UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA

INTELIGENCIA DE SEGURIDAD Y ANALÍTICA NACIONAL (ISA): MÉTODO PARA EL ANÁLISIS Y LA INVESTIGACIÓN DEL PANORAMA DE CIBERATAQUES EN MÉXICO MEDIANTE EL USO INTELIGENCIA DE AMENAZAS Y CIENCIA DE DATOS

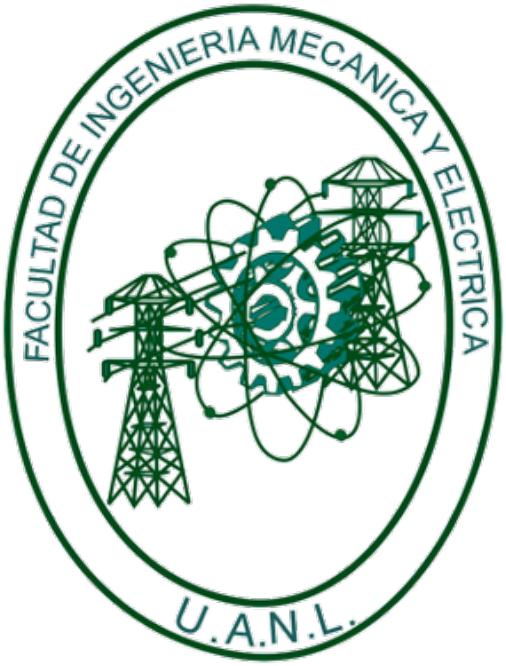
POR

ARTURO ERICK TORRES CAVAZOS

EN OPCIÓN AL GRADO DE
DOCTOR EN INGENIERÍA CON ORIENTACIÓN
EN TECNOLOGÍAS DE LA INFORMACIÓN

SAN NICOLÁS DE LOS GARZA, NUEVO LEÓN. NOVIEMBRE, 2021.

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA
SUBDIRECCIÓN DE ESTUDIOS DE POSGRADO



INTELIGENCIA DE SEGURIDAD Y ANALÍTICA NACIONAL (ISA): MÉTODO PARA EL ANÁLISIS Y LA INVESTIGACIÓN DEL PANORAMA DE CIBERATAQUES EN MÉXICO MEDIANTE EL USO INTELIGENCIA DE AMENAZAS Y CIENCIA DE DATOS

POR

ARTURO ERICK TORRES CAVAZOS

EN OPCIÓN AL GRADO DE
DOCTOR EN INGENIERÍA CON ORIENTACIÓN
EN TECNOLOGÍAS DE LA INFORMACIÓN

SAN NICOLÁS DE LOS GARZA, NUEVO LEÓN. NOVIEMBRE, 2021

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
Facultad de Ingeniería Mecánica y Eléctrica
Posgrado

Los miembros del Comité de Evaluación de Tesis recomendamos que la Tesis "Inteligencia de Seguridad y Analítica Nacional (ISA): Método para el Análisis y la Investigación del Panorama de Ciberataques en México mediante el uso Inteligencia de Amenazas y Ciencia de Datos", realizada por el estudiante Arturo Erick Torres Cavazos, con número de matrícula 1328808, sea aceptada para su defensa como requisito parcial para obtener el grado de Doctor en Ingeniería con orientación en Tecnologías de la Información..

El Comité de Evaluación de Tesis

Dr. Francisco Torrres Guerrero
Director

Dra. Leticia Amalia Neira Tovar
Revisor

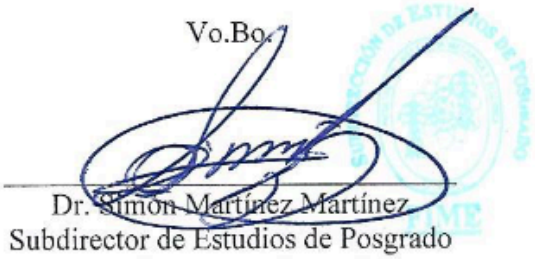
Dr. Carlos Esteban Chavez Pech
Revisor

Dr. Sergio Antonio Ordoñez Gonzalez
Revisor

Dr. Alvaro Eduardo Cordero Franco
Revisor

Dra. Maria Teresa Perez Morales
Revisor

Vo.Bo.



Dr. Simón Martínez Martínez
Subdirector de Estudios de Posgrado

Institución 190001

Programa 514622

Acta Núm. 358

Resumen

El objetivo principal de este estudio es desarrollar un método basado en Ciencia de Datos e Inteligencia de Ciber Amenazas (CTI) para investigar y analizar exhaustivamente el panorama de amenazas cibernéticas en México. Este método tiene como propósito describir las fases, tácticas, técnicas y tendencias de actividad maliciosa en el ciberespacio mexicano, con el fin de generar una estrategia de ciberseguridad nacional fundamentada en el análisis y comprensión de los ciberataques.

La investigación se centra en resolver el problema de la falta de una estrategia integral de ciberseguridad y la ausencia de un panorama claro de los ciberataques en las organizaciones mexicanas. A pesar de la abundancia de reportes de inteligencia contra amenazas a nivel global, estos no proporcionan una visión específica del contexto nacional. Por lo tanto, se desarrolló un método que combina Ciencia de Datos y metodologías de CTI, como MITRE ATT&CK, para recolectar, analizar y visualizar eventos de ciberseguridad detectados en México. Los resultados obtenidos incluyen una descripción detallada del panorama de amenazas cibernéticas en México, la identificación y categorización de las fases específicas de los ciberataques, y la generación de recomendaciones automatizadas para reforzar la ciberseguridad en las organizaciones mexicanas. Asimismo, se propuso una estrategia nacional de ciberseguridad basada en evidencia concreta, proporcionando un marco integral para la defensa contra ciberamenazas en el contexto mexicano.

Las conclusiones de esta investigación demuestran que el método desarrollado es efectivo y basado en evidencia, lo que permite abordar de manera integral el panorama de amenazas cibernéticas en México. La integración de inteligencia de ciber amenazas y la generación de recomendaciones específicas son contribuciones significativas para la formulación de una estrategia nacional de ciberseguridad, respondiendo a la necesidad de una defensa coordinada y eficaz contra las ciberamenazas.

***Palabras Clave* — Ciencia de Datos, Inteligencia de Ciber Amenazas, Ciberseguridad, Panorama de Amenazas, México, MITRE ATT&CK, Análisis de Ciberataques, Recomendaciones de Seguridad.**

Agradecimientos

Quiero expresar mi más profundo agradecimiento a todas las personas que han sido parte esencial en el desarrollo de esta tesis doctoral y en cada etapa de mi vida académica y profesional.

A mis padres, quienes con su apoyo incondicional, valores y sabiduría me han guiado siempre y me han dado las herramientas necesarias para alcanzar mis metas. Gracias, papá (Dr. Arturo Torres Bugdud) y mamá (Mtra. Isabel Maria Cavazos Cerda), por su amor, enseñanza, guia y dedicación, sin los cuales no habría llegado hasta aquí.

A mis asesores, Dr. Francisco Torres Guerrero, Dra. Leticia Neira Tovar, Dr. Arturo Torres Bugdud quienes con su guía y conocimientos me ayudaron a construir y fortalecer este trabajo. Su orientación y paciencia han sido fundamentales para avanzar en este desafío, y su compromiso ha sido una inspiración constante.

A mis hermanas Dra. Zaida Torres Cavazos y Mtra. Irasema Torres Cavazos, por ser siempre una fuente de apoyo y aliento. Sus palabras de ánimo y cariño han sido indispensables en los momentos difíciles y en cada logro alcanzado.

A mi esposa, Lic. Yabari Gemmali Alanis Hernandez, cuyo amor y comprensión han sido un pilar en esta etapa. Gracias por tu apoyo constante y por caminar a mi lado, especialmente en los momentos de mayor exigencia. A mis hijos, quienes son mi mayor motivación para seguir adelante y alcanzar mis sueños; su alegría y amor me han impulsado a dar siempre lo mejor de mí.

A mis colegas de la industria, a mis jefes y líderes en el ramo, quienes me brindaron oportunidades para aprender y crecer profesionalmente. Gracias por compartir su experiencia y enseñanzas, las cuales han sido invaluables en mi desarrollo y en la realización de esta investigación.

Y a todos los involucrados en esta tesis, quienes, de una manera u otra, contribuyeron a que este proyecto fuera posible. Cada contribución ha dejado una huella en este logro, y por ello, les estaré siempre agradecido.

A todos, gracias de corazón.

Índice

1 CAPITULO 1 – INTRODUCCIÓN

En la era actual marcada por una dependencia y utilización continua de la tecnología, impulsada por la innovación y la transformación digital como el Internet de las Cosas (IoT) y la computación en la nube, se ha vuelto crucial implementar medidas de protección eficaces para salvaguardar nuestros activos de información digital frente a los riesgos y consecuencias derivadas de las amenazas cibernéticas y el cibercrimen. El concepto de riesgo cibernético está estrechamente relacionado con las nociones de amenaza digital y ciberataque. Según el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) [1], el riesgo cibernético se define como el peligro de incurrir en pérdidas financieras, interrupciones operativas o daños asociados al fallo de las tecnologías digitales utilizadas en funciones informativas y/o operativas. Estos riesgos surgen cuando sistemas son comprometidos por medios electrónicos sin autorización, lo que podría llevar al uso indebido, divulgación, interrupción, alteración o destrucción de los sistemas.. Ante estos incidentes y la gran cantidad de amenazas cibernéticas rondando el internet afectando a los diferentes sectores de la industria, se han realizado investigaciones en sectores tales como en el sector salud [2], donde los autores señalan dicho sector como un objetivo principal de los adversarios para el robo de información personal, critica y confidencial, así mismo también existen investigaciones de ciberseguridad en otros sectores como el de manufactura [3], donde se presenta una investigación de la ciberseguridad en los sistemas de manufactura digital con un enfoque particular en la caracterización del sistema, identificación de amenazas, vulnerabilidades, escenarios de ataque, métodos de control y técnicas de determinación de riesgos, también podemos encontrar investigaciones basadas en las reacciones del mercado financiero ante un ataque de ciberseguridad [4].

Por otro lado, consultorías como Cybersecurity Venture [5], predice que la ciberdelincuencia costará alrededor de $ 10 billones a partir del 2026, lo que lo hará más rentable que el comercio global de todas las principales drogas ilegales combinadas. Por otro lado, en el reporte anual de riesgos 2023 publicado por el "World Economic Forum" [6] se catalogan a los Ciberataques como un riesgo latente de el que hay que estar preparados, ya que la probabilidad e impacto a la economía causado por este fenómeno esta solo por debajo de riesgos como Desastres Naturales, Crisis por falta de agua, Climas extremos, seguidos de riesgos como Enfermedades Infecciosas, Desastres ambientales creados por los humanos, Crisis por alimentos, etc. En el mismo estudio se habla sobre "Los peligros de la evolución digital" y de como el IoT también está amplificando el potencial de la superficie de ciberataque, estimando que el día de hoy existen más de 21 mil millones de dispositivos inteligentes o Internet de las Cosas (IoT) en todo el mundo y se espera que se duplique para el 2025 [7], los cuales han se han convertido en herramientas utilizadas por cibercriminales, caso ocurrido a finales de 2016 [8], en el cual lanzaron un ataque importante conocido Denegación de Servicio Distribuido (DDoS), causando una interrupción en los servicios de Internet que afectó a muchas empresas, incluidas Amazon, PayPal, Netflix, Spotify y Twitter. Por otro lado, la revista Forbes [9] publico que investigadores de la empresa de ciberseguridad F-Secure detectaron un aumento de más del 300% en los ataques a dispositivos IoT en la primera mitad de 2019 [10], mientras que en septiembre de ese mismo año, dichos dispositivos fueron utilizados para derribar los servicios de páginas como Wikipedia a través de un ataque de Denegación de Servicio Distribuida (DDoS)

[11] y se estima que existirá un aumento sobre el uso de los dispositivos IoT como intermediarios entre los atacantes y sus víctimas. Desafortunadamente, la dependencia de la tecnología, así como la gran cantidad de información crítica y confidencial manejada por las organizaciones hoy en día, se han convertido en el objetivo de los ciberdelincuentes, los cuales han desarrollado nuevas formas de poder afectar la integridad, disponibilidad y confidencialidad de los sistemas y datos de las organizaciones, utilizando técnicas avanzadas como el secuestro y extorsión digital, mejor conocido como Ransomware [12], el cual registro una perdida aproximada de 10.1 billones de euros en 2019 [13].

En México hemos sido testigos de un aumento de amenazas cibernéticas que han afectado diferentes sectores de la industria en los últimos años, tales como el que afecto al Instituto Nacional Electoral (INE) en el 2016, en donde se logró vulnerar una base de datos alojada en la nube de Amazon Web Services (AWS), en el cual se expusieron datos de más de 93.4 millones de mexicanos [15]. Otro caso en 2018 donde se dio a conocer que algunos ciber atacantes vulneraron algunos sistemas de instituciones financieras que interactuaban con el Sistema de Pagos Electrónicos (SPEI), el cual tuvo como consecuencia el robo y perdida aproximada de 300 millones de pesos desde destinas locaciones, en el cual los atacantes crearon cuentas falsas para enviar instrucciones de pago fraudulentas mediante un código malicioso engañando a las instituciones financieras para enviar las transacciones el Banco de México a través del SPEI como ocurre habitualmente. En consecuencia, de esto, diversas empresas fueron afectadas, como es el caso de AXA Seguros, quien reporto inconsistencias relacionadas con el sistema de pagos y su área operativa declaro que el ataque fue a sus sistemas de conexión con la plataforma SPEI ocasionando una pérdida económica aproximada de 57 millones de pesos [16] [17].

Como se detalla en el documento de McKinsey & Company en colaboración con COMEXI [18] existen grupos autodenominados como hacktivistas con el propósito de realizar un ciberataque con el objetivo principal de realizar una declaración o protesta política hacia un gobierno o institución. En el año 2012 el grupo Ciber Protesta Mexicana llevo a cabo un ciberataque simultaneo, en donde por lo menos en 10 sitios web de gobierno, partidos políticos y prensa se publicaron mensajes de protesta. Este grupo, que ya había atacado de manera similar en 2009, posicionó su ciberataque como una protesta pacífica ante la situación política del país, en el que sus actividades han llegado a ser notas de carácter global [19]. Tan sólo en México, durante el cuarto trimestre del 2019, los fraudes cibernéticos crecieron 36% respecto al mismo periodo del año anterior, representando un monto aproximado de 11,171 millones de pesos y solo se bonifico el 45% y 86 de cada 100 fraudes cibernéticos pudieron ser resueltos a favor del usuario afectado según el documento elaborado por la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) a partir de las reclamaciones con impacto monetario presentadas por los clientes de la Banca en México contenidas en el Reporte Regulatorio R27 (CNBV) [20]. Ante esto, las empresas, gobiernos y especialistas de ciberseguridad han mostrado un gran interés en la aplicación y consumo de fuentes de inteligencia para la generación de una estrategia de ciberdefensa basada en inteligencia. A esta práctica se le conoce como Cyber Threat Intelligence (CTI) [14], la cual se describe como el conocimiento fundamentado en pruebas concretas, abarcando contexto, mecanismos, indicadores, repercusiones y recomendaciones prácticas, acerca de una amenaza actual o emergente a los activos informativos de las organizaciones. Este conocimiento es esencial

para orientar las decisiones relacionadas con la manera en que la entidad afectada debería responder ante dicha amenaza..

1.1 Motivación

Aunque distintos organismos pueden implementar iniciativas de ciberseguridad de forma independiente, la organización e integración de estos esfuerzos requiere de un organismo que los pueda gestionar adecuadamente. Ante esto, en 2017, el gobierno de México emitió La Estrategia Nacional de Ciberseguridad [21], que refleja la visión del Estado mexicano respecto a este tema, considerando la relevancia de las tecnologías de la información y comunicación (TIC), los riesgos vinculados al uso de estas tecnologías y los ciberdelitos, así como la necesidad de fomentar una cultura de ciberseguridad generalizada. El propósito principal de esta estrategia era identificar y definir las acciones de ciberseguridad relevantes para los sectores social, económico y político, facilitando así a la población y a las entidades públicas y privadas el uso seguro y efectivo de las TIC para el desarrollo sostenible de México. Esta estrategia se inició con la realización de diversas mesas de discusión que involucraron a representantes del sector público, privado, la sociedad civil y la academia, llevadas a cabo a inicios de 2017 con el apoyo de la Organización de Estados Americanos (OEA). Este proceso resultó en la redacción de un documento que asignaba la implementación de la estrategia al Poder Ejecutivo y proponía la creación de un Subcomité de Ciberseguridad bajo la Secretaría de Gobernación (Segob). Sin embargo, este subcomité nunca se materializó.

Años más tarde, México publicó una Estrategia Nacional Digital 2021-2024 (EDN) [22] , centrada en perfeccionar y armonizar su marco regulatorio, optimizar el uso de la infraestructura existente y adoptar un enfoque basado en la seguridad de la información, además de la integración de información para aumentar la eficiencia en la gestión, así como ampliar el acceso a áreas sin cobertura. No obstante, hasta la fecha (2023), no se han especificado los métodos para alcanzar estos objetivos.

Mi Motivación es poder comprender el panorama de ciber ataques en México utilizando el Método Científico en Ingeniería de la Información mediante el Análisis de eventos de ciberseguridad detectados en México y la Aplicación de metodologías de Inteligencia contra Amenazas (CTI), integrando técnicas de visualización para el Análisis de los datos recolectados.

1.2 Justificación

En la era digital, la ciberseguridad se ha convertido en una preocupación central para las naciones, organizaciones y empresas. México, como una economía emergente y un actor clave en América Latina, enfrenta desafíos significativos en el ámbito de la ciberseguridad. La creciente frecuencia y sofisticación de los ciberataques subraya la necesidad urgente de una estrategia de ciberseguridad nacional robusta y bien informada.

La presente tesis doctoral se justifica en múltiples dimensiones que abarcan desde la necesidad de una estrategia de ciberseguridad nacional hasta la contribución académica y práctica en el campo de la ciberseguridad en México.

1.2.1 Necesidad de una Estrategia Nacional de Ciberseguridad

El reporte "Estrategias Nacionales de Ciberseguridad: Enseñanzas y reflexiones de las Américas y otras regiones", elaborado por la Organización de Estados Americanos (OEA) y Global Partners Digital, destaca que países como Costa Rica, a pesar de contar con una estrategia más robusta, han sido gravemente afectados por ciberataques. Este contraste subraya la necesidad de una estrategia nacional de ciberseguridad en México que no solo sea robusta, sino también adaptativa y proactiva frente a las amenazas.

1.2.2 Inteligencia contra Amenazas (CTI) y Ciencia de Datos

La inteligencia contra amenazas (CTI) y la ciencia de datos ofrecen herramientas poderosas para analizar y comprender las tácticas, técnicas y procedimientos (TTP) de los adversarios. Sin embargo, México carece de un marco metodológico que combine efectivamente estos enfoques para proporcionar una visión clara y específica de las amenazas cibernéticas que enfrenta el país. Este vacío limita la capacidad de las organizaciones para tomar decisiones informadas y formular estrategias de defensa eficaces.

1.2.3 Generación de Recomendaciones Automatizadas

La capacidad de traducir el análisis de amenazas en recomendaciones específicas y automatizadas es crucial para mejorar la resiliencia cibernética de las organizaciones mexicanas. Al automatizar la generación de recomendaciones basadas en datos concretos y lecciones aprendidas, las organizaciones pueden responder más rápidamente a las amenazas y fortalecer sus defensas de manera continua.

1.2.4 Contribución a la Comunidad Científica y Práctica

Esta investigación no solo contribuirá al conocimiento académico sobre ciberseguridad en el contexto mexicano, sino que también proporcionará herramientas prácticas y recomendaciones para mejorar las políticas y estrategias de ciberseguridad. Al abordar las amenazas específicas que enfrentan las organizaciones mexicanas, esta tesis ofrecerá una base sólida para la formulación de una estrategia nacional de ciberseguridad.

En resumen, esta tesis doctoral se justifica plenamente por su potencial para llenar un vacío crítico en la ciberseguridad nacional de México, proporcionar conocimientos académicos valiosos y ofrecer soluciones prácticas a las organizaciones mexicanas para enfrentar y mitigar las amenazas cibernéticas.

1.3 Descripción y Planteamiento del Problema

En el contexto actual, la ciberseguridad se ha convertido en una preocupación primordial para gobiernos, empresas y organizaciones de todo el mundo. México no es la excepción, enfrentando una creciente ola de ciberataques que amenazan la integridad, confidencialidad y disponibilidad de sus sistemas de información. Sin embargo, a pesar de la gravedad de la situación, el país carece de una estrategia integral de ciberseguridad que permita enfrentar estos desafíos de manera efectiva y coordinada.

Según el informe "Estrategias Nacionales de Ciberseguridad: Enseñanzas y reflexiones de las Américas y otras regiones", desarrollado por la Organización de Estados Americanos (OEA) y Global Partners Digital, se efectuaron varias comparativas entre México y otros países de Centroamérica, región a la que la OEA también asigna a México. En este análisis, se destacó a Costa Rica por tener una Estrategia Nacional de Ciberseguridad considerablemente más desarrollada que la de México. No obstante, a pesar de su avanzada estrategia, Costa Rica fue el escenario donde numerosas instituciones gubernamentales sufrieron ataques devastadores por parte del grupo cibercriminal Conti durante abril y mayo de 2022, lo que resultó en significativos impactos tanto a nivel nacional como económico. Ante estas situaciones, diversas comunidades, así como fabricantes e investigadores de ciberseguridad, han mostrado un gran interés por publicar sus hallazgos e investigaciones al público en general, teniendo como resultado una gran cantidad de información que puede consumirse por los analistas para tomar decisiones importantes a la hora de realizar una estrategia de ciberdefensa, tales como asignar recursos, presupuestos y priorizar acciones ante una amenaza cibernética [23] [24] [25]. Sin embargo, esto no es suficiente, ya que la mayoría de los reportes de Inteligencia contra Amenazas buscan cubrir un panorama global y no nacional.

El principal problema que se enfrentan las organizaciones mexicanas es que, hoy en día, no se cuenta con una estrategia integral de ciberseguridad y no se cuenta con panorama claro de los ciberataques que ocurren en el ciberespacio mexicano. Por lo tanto, la generación de estrategias de ciber defensa basada con un lenguaje común integrando inteligencia sobre las amenazas y eventos de ciberseguridad ocurridos en el territorio nacional se considera un problema potencial e inmediato que se busca resolver.

1.3.1 Falta de un Panorama Claro de Amenazas Cibernéticas

Actualmente, México no cuenta con un panorama claro y actualizado de las amenazas cibernéticas que enfrenta. La mayoría de los informes de inteligencia contra amenazas se centran en un contexto global, lo cual no proporciona la información específica necesaria para formular políticas y estrategias efectivas a nivel nacional. Esta falta de información específica impide una adecuada asignación de recursos, presupuestos y prioridades en las acciones de ciberseguridad.

1.3.2 Necesidad de Integrar CTI y Ciencia de Datos

La recolección y análisis de eventos de ciberseguridad reales detectados en el ciberespacio mexicano pueden proporcionar una visión detallada y precisa de las tácticas, técnicas y procedimientos (TTP) utilizados por los adversarios. Sin embargo, actualmente no existe un marco metodológico en México que integre de manera efectiva la ciencia de datos y la inteligencia contra amenazas para abordar este problema.

1.3.3 Importancia de Generar Recomendaciones Automatizadas

Además de la identificación y análisis de las amenazas, es crucial que los resultados de esta investigación se traduzcan en recomendaciones específicas y automatizadas que puedan ser implementadas por las organizaciones mexicanas. La capacidad de generar estas recomendaciones de manera automatizada, basada en lecciones aprendidas y datos concretos, representa un avance significativo para fortalecer las medidas de ciberseguridad y mejorar la resiliencia ante futuros ataques.

1.3.4 Problema Central

El principal problema que enfrenta México es la falta de una estrategia integral de ciberseguridad y un panorama claro de los ciberataques que ocurren en el ciberespacio nacional. Esta carencia dificulta la generación de estrategias de ciberdefensa basadas en un lenguaje común que integre inteligencia sobre las amenazas e incidentes de ciberseguridad específicos del territorio nacional.

Por lo tanto, esta tesis se propone desarrollar un método basado en la Ciencia de Datos e Inteligencia contra Amenazas (CTI) para investigar y analizar de manera exhaustiva el panorama de amenazas cibernéticas en México. El objetivo es describir las fases, tácticas, técnicas y tendencias de actividad maliciosa, y generar una estrategia de ciberseguridad nacional a través del análisis y comprensión de los ciberataques que ocurren en el ciberespacio mexicano. Esta investigación busca llenar un vacío crítico en la ciberseguridad nacional de México, proporcionando un análisis detallado y contextualizado de las amenazas cibernéticas, y ofreciendo soluciones prácticas para mejorar la defensa cibernética del país.

