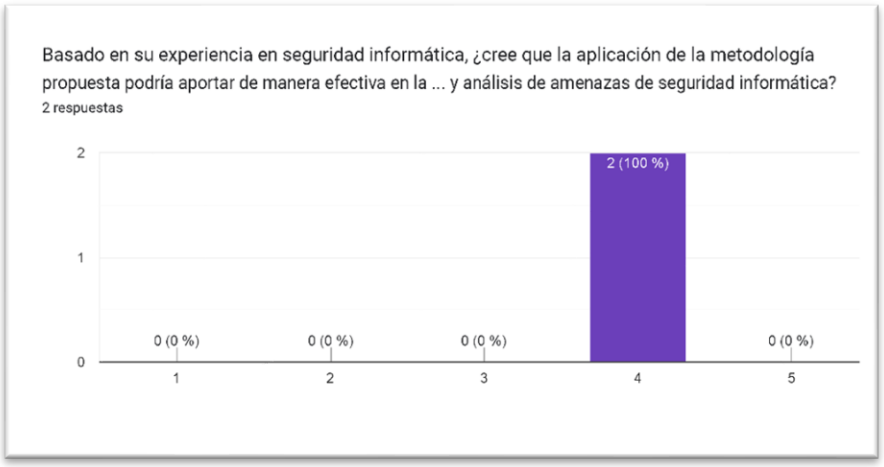
Figura 33. *Pregunta # 2, encuesta sobre la metodología*



Nota: Resultado pregunta #2. Generado desde Formularios de Google

Pregunta #2. Tiene como finalidad obtener la valoración de expertos basado en la experiencia que cada uno mantiene en el campo de la Seguridad Informática sobre como la metodología aporta de manera efectiva en la detección y análisis de amenazas de seguridad informáticas. Se obtiene un resultado de 4 en la escala de 5 por parte de los dos expertos. Lo que quiere decir se obtiene un 80% de aceptación sobre la metodología propuesta y su efectividad en la investigación de amenazas de seguridad informática.

Figura 34. *Pregunta # 3, encuesta sobre la metodología*



Nota: Resultado pregunta #3. Generado desde Formularios de Google

Pregunta #4. Tiene como finalidad conocer las sugerencia y/o recomendaciones que los expertos pueden emitir para mejorar la propuesta metodológica.

- Experto #1. Que el personal que ejecute la metodología tenga conocimiento experto y años de experiencia en ciberseguridad y sus conceptos.
- Experto #2. Para minimizar el global de la metodología debe aplicarse a un proceso de valor, o de la cadena de valor para aplicarse más efectivamente o a su vez definido por el Negocio.

2. Utilizar la retroalimentación de los expertos para ajustar y mejorar la metodología propuesta.
    - Ver Anexo 3

2.8 Matriz de articulación de la propuesta

La presente matriz considera la articulación del producto, la cual fue desarrollada con soporte teórico, metodológico, estratégico, técnico y tecnológico.

Tabla 7.
Matriz de articulación

Ejes o partes principales del proyecto		Breve descripción de los resultados de cada parte	Sustento teórico que se aplicó en la construcción del proyecto	Metodologías, herramientas técnicas y tecnológicas que se emplearon
1	Amenazas Informáticas	Identificación y análisis de diversas amenazas cibernéticas y sus patrones de ataque.	Concepto de amenazas cibernéticas, técnicas de ataque y su evolución.	Recopilación de datos de amenazas, análisis de patrones y tendencias.
2	MITRE ATT&CK	Mapeo de tácticas, técnicas y procedimientos utilizados por diferentes actores maliciosos.	Marco MITRE ATT&CK y su relación con la ciberseguridad.	Identificación de técnicas utilizadas en amenazas y mapeo a MITRE ATT&CK.
3	Inteligencia de Amenazas	Generación de informes y análisis basados en la información recopilada.	Concepto de inteligencia de amenazas y su importancia en la ciberseguridad.	Producción de informes y análisis de amenazas detectadas.
4	OSINT como Herramienta	Utilización de fuentes abiertas para obtener información relevante.	Concepto de OSINT como fuente de datos en la ciberseguridad.	Selección y aplicación de herramientas OSINT para recopilación y análisis.
5	Ciclo de Vida OSINT	Establecimiento de un proceso estructurado para la recolección y análisis de datos de fuentes abiertas.	Etapas del ciclo de vida OSINT y sus implicaciones en la inteligencia de amenazas.	Definición de etapas del ciclo OSINT en la investigación.