En resumen, esta investigación busca llenar un vacío crítico en la ciberseguridad nacional de México, proporcionando un análisis detallado y contextualizado de las amenazas cibernéticas, y ofreciendo soluciones prácticas para mejorar la defensa cibernética del país.

1.4 Objetivos de la investigación

En esta sección se presentan los objetivos generales de la investigación.

1.4.1 Objetivo General

Desarrollar un método basado en Ciencia de Datos e Inteligencia de Ciber Amenazas (CTI) que nos permita investigar y analizar de manera exhaustiva el panorama de amenazas cibernéticas en

México mediante la recolección y análisis de eventos de ciberseguridad reales detectados en el ciber espacio mexicano para de describir las fases, tácticas, técnicas y tendencias de actividad maliciosa que permita generar una estrategia de ciberseguridad nacional a través del análisis y comprensión de los ciberataques que ocurren en el ciberespacio mexicano.

1.4.2 Objetivo Específicos

1.4.2.1 Objetivo Específico 1 - Describir el Panorama de Amenazas Cibernéticas en México

Este objetivo busca proporcionar una visión detallada y actualizada del panorama de amenazas cibernéticas en México, basándose en el análisis de eventos reales de ciberseguridad detectados en organizaciones mexicanas.

1.4.2.2 Objetivo Específico 2 – Aplicación de Metodologías de Inteligencia contra Amenazas (CTI):

Seleccionar y aplicar metodologías de CTI en el análisis de los eventos de ciberseguridad recolectados para identificar y categorizar las fases específicas de los ciberataques para analizar y modelar tácticas, técnicas y procedimientos (TTP) de adversarios en el contexto mexicano.

1.4.2.3 Objetivo Específico 3 – Generación Automatizada de Recomendaciones para Reforzar la Ciberseguridad Nacional

Al finalizar el análisis, la tesis se propone proporcionar recomendaciones específicas para reforzar las medidas de ciberseguridad en las organizaciones mexicanas, basadas en las lecciones aprendidas del análisis de amenazas.

Estos objetivos y metas son fundamentales para contribuir al conocimiento y fortalecimiento de las capacidades de ciberseguridad en México, abordando de manera específica y efectiva los desafíos presentes en el panorama de amenazas cibernéticas.

1.5 Hipótesis

La hipótesis principal busca validar la premisa fundamental de que, al analizar eventos reales de ciberseguridad en organizaciones mexicanas, será posible obtener una visión detallada y actualizada que permitirá describir el panorama de amenazas cibernéticas en el país y emitir una estrategia de ciberseguridad nacional basada en los ciberataques analizados. Esta afirmación se basa en la idea de que la recolección y análisis de eventos concretos proporcionará una comprensión más precisa de los desafíos de ciberseguridad en el entorno mexicano.

1.5.1 Hipótesis 2 Relacionada a la Aplicación de Metodologías de CTI:

Se hipotetiza que la selección y aplicación de metodologías de Inteligencia contra Amenazas (CTI) en el análisis de eventos de ciberseguridad permitirá identificar y categorizar las fases específicas de los ciberataques, así como analizar y modelar tácticas, técnicas y procedimientos

(TTP) de ciber ataques ocurridos en el ciber espacio mexicano, lo cual permitirá la generación de estrategias y recomendaciones para una estrategia nacional.

1.5.2 Hipótesis 3 Relacionada a la Generación Automatizada de Recomendaciones:

Se hipotetiza que, al finalizar el análisis, será posible generar recomendaciones específicas para reforzar las medidas de ciberseguridad en las organizaciones mexicanas, utilizando lecciones aprendidas del análisis de amenazas y datos recopilados durante la investigación.

Estas hipótesis forman la base de la investigación y se buscará validar su veracidad a lo largo del desarrollo de la tesis doctoral.

1.6 Diseño Experimental y Metodologías de la Investigación

En esta sección, se describe el diseño experimental y las metodologías específicas que se implementarán para abordar los objetivos y metas establecidos en la tesis doctoral. Cada objetivo se acompaña de la metodología correspondiente para asegurar un enfoque integral y riguroso.

1.6.1 Metodología: Recolección y Análisis de Eventos de Ciberseguridad

Se realizará un análisis exhaustivo de eventos reales de ciberseguridad detectados en organizaciones mexicanas disponibles. Esto implicará la revisión detallada de la información recopilada en esta investigación para identificar patrones, tácticas y técnicas utilizadas por adversarios lo cual nos ayudará a cumplir el ***Objetivo Específico 1 - Describir el Panorama de Amenazas Cibernéticas en México.***

1.6.2 Metodología: Implementación de metodologías de CTI

Se seleccionarán, adaptarán e implementarán las metodologías de CTI para categorizar y analizar las fases específicas de los ciberataques en el contexto mexicano. Esto incluirá la identificación de tácticas, técnicas y procedimientos (TTP) empleados por adversarios ayudando a cumplir el ***Objetivo Específico 2 - Aplicación de Metodologías de Inteligencia contra Amenazas (CTI)***

1.6.3 Metodología: Automatización de Resultados y Lecciones Aprendidas

Al finalizar el análisis, se integrarán los resultados obtenidos de los objetivos anteriores. Las lecciones aprendidas se utilizarán para generar recomendaciones específicas, aprovechando técnicas de aprendizaje automático y análisis predictivo, cumpliendo el ***Objetivo Específico 3 - Generación Automatizada de Recomendaciones para Reforzar la Ciberseguridad***

1.6.4 Consideraciones Éticas y de Privacidad

Se seguirán estrictos protocolos éticos y de privacidad en la recolección y manejo de datos. Se garantizará la anonimización de la información sensible y se obtendrán los consentimientos necesarios de las organizaciones participantes.

Este diseño experimental y las metodologías asociadas proporcionan una estructura sólida para abordar los objetivos de la tesis doctoral, asegurando la rigurosidad y la relevancia de la investigación en el ámbito de la ciberseguridad en México.

1.7 Preguntas de investigación

Las preguntas de investigación se plantean con el propósito de orientar y estructurar la investigación, buscando respuestas detalladas que contribuyan a la consecución de los objetivos específicos de la tesis doctoral.

1.7.1 Pregunta 1: ¿Existen set de datos disponibles que brinden información de eventos de ciberseguridad ocurridos en el sector mexicano?

Esta pregunta se centra en identificar set de datos que se enfoquen en eventos de ciberseguridad detectados en organizaciones mexicanas en los últimos años. el *Objetivo Específico 1 - Describir el Panorama de Amenazas Cibernéticas en México.*

1.7.2 Pregunta 2: ¿Cuáles son los patrones predominantes en los eventos de ciberseguridad detectados en organizaciones mexicanas?

Esta pregunta busca comprender cómo aplicar estas metodologías de CTI para identificar y modelar las distintas fases de los ciberataques en el contexto mexicano cumpliendo con el *Objetivo Específico 2 - Aplicación de Metodologías de Inteligencia contra Amenazas (CTI)*

1.7.3 Pregunta 3: ¿Cuáles son las herramientas y técnicas más efectivas para la recolección, análisis y visualización de los eventos se seguridad recolectados para esta investigación en un entorno experimental avanzado?

La investigación se enfoca en identificar las mejores prácticas y tecnologías para un marco experimental integral.

1.7.4 Pregunta 4: ¿Cómo se pueden integrar los resultados obtenidos de la investigación para generar recomendaciones específicas y automatizadas destinadas a reforzar las medidas de ciberseguridad en las organizaciones mexicanas?

Esta pregunta busca comprender cómo utilizar los hallazgos y lecciones aprendidas para generar recomendaciones automatizadas y específicas. *Objetivo Específico 3 - Generación Automatizada de Recomendaciones para Reforzar la Ciberseguridad*

Estas preguntas de investigación proporcionan una guía clara para la exploración y el análisis detallado en cada uno de los objetivos específicos de la tesis doctoral.

1.8 Alcance/Contribuciones

En esta sección, se delinean los alcances y las contribuciones esperadas de la tesis doctoral, proporcionando una visión clara de los límites de la investigación y el valor que se espera aportar al campo de la ciberseguridad en México.

1.8.1 Alcances de la Tesis

1.8.1.1 Enfoque Geográfico:

El alcance geográfico se limita a México, centrándose exclusivamente en el panorama de amenazas cibernéticas dentro de las organizaciones mexicanas.

1.8.1.2 Datos Utilizados:

Se utilizarán exclusivamente eventos de ciberseguridad detectados de organizaciones mexicanas participantes, limitando el análisis a la información recopilada en esta investigación.

1.8.1.3 Metodologías de CTI:

La aplicación de Inteligencia contra Amenazas CTI se centrará específicamente en metodologías que cuenten con un enfoque y profundidad que ayude a la investigación descriptiva a la información recopilada en esta investigación.

1.8.2 Contribuciones Esperadas

1.8.2.1 Panorama Detallado de Amenazas en México:

Se espera contribuir con una visión detallada y actualizada del panorama de amenazas cibernéticas en México, basada en eventos reales de ciberseguridad.

1.8.2.2 Modelado Preciso de Tácticas y Técnicas de Adversarios:

La aplicación de metodologías de Inteligencia contra Amenazas CTI descriptivas permitirá un modelado preciso de las tácticas, técnicas y procedimientos (TTP) utilizados por adversarios en ciberataques en el contexto mexicano.

1.8.2.3 Recomendaciones Automatizadas para Reforzamiento de Ciberseguridad:

Se espera proporcionar recomendaciones específicas y automatizadas para reforzar las medidas de ciberseguridad en las organizaciones mexicanas, derivadas del análisis detallado de amenazas y eventos de ciberseguridad.

Estos alcances y contribuciones proporcionan un marco claro para la tesis doctoral, definiendo los límites de la investigación y destacando las áreas donde se espera aportar al conocimiento y la práctica de la ciberseguridad en México.

1.9 Organización del Documento

En este documento de investigación se organiza de la siguiente manera:

- En la sección 2 se presentan Antecedentes y Marco Teórico:
    - Sección 2.1 tiene como objetivo presentar la investigación del Estado actual de Ciberseguridad en México con el fin de obtener una perspectiva general de antecedentes e iniciativas de ciberseguridad en el territorio mexicano.
    - Sección 2.2 se presenta el Marco teórico de la CTI y se discuten los retos y oportunidades para las futuras investigaciones en esta área.
- Sección 3 tiene como contribución principal la recopilación e investigación de esquemas, métodos, herramientas y conjuntos de datos de CTI disponibles enfocado al territorio mexicano para el método propuesto.
- Sección 4 se presenta la Experimentación del método propuesto.
- Sección 5 se presentan los Resultados de la experimentación.
- Sección 6 se presentan la Discusión de la investigación.
- Sección 7 se presentan las Conclusiones de la investigación.
- Sección 8 se presenta el Trabajo futuro.
- Sección 9 se presentan los detalles del estudio en el Anexo

2 Marco Teórico

2.1 Antecedentes

En esta sección, se presenta una visión general de la situación actual de ciberseguridad en el territorio mexicano, en la cual se pretende abarcar los distintos artículos emitidos por consultorías en conjunto con el gobierno mexicano, así como estudios sobre diferentes sectores de la industria para tener un panorama amplio sobre la ciberseguridad actual en el país. Para este estudio, utilizaremos el termino Ciberseguridad y Seguridad de la Información definido por la a norma ISO/IEC 27032 [26] como la protección de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. Este último se caracteriza como un entorno complejo generado por la interacción entre personas, software y servicios a través de Internet, utilizando dispositivos tecnológicos y redes que están conectadas a este, y que carecen de una existencia física tangible.

2.1.1 Estado actual de la Ciberseguridad en México

México es una nación que experimenta un crecimiento continuo tanto en el ámbito industrial como tecnológico. Sin embargo, los temas emergentes en las recientes políticas industriales trascienden las áreas tradicionales de promoción, protección y regulación del sector industrial y de servicios.El Foro Consultivo Científico y Tecnológico [27] público un documento donde se abordan cuestiones como el uso eficiente de la energía y el desarrollo sostenible; la competitividad en los mercados nacionales e internacionales; la educación y capacitación; y la promoción de la investigación científica y el desarrollo tecnológico. [28]. Este documento también destaca que estos desarrollos en México se han caracterizado por un predominio del capital y la tecnología

extranjeros, con un bajo valor agregado nacional. A diferencia de países como China, Corea del Sur y la India, donde las empresas de capital nacional han co-invertido significativamente con compañías extranjeras y han desarrollado sus propias tecnologías y exportaciones (a excepción del sector minero en México), las empresas mexicanas no han seguido este modelo. Además, se plantea el considerable desafío que implica generar una economía exitosa que dependa únicamente de la inversión extranjera, estrategia que México y otros países latinoamericanos han adoptado en los últimos años.

La ciberseguridad en México es un tema que ha tomado mucha fuerza en los últimos años y es que los ciberataques que hemos enfrentado en los últimos años han tenido un impacto nacional importante y los medios cada vez le están tomando más valor a las noticias relacionadas con el Cibercrimen [29] [30] [31]. En resumen, el rápido desarrollo tecnológico afecta a todos los sectores en México, marcado por avances en tecnología, redes sociales, sistemas de información e internet, donde se registra una penetración del 71% entre la población de 6 años en adelante, sumando 79.1 millones de usuarios conectados. Como resultado, las empresas mexicanas han adoptado nuevos modelos de negocio, incluyendo el comercio electrónico, que ha mostrado un crecimiento notable: 8 de cada 10 usuarios de internet adultos realizaron al menos una compra en línea durante el último año. Es más, el 85% de estas compras se efectuaron a través de smartphones, mientras que 2 de cada 10 compradores ya hacen algunas compras mediante su Smart TV. Este sector alcanzó un valor de más de 491 mil millones de pesos, reflejando un crecimiento del 24% respecto al año 2017. [32]. Esto nos habla de la adopción y el constante uso de medios digitales para consumir un servicio o adquirir un producto en el territorio mexicano donde los usuarios de internet en México pasan diariamente 8 horas con 20 minutos, 8 minutos más que en 2018 [33].

Casi todos los aspectos de la vida cotidiana en el país dependen hoy en día del uso de las tecnologías de Información y Telecomunicaciones, las cuales favorecen y mejoran las vidas de los mexicanos, así como mejoran la productividad al poder mejora y automatizar procesos. Como evidencia de esto, se ha notado un crecimiento exponencial en el uso de dispositivos conectados a internet y se estima que para el 2025 existirán más de 300 millones de dispositivos con acceso a las redes en México, esto es un 70% más de los 180 millones que se documentan en el 2018 [18]. La creciente dependencia de las tecnologías de la información y el aumento acelerado de las amenazas cibernéticas, así como el Cibercrimen, han forzado a las empresas mexicanas del sector público y privado a incrementar sus inversiones y presupuestos en estrategias y controles de ciberseguridad con el objetivo principal de poder protegerse de estas amenazas que afectas la disponibilidad, confidencialidad e integridad de su información y su negocio. El sector financiero, es un sistema critico que tiene una alta dependencia de las tecnologías de la información, ya que sus transacciones entre clientes, otras instituciones como comercios y pagos electrónicos son realizados de manera digital y en el cual se han relazado estudios donde se muestra el impacto que ocurre en una empresa cuando es víctima de una amenaza cibernética [4]. Así mismo, diferentes sectores de la industria también han adoptado la tecnología como una herramienta del día a día para poder automatizar y optimizar muchos de sus procesos críticos donde hemos mencionado diversos artículos científicos, los cuales buscan poder mejorar su detecciones y proceso de respuestas a incidentes según su sector [2] [3].

En febrero del 2019, la Secretaria de Comunicaciones y Transportes (SCT) [34] en conjunto con la Organización de los Estados Americanos (OEA) [35] publicaron un estudio sobre los hábitos de los usuarios en ciberseguridad en México, en el cual se entrevistaron a más de 5mil personas que residen en diferentes estados de la república y en el cual se destaca el aumento anual de usuarios en internet de manera exponencial con un crecimiento del 2015 al 2016, fue de 4.7% y, del 2016 al 2017, fue de 8.1%. Donde se identifica el acceso libre a internet, así como las aplicaciones de dispositivos móviles para los menores de edad como una de las preocupaciones más importantes, ya que según el estudio solo el 45% de los adultos vigilan el contenido que visitan y/o consumen los menores de edad y el 37% declaro el uso de estos dispositivos y aplicaciones móviles como entretenimiento para sus hijos sin controlar el contenido o páginas con las que se relacionan mientras acceden a internet. Ante este crecimiento anual, se subraya la necesidad inmediata de implementar medidas de ciberseguridad en la vida cotidiana, dado que el estudio reveló que el 42% de los participantes admitió no revisar los permisos que las aplicaciones solicitan antes de instalarlas. Además, más del 20% reconoció haber sido víctima de fraudes financieros a través de medios digitales, principalmente por correo electrónico[36]. Estos incidentes suelen involucrar técnicas como el Phishing, definido por la Policía Federal como una modalidad de estafa diseñada para obtener de manera fraudulenta datos sensibles como claves, números de cuentas bancarias, tarjetas de crédito e identidad personal[37].

En el documento emitido por la consultora McKinsey & Company en colaboración con COMEXI [18] se puntualizan los riesgos cibernéticos como una amenaza nueva que debemos afrontar. Así mismo, definen el concepto de “riesgos cibernéticos” como un conjunto de posibles afectaciones que las empresas, gobiernos y miembros de la sociedad podrían sufrir debido a una falla o vulneración de las tecnologías de información que utilizan día a día. Esto puede reflejarse en un impacto de pérdida económica, danos a la reputación de una empresa o persona, así como en la perdida de disponibilidad para brindar un servicio o en la toma de decisiones mal informadas. Estos pueden ocurrir de diversas maneras, como un error del sistema o vulnerabilidad de este, alguna falla causada accidentalmente o error de configuración, sin embargo, las mayores afectaciones suelen surgir por un ciberataque dirigido ya sea por un actor externo o algún actor interno de la empresa. Se define el termino de ciberataque como un intento no autorizado por alguna vía digital para acceder a un sistema, información y/o recurso con el fin de exfiltrar la información, comprometerla, afectar su disponibilidad hasta llegar a extorsionar a usuarios y organizaciones y corresponde a la materialización de una o varias amenazas cibernéticas.

2.1.2 Cibercrimen en México

Como se ha mencionado a lo largo de este documento, en los últimos años la evolución y dependencia tecnológica a nivel global ha tenido un crecimiento acelerado, el cual si bien nos brinda muchas ventajas, también conlleva riesgos por el uso cotidiano de la tecnología y la información que ingresamos para poder utilizarla, por ejemplo, una aplicación para ir al cine, comprar despensa o comida o transporte, puede pedir información personal y financiera para poder utilizarla e inclusive permisos de administrador en tu dispositivos, acceso a tu localización, fotos y demás, otro ejemplo es el uso exponencial de las redes sociales, las cuales al día de hoy se estima que un usuario promedio en México invierte hasta 8 horas conectado a internet [33] y usa más de 3 redes sociales (Facebook, Twitter, Instagram, twitch, tiktok, etc.) en el día. Esto sumado

a la falta de medida de seguridad por parte de los usuarios al entrar a sitios desconocidos o instalar aplicaciones sin leer o entender los permisos o riesgos que conllevan, aumenta el riesgo de alguna contraer una infección y esparcían de algún tipo de amenaza informática dentro de sus dispositivos que puede desencadenar un delito cibernético teniendo como víctima algún usuario o institución.

El termino Cibercrimen o delito cibernético es una forma de delincuencia que utiliza tanto el internet o tecnología como medio para cometer algún acto ilícito que pueda perjudicar la integridad, confidencialidad o disponibilidad. Algunos problemas relacionados con este tipo de delitos son: fraude, secuestros de información (Ransomware), Phishing, distribución de malware, ataques de Denegación de Servicio Distribuido (DDoS), piratería, explotación infantil, robo de información y/o suplantación de identidad así como violaciones de la privacidad cuando la información confidencial se pierde o es robada se vuelven cada vez más comunes en nuestra sociedad y esto ha alertado a los gobiernos y organizaciones a nivel global para aumentar sus inversiones en controles de ciberseguridad para hacerle frente. De acuerdo con la clasificación internacional generalmente aceptada, presentamos algunos de los términos y definiciones de amenazas cibernéticas definidas por NIST [38].

Amenazas Cibernéticas	Descripción
Malware	El término simplificado para "malicious code" es "código malicioso", que se refiere a cualquier software diseñado para ejecutar procesos no autorizados que afecten negativamente la confidencialidad, integridad o disponibilidad de un sistema de información. Dentro de esta categoría, los tipos más comunes incluyen
Virus	Un virus informático es una sección oculta y autorreplicante de software que se propaga infectando otros programas, es decir, insertando una copia de sí mismo en ellos y convirtiéndose en parte de estos. Un virus no puede operar de manera independiente; necesita que el programa anfitrión se ejecute para activarse.
Spyware	El software espía es un tipo de programa que se instala de manera secreta o subrepticia en un sistema de información con el objetivo de recopilar datos sobre individuos u organizaciones sin su consentimiento o conocimiento. Este software monitorea y recoge información variada que puede incluir hábitos de navegación, datos personales y credenciales de acceso.
Adware	El adware es un tipo de software que, tras ser instalado en una computadora o durante el uso de una aplicación, reproduce, muestra o descarga automáticamente material publicitario. Este programa malicioso está específicamente diseñado para mostrar anuncios no deseados en la computadora de la víctima sin su consentimiento. Los anuncios, como pop-ups, son incontrolables y tienden a comportarse de manera errática, apareciendo repetidamente y dificultando su cierre.
Rootkit	Un rootkit es un conjunto de herramientas que un atacante utiliza después de obtener acceso de nivel de raíz o administrador en un sistema informático. Su principal función es ocultar las actividades del atacante dentro del sistema y permitirle mantener el acceso de nivel de raíz de manera oculta. Esencialmente, un rootkit facilita que un pirata informático acceda o controle un dispositivo informático o una red de forma remota sin ser detectado. Los rootkits son particularmente difíciles de identificar porque pueden activarse incluso antes de que se inicie el sistema operativo del sistema, integrándose profundamente en el mismo y eludiendo así muchas formas de detección convencional.
Trojan Horse	Un troyano es un tipo de programa informático que se presenta como una aplicación útil o legítima, pero que en realidad posee funciones ocultas y potencialmente maliciosas. Estos programas son diseñados para evadir los mecanismos de seguridad, aprovechando en ocasiones las autorizaciones legítimas del usuario que ejecuta el programa. A través de esta doble funcionalidad, los troyanos pueden realizar actividades dañinas sin ser detectados, como el robo de datos o la instalación de software malicioso adicional.
Worm	El término simplificado para "write once, read many" se refiere a un gusano informático. Este es un tipo de código malicioso que opera de forma independiente, es decir, no necesita adjuntarse a un programa anfitrión para su ejecución o propagación. Un gusano tiene la capacidad de replicar una versión completa de sí mismo y dispersarse a otros hosts o redes. Además, puede consumir recursos de un sistema informático de manera significativa y potencialmente destructiva. En esencia, es un programa malicioso que se copia a sí mismo y se propaga a otras computadoras, sistemas o redes sin intervención directa del usuario.
Ransomware	Es un ransomware, un tipo de virus que restringe el acceso a los archivos o programas del usuario, exigiendo un pago de "rescate" para su eliminación. Este pago suele requerirse a través de métodos de

Amenazas Cibernéticas	Descripción
	pago en línea. Una vez que se realiza el pago, se promete al usuario la restauración del acceso a su sistema y archivos, aunque no siempre se garantiza que esto ocurra.
Keylogger	Es un keylogger, un tipo de software diseñado específicamente para registrar las pulsaciones que se realizan en el teclado de una computadora. Este programa captura de manera encubierta toda entrada desde el teclado, incluyendo contraseñas, claves de cifrado y otros datos sensibles, sin el conocimiento o consentimiento del usuario.
Botnet	Es una botnet, una red de dispositivos infectados con software malicioso, como un virus. Los atacantes pueden controlar estos dispositivos de manera colectiva y remota, sin el conocimiento de sus propietarios, para potenciar la magnitud de sus ataques cibernéticos. Comúnmente, las botnets se utilizan para ejecutar ataques de denegación de servicio distribuido (DDoS), con el fin de sobrecargar y desestabilizar sistemas específicos.
Phishing	El phishing es una técnica de engaño utilizada para obtener información confidencial, como números de cuentas bancarias y credenciales de acceso, mediante solicitudes fraudulentas. Estos intentos de estafa suelen realizarse a través de correos electrónicos o sitios web falsificados, donde los perpetradores se hacen pasar por entidades legítimas o individuos de confianza. Esta táctica busca engañar a las víctimas para que divulguen información sensible bajo la falsa impresión de que están interactuando con una fuente legítima.
Man-in-the-middle attack (MitM)	Un ataque de intermediario o "Man-in-the-Middle" (MitM) ocurre cuando un atacante intercepta y modifica la comunicación entre dos partes sin que estas lo sepan. En este tipo de ataque, el perpetrador se hace pasar por cada una de las víctimas, manipulando la conversación para obtener acceso a información confidencial. Los usuarios involucrados en la comunicación no son conscientes de que sus intercambios están siendo controlados y alterados por un atacante en lugar de estar ocurriendo directamente entre ellos.
Distributed denial-of-service attack (DDoS)	Un ataque de denegación de servicio (DoS) consiste en inundar sistemas, servidores o redes con un flujo excesivo de tráfico para consumir sus recursos y ancho de banda. Esto provoca que los sistemas afectados se vuelvan incapaces de procesar y responder a solicitudes legítimas. En una variante más compleja, denominada ataque de denegación de servicio distribuido (DDoS), los atacantes utilizan múltiples dispositivos previamente comprometidos para ejecutar el ataque simultáneamente desde varios puntos, intensificando significativamente su impacto y dificultad para ser mitigado.
SQL injection	Un ataque de inyección SQL ocurre cuando un atacante introduce código malicioso en un servidor que opera con SQL (Structured Query Language). Estos ataques solo resultan exitosos si hay vulnerabilidades de seguridad en el software de la aplicación que está siendo atacada. Un ataque de inyección SQL exitoso puede forzar al servidor a proporcionar acceso no autorizado o a modificar datos sensibles, comprometiendo así la integridad y seguridad de la base de datos.
Zero-Day attack	Un ataque de día cero se refiere a la explotación de una vulnerabilidad en hardware o software que no se conocía previamente. Este tipo de ataque se hace posible, en parte, debido al uso de software obsoleto o no actualizado, lo cual deja abiertas brechas de seguridad que los atacantes pueden explotar. Una vulnerabilidad de día cero puede surgir cuando la información sobre una falla de seguridad se hace pública antes de que el desarrollador tenga la oportunidad de crear y distribuir un parche o solución. Esto pone en riesgo significativo la seguridad de los sistemas afectados hasta que se aborde el problema.

Tabla 1. Descripción de Amenazas Cibernéticas [38]**.**

El Cibercrimen se ha convertido en uno de los temas de seguridad más importantes que continuará surgiendo como un problema critico en los próximos años. Entre los diferentes ataques, el uso de técnicas para explotar una vulnerabilidad es de especial interés debido a su impacto negativo para la economía. En la última década, el crimen cibernético se ha transformado de un crimen de bajo volumen a un crimen de alto volumen. Durante ese tiempo, los perpetradores han cambiado de individuos especializados a atacantes expertos que han establecido estructuras organizadas para llevar a cabo algún ciberataque estructurado. Así mismo, los ataques cibernéticos son considerados unas de los riesgos de mayor impacto en los próximos años según el "Informe de Riesgos Globales 2019", que expone los hallazgos de la más reciente "Encuesta de percepción de riesgos globales", en la que aproximadamente 1,000 líderes y tomadores de decisiones de diversos sectores, incluidos el público, privado, académico y la sociedad civil, evalúan y clasifican los riesgos que enfrenta el mundo. [39].

En México se han realizado emitido diversos estudios relacionados con Cibercrimen, en el cual se explica que este fenómeno se ha convertido en algo mucho más complejo y de mayor impacto, donde se estima que más del 80% de las empresas mexicanas son víctimas de ciberataques por lo menos una vez al año, lo que posiciona a México como uno de los 10 países con mayor cantidad de intentos de ciberataques y amenazas cibernéticas a nivel global [40]. En 2017, 33 millones de mexicanos experimentaron algún tipo de amenaza cibernética relacionada con el cibercrimen, lo que representa un incremento del 50% en comparación con 2016. Esto significa que uno de cada cuatro habitantes del país fue afectado. Adicionalmente, el impacto económico de estos crímenes se estima en aproximadamente 7.7 mil millones de dólares, lo cual supone un aumento del 40% respecto al año anterior [18], siendo el comportamiento humano (negligencia o actos mal intencionados de los trabajadores) uno de los principales factores de estos riesgos cibernéticos.

En México, se ha observado un incremento en las amenazas cibernéticas que han impactado diversos sectores industriales en los últimos años. Un ejemplo significativo ocurrió en 2016, cuando se comprometió una base de datos del Instituto Nacional Electoral (INE) alojada en la nube de Amazon Web Services (AWS). Este incidente resultó en la exposición de datos personales de más de 93.4 millones de ciudadanos mexicanos. [15]. Otro caso en 2018 donde se dio a conocer que algunos ciber atacantes vulneraron algunos sistemas de instituciones financieras que interactuaban con el Sistema de Pagos Electrónicos (SPEI), el cual tuvo como consecuencia el robo y perdida aproximada de 300 millones de pesos desde destinas locaciones, en el cual los atacantes crearon cuentas falsas para enviar instrucciones de pago fraudulentas mediante un código malicioso engañando a las instituciones financieras para enviar las transacciones el Banco de México a través del SPEI como ocurre habitualmente. En consecuencia, de esto, diversas empresas fueron afectadas, como es el caso de AXA Seguros, quien reporto inconsistencias relacionadas con el sistema de pagos y su área operativa declaro que el ataque fue a sus sistemas de conexión con la plataforma SPEI ocasionando una pérdida económica aproximada de 57 millones de pesos [16] [17].

Como se detalla en el documento de McKinsey & Company en colaboración con COMEXI [18] existen grupos autodenominados como hacktivistas con el propósito de realizar un ciberataque con el objetivo principal de realizar una declaración o protesta política hacia un gobierno o institución. En el año 2012 el grupo Ciber Protesta Mexicana llevo a cabo un ciberataque simultaneo, en donde por lo menos en 10 sitios web de gobierno, partidos políticos y prensa se publicaron mensajes de protesta. Este grupo, que ya había atacado de manera similar en 2009, posicionó su ciberataque como una protesta pacífica ante la situación política del país, en el que sus actividades han llegado a ser notas de carácter global [19]. En México, durante el cuarto trimestre de 2019, los fraudes cibernéticos aumentaron un 36% en comparación con el mismo periodo del año anterior, representando un monto aproximado de 11,171 millones de pesos. De esta cantidad, solo el 45% fue reembolsado a los usuarios afectados. Según un informe de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), elaborado a partir de las reclamaciones monetarias presentadas por los clientes de la banca mexicana y contenidas en el Reporte Regulatorio R27 de la CNBV, 86 de cada 100 fraudes cibernéticos fueron resueltos favorablemente para los usuarios afectados. [20].

De acuerdo con varios estudios elaborados desde 2019 por Fortinet y sus laboratorios de investigación FortiGuard [41], México es el país que presenta el mayor número de ataques cibernéticos en América Latina. Esto representa un gran reto para los usuarios y las empresas mexicanas que día a día enfrentan esta nueva ola de delitos digitales.

2.1.3 Iniciativas de Ciberseguridad en México

Aunque distintos organismos pueden implementar iniciativas de ciberseguridad de forma independiente, la organización e integración de estos esfuerzos requiere de un organismo que los pueda gestionar adecuadamente. Ante esto, en 2017, el gobierno de México emitió La Estrategia Nacional de Ciberseguridad [21]. Este documento establece la visión del Estado mexicano en materia de ciberseguridad, tomando en consideración la relevancia de las tecnologías de la información y comunicación (TIC), los riesgos asociados a su uso y los ciberdelitos, así como la imperiosa necesidad de fomentar una cultura general de ciberseguridad. El objetivo principal de esta estrategia es identificar y definir las acciones de ciberseguridad necesarias en los ámbitos social, económico y político, que permitan a la ciudadanía y a las organizaciones públicas y privadas utilizar y aprovechar de manera responsable las TIC, promoviendo el desarrollo sostenible del Estado mexicano.

Por otro lado, el marco legal mexicano también tipifica el ciberdelito aunque de manera desconcentrada, sin embargo, existe un marco legal para la protección de datos personales por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) [42], la cual especifica en el Articulo 7 .- La obtención de datos personales no debe realizarse mediante medios engañosos o fraudulentos, tal como lo establece la ley en su Artículo 20, que dicta que cualquier vulneración de seguridad ocurrida en cualquier fase del tratamiento de los datos, y que afecte de manera significativa los derechos patrimoniales o morales de los titulares, deberá ser informada de forma inmediata por el responsable al titular. Esto tiene como propósito permitir que el titular tome las medidas necesarias para la defensa de sus derechos. Asimismo, el Artículo 58 establece que los titulares que consideren haber sufrido un daño o perjuicio en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en la presente ley por parte del responsable o encargado, podrán ejercer los derechos que consideren pertinentes para obtener la indemnización correspondiente, conforme a las disposiciones legales aplicables. También se cuenta con Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) [43] la cual contiene temas específicos sobre temas tecnológicos, computo en la nube y seguridad especificado en el Articlu0 3.- Las medidas de seguridad técnicas se definen como un conjunto de acciones y mecanismos que emplean tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. En concordancia con lo estipulado en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), el Artículo 19 establece que el responsable no debe obtener ni tratar datos personales mediante medios engañosos o fraudulentos, priorizando siempre la protección de los intereses del titular y respetando su expectativa razonable de privacidad.

Estos marcos legales tienen como objetivo fundamental que toda entidad que maneje datos personales implemente y mantenga medidas de seguridad administrativas, técnicas y físicas que

protejan la información personal frente a daños, pérdidas, destrucción, uso, acceso o tratamiento no autorizado. Además, se especifican obligaciones de confidencialidad que detallan los casos específicos en los que se puede compartir información privada con otras entidades, así como las precauciones que deben tomarse durante dichas transacciones.

Para la implementación de estas medidas de seguridad, los responsables deben tener en cuenta los riesgos existentes, las posibles consecuencias para los titulares de los datos y el desarrollo tecnológico disponible. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) desarrolla y publica materiales de apoyo para ayudar a las organizaciones a cumplir con sus responsabilidades en el manejo de datos personales. Cabe destacar que cualquier organización que no se apegue a este marco legal está sujeta a sanciones; sin embargo, estas pueden ser atenuadas si se demuestra que la organización siguió las recomendaciones del INAI.

Cabe recalcar que un ciberataque no está contemplado como delito en la legislación de nuestro país, es decir, solo los que son considerados delitos informáticos, ya que no se cuenta con una legislación en materia de ciberseguridad, por ejemplo, el robo de redes inalámbricas (Wifi) no es considerado un delito informático, sin embargo, existen algunas que pueden ser denunciadas, por ejemplo, el robo de datos e información personal o el acoso cibernético [44] [45]. En respuesta a los crecientes desafíos en el ámbito digital, el Gobierno del Estado de México, a través de la Secretaría de Seguridad del Estado de México, creó la Unidad de Prevención e Investigación Cibernética, también conocida como la Policía Cibernética. Su principal objetivo es prevenir, atender y combatir delitos que se cometen a través de medios digitales, tales como fraudes, extorsión, robo de identidad, explotación sexual, acoso, maltrato animal, y la venta de sustancias prohibidas y armas, entre otros. Esta unidad opera las 24 horas del día, los 365 días del año, y se organiza en tres áreas clave: Atención Ciudadana y Patrullaje Cibernético, Laboratorio Tecnológico y Prevención de Delitos Cibernéticos, brindando así una respuesta integral a las amenazas digitales en la región. [46].

Por otro lado, En México, algunas de las principales universidades, ya ofrecen carreras o programas educativos en ciberseguridad (p.ej., UNAM, ITAM, ITESM, IPN, UNITEC). Cabe destacar que Universidad Autónoma de Nuevo León (UANL) ofrece la Licenciatura en Seguridad en Tecnologías de la Información en la cual se han realizado acuerdos con la firma de ciberseguridad Fortinet para incluir su programa Fortinet Network Security Academy (FNSA), el cual proporciona a las instituciones académicas (escuelas secundarias, colegios y universidades y organizaciones sin fines de lucro / ONG enfocadas en la preparación profesional), con los recursos necesarios para facilitar el plan de estudios de certificación reconocido por la industria de Fortinet.

2.1.3.1 La adhesión al Convenio de Budapest en México

El convenio de Budapest se trata de un tratado internacional que fue firmado en la ciudad con el mismo nombre en 2001 y que entró en vigor en 2004. Con este tratado, se busca que los Estados que se adhieran al convenio puedan lidiar con la variedad de delitos informáticos que han existido y que existirán con el continuo avance de la tecnología, tomándolas en consideración en sus leyes e investigaciones, así como fomentar la cooperación entre las naciones en la lucha contra los delitos

informáticos; en este convenio se trata especialmente con temas de derechos de autor, de fraude informático, de pornografía infantil y con la transgresión de la seguridad de las redes de computadoras [47].

Una invitación a adherirse al convenio también ha sido extendida a todos los Estados que no son miembros del Consejo de Europa, por lo que cualquier país puede aprovechar lo establecido en el convenio para combatir la ciberdelincuencia, adaptándolo a sus sistemas legales y estrategias nacionales. Dentro del convenio, se establecen artículos sobre las acciones que deben tomar las naciones para que puedan adherirse al tratado y ratificarlo. Estos artículos abordan los diferentes aspectos de la ciberdelincuencia, cada uno de ellos representando la naturaleza del delito informático del que se habla, así se pueden apoyar las naciones en estos artículos para aplicar las medidas necesarias para adaptarlos a sus propios ordenamientos jurídicos.

Como tratado internacional "modelo", los artículos previstos en el convenio de Budapest poseen descripciones más generales con respecto a lo que se considera como delito cibernético. Por sí solo, se puede ver como una guía de política penal que puede usarse para empezar a tomar decisiones en la búsqueda de tipificar los delitos informáticos en materia penal y que se promueva la cooperación con otros países que también han tomado acciones para su adhesión al convenio [47]; con la adhesión al mismo tratado internacional, las definiciones de delitos informáticos mantendrían un grado de homogeneidad que les facilitará a los países la cooperación que se busca al momento de implementar medidas para perseguir los delitos cuando se vea necesario la intervención de dos o más Estados.

México es uno de los países que poseen el estatus de "observador" del convenio de Budapest. Desgraciadamente, a pesar de que el país ha solicitado su ingreso en 2006, no se ha completado su adhesión al convenio. Desde 1999, ya se habían empezado a llevar a cabo reformas al Código Penal Federal para la introducción de los delitos informáticos en materia penal, pero no se han hecho los esfuerzos necesarios para traducir todas las disposiciones del convenio al ordenamiento jurídico del país. Se han realizado intentos para apelar a la Secretaría de Relaciones Exteriores a tomar acciones que encaminen a la adhesión apropiada de México al convenio de Budapest; las proposiciones han intentado exhortar respetuosamente a la SRE, dando a entender la importancia de que el país se encuentre mejor preparado en temas legales y de cooperación internacional para hacer frente a los crímenes cibernéticos que se encuentran en alza con el pasar de los años y con el avance tecnológico que lleva consigo tanto beneficios como amenazas que puedan provocar un impacto negativo en el país [48]. Aun así, en México hoy en día no se ha podido completar la adhesión a este tratado.

En México, los tratados internacionales en materia de derechos humanos son considerados al mismo nivel que cualquier ley federal y pueden ser aplicados inmediatamente al ordenamiento jurídico del país. Sin embargo, algunos de los tratados internacionales requieren que las naciones realicen modificaciones a la legislación actual, no pueden simplemente adherirse a lo que dicen exactamente, sino que debe existir una revisión y adecuación apropiada de las disposiciones del tratado a lo que se encuentra actualmente en el país, ya sea creando una ley específica que cubra los delitos cibernéticos o modificando las leyes existentes.

Otro reto con la aplicación de este convenio en México es el principio de exacta aplicación. El convenio de Budapest presenta las definiciones de delitos informáticos de manera ambigua e imprecisa, dejando que los Estados que busquen perseguir la adhesión al tratado los definan bajo su propia discreción; un ejemplo de esto es en el uso de la palabra "ilegitimo", que no posee una definición clara de lo que puede ser considerada como tal en el convenio. Ni siquiera se especifican las sanciones punibles que deberían de aplicarse. En el Código Penal Federal se indica que las conductas no tipificadas por la legislación nacional pueden ser perseguidas si lo están en tratados internacionales. Aun si México alcanzara la adhesión al convenio de Budapest, una mala implementación puede llevar a que estos delitos sean perseguidos por medio de protocolos que puedan llegar a ser arbitrarios y/o abusivos o puede resultar en que no se persigan los delitos porque no se adecuan al principio de exacta aplicación. Para que México pueda implementar efectivamente el convenio, deberá de decidirse si esto se logrará mediante una nueva ley que se utilice específicamente para temas de delitos informáticos o si se aprovecharan las leyes ya existentes. Por un lado, una ley especial podría facilitar el establecimiento de las disposiciones actuales y nuevas al encontrarse en un mismo lugar; por otro lado, modificar leyes existentes puede facilitar su adoptación por parte de quienes ya poseen experiencia con respecto a la legislación actual

2.1.4 Leyes y Regulaciones Actuales en México

2.1.4.1 Código Penal Federal

El Código Penal Federal [49] que se establecen las características de un delito, tipifica las conductas que son consideradas como delitos en el país y contiene las sanciones que serán aplicables para cada uno. La legislación, publicada originalmente el 14 de agosto de 1931, ha sido objeto de múltiples reformas a lo largo de los años. A partir de 1999, se comenzaron a tipificar delitos informáticos como el acceso ilícito a sistemas y equipos de informática, la revelación de secretos, delitos relacionados con los derechos de autor, la violación de correspondencia y los ataques a las vías de comunicación, entre otros. No obstante, a pesar de estos avances, la ley aún no tipifica de manera más precisa y completa algunos delitos informáticos, lo que deja ciertas conductas sin clasificar adecuadamente, mientras que otras siguen siendo consideradas como delitos tradicionales. Esta falta de actualización integral puede resultar en la falta de sanción efectiva para diversas formas de delincuencia informática.

2.1.4.2 Ley Federal de Protección de Datos Personales en Posesión de Particulares

El 5 de julio de 2010, se publicó la Ley Federal de Protección de Datos Personales en Posesión de Particulares [50] con el objetivo de salvaguardar los datos personales durante su recolección, uso, divulgación o almacenamiento por parte de personas físicas (individuos) o morales (empresas privadas) como parte de sus actividades comerciales y servicios ofrecidos a los titulares de dichos datos. Esta ley establece los principios fundamentales para la protección de los datos personales, así como las normas y obligaciones de los particulares en relación con su tratamiento. Además, tipifica como delitos ciertas conductas relacionadas con la protección de datos personales, tales como provocar una vulneración de seguridad y obtener datos personales mediante engaños.

2.1.4.3 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [51]. La ley, promulgada el 26 de enero de 2017, tiene como objetivo garantizar la protección de los principios y derechos relacionados con los datos personales en posesión de los sujetos obligados, es decir, aquellos organismos y autoridades que forman parte de los poderes legislativo, ejecutivo y judicial de la nación. Esta legislación establece los principios y deberes que deben seguir los sujetos obligados para salvaguardar la privacidad de los titulares de los datos personales que administran, asegurando el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO).

Además, la ley exige que los sujetos obligados sean transparentes con los titulares sobre los datos personales que recopilan y su tratamiento, de manera que los titulares estén debidamente informados y puedan otorgar su consentimiento con la confianza de que sus datos serán utilizados exclusivamente para los fines especificados y estrictamente necesarios para las operaciones y servicios proporcionados por dichos sujetos.

En lo que respecta al tratamiento de datos personales, los sujetos obligados deben implementar medidas de seguridad técnicas, físicas y administrativas adecuadas para proteger los datos contra cualquier daño, pérdida, alteración, destrucción o uso no autorizado, garantizando así la integridad y confidencialidad de la información bajo su control.

2.1.4.4 Ley Federal de Protección de Propiedad Industrial

Esta ley fue publicada el 1 de julio de 2020 y tiene por objeto promover las actividades inventivas de carácter industrial y proteger la propiedad industrial en el país [52]. La propiedad intelectual protegida por esta ley incluye los secretos industriales, refiriéndose a la información confidencial que es utilizada por alguna persona para tener una ventaja competitiva y que debe de ser resguardada para mantener su confidencialidad. La importancia de la protección de secretos industriales recae en la búsqueda por impulsar las innovaciones. Debido a la cantidad significativa de recursos que están dirigidos al desarrollo de invenciones que aporten mayor competitividad en el mercado, las organizaciones necesitan asegurar que dichas invenciones estén salvaguardadas de aquellos que busquen utilizarlos sin autorización y que esto impacte en su capacidad para seguir compitiendo dentro su área de negocio. Con esta protección, las empresas pueden seguir innovando en nuevas tecnologías que tengan una aplicación industrial. En la misma ley se declara delito el revelar y el obtener o realizar un uso indebido de secretos industriales sin consentimiento de quien está autorizado para aprovechar el secreto.

2.1.4.5 Ley de Instituciones de Crédito

Esta ley fue publicada el 18 de julio de 1990, tiene como fin la regulación de servicios bancarios y crediticios que sean prestados por aquellas instituciones de crédito que obtienen fondos o recursos de personas para ofrecer productos y servicios [53]. Dentro de esta ley se encuentran sanciones para conductas consideradas como delito en el artículo 122 Bis, una de ellas es aplicable a delitos informáticos en el que se lleva a cabo el robo y el uso indebido de instrumentos de pagos (tarjetas de crédito, tarjetas de débito, entre otros) y la información contenida en ellos por medios electrónicos; bajo el mismo artículo, esto puede considerarse para los casos de robo de identidad

haciendo uso de los instrumentos de pago y la información contenida en ellos para hacerse pasar por la víctima del robo.

2.1.4.6 Circular 14/2017

La circular 14-2017 [54] se refiere a un conjunto de reglas que son aplicables al uso del Sistema de Pagos Electrónicos Interbancarios (SPEI) en México, un sistema para transferencias electrónicas de fondos administrado por el Banco de México. Aquí se detallan los requisitos y las obligaciones relacionadas con las operaciones y servicios a través de SPEI. Dentro de esta Circular también se establecen reglas que deben de cumplir los Participantes para ofrecer operaciones y servicios a través de SPEI en materia de seguridad de la información, incluyendo el establecimiento de medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información de los Clientes, cumplir con requerimientos de seguridad para programas informáticos proporcionados por los Participantes y proteger las transferencias hechas a través de la infraestructura tecnológica que realiza operaciones por medio de SPEI.

2.1.4.7 Disposiciones de carácter general aplicables a las instituciones de crédito

La Comisión Nacional Bancaria y de Valores [55]. Se ha emitido una compilación de todas las disposiciones de carácter general aplicables a las instituciones de crédito, con el fin de proporcionar un único marco jurídico que permita a dichas instituciones adherirse a las regulaciones vigentes. Dentro de estas disposiciones, las instituciones de crédito están obligadas a implementar planes, procedimientos y medidas en materia de seguridad de la información. Entre estos se incluye la elaboración de un Plan Director de Seguridad, el uso de identificadores de usuario y factores de autenticación para validar la identidad de los usuarios, así como la implementación de controles de seguridad que aseguren la confidencialidad, integridad y disponibilidad de la información y los sistemas que la procesan.

2.1.4.8 NMX-COE-001-SCFI-2018

Como parte de las actividades en comercio electrónico, es necesario contar con una regulación para asegurar que las organizaciones con actividades comerciales puedan aplicar las medidas que correspondan para poder utilizar los medios electrónicos apropiadamente, asegurando al mismo tiempo la seguridad de la información.

Para esto, el 30 de abril del 2019 se publicó en el Diario Oficial de la Federación la NMX- COE-001-SCFI-2018 [56], Este marco regula las actividades relacionadas con el comercio electrónico en los Estados Unidos Mexicanos, mediante varias disposiciones que deben ser seguidas tanto por personas físicas como morales involucradas en la compra y venta de productos y servicios a través de medios electrónicos. El objetivo principal es proteger los intereses de las empresas y los usuarios del comercio electrónico, proporcionando los requisitos y mejores prácticas que los responsables de portales, aplicaciones o sitios web donde se realicen transacciones comerciales deben implementar como parte de sus operaciones.

Estas disposiciones incluyen la implementación de medidas técnicas, físicas y administrativas adecuadas para proteger los equipos de cómputo, servidores e infraestructura de red involucrados

en las transacciones comerciales. Además, exigen el cumplimiento de estándares de seguridad de la industria y la protección de los sistemas de información, plataformas de medios de pago y las conexiones asociadas a estas actividades, garantizando la integridad y seguridad de las transacciones realizadas electrónicamente.