Nota: Plantilla de matriz de propuesta por dirección de posgrado

CONCLUSIONES

1. La investigación de los fundamentos teóricos sobre inteligencia de amenazas y OSINT ha proporcionado una sólida base para comprender la importancia de la detección temprana de amenazas en el entorno de la seguridad informática. La revisión exhaustiva de literatura ha revelado la evolución de los modelos de ciberseguridad y la necesidad de adoptar enfoques proactivos. La integración de OSINT en la inteligencia de amenazas emerge como una estrategia clave para abordar los desafíos actuales de seguridad cibernética y mitigar riesgos.

2. La aplicación de herramientas y técnicas de OSINT en el proceso de investigación de amenazas ha demostrado ser eficaz para recopilar, filtrar y analizar información relevante proveniente de fuentes abiertas. La selección cuidadosa de herramientas especializadas, como rastreadores y motores de búsqueda avanzados, ha permitido obtener datos confiables y precisos sobre tendencias de amenazas, actores maliciosos y vulnerabilidades. Esta aplicación ha proporcionado una visión detallada del panorama de amenazas, respaldando la toma de decisiones informadas en seguridad informática.

3. La propuesta metodológica diseñada para la aplicación de OSINT en la investigación de amenazas informáticas ha sido validada a través de la opinión de expertos en seguridad cibernética. La metodología ha demostrado ser coherente y efectiva en la consecución de los objetivos específicos planteados en este estudio. La identificación de fuentes de información relevantes, la selección de herramientas adecuadas, la recopilación de datos, el filtrado y análisis, la validación de resultados y la evaluación de la metodología han sido etapas sólidas y bien estructuradas.

En síntesis, la investigación sobre el uso de OSINT en la inteligencia de amenazas de seguridad informática ha culminado en una comprensión profunda de la importancia de la anticipación y respuesta temprana a los desafíos cibernéticos. La propuesta metodológica validada refleja un camino concreto para lograr esta meta, fusionando conocimientos teóricos con aplicaciones prácticas.

El uso estratégico de herramientas y técnicas de OSINT, respaldado por la metodología propuesta, constituye un avance significativo en el ámbito de la ciberseguridad, capacitando a las organizaciones para enfrentar las amenazas en constante evolución en el entorno digital.

RECOMENDACIONES

1. La investigación exhaustiva de los fundamentos teóricos relacionados con la inteligencia de amenazas y el OSINT ha permitido establecer una base sólida de conocimiento en la detección y mitigación temprana de riesgos en el ámbito de la seguridad informática. La comprensión profunda de los modelos de ciberseguridad y la evolución de las amenazas cibernéticas ha destacado la necesidad urgente de adoptar enfoques proactivos. La integración estratégica de OSINT como fuente clave de información en la inteligencia de amenazas se erige como una respuesta eficaz para anticipar y contrarrestar amenazas digitales en constante evolución.

2. La aplicación de herramientas y técnicas de OSINT en la investigación de amenazas ha demostrado ser una estrategia altamente efectiva para la adquisición y análisis de información crítica. La selección cuidadosa de herramientas especializadas, junto con enfoques metodológicos sólidos, ha permitido una recopilación precisa de datos provenientes de fuentes abiertas confiables. Los resultados obtenidos han contribuido significativamente a la generación de conocimiento en torno a patrones de ataque, actores maliciosos y vulnerabilidades, brindando una visión integral del panorama de amenazas que respalda decisiones informadas en el ámbito de la ciberseguridad.

3. La propuesta metodológica diseñada para la aplicación de OSINT en la investigación de amenazas informáticas ha resultado en un enfoque sólido y coherente para enfrentar los retos de la seguridad cibernética. La validación por expertos en seguridad informática ha confirmado su viabilidad y pertinencia. La secuencia estructurada de pasos, desde la definición de objetivos hasta la evaluación de resultados, ha demostrado ser una guía efectiva para la recopilación, análisis y validación de datos. La metodología propuesta se erige como un recurso valioso para las organizaciones que buscan fortalecer su capacidad de anticipación y respuesta ante amenazas digitales.

BIBLIOGRAFÍA

Alexroland. ¿Qué es Inteligencia sobre amenazas de Microsoft Defender (Defender TI)? Microsoft.com. Retrieved August 22, 2023, from https://learn.microsoft.com/es-es/defender/threat-intelligence/what-is-microsoft-defender-threat-intelligence-defender-ti

Alumnos, A. OSINT (Inteligencia de Fuentes Abiertas): tipos, métodos y salidas profesionales. LISA Institute. Retrieved May 6, 2023, from https://www.lisainstitute.com/blogs/blog/osint-inteligencia-fuentes-abiertas

Alumnos, A. Ciclo de inteligencia: qué es, para qué sirve y cuáles son sus límites. LISA Institute. Retrieved August 22, 2023, from https://www.lisainstitute.com/blogs/blog/ciclo-de-inteligencia

Alumnos, A. OSINT (Inteligencia de Fuentes Abiertas): tipos, métodos y salidas profesionales. LISA Institute. Retrieved August 22, 2023, from https://www.lisainstitute.com/blogs/blog/osint-inteligencia-fuentes-abiertas

AMR. (2023, June 7). Evolución de las amenazas informáticas en el primer trimestre de 2023. Estadísticas de computadoras personales. Kaspersky. https://securelist.lat/it-threat-evolution-q1-2023-pc-statistics/97924/

Ataques de phishing utilizan nuevos métodos para robar datos. (2022, November 4). eSemanal - Noticias del Canal. https://esemanal.mx/2022/11/ataques-de-phishing-utilizan-nuevos-metodos-para-robar-datos/

Big, E. T. (2022, May 11). Open Source Inteligence: qué hay detrás de OSINT. Blogthinkbig.com. https://blogthinkbig.com/open-source-inteligence-que-hay-detras-de-osint

Cloudflare.com. Retrieved August 22, 2023, from https://www.cloudflare.com/es-es/learning/security/glossary/what-is-threat-intelligence/

Crecimiento de Ciberataques en la industria bancaria latinoamericana. (n.d.). Goanywhere.com. Retrieved May 6, 2023, from https://www.goanywhere.com/es/blog/bancos-latinoamerica-crecimiento-ciberamenazas

Cruz Lucas, G. I., Delgado Tejena, L. E., Ponce Solorzano, B. R., & Marcillo Merino, M. J. (2022). Riesgos de seguridad de los datos en la web. Journal TechInnovation, 1(2), 43–49. https://doi.org/10.47230/journal.techinnovation.v1.n2.2022.43-49

De Investigación, P., Desarrollo, Y., Cusme, K. D., Leydi, Z., Zambrano Mendoza, T., Jessica, I., & Carrillo, J. M. INFORME DE TRABAJO DE TITULACIÓN. Edu.Ec. Retrieved May 6, 2023, from https://repositorio.espam.edu.ec/bitstream/42000/1683/1/TTMTI03D.pdf

De la Iglesia, E. D. (2021, February 4). La inteligencia de amenazas o Cyber Threat Intelligence. Campusciberseguridad.com; Campus Internacional de Ciberseguridad. https://www.campusciberseguridad.com/blog/item/150-la-inteligencia-de-amenazas-o-cyber-threat-intelligence

De Sousa, B. (2023, May 16). Inteligencia de amenazas: ¿Por qué es importante conocerla? Blog IPNET; IPNET Growth Partner. https://ipnet.cloud/blog/es/innovacion/inteligencia-de-amenazas/

Follow, N. (2023, April 9). OSINT intelligence cycle. GeeksforGeeks. https://www.geeksforgeeks.org/osint-intelligence-cycle/

Fonte, A. (2021, March 8). OSINT, ¿Qué es? ¿Para qué sirve? Derecho de la Red; derechodelared. https://derechodelared.com/osint/

Función de la inteligencia sobre amenazas en la nube. Microsoft.com. Retrieved August 22, 2023, from https://learn.microsoft.com/es-es/azure/cloud-adoption-framework/organize/cloud-security-threat-intelligence

Gill, R., Ross, V., & SANS Institute. What is OSINT (Open-Source Intelligence?). Sans.org. Retrieved August 22, 2023, from https://www.sans.org/blog/what-is-open-source-intelligence/

Gob.Mx. Retrieved August 22, 2023, from https://www.gob.mx/cms/uploads/attachment/file/535135/Que_es_Inteligencia.pdf

González, B. (2023, June 12). OSINT: Tipos, Usos, Últimas tendencias y Tecnologías Emergentes. Hard2bit CyberSecurity | Nuestro Blog de Seguridad Informática, Informática Forense y Noticias de Tecnología; Hard2bit CyberSecurity. https://hard2bit.com/blog/osint-tipos-usos-ultimas-tendencias-y-tecnologias-emergentes/