2.1.4.9 NormaOficialMexicanaNOM-151-SCFI-2016

Con la existencia de medios electrónicos para almacenar, transmitir y procesar información, así como de facilitar su acceso y utilización, la digitalización de información almacenada en medios físicos resulta de gran importancia, sobre todo en un mundo digital en el que se tiene la habilidad de acceder a una gran variedad de información. En el caso de documentos, su digitalización permite que las organizaciones sean capaces de acceder y gestionar a ellas de manera más fácil y rápida cuando se necesita como parte de sus procesos y operaciones que requieren la disponibilidad de esta información. También permite ahorrar en medios físicos como el papel para el almacenamiento de la información, facilita la creación de respaldos y la implementación de medidas de seguridad como la encriptación para asegurar que están protegidas de accesos y alteraciones no autorizadas. Además, cuando se trata de regulaciones respecto a la preservación y retención de datos, la digitalización facilita a las organizaciones su cumplimiento con dichas regulaciones.

Con el fin de regular la conservación de mensajes de datos y la digitalización de documentos, se ha creado la Norma Oficial Mexicana NOM-151-SCFI-2016. Esta norma establece los requisitos específicos que deben cumplirse para garantizar la autenticidad, integridad y conservación de los mensajes de datos y documentos digitalizados. Entre otras disposiciones, la norma se enfoca en asegurar que los documentos electrónicos puedan ser preservados de manera segura, evitando su alteración no autorizada, y proporcionando un marco regulatorio que permita su uso como prueba en procedimientos legales o administrativos [57].Contiene métodos que deben utilizarse para conservar mensajes de datos y digitalizar documentos de manera que la información siga siendo veraz, completa e inalterada.

2.1.4.10 NMX-I-27001-NYCE-2015

Para que las organizaciones puedan proteger adecuadamente sus activos más importantes, es fundamental que consideren seriamente la seguridad de la información. No es suficiente con la simple implementación de controles; es necesario contar con el respaldo de la alta dirección, establecer políticas claras de seguridad de la información, definir roles y responsabilidades dentro de la organización, y llevar a cabo un proceso integral de administración de riesgos. Estos aspectos permiten asegurar que la seguridad se gestione a lo largo de toda la estructura organizacional.

Con el fin de proporcionar una guía clara para que las organizaciones puedan tomar decisiones adecuadas al implementar un sistema de gestión de seguridad de la información adaptado a sus necesidades y contexto, el 14 de abril de 2015 se publicó en el Diario Oficial de la Federación

[58] una norma mexicana que detalla los requisitos para la implementación de dicho sistema. Esta norma permite a las organizaciones desarrollar políticas, procesos y tecnologías pertinentes para

proteger su información. Asimismo, el documento incluye un apéndice en el que se enumeran objetivos de control y controles correspondientes, que pueden ser utilizados para la implementación de medidas de seguridad destinadas a gestionar los riesgos de seguridad de manera efectiva.

Cada objetivo de control está asociado a un dominio específico de la seguridad de la información, abarcando áreas como seguridad en las comunicaciones, políticas de seguridad, controles de acceso, seguridad en las operaciones, continuidad del negocio, entre otros, sumando un total de 14 dominios clave. Esta estructura facilita a las organizaciones la implementación de un enfoque integral y coherente en la gestión de la seguridad de la información.

2.1.5 Ciberseguridad en el Sistema Financiero Mexicano

Los riesgos cibernéticos para el sistema financiero a nivel global siguen siendo un tema de gran relevancia, dado el creciente aumento en la frecuencia y sofisticación de los ciberataques. Un ataque exitoso contra una institución financiera podría tener repercusiones significativas en los servicios financieros de un país, además de minar la confianza de los clientes en dichos servicios. En respuesta a esta amenaza, tanto las instituciones como las autoridades financieras han implementado diversas medidas para monitorear los riesgos y amenazas en materia de ciberseguridad, tanto en México como a nivel internacional. En particular, con el incremento de los conflictos geopolíticos, se ha prestado especial atención a los riesgos que pueden comprometer la ciberseguridad de los sistemas financieros, ya que estos podrían derivar en eventos que afecten infraestructuras críticas a través de ataques cibernéticos.

En México, se han acordado recientemente estrategias específicas de ciberseguridad tanto para el sector financiero como para el país en general. Esto se debe, en parte, a que en 2017 México ocupó la séptima posición entre los 20 mercados más importantes del mundo en términos de adopción de empresas Fintech, definida como la proporción de la población adulta que ha utilizado al menos dos servicios de empresas Fintech en los últimos seis meses [59]. Este crecimiento ha contribuido a hacer del sector financiero mexicano un espacio más eficiente e inclusivo en comparación con años anteriores. Sin embargo, el surgimiento de nuevas industrias, como la Fintech, también ha incrementado el riesgo de ciberataques en el sector financiero

Frente al acelerado aumento de los ciberataques, en octubre de 2017 se celebró el Foro de Ciberseguridad titulado "Fortaleciendo la Ciberseguridad para la Estabilidad del Sistema Financiero Mexicano" [60]. Este foro reunió a autoridades, representantes de instituciones financieras, y expertos tanto nacionales como internacionales, con el objetivo de analizar las mejores prácticas internacionales para fortalecer las medidas de ciberseguridad. Asimismo, el evento sirvió para establecer una agenda común, coordinar esfuerzos entre las autoridades y el sector privado, y divulgar los Principios para el Fortalecimiento de la Ciberseguridad con miras a garantizar la estabilidad del sistema financiero mexicano [61]:

1. **Adoptar y mantener actualizadas políticas y controles**: Las organizaciones deben establecer y revisar continuamente sus políticas, métodos y controles de ciberseguridad para identificar, evaluar, prevenir y mitigar los riesgos emergentes. Estas políticas deben ser aprobadas por los órganos de mayor autoridad dentro de la organización y aplicarse en todos los niveles, asegurando una cultura integral de seguridad.

2. **Intercambio seguro de información**: Es esencial crear mecanismos seguros para el intercambio de información entre las entidades financieras y las autoridades sobre ataques cibernéticos en tiempo real, incluyendo sus modos operativos, estrategias de respuesta y nuevas amenazas. Estos mecanismos permiten a las organizaciones anticiparse y mitigar riesgos de ciberataques, garantizando la confidencialidad de la información compartida.
3. **Actualizar marcos regulatorios y legales**: Se deben promover iniciativas que actualicen los marcos legales y regulatorios para apoyar y coordinar los esfuerzos de todas las partes involucradas. Esto debe incluir las mejores prácticas internacionales y acuerdos que fortalezcan las capacidades de respuesta ante ciberamenazas.
4. **Colaboración para fortalecer infraestructuras**: Es fundamental trabajar en conjunto para fortalecer los controles de seguridad en infraestructuras críticas y plataformas operativas del sistema financiero. Esto implica aprovechar la tecnología para prevenir, detectar, reaccionar y comunicar ante amenazas presentes y futuras, además de unificar esfuerzos en la lucha contra el cibercrimen.
5. **Fomentar la cultura de ciberseguridad**: Se debe promover una cultura de ciberseguridad tanto entre los usuarios finales como dentro del personal de las instituciones. La capacitación continua es clave para reducir los riesgos de ciberataques, asegurando que todos los participantes comprendan su rol en la protección de la información y los sistemas.

Sin embargo, la Comisión Nacional Bancaria de Valores (CNBV) en colaboración con la Organization of American States (OAS) [62] revelaron que el 100% de las entidades e instituciones financieras mexicanas afirman que identificaron algún tipo de evento de seguridad digital, es decir, ataques exitosos y/o ataques fallidos que intentaron vulnerarlos. Los eventos de seguridad digital más comúnmente identificados durante 2018 fueron, malware con un 56%, Phishing dirigido con un 47% y violación de políticas de seguridad con un 31%. Así mismo, se destaca que el 19% de las entidades e instituciones financieras identifican diariamente la ocurrencia de eventos de algún tipo de amenaza cibernética, teniendo en cuenta que uno de los principales motivos por los que se llevan a cabo ataques a este sector en específico son por razones económicas principalmente. Así mismo, en este estudio se mencionan que las principales acciones de ciberseguridad realizadas por las instituciones financieras mexicanas consisten en implementaciones de controles como firewalls (85%), consolas automatizadas de antimalware (76%), respaldos automatizados (68%) y seguridad en la red (VPN, NAC, ISE, IDS / IPS, filtrado web, correo electrónico seguro, etc.) (54%). Por los tanto podemos asumir que existe una gran oportunidad de desarrollo en el área de investigación y desarrollo en campos tecnológicos y de ciberseguridad en el territorio mexicano.

Con el propósito de fortalecer las capacidades de las instituciones financieras para enfrentar incidentes cibernéticos, en septiembre de 2023 se llevó a cabo un ejercicio de ciberresiliencia en el que participaron el Banco de México y cinco instituciones financieras de importancia sistémica local. Durante el ejercicio se evaluaron las habilidades de los participantes para identificar, contener, investigar y remediar un ciberataque. Los resultados demostraron que las instituciones financieras cuentan con protocolos claros de respuesta, abordando la ciberresiliencia desde una perspectiva multidisciplinaria, con un enfoque en garantizar la continuidad de los servicios a sus clientes.

Por otro lado, se identificaron áreas de mejora en cuanto a la coordinación y comunicación entre instituciones, con el objetivo de fortalecer la respuesta conjunta del sector y no solo de manera individual. El Instituto Central se compromete a continuar promoviendo este tipo de ejercicios, con el fin de mejorar las capacidades de respuesta del sector financiero mexicano frente a diversos incidentes cibernéticos que puedan afectar distintos procesos del Banco de México.

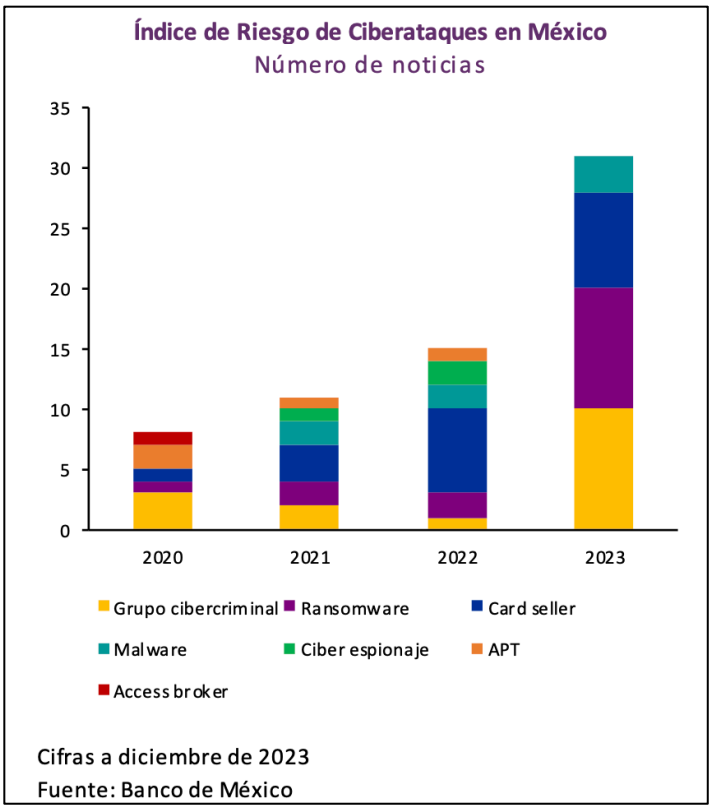


Figura 1. Numero de noticias de Ciberataques en México [63].

El Índice de Riesgo de Ciberataques en México106 (Gráfica 143) reveló que, durante 2023, las amenazas cibernéticas más frecuentes fueron: la actividad de grupos cibercriminales, el secuestro de datos (Ransomware) y la venta de información de tarjetas bancarias (Card Seller). Es importante destacar que la actividad de los grupos cibercriminales representó el mayor incremento del año, con un notable aumento en los intentos de vulnerar los sistemas de seguridad del sistema financiero, extendiendo sus ataques a corresponsales, comisionistas y clientes corporativos de las instituciones de crédito. Por otro lado, el Ransomware presentó la segunda tasa de crecimiento más significativa en comparación con el año anterior, principalmente debido al aumento de ataques dirigidos a la infraestructura tecnológica de la banca en línea, sucursales, transferencias electrónicas y cajeros automáticos de algunas entidades financieras.

2.2 Inteligencia Contra Amenazas Cibernéticas (CTI)

Ante el crecimiento acelerado de los ciberataques, así como el desarrollo constante y uso de nuevas plataformas digitales, las organizaciones enfrentan retos más complejos cada día a la hora de monitorear sus información, es decir, cada aplicación, dispositivo o proceso que interactúa con la tecnología genera información digital que está a su vez, representa un evento (log) en un sistema que los analistas de ciberseguridad deberían tomar en cuenta para monitorear cualquier tipo de actividad sospechosa. Sin embargo, como hemos mencionado anteriormente, el constante uso, evolución y dependencia de la tecnología ha dado como resultado una cantidad impresionante de información, entre ellas posibles amenazas que en muchos casos supera la capacidad de análisis de los especialistas, esto puede llegar a tener consecuencias graves en la organización, ya que

corren el riesgo de omitir dicha información o catalogarla como ruido. Así mismo, las amenazas cibernéticas se están tornando cada vez más complejas, desarrollando nuevas formas de vulnerar los sistemas utilizando nuevas técnicas, así como la facilidad de uso de herramientas que le permiten a cualquier usuario el poder generar este tipo de amenazas con muy poco esfuerzo y causar un gran impacto. Ante esto, el reto principal radica en poder transformar toda esta información en algo accionable que pueda utilizarse para tomar decisiones para la alta dirección. Por ejemplo, el poder priorizar actividades, asignar presupuesto o personal en base a los impactos que se pueden llegar a tener basado en los datos recolectados. Esto requiere no solo de tiempo y/o esfuerzo del equipo de TI o ciberseguridad, sino también de organización, colaboración entre las distintas áreas, experiencia y recursos asignados por la alta dirección para realizar estas investigaciones con éxito. Esto nos lleva a lo que se denomina Inteligencia Contra Amenazas Cibernéticas o Cyber Threat Intelligence (CTI), la cual se define [64] La inteligencia de amenazas se refiere al conocimiento basado en evidencia que incluye el contexto, mecanismos, indicadores, implicaciones y recomendaciones prácticas sobre una amenaza o riesgo, ya sea existente o emergente, dirigido a activos críticos. Este conocimiento se utiliza para informar y guiar las decisiones con respecto a la respuesta ante dicha amenaza. Por otro lado, SANS [65] define la inteligencia contra amenazas (CTI, por sus siglas en inglés) como la información analizada sobre las capacidades, oportunidades e intenciones de los adversarios, la cual satisface los requisitos específicos establecidos por una parte interesada.

Sin embargo, uno de los puntos principales que se necesita comprender en este ámbito, es la diferencia entre datos, información e inteligencia para comprender la CTI. Por lo tanto, podemos definir a los datos como un elemento individual que contiene información ya sea de un sistema, acción o proceso ejecutado, es decir, elementos individuales con un significado especifico. Por otro lado, podemos definir el termino amenaza como el posible peligro que puede utilizarse para explotar una vulnerabilidad existente con la intención de causar daños a los sistemas, redes u organizaciones enteras.

Diferencias entre datos, información e inteligencia
Los datos consisten en hechos discretos y estadísticas recopiladas como base para análisis posteriores.
La información son múltiples puntos de datos combinados para responder preguntas específicas.
La inteligencia analiza datos e información para descubrir patrones e historias que informan la toma de decisiones.

Tabla 2. Diferencias entre Datos, Información e Inteligencia [66]**.**

Estos tres términos a veces se usan sin mucha atención según el Dr. Christopher Ahlberg [66], Este enfoque explica que algunos *feeds* de amenazas se presentan como inteligencia, cuando en realidad son simplemente conjuntos de datos. A menudo, las organizaciones integran estas fuentes de datos en sus redes, solo para descubrir que no tienen la capacidad de procesar el gran volumen de información adicional, lo que genera una mayor carga para los analistas, quienes deben clasificar y priorizar las amenazas. En contraste, la inteligencia de amenazas alivia esa carga al ayudar a los analistas a determinar qué debe ser priorizado y qué puede ser ignorado. Por esta razón, es fundamental distinguir entre los términos datos, información e inteligencia en el contexto de la ciberseguridad.

Ciberseguridad: datos, información e inteligencia
Los datos suelen ser solo indicadores como direcciones IP, URL o hashes. Los datos no nos dicen mucho sin análisis.
La información responde preguntas como, "¿Cuántas veces se ha mencionado a mi organización en las redes sociales este mes?" Aunque este es un resultado mucho más útil que los datos sin procesar, todavía no informa directamente una acción específica.
La inteligencia es el producto de un ciclo de identificación de preguntas y objetivos, recopilación de datos relevantes, procesamiento y análisis de esos datos, producción de inteligencia procesable y distribución de esa inteligencia.

Tabla 3. Ciberseguridad en datos, información e inteligencia [66]**.**

Por lo tanto, la CTI (Inteligencia contra Amenazas) puede definirse como la capacidad de adquirir conocimiento detallado sobre una empresa, organización o país, así como sobre sus condiciones y capacidades, con el fin de anticipar posibles acciones de actores maliciosos o amenazas que podrían explotar vulnerabilidades críticas existentes. Esta disciplina no opera de manera aislada, sino que se apoya en diversas áreas de la seguridad de la información, como la inteligencia de amenazas, la gestión de vulnerabilidades, la administración de configuración de seguridad y la respuesta a incidentes. Además, emplea un conjunto de herramientas y técnicas para recopilar información a través del monitoreo continuo y la generación de informes. El objetivo es proporcionar a los tomadores de decisiones, a todos los niveles, información clave que les permita priorizar la asignación de recursos y mitigar los riesgos de manera eficiente.

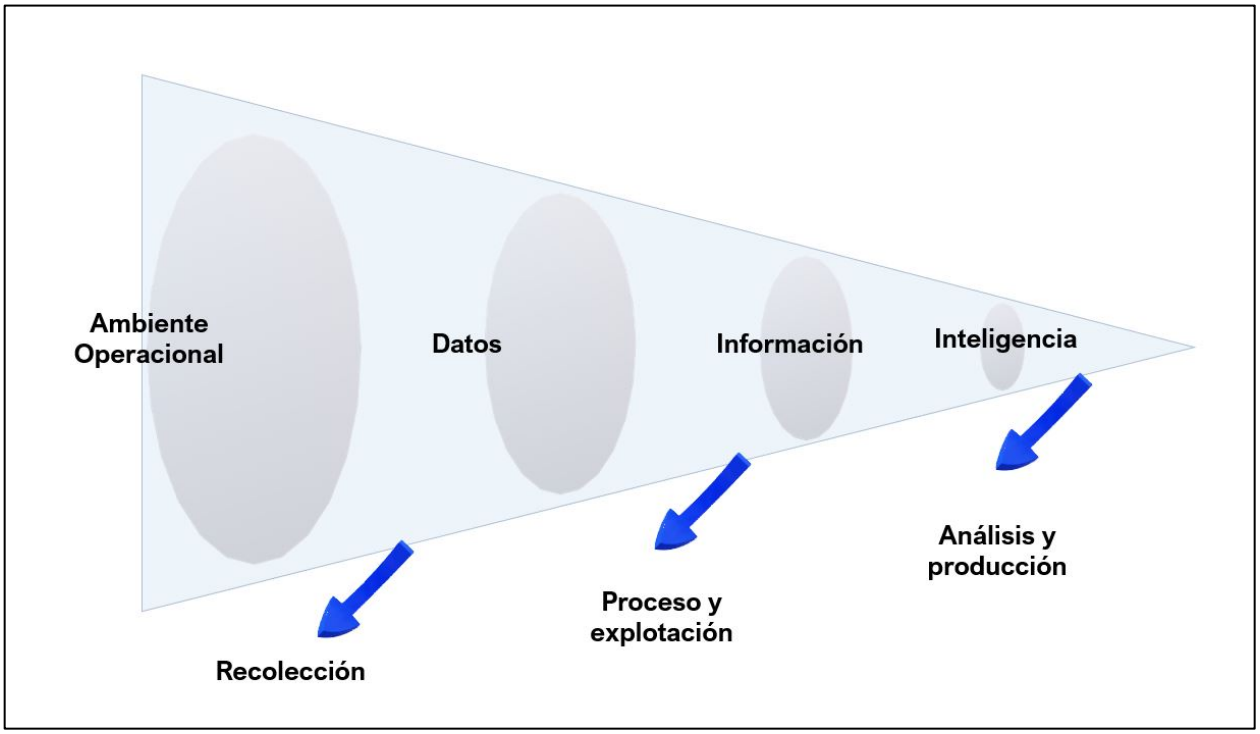


Figura 2. Relación entre datos, información e inteligencia [66]**.**

2.2.1 El ciclo de vida de Inteligencia

Independientemente de si una organización produce y / o consume inteligencia, se requiere un

proceso para pasar de la identificación de las preguntas que deben responderse utilizando inteligencia de amenazas a acciones que beneficien las defensas de una organización. Según SANS [65], para muchas organizaciones, ese proceso es una versión del ciclo de inteligencia clásico. El ciclo de Inteligencia es un proceso para generar información precisa y accionable para la organización [65]. Este, comienza con una fase de planificación, en la que se generan las preguntas o requisitos de inteligencia que deben responderse. Cuando se conocen los requisitos, la siguiente fase es la recopilación, la recopilación de datos para ayudar a responder las preguntas y cumplir con los requisitos. La siguiente fase es el procesamiento, donde los datos se ponen en un formato utilizable para su análisis. Esto lleva a la cuarta fase, el análisis, en el que se sintetizan los datos para identificar las respuestas a los requisitos de inteligencia. La última fase es la difusión, donde los hallazgos se capturan en el formato correcto para llegar a la audiencia prevista descrita en la fase de planificación. Es importante tener en cuenta que, si bien el ciclo de inteligencia es un proceso cíclico, a veces es necesario retroceder en el proceso; por ejemplo, si durante la fase de análisis se determina que se necesita información adicional o si la información debe procesarse en un formato diferente, es importante volver al paso anterior apropiado para que el resultado final sea un hallazgo analítico informado y preciso.

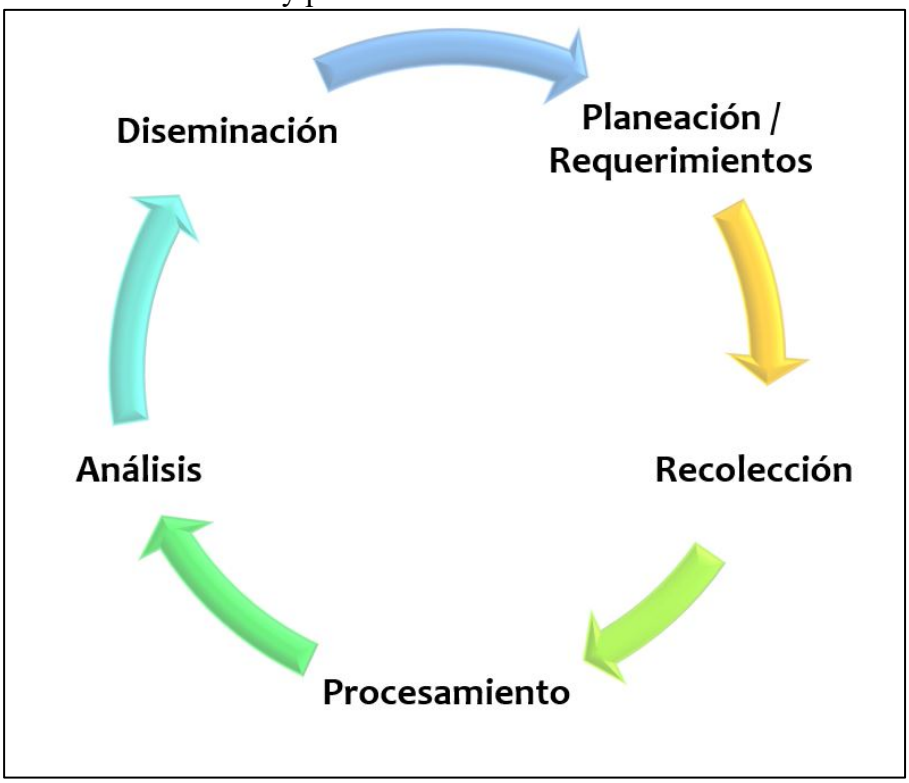


Figura 3. El Ciclo de vida de Inteligencia [65].

2.2.1.1 Planificación y dirección

Esta categoría incluye la recepción, identificación y priorización de los requisitos de inteligencia; el desarrollo de conceptos de operaciones y arquitecturas de inteligencia; asignar elementos de inteligencia apropiados para la recopilación de información o la producción de inteligencia completa; y enviar solicitudes de recopilación, explotación o apoyo de producción de

todas las fuentes a entidades de inteligencia de apoyo externas.