How to kill passwords: Does MITRE ATT&CK framework help or hinder? (2021, July 1). Hypr.com. https://blog.hypr.com/how-to-kill-the-password-does-the-mitre-attck-framework-help-or-hinder

Inteligencia de amenazas. CYREBRO. Retrieved August 22, 2023, from https://www.cyrebro.io/es/threat-intelligence/

Inteligencia de amenazas, todo lo que debes saber. (2021, July 14). Ciberseguridad. https://ciberseguridad.com/guias/prevencion-proteccion/inteligencia-amenazas/

Hassan, N. A., & Hijazi, R. (2018). Open source intelligence methods and tools: A practical guide to online intelligence (1st ed.). APRESS. https://books.google.at/books?id=AqNiDwAAQBAJ

Iniseg, D. (2018, December 20). Ciberinteligencia: la inteligencia en el ciberespacio. Ciberseguridad para Empresas. https://www.iniseg.es/blog/ciberseguridad/ciberinteligencia/

Jaramillo Burbano, Jorge Luis (2022) Consideraciones para la implementación del esquema gubernamental de seguridad de la información basado en la ley de protección de datos personales caso de estudio: instituto nacional de patrimonio cultural, MAESTRÍA EN SEGURIDAD INFORMÁTICA, Quito: Universidad Israel 2022, 76p. Mg. Christian Patricio Vaca Benalcázar, UISRAEL-EC-MASTER-SEG. INF-378-242-2022-004

Jaramillo Burbano, Jorge Luis (2022) Análisis de uso de soluciones Data Loss prevención para instituciones financieras como mecanismo para el cumplimiento de normativa pci-dss. MAESTRÍA EN SEGURIDAD INFORMÁTICA, Quito: Universidad Israel 2022, 44p. Mg. Christian Patricio Vaca Benalcázar, UISRAEL-EC-MASTER-SEG. INF-378-242-2022-005

Matrix - Enterprise. Mitre.org. Retrieved August 22, 2023, from https://attack.mitre.org/matrices/enterprise/

Matriz Mitre Tacticas Y Tecnicas Entornos Industriales. Incibe.es. Retrieved August 22, 2023, from https://www.incibe.es/incibe-cert/blog/matriz-mitre-tacticas-y-tecnicas-entornos-industriales

NetGain Systems. (2021, July 29). Adopting the MITRE ATT&CK framework to strengthen IT security -. Netgain-systems.com. https://www.netgain-systems.com/adopting-the-mitre-attack-framework-to-strengthen-it-security/

Netskope.com. Retrieved August 22, 2023, from https://www.netskope.com/wp-content/uploads/2022/11/cloud-and-threat-report-phishing.pdf

Open Source Intelligence - OSINT. Com.Pe. Retrieved August 22, 2023, from https://academy.seguridadcero.com.pe/blog/open-source-intelligence-osint

Páez Padilla Mónica Elizabeth (2023) Descripción del ataque del Ransomware Exx bajo un entorno controlado en máquinas virtuales. Quito: Universidad Israel, 2023 43p Mg. Recalde Varela Pablo Marcel, UISRAEL-EC-MASTER-SEG-INF-378.242-2023-007

Publications Combined: Studies In Open Source Intelligence (OSINT) And Information. (2019). Jeffrey Frank Jones.

¿Qué es la inteligencia de amenazas?. Ibm.com. Retrieved August 22, 2023, from https://www.ibm.com/es-es/topics/threat-intelligence

Raggi, N. Emulación de adversarios: qué es y cuál es su objetivo. Welivesecurity.com. Retrieved August 22, 2023, from https://www.welivesecurity.com/la-es/2021/01/15/emulacion-adversarios-que-es-cual-es-su-objetivo/

Ramírez, K. (2023, June 8). Ciberseguridad: protege tus datos personales en la era digital. Conexion PUCE. https://conexion.puce.edu.ec/ciberseguridad-protege-tus-datos-personales-en-la-era-digital/

Rodríguez, P. Ciberseguridad y ciberinteligencia, ¿es lo mismo? Ambit-bst.com. Retrieved August 22, 2023, from https://www.ambit-bst.com/blog/ciberseguridad-y-ciberinteligencia-es-lo-mismo

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Editorial Científica 3Ciencias.

Ricchiardi, S. La inteligencia de fuentes abiertas: clave para desmontar la desinformación rusa. Red internacional de periodistas. Retrieved May 6, 2023, from https://ijnet.org/es/story/la-inteligencia-de-fuentes-abiertas-clave-para-desmontar-la-desinformaci%C3%B3n-rusa

Silva Llaguno, Esteban Leonardo (2022) Modelo de seguridad informática en los aspectos organizativos del Sistema Integrado de Gestión Estratégica de la Universidad Israel, aplicando ISO 27002 y CSF de NITS MAESTRÍA EN SEGURIDAD INFORMÁTICA, Quito: Universidad Israel 2022, 54p. Mg. Recalde Varela Pablo Marcel, UISRAEL-EC-MASTER-SEG. INF-378-242-2022-008

Schaurer, F., & Störger, J. From FIO'sThe Intelligencer. Afio.com. Retrieved May 6, 2023, from https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf

Tossolini, L. E. F., Macia, M. N., & Díaz, L. F. J. (2021). Análisis de OSINT aplicado a la detección de amenazas y vulnerabilidades en las organizaciones.

Trabajo Final Presentado Para Obtener el Grado, de E. en R. y. S. Análisis de OSINT aplicado a la detección de amenazas y vulnerabilidades en las organizaciones. Edu.Ar. Retrieved August 22, 2023, from http://sedici.unlp.edu.ar/bitstream/handle/10915/129027/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Trujillo Morales, Andrea Paulina (2022) Comparativa de las principales vulnerabilidades de dominios de ISP extraídos mediante API'S públicas, MAESTRÍA EN SEGURIDAD INFORMÁTICA, Quito: Universidad Israel 2022, 57p. MSc. Recalde Varela Pablo Marcel UISRAEL-EC-MASTER-SEG-INF-378-242-2022-009

Urrutia, D. (2023, April 7). Qué es OSINT - Definición, aplicaciones y ventajas. Arimetrics. https://www.arimetrics.com/glosario-digital/osint-open-source-intelligence

Villanueva, A. (2022, September 20). Fases de la Inteligencia de Amenazas - OSTEC. OSTEC | Segurança digital de resultados; OSTEC Business Security. https://ostec.blog/es/aprendizaje-descubrimiento/fases-de-la-inteligencia-de-amenazas/?cn-reloaded=1

Yoachimik, O. (2023, April 11). Informe sobre las amenazas DDoS en el 1.er trimestre de 2023. The Cloudflare Blog. https://blog.cloudflare.com/es-es/ddos-threat-report-2023-q1-es-es/

ANEXOS

ANEXO 1

Modelo de cuestionario: Validación de Propuesta Metodológica

1. En una escala del 1 al 10, ¿cuál es su nivel de familiaridad con el concepto de OSINT y su aplicación en la ciberseguridad? (1 = Muy Poco Familiar, 10 = Muy Familiar)
2. ¿Considera que la propuesta metodológica presenta una secuencia lógica y completa para la aplicación de OSINT en la investigación de amenazas informáticas? (Seleccione una opción)

   Sí ( )

   No ( )

   No Estoy Seguro ( )
3. ¿Encuentra adecuada la selección de los pasos en la metodología propuesta? ¿Agregaría algún paso adicional o sugeriría alguna modificación? (Por favor, explique su respuesta)
4. En relación con la validación por expertos, ¿cree que la inclusión de encuestas y entrevistas es apropiada para medir la efectividad y aplicabilidad de la metodología? ¿Tiene alguna sugerencia para mejorar este proceso? (Por favor, explique su respuesta)
5. Basado en su experiencia en seguridad informática, ¿cree que la aplicación de la metodología propuesta podría aportar de manera efectiva en la detección y análisis de amenazas informáticas? (Seleccione una opción)

   Sí, Aportaría Significativamente ( )

   Sí, Aportaría de Alguna Manera ( )

   No Estoy Seguro ( )

   No, No Aportaría ( )

Sus respuestas y opiniones son fundamentales para mejorar y afinar la metodología propuesta. Agradecemos su tiempo y contribución para fortalecer la efectividad de la investigación en ciberseguridad.

ANEXO 2

Modelo de encuesta: Percepción de Expertos sobre la Metodología de OSINT en Investigación de Amenazas Informáticas

Instrucciones: Responda las siguientes preguntas evaluando la efectividad y aplicabilidad de la propuesta metodológica para la aplicación de OSINT en la inteligencia de amenazas informáticas. Las respuestas serán confidenciales y se utilizarán para mejorar la metodología. Utilice una escala del 1 al 5, donde 1 significa "Totalmente en Desacuerdo" y 5 significa "Totalmente de Acuerdo".