2.2.1.2 Colección

Incluye aquellas actividades relacionadas con la adquisición de datos necesarios para satisfacer requisitos específicos. Esto es administrado por administradores de cobranza, cuyas funciones incluyen seleccionar los activos disponibles más apropiados y el procesamiento, explotación y difusión (PED, por sus siglas en inglés) asociados y luego asignar los activos seleccionados y PED asociados para llevar a cabo misiones de cobranza.

2.2.1.3 Procesamiento y Explotación

Los datos recibidos inicialmente del sensor llegan en varias formas, dependiendo de la naturaleza del dispositivo sensor. Dependiendo de la fuente, la entrada sin procesar puede ser en forma de datos digitalizados, transmisiones de voz ininteligibles o grandes archivos digitales que contienen imágenes de la Tierra sin rectificar. Esta recopilación de resultados se convierte mediante medidas de procesamiento específicas del sensor en información visual, auditiva o textual que es inteligible para los humanos, y luego puede ser utilizada por analistas de inteligencia y otros consumidores. La conversión de datos puede automatizarse mediante fusión algorítmica, señalización, análisis de datos y explotación automatizada. La explotación implica la posterior traducción y contextualización de la información resultante de la recopilación y el procesamiento inicial en un producto que el planificador, el tomador de decisiones o el analista de inteligencia pueden asimilar cognitivamente.

2.2.1.4 Análisis y producción

Durante el análisis y la producción, la inteligencia se produce a partir de la información recopilada por las capacidades de recopilación y del refinamiento y compilación de la inteligencia recibida de organizaciones externas. Toda la información procesada disponible se integra, evalúa, analiza e interpreta para crear productos que satisfagan a los solicitantes o usuarios.

2.2.1.5 Difusión y retroalimentación

Esta categoría implica la distribución oportuna de información crítica e inteligencia completa, fácilmente accesible por el usuario, al consumidor apropiado.

- **El formato correcto:** elija presentar su inteligencia en un formato que sus partes interesadas puedan consumir y comprender. Por ejemplo, es posible que no necesite incluir todo lo que descubrió para la toma de decisiones, así que trabaje en resumir la información.
- **Las manos adecuadas:** la inteligencia solo se puede aplicar cuando está disponible para las personas adecuadas. Asigne tipos de inteligencia no solo a los títulos de trabajo, sino también a las responsabilidades del equipo.
- **El momento adecuado:** incluso la inteligencia más relevante puede volverse inútil si está desactualizada. Esto significa que debe equilibrar el tiempo que llevará producir inteligencia con cualquier acción que deba realizarse.

- **El medio correcto:** no es solo lo que comunica, sino cómo. Elija métodos de comunicación que lleguen a sus partes interesadas relevantes de la manera más rápida y efectiva.

Entonces, como ejemplo de dónde y cómo la inteligencia realmente agrega valor a la organización, básicamente, nos dará visibilidad. Permitirá que el analista de inteligencia de amenazas agregue valor muy rápidamente, información oportuna, información procesable, que se pueda alimentar a los equipos de defensa a lo largo de los diversos roles dentro de la organización y a las personas de operaciones de TI para ejecutar y configurar cualquier control necesario para disminuir el riesgo de una incidencia y/o amenaza cibernética. Por lo tanto, las organizaciones que cuentan con procesos de CTI se centran en comprender las amenazas cibernéticas que enfrentan con el objetivo principal de proporcionar información de valor y accionable para ayudar a defenderse de esas amenazas que ponen en riesgo la información de la organización.

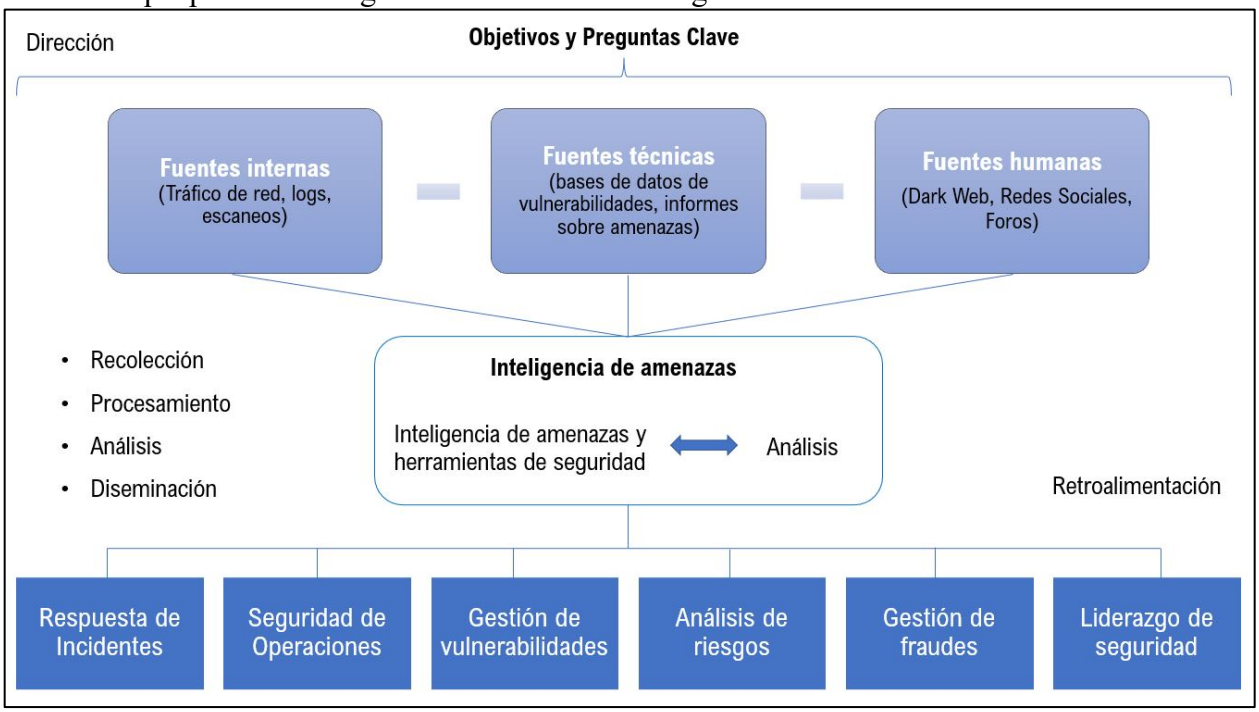


Figura 4. Inteligencia de amenazas y las seis fases del ciclo de inteligencia [66]**.**

Para poner eso en un formato diferente, comenzamos con nuestros objetivos y nuestras preguntas clave y eso a su vez se alimenta de varias cosas como, fuentes internas, fuentes técnicas y por supuesto, fuentes humanas. Por lo tanto, algunos de ellos pueden ser automatizados, otros pueden ser a través de la intervención manual, así como hablar con otros analistas también para ver lo que está sucediendo en su espacio o en su parte del mundo, etc. Todas estas cosas, nuevamente, están alimentadas con inteligencia de amenazas en sí y las diversas herramientas de seguridad, como las herramientas de SIEM, Firewalls, Honeypots, etc.; y eso irá de un lado a otro. Esas dos cosas se alimentan entre sí a partir de estas diferentes fuentes y nos aseguramos de que comencemos por comprender qué es lo que estamos tratando de lograr. ¿Cuáles son nuestras metas y objetivos clave, etc.? Entonces, todo eso se da vuelta y alimenta a los equipos reales que saldrán y utilizarán esa información para defender la organización e información crítica de la misma. Los equipos de respuesta a incidentes, podrían ser operaciones de seguridad, así como también podrían ser un

equipo de gestión de vulnerabilidades, un equipo de análisis de riesgos o tal vez un equipo de gestión de fraudes y por supuesto, un liderazgo en seguridad. Hablamos sobre los diferentes equipos, por qué eso es importante y por qué necesitan esa información. Comenzando con la defensa de la red, las personas que están en primera línea de defensa se aseguran de que estas amenazas se mitiguen tanto como sea posible o se corrijan lo más rápido posible antes de que lleguen a infiltrarse en la organización y afecten algún activo sensible. Los equipos de operaciones de seguridad, gestión de vulnerabilidades, parches, etc., hasta el liderazgo de seguridad deben siempre estar informados y listos para que cuenten con los datos adecuados para tomar decisiones informadas sobre dónde invertir tiempo, recursos, dinero, infraestructura, etc.

2.2.2 Fuentes de Datos y Tipos de Inteligencia

Como se ha mencionado anteriormente, la clave para poder realizar un buen proceso de CTI consiste en definir las fuentes para la recopilación de información, es decir, una vez identificados los requisitos, el siguiente paso es identificar cómo obtener acceso a la información que ayudará a responder a los requisitos. Dichas fuentes de información se les denominan Feeds de inteligencia, los cuales emiten información relevante para los analistas que pueden consumir de distintas formas. En este mismo artículo, SANS muestra cuales son las fuentes de inteligencia que más consumen las organizaciones para poder realizar CTI:

Sources for Gathering Intelligence	2020
Open source or public CTI feeds (DNS, MalwareDomainList.com)	74.30%
Threat feeds from CTI-specific vendors	68.90%
Threat feeds from general security vendors	68.50%
Community or industry groups such as information sharing and analysis centers (ISACs) and Computer Emergency Readiness Teams (CERTs)	68.20%
Security data gathered from our IDS, firewall, endpoint and other security systems	63.40%
External sources such as media reports and news	63.10%
Incident response and live forensics	63.10%
SIEM platform	62.00%
Vulnerability data	60.60%
Network traffic analysis (packet and flow data)	57.00%
Forensics (postmortem)	56.40%
CTI service provider	45.90%
Application logs	44.40%
Other formal and informal groups with a shared interest	43.30%
Closed or dark web sources	42.10%
Honeypots data	29.90%
Shared spreadsheets and/or email	21.00%
Other	1.50%

Tabla 4. Sources for Gathering Intelligence [65]**.**

Esta definición puede explicarse con un ejemplo desde la perspectiva del análisis de incidentes cibernéticos de tal manera que los datos pueden ser tales como la IP, el dominio, la URL o el correo electrónico que se pueden recopilar de los sistemas o fuentes de información abiertas en internet como Google. Además, la información puede describirse como la URL explotada para el Phishing, el dominio que difunde el código malicioso y la IP que establece la comunicación C&C con el código malicioso [67]. La CTI es el resultado del análisis integral que informa que un grupo de

ciberdelincuentes tiene como objetivo vulnerar principalmente a entidades financieras, y recientemente se descubrió que el código malicioso era una variante de alguna amenaza antes vista. Por lo tanto, se requieren acciones para bloquear la dirección IP del servidor de C&C frecuentemente utilizado por el código malicioso.

Existen distintos tipos de herramientas que pueden brindar información muy relevante a las organizaciones en cuanto a Feeds para CTI, las cuales tienen como objetivo el poder realizar las fases de inteligencia mencionadas, para entregar información ya procesada a las organizaciones con el objetivo principal de compartir información, estudios y hallazgos de ciberseguridad para ayudar a las organizaciones a proteger su información y minimizar el riesgo de una vulneración. Ante esto, las organizaciones y/o compañías dedicadas a la ciberseguridad han adoptado el uso de CTI en sus sets de herramientas y se complementan con productos o servicios que proporcionan información ya digerida o consumible de CTI [68] [69] [70], inclusive plataformas de redes sociales como Facebook a lanzado su proyecto ThreatExchange [71] para compartir información sobre CTI, así como se han realizado estudios relacionados con la extracción de CTI mediante Twitter [72] [73].

Las fuentes de datos de amenazas son flujos de información en tiempo real que proporcionan datos sobre posibles riesgos y amenazas cibernéticas. Por lo general, estas fuentes consisten en listas de indicadores o artefactos simples que se centran en una única área de interés. Ofrecen una visión rápida y actualizada del panorama de amenazas. Sin embargo, muchas de estas fuentes pueden estar saturadas de errores, redundancias y falsos positivos, lo que puede dificultar su utilidad. Por ello, es fundamental seleccionar fuentes de datos de alta calidad que sean precisas y confiables, para que los equipos de seguridad puedan tomar decisiones informadas y eficaces. [74]. Algunos criterios para evaluar la calidad de la fuente de datos son:

- Fuente sea relevante a la industria a la que pertenece su organización
- Exista transparencia de las fuentes
- Alto porcentaje de datos únicos
- Buscar una periodicidad de los datos adecuada y relevante para su organización
- Asegurarse de obtener resultados medibles.

2.2.2.1 Fuentes de Datos

La inteligencia puede ser generada de una amplia variedad de fuentes [75] como lo son: i) fuentes internas; ii) fuentes externas. Las fuentes externas a su vez se dividen en i) fuentes externas observables; e ii) fuentes abiertas de inteligencia u OSINT por sus siglas en ingles [76].

La información puede presentarse de forma estructurada o no estructurada. Las fuentes estructuradas, como los datos obtenidos de bases de datos de vulnerabilidades, son técnicas y organizadas, lo que las hace fácilmente analizables y procesables por computadoras, permitiendo un tratamiento rápido y sencillo. Por otro lado, las fuentes no estructuradas incluyen información generada a través del lenguaje natural, como discusiones en foros. Estas requieren el uso de procesamiento de lenguaje natural (NLP) y técnicas de aprendizaje automático para transformar

los datos en inteligencia útil, debido a su complejidad y falta de estructura clara.[75].

2.2.2.2 Fuentes Internas

Las fuentes internas son eventos observables que han ocurrido en la red interna y los dispositivos de la organización, como lo son las computadoras, servidores y dispositivos móviles. El análisis de estos eventos ayuda a construir indicadores sobre amenazas que por ejemplo hayan violado el perímetro de seguridad, hayan violado las reglas de control de acceso interno, hayan infectado un sistema o que hayan intentado acceder a un sistema restringido. Por otro lado, el análisis estadístico de los datos permite crear una línea base de comportamiento, por lo que cualquier anomalía es relativamente fácil de identificar e investigar.

Las fuentes internas que generan estos datos pueden provenir de dispositivos como, por ejemplo:

- los registros y eventos de los sistemas
- eventos de la red interna como las conexiones y accesos a dispositivos
- utilización de la red y perfil del tráfico
- alertas de dispositivos perimetrales como lo son los IPS y Firewalls
- Alertas generadas por el Anti-Virus. Pero también del personal interno, por ejemplo: i) Observación de anomalías o eventos por parte del personal; y ii) análisis forense de un evento. [76]

2.2.2.3 Fuentes externas observables

Las fuentes externas observables pueden provenir de i) fuentes patrocinadas por organizaciones gubernamentales; ii) La misma industria; y iii) fuentes comerciales de proveedores de seguridad. Estas fuentes consisten en datos maliciosos observados, como lo son: i) direcciones IP de un atacante; ii) dominio y URL maliciosa; iii) nombres de archivo y su hash.

Uno de los principales usos de este tipo de información es generar reglas de seguridad para los dispositivos de seguridad perimetral como lo son los IPS (Sistemas de Prevención de Intrusos) y los Firewalls, para los dispositivos de red como ruteadores y dispositivos finales como lo son los servidores.

2.2.2.4 Inteligencia de fuentes externas de código abierto

Estas fuentes ayudan a comprender el panorama de amenazas, los motivos que tienen los atacantes y los vectores de ataque que utilizan. Algunos ejemplos de este tipo de fuentes son: Es decir, ayudan a conocer al atacante y por supuesto son usualmente datos no estructurados. Ejemplos típicos de este tipo de datos son: un anuncio de una gran fuga de datos que compromete los datos del usuario que podrían usarse para acceder a otros sistemas o un ataque de Phishing.

Algunas fuentes de este tipo de datos pueden ser:

i) Noticias

ii) Vulnerabilidades
iii) Buscadores como Google dorks y Shodan
iv) Información publicada por proveedores de antivirus
v) Redes sociales como Twitter
vi) La red oscura o Dark web.

2.2.2.5 La red oscura (Dark Web)

Se puede recopilar inteligencia operativa y estratégica muy valiosa sobre ataques específicos, TTP de atacantes, objetivos políticos de hacktivistas y grupos de atacantes, y otros temas clave al infiltrarse o irrumpir en canales privados de comunicación utilizados por grupos de amenazas. [74] Sin embargo, acceder a la red oscura no es fácil, presenta barreras como lo son lograr el acceso, entender el idioma y las maniobras de obstrucción de los propios grupos. Para superar estas barreras se requiere de inversión en herramientas y conocimiento en monitoreo de canales privados.

2.2.3 Tipos de Inteligencia contra amenaza

Los tipos más comunes de inteligencia contra amenaza incluyen indicadores, tácticas, técnicas y procedimientos, alertas de seguridad, reportes y herramientas de configuración [77].

Indicadores. Los indicadores son artefactos técnicos u observables que proporcionan evidencia de que un ataque es inminente, está en curso o ya ha sido ejecutado, lo que indica que un elemento de la red ha sido comprometido. Estos indicadores se utilizan como herramientas clave para detectar y defenderse de posibles amenazas, permitiendo a los equipos de seguridad identificar patrones de ataque y tomar medidas preventivas o correctivas de manera oportuna.

Tácticas, Técnicas y Procedimientos o TTP por sus siglas en ingles. Ayudan a describir el comportamiento de un atacante. Las tácticas describen el comportamiento del atacante a alto nivel, las técnicas es la explicación detallada de una táctica y los procedimientos describen a un nivel aún más detallado el contexto de una técnica. Los TTP ayudan a conocer a un atacante y predecir sus tendencias y preferencias de ataque, sus métodos de entrega y los exploits que utiliza.

Alertas de seguridad. Los boletines y notas de vulnerabilidad son notificaciones técnicas concisas que, en su mayoría, contienen información no estructurada sobre vulnerabilidades, exploits y otros problemas de seguridad actuales. Estos documentos brindan actualizaciones rápidas y relevantes para que los equipos de seguridad estén informados sobre amenazas emergentes y puedan tomar medidas preventivas o correctivas con prontitud.

Reportes de inteligencia contra amenazas. Los documentos en prosa describen tácticas, técnicas y procedimientos (TTP), actores maliciosos, tipos de sistemas afectados y la información que estos actores intentan comprometer, entre otros detalles relevantes sobre amenazas. Estos documentos proporcionan a las organizaciones una mayor conciencia situacional. Un reporte de inteligencia procesa datos en bruto, los analiza, genera interpretaciones a partir de ellos y los enriquece con contexto adicional, facilitando así la toma de decisiones informadas para mejorar la postura de

seguridad de la organización.

Configuración de herramientas. Estas son recomendaciones diseñadas para la configuración y uso adecuado de herramientas o mecanismos que faciliten la recopilación, el intercambio, el procesamiento, el análisis y la utilización automatizada de información sobre amenazas. Estas directrices tienen como objetivo optimizar la eficiencia y efectividad de los procesos relacionados con la inteligencia de amenazas, permitiendo una respuesta más rápida y precisa ante posibles riesgos de seguridad.

2.2.4 Subdominios de la inteligencia contra amenazas

Hemos identificado que hoy en día, la etapa de recolección de información puede ser complicada, ya que existe una amplia y variada fuente de información, para generar inteligencia, las cuales generan grandes volúmenes de información. Posteriormente a la recolección, se deben ejecutar diversas actividades para su procesamiento y análisis, así como enriquecerla con contexto y enfocarla a la audiencia objetivo.

Por las razones anteriores es de mucha utilidad generar divisiones para administrar mejor la información recopilada y enfocar los esfuerzos. Una forma simple de división es dividir la inteligencia de acuerdo con el nivel de audiencia a la que va enfocada.

El autor del libro “Threat mitigation and detection of cyber warfare and terrorism activities” [78], Maximiliano Korstanje, hace una división de inteligencia contra amenazas de cuatro dominios:

i) Inteligencia Estratégica
ii) Inteligencia Operativa
iii) Inteligencia Táctica
iv) Inteligencia Técnica

2.2.4.1 Inteligencia Estratégica.

La inteligencia estratégica va enfocada a los tomadores de decisiones. El objetivo es ayudar a los estrategas a entender los riesgos actuales y futuros. Ayuda a entender el posible impacto financiero de un ataque, a entender las tendencias de los ataques, los datos históricos o las predicciones sobre la actividad de la amenaza. Como resultado, los estrategas pueden:

i) Tomar decisiones mejor informadas
ii) Priorizar riesgos
iii) Hacer las inversiones adecuadas
iv) Enfocar al equipo
v) Establecer la defensa adecuada.

Con la finalidad de mitigar o eliminar el riesgo identificado. La información se presenta en forma de reportes ejecutivos, sesiones informativas o conversaciones con lenguaje de negocio, evitando

el lenguaje técnico [75].

La inteligencia estratégica se enfoca en información sobre características comunes de atacantes y las tácticas, técnicas y procedimientos que utilizan en sus métodos de ataque. La información estratégica nos permite realizar acciones mucho más cercanas al origen de los ataques. A este nivel de estrategia, se busca en lugar de bloquear una dirección IP o bloquear acciones de un botnet. Se busca aprender de los atacantes y generar indicadores estratégicos que apoyen la toma de decisiones de los responsables de la seguridad en la organización [79].

La CTI a nivel estratégico proporciona a las organizaciones información crucial para contestar el ¿Quién? Y el ¿Por qué? Su objetivo es identificar quién está detrás de una amenaza específica o una familia de amenazas, al tiempo que afronta las tendencias actuales. Busca el ¿por qué una organización es el objetivo de un ataque?, ¿por qué un actor cibernético malicioso (MCA) o grupo se encuentra interesado en una organización o industria?

Los usuarios de la inteligencia estratégica contra amenazas son personas del nivel "C": CEO, CFO, CIO, etcétera. En otras palabras, este personal son los ejecutivos de alto nivel, los líderes y la administración de una organización. Ellos consumen información para respaldar sus necesidades al tomar decisiones basadas en riesgos con respecto a la dotación de personal, las tecnologías, los requisitos de ciberseguridad y, en última instancia, los presupuestos.

2.2.4.2 Inteligencia operativa

La información sobre ataques inminentes específicos contra la organización es crítica y suele ser consumida inicialmente por personal de seguridad de alto nivel. Esta inteligencia permite a los responsables de la seguridad anticipar cuándo y dónde podrían ocurrir los ataques, facilitando una respuesta proactiva y fortaleciendo la capacidad de la organización para mitigar o prevenir daños antes de que los ataques se materialicen[75]. En esta inteligencia se da contexto a los eventos identificados con los motivos, las capacidades y los vectores de ataque que utiliza un atacante. Lo que ayuda a entender como un atacante planea, conduce y mantiene una campaña de ataque.

La inteligencia contra amenazas operativa se enfoca en el ¿Cómo? Y en el ¿Dónde? El observar y analizar las tácticas, técnicas y procedimientos de los atacantes responde el ¿Cómo? Entender las TTPs ayuda a las organizaciones a entender el tamaño de una brecha y/o a preparar las medidas defensivas incluso antes de ser atacados. El dónde, ayuda a las organizaciones a conducir búsquedas de amenazas proactivamente, antes de que ocurra un compromiso o después de un incidente. Sin esta información sería como buscar una aguja en un pajar.

Algunos de los usuarios de la inteligencia operativa son: equipos y personal de respuesta a incidentes, defensores de la red, analistas de dispositivos, analistas de malware, analistas forenses y más. Ellos consumen la información para el contexto técnico, con un enfoque en sus propios indicadores de compromiso, los vínculos relacionados y si se pueden encontrar o no en los entornos que son responsables de proteger.

2.2.4.3 Inteligencia táctica.

La inteligencia táctica, también conocida como Tácticas, Técnicas y Procedimientos (TTP, por sus siglas en inglés), se refiere al análisis detallado de cómo los adversarios llevan a cabo sus ataques. Esta forma de inteligencia proporciona información sobre los métodos específicos que los actores maliciosos emplean para comprometer sistemas, desde las tácticas utilizadas para acceder a redes hasta las técnicas que aplican una vez dentro, y los procedimientos para mantener el acceso o exfiltrar datos. La inteligencia TTP es crucial para entender el comportamiento de los atacantes y mejorar las defensas de seguridad en función de sus patrones de ataque. [75]. Esta inteligencia es utilizada principalmente por el equipo de respuesta a incidentes, con el objetivo de garantizar que sus estrategias y métodos defensivos estén alineados y preparados para contrarrestar las tácticas de ataque más recientes. Al comprender las Tácticas, Técnicas y Procedimientos (TTP) empleados por los adversarios, el equipo puede ajustar sus defensas y responder de manera más efectiva a los ataques, mitigando los posibles impactos en la organización.

Usualmente esta información se obtiene de fuentes como libros y documentos técnicos, pláticas con colegas, documentos especializados e información generada por proveedores de seguridad.
Se enfoca en indicadores de amenazas que ayudan a cazar y defenderse de los atacantes y no se contextualiza la información. Simplemente busca detectar y responder a los eventos que generan altos volúmenes de información técnica.