- La metodología propuesta presenta una secuencia lógica y completa para la aplicación de OSINT en la investigación de amenazas informáticas.

  1 (Totalmente en Desacuerdo)

  2

  3

  4

  5 (Totalmente de Acuerdo)

- La selección de los pasos en la metodología es adecuada y aborda de manera efectiva los aspectos clave de la investigación de amenazas informáticas.

  1 (Totalmente en Desacuerdo)

  2

  3

  4

  5 (Totalmente de Acuerdo)

- La inclusión de encuestas y entrevistas como parte de la validación por expertos es apropiada para medir la efectividad y aplicabilidad de la metodología propuesta.

  1 (Totalmente en Desacuerdo)

  2

  3

  4

5 (Totalmente de Acuerdo)

- Basado en su experiencia en seguridad informática, ¿cree que la aplicación de la metodología propuesta podría aportar de manera efectiva en la detección y análisis de amenazas informáticas?

  1 (Totalmente en Desacuerdo)

  2

  3

  4

  5 (Totalmente de Acuerdo)

- ¿Tiene alguna sugerencia o recomendación para mejorar la metodología propuesta en relación con la aplicación de OSINT en la investigación de amenazas informáticas? (Por favor, comparta sus ideas en el espacio proporcionado)
- Comentarios Adicionales: (Espacio para comentarios abiertos)

Agradecemos sinceramente su participación en esta encuesta y su valiosa contribución para mejorar la metodología de investigación en ciberseguridad.

ANEXO 3

Quito, 19 septiembre 2023

Señor **Ing. Javier Logroño :**

Presente :

A petición del Interesado.

Yo, Luis Andres Montenegro Morales con cédula 1002312690, he revisado el trabajo de titulación con nombre: **Osint para inteligencia de amenazas de seguridad informática**, elaborado por el señor Ingeniero Javier Logroño, solicitando un criterio de este al cual refiero lo siguiente:

Como profesional en el campo de Control Interno de Tecnología y Ciberseguridad, me he permitido revisar, entender y valorar el trabajo recibido, el mismo que se encuentra en el campo profesional donde me desempeño.

El proyecto de titulación incluye información sobre la metodología que utiliza el OSINT, el cual permite dentro de sus fases generar un trabajo de investigación profunda y que dentro de sus aspectos destaca la información que se mantinen publicamente expuesto, y así identificar posibles brechas de seguridad que pueden ser explotables de acuerdo con las técnicas de intrusión y ciberataque.

Al ser un trabajo de titulación, toda informacion plasmada en este documento se debe manejar con el sigilo y el cuidado que exige este tipo de información, la misma que es clasificada como confidencial y restringida, para no comprometer la normal operación de la empresa a la cual se generó el ejercicio basado en la metodología OSINT.

Como punto a ser observado es importante señalar una ruta crítica, la misma que forma parte del resultado obtenido de esta investigación, así como su valoración de riesgo e impacto, el cual permite identificar de manera concreta si la brecha identificada es explotable o no. Adicional identificar cada uno de los posibles vectores de ataque y sus controles mitigantes con el fin de generar un plan de accion a ser ejecutado dentro de los marcos legales y normativos que tiene actualmente la legislación ecuatoriana.

Esto es lo que puedo mencionar brevemente en honor a la verdad Atentamente.

Andres Montenegro M.

CC: 1002312690

Gerente de Control Interno de TI y Ciberseguridad

Quito, 15 septiembre 2023

Señor **Ing.**

Javier Logroño :

Presente :

A petición del interesado.

Yo, Eduardo W. Alvarado. C. con cedula 1711849453, he recibido el trabajo de tesis con titulo: ***metodología inteligencia amenazas – utilizando Open source Intelligence OSINT*** , elaborado por el señor Ingeniero Javier . Logroño solicitando un criterio de este al cual refiero lo siguiente:

Como conocedor y profesional del campo de Seguridad de la información empresarial y Ciberseguridad, me he permitido leer el contenido y valorado el mismo de acuerdo con el campo profesional donde me desempeño.

La misma contiene información relevante de la metodología OSINT, que como marco metodológico es manejable a cualquier proceso o desarrollo en seguridad con la aplicabilidad a la infraestructura tecnológica, servicios publicados o demás de temas digitales e ingeniería social, entre otras de las mencionadas en el mismo documento.

El ordenamiento del trabajo y de los resultados de esta metodología se pueden obtener un sinfín de detalles técnico y de seguridad aplicados a la vulnerabilidad, amenazas, hardening, o remediación, dando un gran espectro de ejecución por varias integrantes, sean áreas Tecnología, Seguridad, Infraestructura e incluso las áreas competentes al negocio.

La clasificación de esta información a su vez debe ser de tipo RESTRINGIDA, por el tipo de resultados que pueden traer y más aun cuando son resultados de una marca reconocida en el país que pueden comprometer la C.I.D. de la Seguridad de la información.

Una recomendación sobre la ejecución de los resultados de esta metodología quizás se puedan incorporar en Mallas de resultados, clasificarlas por riesgos y generar un plan de seguimiento que puede ser un resultado con evaluación para un plan estratégico de seguridad o que también puede apalancar a regulaciones internas normativas o por buena práctica empresarial de seguridad, ya que estos análisis , hará que se cumpla de acuerdo a su apetito de riesgo la ejecución de estos planes , que también se trasladan a PRESUPUESTOS y a PROYECTOS institucionales, que a la larga deben provisionarse para su ejecución dependiendo de estos análisis.

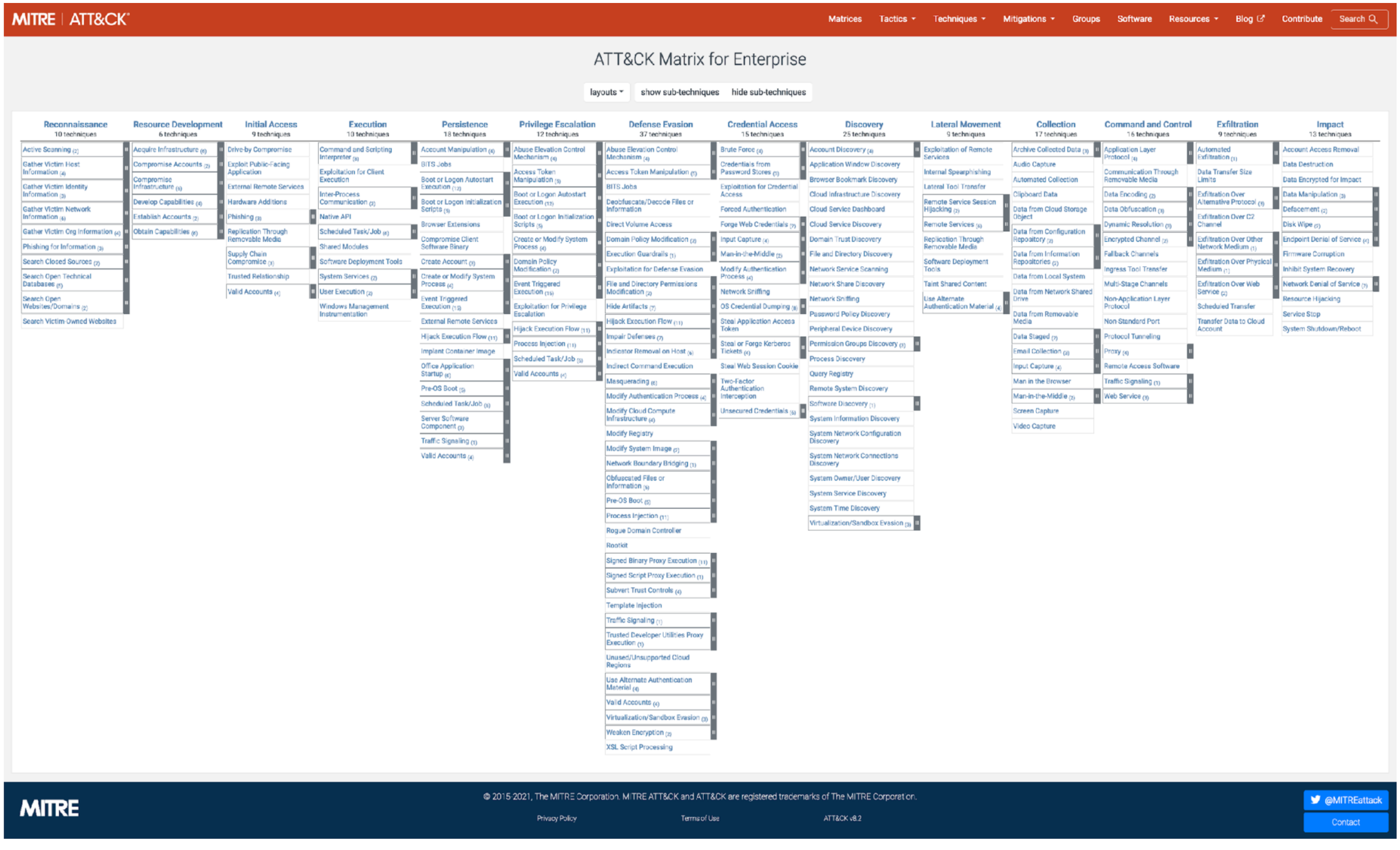
Esto es lo que puedo mencionar brevemente en honor a la verdad

Atentamente.