La inteligencia táctica se enfoca en el responder el ¿Qué? Indicadores de compromiso, como nombres de archivo, archivos hash, dominios, direcciones IP, entre otras. Esta información se utiliza para clasificar y validar alertas, soportar reglas para firewalls o sistemas de detección / prevención de intrusiones, sistemas de respuesta y detección de puntos finales y otras herramientas similares.

Los usuarios de esta información son los técnicos. Los usuarios tácticos están al frente de las ciberdefensas de una organización. Administran todo, desde firewalls, sistemas IDS / IPS, puertas de enlace de seguridad, sistemas de monitoreo de eventos e información de seguridad (SIEM), capacidades de orquestación de seguridad, automatización y respuesta (SOAR), detección y respuesta de puntos finales (EDR). Los usuarios técnicos aprovechan los indicadores de compromiso, el contenido y el contexto para prevenir directamente los ataques de MCA a sus organizaciones. Las fuentes deben ser confiables y estar bien configuradas para que no generen una gran cantidad de falsos positivos.

2.2.4.4 Inteligencia Técnica

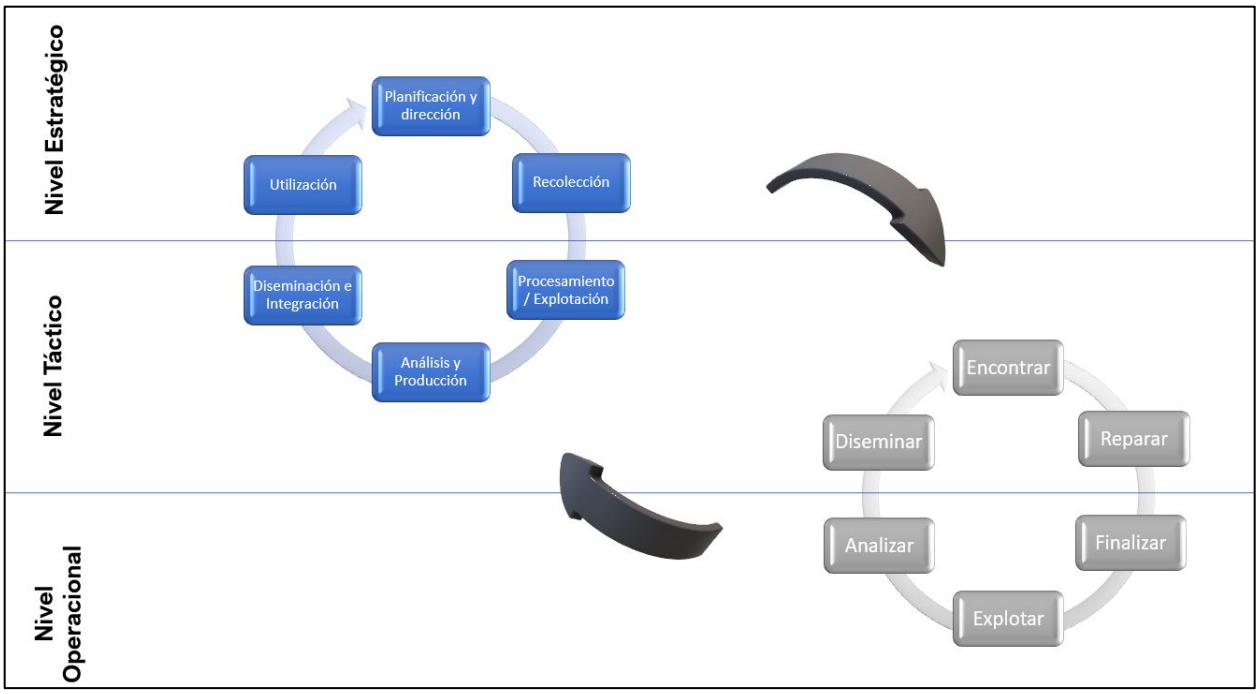
Información que normalmente se consume a través de recursos técnicos [75]. Esta inteligencia busca apoyar las funciones de investigación o supervisión de una organización. Además, ayuda a alimentar herramientas analíticas que ayudarán a identificar anomalías de comportamiento e identificar ataques mediante la búsqueda de registros de conexiones o binarios previamente observados [80].

2.3 Frameworks y Metodologías de CTI

Existen diferentes estudios, marcos y metodologías en el campo de CTI, las cuales podrían ser definidas como una estructura para pensar cómo operan los atacantes, descubrir sus métodos y en qué parte del ciclo de vida general del ataque está ocurriendo ese evento. Más específicamente, las metodologías de CTI nos permiten ser muy prescriptivos en cómo atacamos una situación específica, es decir, nos permiten centrar la atención en las áreas adecuadas para garantizar el seguimiento y mitigación de amenazas existentes o emergentes. También proporcionan un lenguaje común para comunicarse internamente y también externamente con respecto a detalles de amenazas, interrelaciones entre eventos y correlaciones con fuentes de datos externas. Por lo tanto, podemos decir que nos permiten conectarnos y comprender dónde está ocurriendo algo y enfocar nuestros recursos dentro de esa pequeña área en lugar de intentar adoptar un enfoque reactivo. Además, nos permite ser mucho más enfocados en el área específica que necesita nuestra atención para asignar recursos específicos a una amenaza o técnica que utilice algún adversario que pueda dañar a nuestra organización. De esa forma, los defensores no pierden tiempo, esfuerzo y recursos trabajando en áreas que no necesariamente están afectadas o tal vez no son necesariamente relevantes al incidente que se enfrentan o están a punto de enfrentar.

2.3.1 El Ciclo F3EAD

Por otro lado el **Forum of Incident Response and Security Teams (FIRST)** [81] una de las principales organizaciones que facilita plataformas, medios y herramientas para que los equipos de respuesta a incidentes encuentren socios adecuados y colaboren de manera eficiente, menciona el ciclo **F3EAD** [82] (por sus siglas en inglés: *Find, Fix, Finish, Exploit, Analyze and Disseminate*), como un ciclo alternativo de inteligencia. Este ciclo es comúnmente utilizado en operaciones militares occidentales, particularmente en fuerzas especiales, y puede adaptarse para cumplir con los requisitos y objetivos generales de la inteligencia de una organización.



Proceso de Integración de CTI [82]**.**

Así mismo, el FIRST recomienda utilizar este marco para alinear recursos limitados en una situación presurizada para responder preguntas muy específicas, tales como:

- ¿Sufrimos una fuga de información?
- ¿Estamos siendo víctimas de un ciberataque?
- ¿Hay algún actor malicioso o actor de amenaza en nuestra red?

Este tipo de preguntas suelen tener respuestas muy simples, las cuales se les denomina respuestas binarias, es decir, si/no; sin embargo, suelen tener una gran relevancia para evaluar la situación actual y lo siguientes pasos a seguir, tales como priorizar recursos de acuerdo con el impacto que tendrá la respuesta a la pregunta en el desarrollo general de la situación. Basado en esto, F3EAD es una herramienta que debe usarse con moderación, en el entendimiento de que enfocarse en responder una pregunta, quita prioridad a otras preguntas. Se debe tener cuidado para realizar y priorizar la pregunta correcta según el interés central de la empresa.

2.3.2 Modelo de Cyber Kill Chain

El estudio desarrollado por la Corporación Lockheed Martin [83] [84], la cual se basa en el concepto militar de "Kill Chain". La cual consiste en siete áreas distintas que nos permiten comprender en qué parte del proceso o parte de la cadena del ataque se produce una amenaza específica, ya sea en reconocimiento, armamento, entrega, etc. Por lo tanto, si entendemos en qué parte del proceso se encuentra esa amenaza, podemos enfocar nuestros recursos y nuestros esfuerzos en la mitigación de esta. Y si tenemos un marco adecuado, podemos entender qué acciones deben tomarse en esa área para que podamos responder rápidamente.

Por ejemplo, una defensa de redes informáticas impulsada por inteligencia [83], es una estrategia de gestión de riesgos y amenazas que incorpora el análisis de los adversarios, sus capacidades, objetivos, herramientas y limitaciones. Este es un proceso continuo, aprovechando indicadores específicos de alguna actividad o comportamiento anómalo para descubrir nuevas actividades con aún más indicadores para así poder ampliar el panorama de las amenazas que estamos enfrentando y documentar todos sus vectores de ataque.

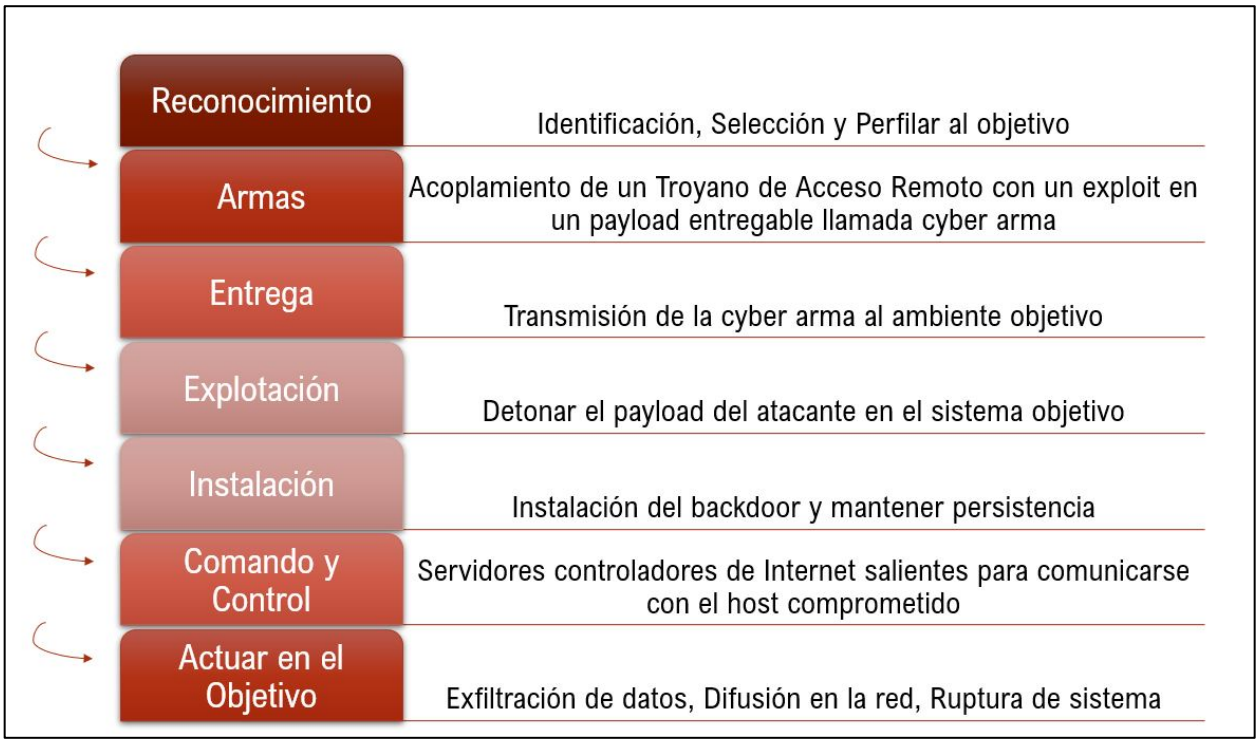
Este efecto defensivo impulsado por inteligencia es una postura de seguridad basada en datos relevantes para la organización y a su ves aporta el contexto para que la alta dirección pueda asignar los recursos necesarios basado en la evidencia recolectada. Los actores maliciosos, por su naturaleza, intentan intrusión tras intrusión, ajustando sus operaciones y técnicas basadas en función del éxito o el fracaso de cada intento realizado. En un modelo de cadena de muerte o "Cyber Kill Chain", basta con realizar solo una mitigación de manera efectiva para detener al atacante, por lo tanto, cualquier intento por parte del actor o amenaza es una responsabilidad que los defensores de la red deben tener la capacidad de reconocer, responder y tener todos los recursos para poder mitigar dicha amenaza. Si los defensores implementan contramedidas más rápido de lo que evolucionan los adversarios, aumentan los costos que un adversario debe gastar para lograr sus objetivos y este enfocara su tiempo y recursos en otros objetivos u organizaciones. Este modelo muestra, contrariamente a la sabiduría convencional, que tales agresores no tienen una ventaja inherente sobre los defensores

2.3.2.1 Las Fases del modelo de Cyber Kill Chain

Este estudio consiste en siete áreas distintas que nos permiten comprender en qué parte del proceso o parte de la cadena del ataque se produce una amenaza específica, ya sea en reconocimiento, armamento, entrega, etc. Por lo tanto, si entendemos en qué parte del proceso se encuentra esa amenaza, podemos enfocar nuestros recursos y nuestros esfuerzos en la mitigación de esta. Y si tenemos un marco adecuado, podemos entender qué acciones deben tomarse en esa área para que podamos responder rápidamente ante las técnicas del adversario [84].

Por ejemplo, primero viene el reconocimiento, donde el adversario está buscando una debilidad, es decir, la obtención de credenciales de registro o información que se puede utilizar para un ataque de Phishing, donde en este caso, la debilidad es el usuario que recibe el Phishing sumado a las vulnerabilidades de su dispositivo. Lo siguiente es la armamentización, el cual consiste en crear la entrega de la amenaza, utilizando una técnica de explotación (exploit) como un Backdoor típicamente. La entrega es el proceso de enviar esa carga útil a la víctima, el cual podría ser un correo electrónico malicioso, podría ser una memoria USB que queda en un escritorio en el piso de algún estacionamiento cercano a la organización o inclusive en el estacionamiento de esta. Después tenemos vulnerabilidades, en el cual el atacante realizara el acto de ejecutar el código en el sistema remoto para después pasar a la fase de la instalación real de malware en ese objetivo. Y eso nos lleva al C&C, el cual creara un canal o persistencia donde el atacante puede controlar el sistema de forma remota enviando instrucciones con algún objetivo o fin especifico. En ese punto, el atacante ya tiene el control de quizás mas de un sistema, por lo tanto, es muy importante el

monitorear los distintos canales de C&C detectados en nuestra red. Y al final de esto, se realizan las acciones deseadas. Entonces, ese es el objetivo previsto, ya sea cifrar datos, destruirlos, ex filtrarlos, etc.



Las fases de "Cyber Kill Chain". [85] [84]

El modelo de **Cyber Kill Chain** describe un enfoque basado en inteligencia y centrado en las amenazas, cuyo propósito es estudiar las intrusiones desde la perspectiva de los adversarios. Cada fase de la intrusión se asocia con acciones específicas para la detección, mitigación y respuesta, destacando que los atacantes deben cumplir ciertas fases para lograr su objetivo. Este modelo ha sido aplicado en diversos sectores de la industria, permitiendo la creación de estrategias fundamentadas en taxonomías de amenazas específicas, como troyanos que afectan al sector financiero [86] Además, se han explorado investigaciones que buscan predecir ciertos comportamientos o amenazas de los adversarios [87], lo que sugiere que este enfoque se basa en la reconstrucción de un ataque para comprenderlo mejor y, en consecuencia, mitigarlo de manera más efectiva.

2.3.2.2 Reconocimiento

El **reconocimiento** se refiere a la investigación, identificación y selección de objetivos por parte de los atacantes. Este proceso a menudo involucra el uso de herramientas y plataformas como Shodan [88], listas de correo para obtener direcciones de correo electrónico, información pública disponible en Internet, redes sociales o datos sobre tecnologías específicas. Los objetivos pueden ser tanto individuos como entidades organizacionales. La información obtenida durante la fase de reconocimiento se utiliza en las etapas posteriores de la cadena de ataque o **Cyber Kill Chain** para llevar a cabo las intrusiones y explotar las vulnerabilidades detectadas.

- **Reconocimiento pasivo** [85]**:** se realiza recopilando información sobre el objetivo sin que este lo perciba. Un ejemplo de ello es la recolección de información pública disponible en Internet, como detalles publicados en redes sociales, bases de datos públicas, foros o sitios web. El objetivo es obtener la mayor cantidad de datos posibles sin alertar a la entidad o individuo que está siendo investigado, preparando el terreno para futuras fases de un ciberataque.

- **Reconocimiento activo** [85]**:** esta fase implica un análisis más profundo y directo del objetivo, lo cual puede generar alertas en los sistemas de seguridad de la entidad bajo investigación. A diferencia del reconocimiento pasivo, el reconocimiento activo involucra actividades como el escaneo de servidores, sitios web o redes en busca de vulnerabilidades y puntos débiles que puedan ser explotados. Este tipo de acciones tiene un mayor riesgo de ser detectado por el objetivo, ya que suele involucrar interacciones más directas con los sistemas.

Por lo tanto, podemos decir que la fase de reconocimiento proporciona al atacante los conocimientos sobre los objetivos potenciales, que le permitirán decidir que tipo de arma o técnica es la adecuada para vulnerar el objetivo, así como los tipos de métodos de entrega posibles y mapear todas las dificultades que se enfrentara antes de realizar alguna instalación de algún malware, teniendo en cuenta los mecanismos de seguridad que deben evitarse.

2.3.2.3 Armamento

La fase de armado del Cyber Kill Chain se ocupa de diseñar una puerta trasera (Backdoor) y un plan de penetración, utilizando la información recopilada de la fase de reconocimiento, para permitir la entrega exitosa de la puerta trasera (Backdoor). Técnicamente, se trata de vincular exploits de software / aplicaciones con una herramienta de acceso remoto (RAT). La creación de armamento cibernético implica el diseño y desarrollo de los dos componentes siguientes [85]:

RAT (Remote Access Tool): Software que se ejecuta en el sistema del objetivo vulnerado con el objetivo principal de brindar acceso remoto, oculto y sin ser detectado al atacante. Los tipos de acceso que proporciona un RAT típico son exploración del sistema, carga o descarga de archivos, ejecución remota de archivos, monitor de pulsaciones de teclas, captura de pantalla, cámara web o encendido / apagado del sistema con privilegios limitados o de nivel de usuario.

Exploit: Es la parte de un arma cibernética que facilita la ejecución del RAT. Este actúa como portador del RAT y utiliza las vulnerabilidades del sistema o software para eliminar y ejecutar el RAT. El principal objetivo del uso de exploits es evadir la atención del usuario mientras se establece un acceso de un Backdoor silencioso utilizando la RAT.

Durante los ultimo años, los archivos de datos de las aplicaciones del cliente, como el formato de documento portátil de Adobe (PDF) o los documentos de Microsoft Office, sirven como una vía

para entregar este tipo de amenazas cibernéticas, ya que los atacantes están conscientes que casi cualquier sistema manejado por un usuario utiliza este tipo de archivos.

2.3.2.4 Entrega

La entrega es la parte crítica de la Cyber Kill Chain que es responsable de un ciberataque eficiente y eficaz. Para cualquier ciberataque, es preferible tener la mayor información disponible sobre el objetivo para garantizar un ataque exitoso, la cual proviene de la información recopilada durante la fase de reconocimiento activo y pasivo.

En la mayoría de los ataques cibernéticos, es obligatorio tener algún tipo de interacción con el usuario, como descargar y ejecutar archivos maliciosos o visitar páginas web maliciosas en Internet. Por lo tanto, podemos asumir que la fase de Entrega es una tarea de alto riesgo para un atacante, ya que, si no se realiza de una manera adecuada, esta fase puede dejar rastros, eventos o alguna evidencia que pueda dejar algún rastro de la actividad y el atacante. Por lo tanto, la mayoría de los ataques se realizan de forma anónima utilizando técnicas y servicios anónimo, así como sitios web o dispositivos previamente comprometidos y cuentas de correo electrónico comprometidas. Mientras se realiza la entrega de la amenaza, se utilizan múltiples métodos o técnicas a la vez, ya que ningún método puede garantizar el 100% de éxito. Los ataques fallidos a veces son muy útiles para obtener información básica sobre la información del sistema del objetivo.

2.3.2.5 Explotación

En la mayoría de los casos, las técnicas de explotación se centran en vulnerabilidades de aplicaciones o sistemas operativos, aunque también pueden dirigirse directamente a los propios usuarios mediante tácticas de ingeniería social. Otra posibilidad es aprovechar funciones del sistema operativo que permiten la ejecución automática de código malicioso. Esto significa que, tras la entrega de la amenaza o "arma cibernética", el atacante depende de que el objetivo realice una interacción mínima, como abrir un archivo o hacer clic en un enlace, para que el código malicioso se ejecute en el sistema de la víctima.

En la ejecución, el siguiente paso es activar el exploit. Para activar el exploit, hay ciertas condiciones que deben cumplirse:

- El usuario debe estar utilizando el software / sistema operativo para el que se creó el exploit.
- El software / sistema operativo no debe actualizarse o actualizarse a las versiones en las que un exploit no funciona.
- Los antivirus, sistema de prevención de intrusos (IPS) o cualquier otro mecanismo de seguridad no deben detectar el exploit durante el tiempo de ejecución.

2.3.2.6 Instalación

Tradicionalmente, los dispositivos se infectaban de diversas maneras, como a través de medios

extraíbles contaminados, que instalaban y ejecutaban archivos maliciosos en ubicaciones inusuales del sistema. Esto permitía que el malware se activara cada vez que el dispositivo se iniciaba. Este tipo de persistencia es fundamental para los atacantes, ya que la instalación de un troyano de acceso remoto (RAT) o una puerta trasera en el sistema de la víctima les permite mantener acceso continuo y no detectado dentro del entorno comprometido, facilitando la explotación prolongada de los recursos o datos del objetivo.

Hoy en día, el malware tiene varias etapas y depende en gran medida de los "Droppers" y los "Downloaders", quienes se encargan de entregar los módulos de malware de una manera mucho más sofisticada.

- Dropper es un programa que instalará y ejecutará el malware en un sistema de destino. Antes de ejecutar el código malicioso, el dropper intenta deshabilitar los controles de seguridad basados en el host en el objetivo y oculta el malware instalado.

- Downloader fueron diseñados para realizar las mismas acciones que los Droppers, ocultando los componentes centrales y ofuscando el vector de infección, etc. pero tendían a ser más pequeños que los Droppers, ya que estos no contienen los componentes principales de la infección, es decir, en lugar de descomprimir una copia incrustada del malware principal, el Downloader se conectaría a un repositorio de archivos remoto y descargaría los componentes principales para realizar la infección.

2.3.2.7 Comando y control (C&C)

Por lo general, los dispositivos que fueron comprometidos deben enviar una señal de salida a un servidor controlador en Internet para establecer un canal de comunicación y así poder seguir instrucciones o descargar actualizaciones para realizar algún tipo de acción maliciosa (a esto se le conoce como Canal de Comando y Control C&C). Una vez que se establece el canal de C&C, los intrusos tienen acceso dentro del entorno objetivo.

A lo largo de los años, la arquitectura de los canales C&C ha evolucionado exponencialmente debido al desarrollo exponencial de mecanismos defensivos, tales como los antivirus, IPS/IDS, Firewalls, etc. Sin embargo, existen diferentes tipos de estructuras de comunicación de canales de C&C:

Estructura centralizada: tradicionalmente, el malware dependía de un modelo clásico de servidor cliente en el que se utiliza un servidor central para controlar y controlar las máquinas infectadas. Dado que solo hay un servidor, es fácil de administrar, no hay dependencia de las máquinas infectadas para transmitir señales de control de comandos. Por lo tanto, la falla de las máquinas infectadas al azar no afectará la arquitectura de C&C. Pero la cantidad de bots que se pueden controlar depende de los recursos de hardware / softwares disponibles para el servidor de C&C. Además, si se desactiva el servidor principal, se vera afectada toda la infraestructura de C&C.

Estructura descentralizada: debido al hecho de que la arquitectura centralizada se puede romper

fácilmente y cuenta con limitaciones de desempeño, se comenzó a utilizar la arquitectura P2P peer-to-peer para realizar los canales de C&C. Los principales objetivos del uso de esta arquitectura son la escalabilidad, es decir, los dispositivos infectados se utilizan como nodos, y cada nodo, a su vez, es responsable solo de un subconjunto de la botnet total, también la tolerancia a fallas es un factor muy importante en esta arquitectura, ya que se pueden formar enlaces de comunicación redundantes para enrutar información. Por lo tanto, la arquitectura descentralizada elimina la dependencia significativa de un solo punto de fallas y de desempeño sobre las arquitecturas centralizadas.

2.3.2.8 Acciones sobre los objetivos

Esta fase se realiza después de tener éxito en las primeras seis fases, en el cual los intrusos o amenazas pueden realizar acciones para lograr sus objetivos, tales como, el robo de información, modificar algún sistema, ejecutar alguna instrucción con algún fin malicioso, hasta realizar un secuestro de la información. Por otro lado, los intrusos o amenazas pueden desear acceder al dispositivo de la víctima inicial para usarlo como un puente o canal para comprometer otros sistemas adicionales (a esto se le conoce como movimiento lateral).