Firmado digitalmente por EDUARDO WILINTON ALVARADO CANDO
Fecha: 2023.09.15 12:04:55 -05'00'

Ing. Eduardo Alvarado, Msc
CC: 1711849453
Gerente de Seguridad Información y ciberseguridad

ANEXO4


MITRE | ATT&CK
Matrices
Tactics
Techniques
Mitigations
Groups
Software
Resources
Blog
Contribute
Search
ATT&CK Matrix for Enterprise
layouts
show sub-techniques
hide sub-techniques
Reconnaissance
10 techniques
Active Scanning (2)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (3)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (2)
Search Victim-Owned Websites
Resource Development
6 techniques
Acquire Infrastructure (6)
Compromise Accounts (2)
Compromise Infrastructure (6)
Develop Capabilities (4)
Establish Accounts (2)
Obtain Capabilities (6)
Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (3)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)
Execution
10 techniques
Command and Scripting Interpreter (8)
Exploitation for Client Execution
Inter-Process Communication (2)
Native API
Scheduled Task/Job (6)
Shared Modules
Software Deployment Tools
System Services (2)
User Execution (2)
Windows Management Instrumentation
Persistence
18 techniques
Account Manipulation (4)
BITS Jobs
Boot or Logon Autostart Execution (12)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (15)
External Remote Services
Hijack Execution Flow (11)
Implant Container Image
Office Application Startup (6)
Pre-OS Boot (5)
Scheduled Task/Job (5)
Server Software Component (3)
Traffic Signaling (1)
Valid Accounts (4)
Privilege Escalation
12 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (12)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Domain Policy Modification (2)
Event Triggered Execution (15)
Exploitation for Privilege Escalation
Hijack Execution Flow (11)
Process Injection (11)
Scheduled Task/Job (5)
Valid Accounts (4)
Defense Evasion
37 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
BITS Jobs
Deobfuscate/Decode Files or Information
Direct Volume Access
Domain Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (7)
Hijack Execution Flow (11)
Impair Defenses (7)
Indicator Removal on Host (6)
Indirect Command Execution
Masquerading (6)
Modify Authentication Process (4)
Modify Cloud Compute Infrastructure (4)
Modify Registry
Modify System Image (2)
Network Boundary Bridging (1)
Obfuscated Files or Information (5)
Pre-OS Boot (5)
Process Injection (11)
Rogue Domain Controller
Rootkit
Signed Binary Proxy Execution (11)
Signed Script Proxy Execution (1)
Subvert Trust Controls (4)
Template Injection
Traffic Signaling (1)
Trusted Developer Utilities Proxy Execution (1)
Unused/Unsupported Cloud Regions
Use Alternate Authentication Material (4)
Valid Accounts (4)
Virtualization/Sandbox Evasion (3)
Weaken Encryption (2)
XSL Script Processing
Credential Access
15 techniques
Brute Force (4)
Credentials from Password Stores (3)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Man-in-the-Middle (2)
Modify Authentication Process (4)
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Kerberos Tickets (4)
Steal Web Session Cookie
Two-Factor Authentication Interception
Unsecured Credentials (6)
Discovery
25 techniques
Account Discovery (4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (1)
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion (3)
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Collection
17 techniques
Archive Collected Data (3)
Audio Capture
Automated Collection
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository (2)
Data from Information Repositories (2)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Input Capture (4)
Man in the Browser
Man-in-the-Middle (2)
Screen Capture
Video Capture
Command and Control
16 techniques
Application Layer Protocol (4)
Communication Through Removable Media
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Software
Traffic Signaling (1)
Web Service (3)
Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (2)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Endpoint Denial of Service (4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (2)
Resource Hijacking
Service Stop
System Shutdown/Reboot
MITRE
© 2015-2021, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.
Privacy Policy
Terms of Use
ATT&CK v8.2
@MITREattack
Contact