Por lo tanto, si podemos entender en qué parte del proceso se encuentra una acción específica, sabremos cómo enfocar nuestros esfuerzos y recursos para mitigar la amenaza antes de que llegue a una fase final, tal como se rompe un eslabón en una cadena, entonces la cadena se rompe ya no es útil y se evita el progreso del ciberataque [89].

2.3.3 El modelo de Diamante de análisis de intrusión

El análisis de intrusiones se ha considerado durante mucho tiempo un arte que debe aprenderse y practicarse, más que una ciencia que debe estudiarse y perfeccionarse. Sin embargo, abordarlo solo como un arte ha retrasado durante mucho tiempo las mejoras y la comprensión, lo que ralentiza aún más la evolución de la mitigación de amenazas que se basa en un análisis eficiente, efectivo y preciso. Sin saberlo, los analistas han utilizado el modelo de Diamante durante décadas, pero les ha faltado el marco completo para comprender, mejorar y enfocar sus esfuerzos. Este modelo describe las capacidades y características principales de un evento de intrusión: adversario, capacidad (técnicas y herramientas utilizadas por un adversario), infraestructura y víctima, las cuales están vinculadas en un diagrama en forma de diamante, en los cuales los bordes se utilizan para representar las relaciones entre las características que se pueden explotar analíticamente para descubrir y desarrollar más el conocimiento de la actividad maliciosa [90], es decir, el modelo describe que un adversario despliega una capacidad sobre alguna infraestructura contra una víctima.

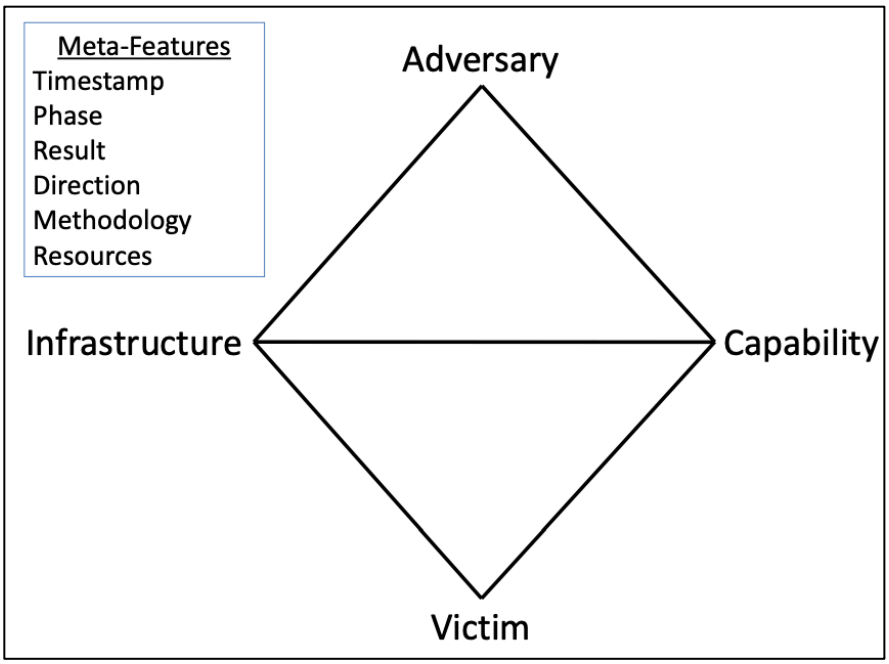


Figura 3. The Diamond Model of intrusion analysis [90]

Estas actividades, a su vez se les conoce como eventos, los cuales definen una serie de pasos que el adversario debe ejecutar para lograr su objetivo. Así mismo, los autores del modelo describen 7 bases fundamentales a entender en el proceso del modelo de intrusión en forma de Axiomas, donde se definen los objetivos y/o necesidades de los adversarios para poder cumplir sus objetivos:

Diamond Model Axioms	
Axioma 1	Por cada evento de intrusión, existe un adversario que da un paso hacia un objetivo previsto mediante el uso de una capacidad sobre la infraestructura contra una víctima para producir un resultado.
Axioma 2	Existe un conjunto de adversarios (internos, externos, individuos, grupos y organizaciones) que buscan comprometer los sistemas o redes informáticos para promover su intención y satisfacer sus necesidades.
Axioma 3	Todos los sistemas y por extensión, todos los activos de las víctimas tienen vulnerabilidades y exposiciones.
Axioma 4	Cada actividad maliciosa contiene dos o más fases que deben ejecutarse con éxito en sucesión para lograr el resultado deseado.
Axioma 5	Cada evento de intrusión requiere uno o más recursos externos para ser satisfecho antes de tener éxito.
Axioma 6	Siempre existe una relación entre el Adversario y sus Víctimas, aunque sea distante, fugaz o indirecta.
Axioma 7	Existe un subconjunto del conjunto de adversarios que tienen la motivación, los recursos y las capacidades para sostener efectos maliciosos durante un período de tiempo significativo contra una o más víctimas mientras se resisten a los esfuerzos de mitigación. Las relaciones adversario-víctima en este subconjunto se denominan relaciones adversas persistentes.

Tabla 3. Axiomas del Modelo de Diamante [90]

El modelo establece, un método formal que aplica principios científicos al análisis de amenazas, en particular los de medición, capacidad de prueba y respetabilidad, proporcionando un método integral de documentación, síntesis y correlación de la actividad [91]. Por esta razón, podemos decir que tanto los eventos como los procesos o hilos de cada actividad que realiza el atacante, son elementos necesarios para una comprensión completa de la actividad maliciosa en si, ya que una mitigación más efectiva y estratégica requiere de una comprensión y contexto de las intrusiones en si, con el objetivo principal de poder ampliar el panorama de la amenaza y entender las fases y

procesos de esta. Este enfoque científico y la simplicidad producen mejoras en la efectividad, eficiencia y precisión analíticas. En última instancia, el modelo brinda oportunidades para integrar y generar inteligencia en tiempo real para la defensa de la red, automatizando la correlación entre eventos, clasificando eventos con confianza en campañas adversas y pronosticando operaciones adversas mientras planifica y juega estrategias de mitigación.

Mientras que el modelo de "Cyber Kill Chain" proporciona la información de las operaciones de los atacantes, el modelo de Diamante amplia la perspectiva y contexto de los atacantes entre cada una de las fases de la Intrusion, es decir, que en conjunto permite tener un panorama mas amplio del atacante y no solo los indicadores técnicos. Además, el modelo de Diamante proporciona un método matemático formal para el análisis y agrupamiento de gráficos efectivos (por ejemplo, agrupamiento / clasificación) para resolver muchas clases de problemas analíticos [90]. El modelo de Diamante identifica cómo y por qué ocurre un ataque, ya que podemos ver que un atacante ataca a una víctima en función de dos atributos principales llamados Infraestructura y Capacidad, capturando y organizando con precisión los conceptos fundamentales que sustentan todo lo que hacen los analistas de intrusiones, así como la forma en que el análisis de intrusiones se sintetiza y utiliza para la mitigación y la defensa de la red [92]. Sin embargo, su mayor contribución es que finalmente aplica el rigor científico y los principios de medición, capacidad de prueba y respetabilidad al dominio, lo que permite que el análisis de intrusiones sea más efectivo, eficiente y preciso, lo que conduce a una mitigación más rápida, más efectiva y eficiente para derrota a los adversarios.

2.3.4 MITRE ATT&CK

MITRE es una organización sin fines de lucro que trabaja en favor del interés público, colaborando con gobiernos federales, estatales y locales, así como con la industria y el ámbito académico. Además, contribuye en diversas áreas, como la inteligencia artificial, la ciencia de datos intuitivos, la ciencia de la información cuántica, la informática de la salud, la seguridad espacial, la política y economía, la autonomía confiable, el intercambio de amenazas y la resiliencia cibernética [93].

Una de sus contribuciones más destacadas es el desarrollo de la metodología ATT&CK, que sirve como base para la creación de modelos de amenazas específicas tanto en el sector privado como en el gobierno y la comunidad de productos y servicios de ciberseguridad. ATT&CK documenta comportamientos conocidos de atacantes o adversarios, comúnmente denominados Amenazas Persistentes Avanzadas (APT, por sus siglas en inglés). Estos grupos de ataque están altamente organizados y cuentan con una gran cantidad de recursos, empleando técnicas avanzadas que les permiten llevar a cabo ataques complejos[94] . Las investigaciones sobre esta metodología también se han aplicado en infraestructuras críticas [95].

Un ejemplo común de las APT es su capacidad para infiltrarse en las redes de una organización y permanecer en ellas durante largos periodos, recopilando información antes de proceder con las siguientes fases de su ataque. ATT&CK se enfoca principalmente en cómo los adversarios externos comprometen y operan dentro de redes de información, proporcionando un marco detallado de los comportamientos y técnicas utilizados por los atacantes.

El modelo ATT&CK se originó a partir de un proyecto cuyo objetivo era documentar y categorizar las Tácticas, Técnicas y Procedimientos (TTP) utilizados por adversarios después de comprometer sistemas basados en Microsoft Windows, con el fin de mejorar la detección de comportamientos maliciosos [96]. Desde su creación, este modelo ha evolucionado para abarcar no solo sistemas operativos adicionales, sino también otras áreas clave como dispositivos móviles, sistemas en la nube y sistemas de control industrial. Esto ha ampliado su utilidad y alcance en el análisis y defensa contra una variedad de amenazas cibernéticas en distintos entornos tecnológicos.

Componentes centrales de MITRE ATT&CK	
Tácticas	Describe los objetivos tácticos durante un ataque
Técnicas	Describen los medios por los cuales los adversarios logran objetivos tácticos
Sub-técnicas	Describen medios más específicos por los cuales los adversarios logran objetivos tácticos a un nivel más bajo que las técnicas
Procedimientos	Son las implementaciones específicas que los adversarios han utilizado para técnicas o sub-técnicas.

Tabla 4. Componentes centrales de MITRE ATT&CK [96]

La base de ATT&CK radica en su conjunto de técnicas y sub-técnicas, que representan acciones específicas que los adversarios pueden llevar a cabo para alcanzar sus objetivos. Estos objetivos se organizan en categorías de tácticas, a las cuales pertenecen tanto las técnicas como las sub-técnicas. Las tácticas representan las metas generales que los atacantes buscan lograr, mientras que las técnicas y sub-técnicas detallan los métodos específicos que emplean para conseguirlo. La relación entre estas tácticas, técnicas y sub-técnicas se visualiza de manera clara en la **Matriz ATT&CK**, lo que permite a los defensores comprender de manera estructurada los comportamientos de los atacantes y mejorar las estrategias de detección y respuesta.

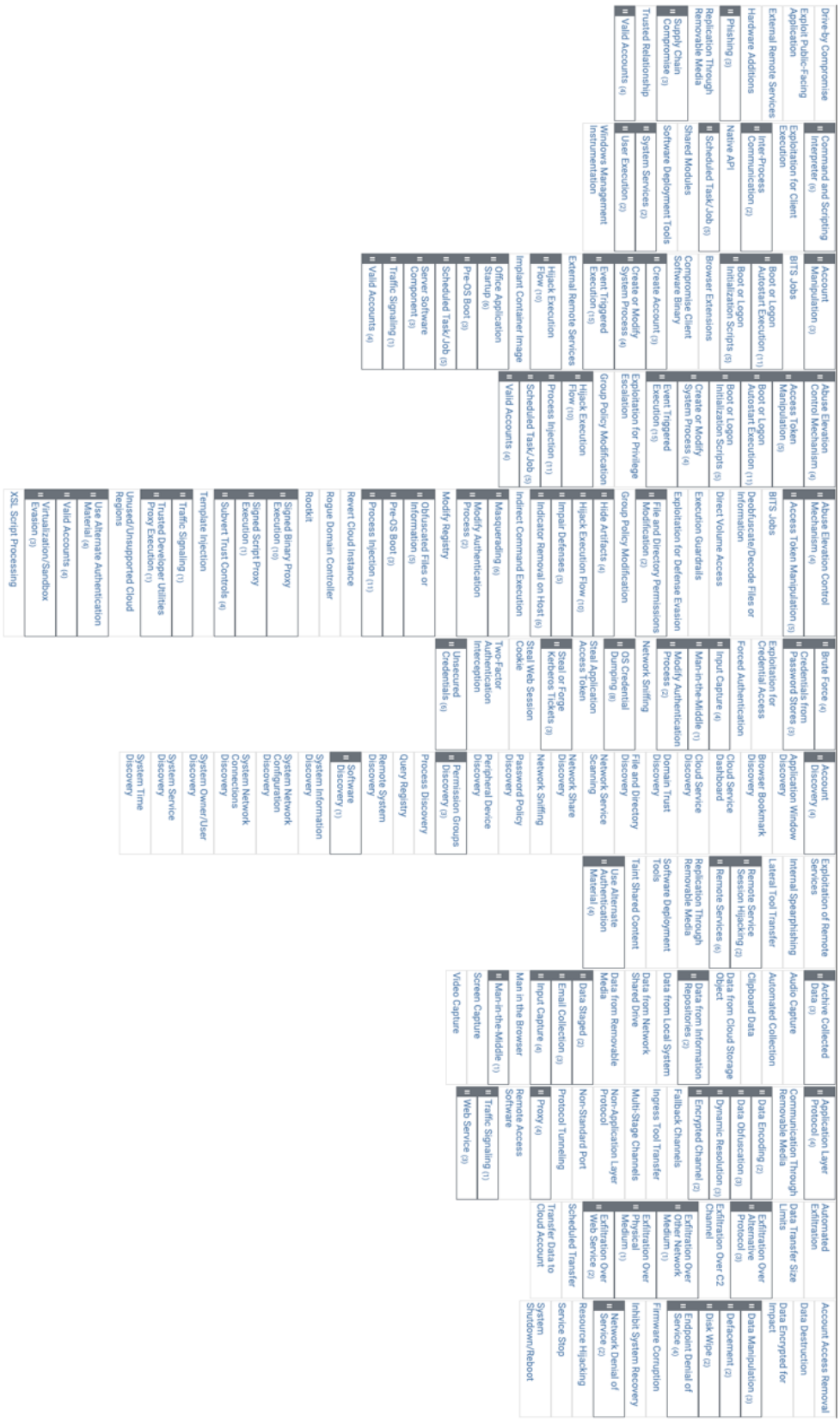


Figura 4. MITRE ATT&CK Enterprise Matrix [97]**.**

MITRE ATT&CK proporciona a los analistas de ciberseguridad un lenguaje común y estructurado para organizar, comparar y analizar la inteligencia contra amenazas (CTI) de manera efectiva. Este marco es especialmente útil para organizaciones que buscan fortalecer su defensa frente a amenazas, tanto existentes como emergentes. ATT&CK incluye información detallada sobre malware, herramientas utilizadas por los atacantes, tácticas, técnicas y procedimientos (TTP), así como comportamientos y otros indicadores asociados con amenazas. De esta manera, permite a las organizaciones adaptar sus estrategias de ciberseguridad con base en un conocimiento más profundo y estructurado del panorama de amenazas.

2.3.5 MITRE Shield/Engage

A partir de la metodología de ATT&CK, se desarrolló una nueva metodología llamado MITRE Shield, el cual está basado en la implementación del concepto de Defensa cibernética activa, la cual tiene como objetivo el realizar acciones ciberdefensas hasta poder llegar a engañar al adversario, teniendo una participación con el para estudiar y aprender mas sobre las tácticas y técnicas utilizadas para poder generar una CTI y prepararse para futuras amenazas. La matriz Shield consta de los siguientes componentes:

Componentes centrales de MITRE Shield	
Tácticas	Son metas abstractas de los defensores.
Técnicas	Son acciones generales que puede realizar un defensor que puede tener varios efectos tácticos diferentes dependiendo de cómo se implementen.
Procedimientos	Son implementaciones de una técnica.
Espacios de oportunidad	Describen posibilidades de defensa activa de alto nivel que se introducen cuando los atacantes emplean sus técnicas.
Casos de uso	Descripciones de alto nivel de cómo un defensor podría hacer algo para aprovechar la oportunidad que presenta la acción del atacante

Tabla 5. Componentes centrales de MITRE Shield [98]

Dentro de Shield, también se cuentan con una matriz de tácticas que denotan lo que el defensor está tratando de lograr por medio de columnas y técnicas, las cuales describen cómo la defensa logra las tácticas. Sin embargo, se han esos términos para que se ajusten al dominio de la Defensa cibernética activa. Estas tácticas dentro de MITRE Shield debe ser tomadas en cuenta como una estrategia de cada operación de defensa activa planificada para así responder ante alguna Intrusion de algún adversario o amenaza. Ante esto, es necesario desarrollar las técnicas descritas dentro de Shield para implementar los controles de seguridad en un entorno operativo. MITRE encontró que una sola técnica puede ser compatible con varias tácticas diferentes, y para cualquier táctica existen múltiples técnicas que se pueden utilizar. Además, cuenta con una sección donde se mapean las tácticas y técnicas de ATT&CK con el objetivo de que los defensores puedan contar con la información de defensa activa aplicable, incluido el espacio de oportunidad presentado, la técnica de defensa activa que se implementará y el caso de uso para esa implementación

Channel	Collect	Contain	Detect	Disrupt	Facilitate	Legitimize	Test
Admin Access	API Monitoring	Admin Access	API Monitoring	Admin Access	Admin Access	Application Diversity	Admin Access
API Monitoring	Application Diversity	Baseline	Application Diversity	API Monitoring	Application Diversity	Burn-In	API Monitoring
Application Diversity	Backup and Recovery	Decoy Account	Behavioral Analytics	Application Diversity	Behavioral Analytics	Decoy Account	Application Diversity
Decoy Account	Decoy Account	Decoy Network	Decoy Account	Backup and Recovery	Burn-In	Decoy Content	Backup and Recovery
Decoy Content	Decoy Content	Detonate Malware	Decoy Content	Baseline	Decoy Account	Decoy Credentials	Decoy Account
Decoy Credentials	Decoy Credentials	Hardware Manipulation	Decoy Credentials	Behavioral Analytics	Decoy Content	Decoy Diversity	Decoy Content
Decoy Network	Decoy Network	Isolation	Decoy Network	Decoy Content	Decoy Credentials	Decoy Network	Decoy Credentials
Decoy Persona	Decoy System	Migrate Attack Vector	Decoy System	Decoy Credentials	Decoy Diversity	Decoy Persona	Decoy Diversity
Decoy Process	Detonate Malware	Migrate Compromised System	Detonate Malware	Decoy Network	Decoy Network	Decoy Process	Decoy Network
Decoy System	Email Manipulation	Network Manipulation	Email Manipulation	Detonate Malware	Decoy Persona	Decoy System	Decoy Persona
Detonate Malware	Network Diversity	Security Controls	Hunting	Email Manipulation	Decoy System	Network Diversity	Decoy System
Migrate Attack Vector	Network Monitoring	Software Manipulation	Isolation	Hardware Manipulation	Network Diversity	Pocket Litter	Detonate Malware
Migrate Compromised System	PCAP Collection		Network Manipulation	Isolation	Network Manipulation		Migrate Attack Vector
Network Diversity	Peripheral Management		Network Monitoring	Migrate Compromised System	Peripheral Management		Network Diversity
Network Manipulation	Pocket Litter		PCAP Collection	Network Manipulation	Pocket Litter		Network Manipulation
Peripheral Management	Protocol Decoder		Pocket Litter	Security Controls	Security Controls		Peripheral Management
Pocket Litter	Security Controls		Protocol Decoder	Standard Operating Procedure	Software Manipulation		Pocket Litter
Security Controls	System Activity Monitoring		Standard Operating Procedure	User Training			Security Controls
Software Manipulation	Software Manipulation		System Activity Monitoring	Software Manipulation			Software Manipulation
			User Training				
			Software Manipulation				

Figura 5. The Shield Matrix [99]**.**

La combinación de las metodologías de ATT&CK y Shield pueden ayudar a los defensores a profundizar su comprensión del comportamiento y los enfrentamientos del adversario y sugerir formas en que el defensor puede implementar una estrategia de defensa activa [99]. Por lo tanto, el objetivo de Shield es que los defensores puedan aprovechar las tácticas y técnicas de esta metodología para crear, instrumentar y operar mejor sus soluciones de defensa activa, mostrando cómo el lado defensivo de Shield para alinearse con ATT&CK, con el objetivo principal de que a las organizaciones y sus defensores puedan aprovechar ambas estrategias para maximizar sus esfuerzos defensivos y poder generar una estrategia más sólida que les permita aprender de los adversarios mientras se defienden de ellos.

2.4 Threat Intelligence Platforms (TIP)

Las técnicas y resultados que han brindado el CTI en los últimos años, ha ganado una gran cantidad de atención en las comunidades de ciberseguridad como una forma de pronosticar amenazas potenciales y reducir el tiempo de detección de ataques en términos de los procesos de la cadena de muerte, así como el uso de información de inteligencia de código abierto (OSINT) se está convirtiendo en un enfoque fundamental para obtener conciencia sobre las amenazas de ciberseguridad, sin embargo, la gran cantidad de información a procesar suele ser uno de los retos más importantes en esta área para los defensores. Por ello, los investigadores y analistas de ciberseguridad han adoptado el uso de herramientas y plataformas de inteligencia para gestionar de manera eficiente las tareas de análisis de amenazas. Una **Plataforma de Inteligencia de Amenazas** (TIP, por sus siglas en inglés) permite a las organizaciones agregar, correlacionar y analizar datos de amenazas provenientes de múltiples fuentes en tiempo real. Estas plataformas incluyen diversas características clave que facilitan la implementación de un enfoque de seguridad

basado en inteligencia, apoyando así las acciones defensivas. El objetivo principal de una TIP es ayudar a las organizaciones a comprender los riesgos a los que están expuestas y protegerse contra una amplia gama de amenazas, recolectando información de diversas fuentes de inteligencia para fortalecer la postura de seguridad en sus entornos.

Threat Intelligence Platforms Stages	
Collect	Una plataforma de inteligencia de amenazas recopila y agrega múltiples formatos de datos para múltiples fuentes, incluidos formatos como STIX, CSV, XML, correo electrónico y varias fuentes de inteligencia.
Correlate	La plataforma de inteligencia de amenazas permite a las organizaciones comenzar a analizar automáticamente la correlación y pivotar sobre los datos para que la inteligencia procesable sobre quién, por qué y cómo de nuevo de un ataque se pueda obtener en las medidas de bloqueo introducidas.
Enrichment & Contextualization	Una plataforma de inteligencia de amenazas debe poder mejorar automáticamente o permitir que los analistas de inteligencia de amenazas utilicen aplicaciones de análisis de amenazas de terceros para enriquecer los datos recolectados en una investigación.
Analyze	Analiza automáticamente el contenido de los indicadores de amenazas y las relaciones entre ellos para permitir la producción de inteligencia de amenazas útil, relevante y oportuna del recopilador de datos.
Integrate	Los datos de la plataforma deben encontrar un camino de regreso a las herramientas y productos de seguridad que utiliza una organización para permitir la automatización de procesos y comunicación.
Act	Los flujos de trabajo y procesos integrados aceleran la colaboración dentro del equipo de seguridad y comunicaciones más amplias, como organizaciones de análisis e intercambio de información.

Tabla5. Threat Intelligence Platforms Stages

Una TIP analiza automáticamente el contenido de los indicadores de amenazas y las relaciones entre ellos para permitir la producción de inteligencia de amenazas útil, relevante y oportuna del recopilador de datos. Este análisis permite la identificación de tácticas, técnicas y procedimientos de los actores de amenazas o TTP's. Estas plataformas pueden ser un sistema en la nube o en las instalaciones para facilitar la administración de datos de amenazas de una variedad de herramientas de seguridad existentes, como SIEM, Firewall, API, software de administración de terminales o sistema de prevención de intrusiones (IPS). Se han presentado investigaciones y trabajos donde se evalúan algunas plataforma de intercambio de inteligencia sobre amenazas [100] [101], donde los usuarios de la comunidad de TI y otras comunidades en general, pueden compartir su información sobre incidentes en un entorno confiable, como lo es Malware Information Sharing Platform (MISP) [102], la cual nos permite compartir, almacenar y correlacionar indicadores de compromiso de ataques dirigidos, inteligencia de amenazas, información de fraude financiero, información de vulnerabilidad [103]. Se puede acceder a la plataforma de intercambio de información de malware desde diferentes interfaces, como una interfaz web (para analistas o controladores de incidentes) o mediante una API ReST (para sistemas que empujan y extraen IOC). El objetivo inherente de MISP es ser una plataforma sólida que garantice un funcionamiento sin problemas al revelar, madurar y explotar la información de amenazas.

En esta sección se presentan las diferentes TIP más utilizadas en la actualidad.

2.4.1 Malware Information Sharing Platform (MISP)

El proyecto MISP o Plataforma de intercambio de información sobre malware [104] es un proyecto el cual permite a analistas de todo el mundo compartir y consultar inteligencia de demás analistas, permite generar una red de intercambio de información inmensa la cual solamente crece con el tiempo, actualmente más de 6000 organizaciones se encuentran utilizando la plataforma MISP.

La plataforma de intercambio de amenazas **MISP** [102] es un software gratuito y de código abierto diseñado para facilitar el intercambio de información sobre amenazas. Esta plataforma de inteligencia de amenazas cibernéticas permite recopilar, compartir, almacenar y correlacionar indicadores de compromiso relacionados con ataques dirigidos, inteligencia sobre amenazas, información sobre fraudes financieros, vulnerabilidades e incluso información antiterrorista. MISP se ha convertido en una herramienta valiosa para organizaciones que buscan mejorar su capacidad de respuesta frente a ciberamenazas al aprovechar la colaboración y el intercambio de inteligencia entre diversas entidades.

Figura 6. Malware Information Sharing Platform (MISP) [102].

Como se ha mencionado anteriormente, el uso de una plataforma tan útil como lo es MISP, facilita muchas tareas y ayuda a hacer mas eficiente el tiempo y recursos. Además, ayuda a tener mejores resultados y a generar una base de conocimiento compartido libre y abierto, inclusive si solo se utiliza MISP a forma de consulta y no de aportación, es sumamente útil puesto que es una base de datos compartida la cual ayudara, apoyara y complementara la inteligencia de amenazas cibernéticas privada. La clave de MISP se encuentra en su automatización de trabajo, al tener mucha información y no poder procesarla por ser una cantidad inmensa de trabajo se está perdiendo potencial inteligencia para toma de decisiones más acertadas, MISP también permite la exportación automatizada para soluciones de seguridad como IDS o SIEM. MISP es una herramienta fácil de instalar, configurar y utilizar, la simplicidad es el motor del proyecto, permite llevar una correcta gestión de inteligencia de amenazas sin representar mayores esfuerzos para el equipo y dando resultados sumamente útiles.

Compartir inteligencia es la clave para una detección rápida y eficaz de los ataques. Muy a menudo, organizaciones similares son objetivo del mismo actor de la amenaza, en la misma o diferente campaña. MISP le facilitará compartir con, pero también recibir de, socios de confianza

y grupos de confianza. Compartir también permite el análisis colaborativo y evita que usted haga el trabajo que otro ya hizo antes.

2.4.2 Virus Total

VirusTotal fue fundada en 2004 como un servicio gratuito destinado a analizar archivos y URL en busca de virus, gusanos, troyanos y otro contenido malicioso, con el objetivo de hacer de Internet un lugar más seguro mediante la colaboración entre miembros de la industria antivirus, investigadores y usuarios finales. Entre sus usuarios destacan empresas de la **Fortune 500**, gobiernos y empresas líderes en seguridad, que forman parte de su comunidad [105].

Cuando un usuario ingresa un archivo o URL, VirusTotal inspecciona el contenido utilizando más de **70 escáneres antivirus** y servicios de listas de bloqueo de URL/dominios. Además, dispone de varias herramientas que extraen señales del contenido analizado. Los usuarios pueden subir archivos desde su navegador web y enviarlos para su análisis. VirusTotal ofrece varios métodos de envío de archivos, entre ellos, la **interfaz web**, aplicaciones de escritorio, extensiones de navegador y una API. La **interfaz web** tiene prioridad en los escaneos, mientras que los archivos y URL también pueden enviarse a través de la **API pública** basada en HTTP, lo que permite integrar el servicio en cualquier lenguaje de programación [106].

Una de las principales ventajas de la plataforma es que, al enviar un archivo o URL, los resultados básicos se comparten con el remitente y con los socios de VirusTotal, quienes utilizan los resultados para mejorar sus propios sistemas. Este sistema de retroalimentación no solo mejora la seguridad del usuario, sino también la de toda la comunidad. Además, VirusTotal ofrece la **Comunidad VirusTotal**, una red donde los usuarios pueden comentar y compartir observaciones sobre archivos y URL.

VirusTotal también permite identificar **falsos positivos**, y el contenido enviado puede ser compartido con **clientes Premium**. La base de datos generada proporciona a los profesionales de seguridad cibernética información valiosa sobre el comportamiento de las amenazas emergentes y el malware. Los clientes pueden realizar búsquedas avanzadas para acceder a muestras de archivos dañinos y analizar nuevas amenazas, lo que les ayuda a desarrollar mitigaciones y defensas. Además, la plataforma se actualiza constantemente con las firmas de malware más recientes proporcionadas por las empresas antivirus, lo que garantiza que los análisis sean precisos.

En cuanto al análisis de sitios web, VirusTotal consulta tanto las bases de datos almacenadas en sus instalaciones como los servicios API de empresas antivirus para obtener resultados actualizados. Aunque la plataforma afirma que los cambios en la detección de URLs bloqueadas por colaboradores se reflejan inmediatamente, otras fuentes sugieren que no todas las actualizaciones son instantáneas [106].

VirusTotal no solo valida si un archivo es detectado como malicioso por algún motor antivirus, sino que también muestra la **etiqueta de detección** de cada uno. Lo mismo ocurre con los escáneres de URL, que clasifican entre **sitios de malware, Phishing y sitios sospechosos**. Algunos motores incluso proporcionan información adicional, como si una URL está asociada con una botnet o una campaña de Phishing dirigida a una marca específica.

Además, se han realizados diversas investigaciones sobre los usos y aplicaciones de la plataforma VirusTotal, así como sobre su funcionamiento con el fin de que sea utilizada de una forma mas eficiente y eficaz. Lo anterior debido a que también existen mitos sobre lo que realmente puede o no puede hacer la plataforma, además de sus capacidades reales en el aspecto de su índice de error y la idea de que substituye otros procesos que en realidad no realiza. Uno de estos casos es el del articulo "Opening the Blackbox of VirusTotal: Analyzing Online Phishing Scan Engines" [107], en el que se realizó un experimento para probar la efectividad de la plataforma VirusTotal, en el se describe la creación de dos tipos de páginas de Phishing unas imitando a Pay Pal y las otras imitando al Internal Revenue Service (ISR), estas páginas fueron escaneadas tanto con VirusTotal como con los escáneres particulares de otras organizaciones que colaboran VirusTotal, en total se utilizaron 66 páginas para el desarrollo del experimento. Al realizar el experimento se encontró que solo 15 escáneres de 68 detectaron al menos una página, y el que tuvo mejor resultado solo pude detectar 26 de las páginas de Phishing, también se detectó principalmente las páginas de Phishing de Pay Pal mientras que algunas de las de ISR no pudieron ser detectadas por ningún escáner. Además, se halló que en realidad no se actualiza la información de los escaneos hasta que no se realiza un segundo escaneo, creando así un retraso en la actualización de la información que reciben los usuarios. Finalmente se probó la efectividad de la plataforma para detectar los intentos de Phishing a pesar de las técnicas de ofuscación, los resultados fueron que es posible que VirusTotal puede detectar el Phishing a pesar de las técnicas para ocultarlo si estas son simples como el acortar URL's, pero tiene problemas con otras más complejas como las basadas en imágenes y código.

2.4.3 Threat Hunting with Twitter

El uso de las redes sociales ha incrementado drásticamente en la última década y no cabe duda de que su popularidad seguirá aumentando conforme pase el tiempo. La utilidad que se le puede sacar a estas plataformas ya no es solo compartir fotos con tus amigos, sino que se ha expandido de manera que ahora se considera una fuente de ingreso para pequeños y grandes negocios, y en el caso de la seguridad, también se considera una fuente, pero de información que puede ser empleada para Threat Intelligence y Threat Hunting. De hecho, en una encuesta se encontró que el 44% de las organizaciones comprenden la importancia de agregar "SOCMINT", es decir, Social Media Intelligence, a sus soluciones de protección digital.
Twitter es una fuente principal para la OSINT, muchos expertos en ciberseguridad están utilizando esta plataforma abierta para difundir información sobre las amenazas cibernéticas. Cada tweet está conformado por un texto de no más de 280 caracteres los cuales son aprovechados por organizaciones e individuos para compartir datos sobre vulnerabilidades, exploits e Indicadores de Compromiso. Cabe destacar que para que estos datos puedan convertirse en Cyber Threat Intelligence para las empresas debe existir un proceso de validación, dado que desafortunadamente hay usuarios de Twitter que se dedican a publicar noticias falsas, crear engaños, cometer fraude y aportar al Cibercrimen.

Aunado a esto último, usualmente cuando se comparten tweets con Indicadores de Compromiso tales como URLs y direcciones IP se les aplica un método para neutralizarlos, es decir, se reemplazan ciertos caracteres para evitar que el usuario de un clic por accidente que

le cause entrar al sitio web malicioso. Un ejemplo de esta neutralización es cambiar “http” por “hxxp”, de manera que esto agrega un nivel más de dificultad al extraer datos de Twitter que pudiesen ser empleados para CTI o TH. De acuerdo con un articulo publicado en la biblioteca del ACM, “el 38% de las direcciones IP recopiladas se neutralizaron y el 73% de las URL recopiladas también se neutralizaron. Esto muestra que hay más desafíos en Twitter en el manejo de técnicas de eliminación de colisiones que en blogs de seguridad, foros y listas de correo.” [108]

La recolección de información se puede hacer de manera manual o automatizada. La primera, aunque podría no ser la más eficiente, se lleva a cabo buscando tweets que incluyan conceptos clave utilizados en ciberseguridad como lo pueden ser CVE ID, exploit, toolkit, threat, vulnerability, entre otros. También se han desarrollado Frameworks los cuales se encargan de detectar tweets como una tarea de clasificación de novedades, como se explica en el estudio de “Gathering Cyber Threat Intelligence from Twitter Using Novelty Classification”
[109] que consta de tres fases: preprocesamiento, extracción de características y clasificación de novedad. El siguiente diagrama muestra la infraestructura que se utiliza para clasificar tweets de ciberamenazas como normal, relevante para ciberamenazas o irrelevante para ciberamenazas.

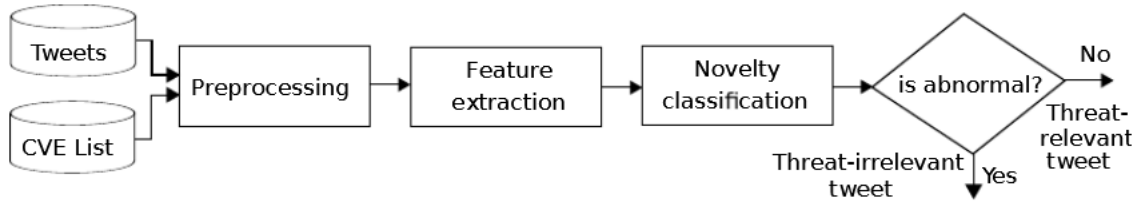


Figura 6. Recolección de CTI con Twitter

La fase de preprocesamiento consiste en eliminar los términos en los documentos de entrada que son innecesarios para identificar la información sobre amenazas cibernéticas. Esta fase convierte los documentos de entrada en minúsculas con puntuación, números, hipervínculos, menciones y hashtags eliminados. Las palabras irrelevantes en los documentos de entrada también se eliminan mediante la lista predeterminada de palabras irrelevantes en el paquete Natural Language Toolkit (NLTK). No aplica derivación ni lematización en los documentos de entrada, ya que puede cambiar el significado de estos.

La fase de extracción de características se encarga de transformar los documentos procesados en representaciones numéricas de vectores para clasificarlos, haciendo uso de la metodología de frecuencia de ocurrencia del término en la colección de documentos (TF-IDF por sus siglas en inglés). Después de esta transformación se utiliza un clasificador de novedad para clasificar cada tweet de entrada como normal o anormal para la clase de inteligencia de amenazas.

Este ejemplo mencionado es solo uno de entre tantos que han sido desarrollados por expertos. En las siguientes páginas se describirán algunas técnicas y herramientas adicionales que se están volviendo populares entre investigadores y analistas de inteligencia de amenazas.

Por otro lado, Twint [110] es una herramienta avanzada de scraping de Twitter y OSINT escrita

en Python que no usa la API de Twitter, lo que permite buscar a los seguidores de un usuario, personas que un usuario sigue, tweets y más de manera anónima mientras evita la mayoría de las limitaciones de la API. Como se mencionó anteriormente, Twitter se volvió recientemente una de las principales herramientas para OSINT y así mismo para Threat Hunting, es para este último fin mencionado que se comenzó con el uso e implementación de nuevas plataformas y herramientas, que volvieran esta tarea en una más fácil y rápida de realizar. TweetDeck [111] es una plataforma especial para la red social Twitter y como se menciona en el artículo "Social Media and Security Concerns" publicado por Yadigar N. Imamverdiyev, es una herramienta para el seguimiento y gestión de la información sobre redes sociales. Esta plataforma tiene como objetivo mejorar el performance de la aplicación, lo cual nos permitirá monitorear conversaciones en tiempo real y además organizarlas a gusto propio. Uno de sus atractivos principales es que se pueden tener distintas cronologías en una misma pantalla. Además, se puede tener conversaciones de distintas cuentas en una misma interfaz.

Específicamente para el fin de Threat Hunting haremos uso de la función de monitoreo de la herramienta, pues como se menciona en el artículo "The Impact of Organizational Structure and Technology Use on Collaborative Practices in Com puter Emergency Response Teams: An Empirical Study" [5] publicado por investigadores de la Technical University of Darmstadt, se muestra como en un caso de uso uno de los CERT usó TweetDeck para apoyar el monitoreo semiautomático de cuentas de Twitter, debido a que la plataforma te permite hacer búsquedas especializadas y en distintos paneles de forma simultanea, el monitoreo se automatiza.

El monitoreo se realiza con la búsqueda avanzada de la herramienta. Esta búsqueda avanzada es posible gracias a que TweetDeck admite operadores booleanos como AND y OR, además de operadores como "- "para excluir cierto contenido de la herramienta.

2.4.4 Plataformas basadas en técnicas de engaño: Honeypots

En la actualidad, existen herramientas y/o plataformas que tienen como objetivo principal el poder simular un ambiente o servicio productivo para mantener una comunicación activa con el adversario, comúnmente conocidas como Honeypots, los cuales, permitiendo a los defensores poder recolectar más información sobre las TTP's para poder generar CTI. Existen diferentes plataformas de Honeypots en el mercado, sobre todo por parte de algunos fabricantes de ciberseguridad, tales como TrapX Security [112], Attivo Networks [113] y Fortinet [114] que ayudan a poder detectar amenazas externas e internas, y que estudios revelan que dos tercios de los incidentes encontrados fueron de actores externos, mientras que el tercio restante involucró a actores internos [115]. Existen algunas investigaciones relacionadas con plataformas que cuentan con sistemas multi Honeypots, las cuales se han enfocado a la investigación y relevancia de los datos recolectados mediante ataques [116]. T-Pot se basa en una imagen ISO de Ubuntu 14.04.02, que depende en gran medida de docker y docker-compose. El objetivo que se propone T-Pot, es crear un sistema cuyo rango completo de red TCP, así como algunos servicios importantes de UDP, actúen como señuelos para los adversarios, con el fin de reenviar todo el tráfico de ataque entrante a los sensores Honeypots más adecuados para interactuar y procesar dicha información [117].

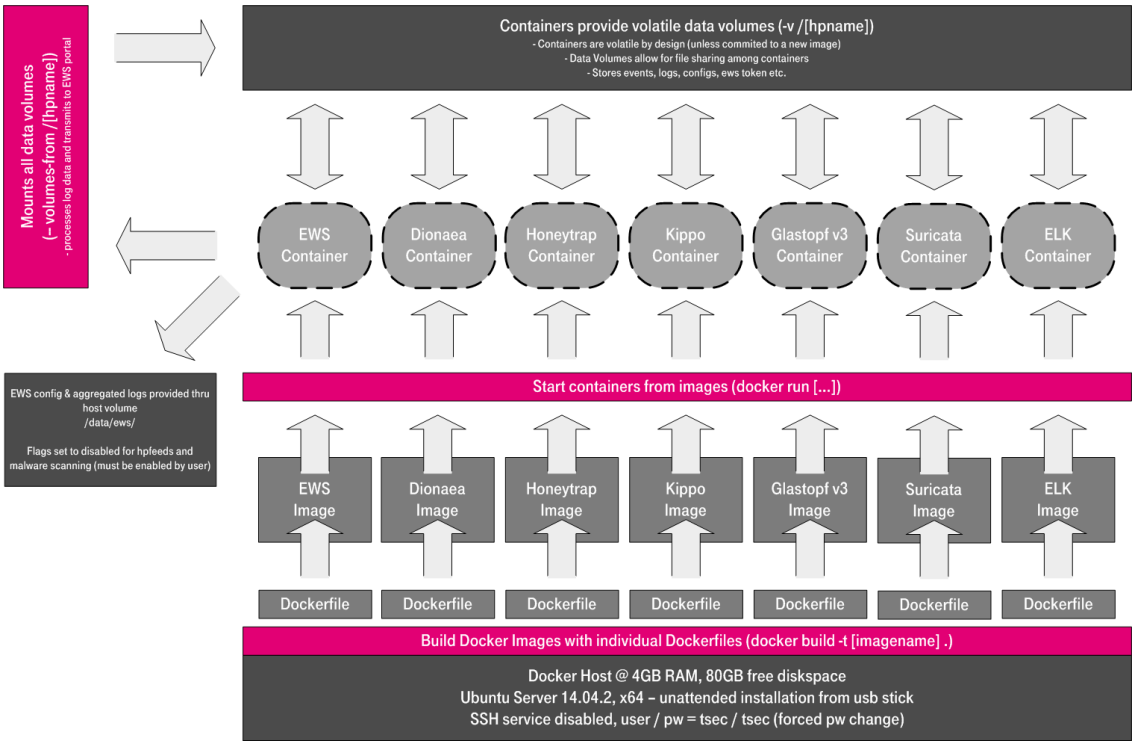


Figura 7. T-Pot arquitectura [117]

El proyecto proporciona múltiples Honeypots acoplados y una gran cantidad de herramientas de investigación preinstalados como ELK, el cual aporta un motor de búsqueda y analítica, así como una interfaz para la visualización de los datos [118], **Spiderfoot** es una herramienta que facilita la realización de tareas de **Footprinting**, al actuar como un agregador de múltiples fuentes de información. Su interfaz web permite realizar búsquedas rápidas y sencillas, ofreciendo una manera eficaz de obtener información relevante sobre objetivos específicos [119]. Por su parte, **CyberChef** es una aplicación web versátil utilizada para **cifrado, codificación, compresión y análisis de datos**, permitiendo a los usuarios manipular datos de forma sencilla a través de su interfaz intuitiva[120].

En el ámbito de la seguridad de la red, **Suricata** se destaca como una herramienta capaz de realizar detección de intrusiones en tiempo real (**IDS**), prevención de intrusiones en línea (**IPS**), monitoreo de seguridad de red (**NSM**) y procesamiento de archivos **pcap** de forma offline [121]. Estas herramientas, entre otras, forman parte de un conjunto de soluciones clave en el análisis y respuesta a ciberamenazas.

T-Pot Honeypots	
adbhoney	Low interaction honeypot designed for Android Debug Bridge over TCP/IP
ciscoasa	A low interaction honeypot for the Cisco ASA component capable of detecting CVE-2018-0101, a DoS and remote code execution vulnerability
citrixhoneypot	Detect and log CVE-2019-19781 scan and exploitation attempts.
conpot	Conpot is a low interactive server-side Industrial Control Systems honeypot designed to be easy to deploy, modify and extend
cowrie	Cowrie is a medium to high interaction SSH and Telnet honeypot designed to log brute force attacks and the shell interaction performed by the attacker.
dicompot	A Digital Imaging and Communications in Medicine (DICOM) Honeypot
dionaea	Dionaea is meant to be a nepenthes successor, embedding python as scripting language, using libemu to detect shellcodes, supporting ipv6 and tls.
elasticpot	This is a honeypot simulating a vulnerable Elasticsearch server opened to the Internet.
glutton	Glutton provide SSH and a TCP proxy. SSH proxy works as a MITM between attacker and server to log everything in plain text.
heralding	Simple honeypot that collects credentials of the following protocols: ftp, telnet, ssh, rdp, http, https, pop3, pop3s, imap, imaps, smtp, vnc, postgresql and socks5.
honeypy	A low interaction honeypot with the capability to be more of a medium interaction honeypot.
honeysap	A low-interaction research-focused honeypot specific for SAP services.
honeytrap	A network security tool written to observe attacks against TCP or UDP services.
ipphoney	This is a honeypot simulating a printer that supports the Internet Printing Protocol and is exposed to the Internet.
mailoney	SMTP Honeypot
medpot	HL7 / FHIR honeypot
rdpy	Remote Desktop Protocol in twisted python.
snare	A web application honeypot sensor
tanner	Decides how SNARE should respond to the client.

Tabla 6. T-Pot Honeypots [117]

2.4.5 Plataformas de Análisis de Malware (Sandbox)

El malware constantemente está evolucionando, todos los días se encuentran nuevas vulnerabilidades y es un hecho que no discrimina plataformas, los números están al alza en todo tipo de tecnologías, desde MacOS disparándose un 420% el malware debido al Ransomware EvilQuest en el tercer trimestre del año 2020 hasta el malware para dispositivos móviles incrementando un 118% entre el tercer y cuarto trimestre del mismo año o con el aumento de 199% en malware de la suite de trabajo de Microsoft Office en el mismo periodo [122], así mismo, se incrementó un 178% el promedio de pagos por rescate de Ransomware entre el año 2019 y 2020, también se detectó que la exigencia de rescate media aumento casi un 300% en el mismo periodo de tiempo [123], se puede notar un crecimiento exponencial entre la probabilidad de pago de rescate y la cuota a pagar, está claro que los ataques cibernéticos incrementan día con día y es importante implementar tecnologías de prevención y defensa. Los atacantes se encuentran en ardua investigación y desarrollo de nuevas amenazas teniendo en cuenta las últimas tecnologías de detección y prevención para poder evadir estos sistemas, por lo tanto, contar con tecnología obsoleta y no adaptarse a los nuevos marcos de trabajo deja a las organizaciones indefensas además de estar teniendo un enfoque incorrecto de tiempo y capital de esta.

El objetivo principal de las plataformas de sandboxing es proteger a los dispositivos finales de

infecciones por malware no conocido, pudiendo detectar previamente en base a la simulación de ejecución de los archivos y poder determinar que se encuentran libres de amenazas. Los malware mas avanzados cuentan con sistemas persistentes y polimórficos los cuales cambian y se adaptan a los sistemas en donde se encuentren con el objetivo de evadir la detección, muchos de los nuevos malware cuentan características de anti-análisis, por esta razón es importante implementar sistemas de sandboxing de última tecnología y aplicar inteligencia de amenazas para detectar posibles falsos negativos, los sistemas sandboxing permiten realizar análisis de malware en base a comportamientos, brindan información de como reacciona el sistema operativo frente a la ejecución del programa en un ambiente controlado.

El análisis de malware es el proceso de examinar un programa potencialmente malicioso con el objetivo de comprender su comportamiento y funcionamiento interno para generar inteligencia que ayude en el combate de nuevas amenazas de seguridad. [124]

Existen dos tipos de análisis de malware [125], los cuales constan de:

- **Análisis estático:** Consiste en analizar la muestra maliciosa sin ejecutarla, la detección se realiza en base a firma de cadenas, n-gramas de secuencia de bytes, sintéticas de bibliotecas, grafico de flujo de control y distribución de frecuencia de opcodes.

- **Análisis Dinámico:** Consiste en analizar la muestra maliciosa ejecutándola en un entorno controlado, antes de ejecutar la muestra de malware se prepara el laboratorio con las herramientas necesarias para recabar los comportamientos y acciones de la muestra.

Los sistemas de sandboxing, gracias a un análisis dinámico de malware, permiten a los analistas recibir información acerca de los eventos y actividades registradas durante el proceso de ejecución del programa presuntamente malicioso, de esta forma el analista puede revisar los eventos en busca de comportamientos anómalos e interceptar su acción en el ambiente controlado.

Las pruebas en entornos aislados detectan proactivamente el malware mediante su ejecución, o detonación, de código en un entorno seguro y aislado para observar el comportamiento y la actividad de salida de ese código. Esto significa agregar una capa extra de seguridad la cual pueda cubrir un espectro mas amplio de amenazas, queda claro que ningún sistema es perfecto e infalible, pero agregar capas de seguridad significa reducir los vectores de ataque, implementar tecnologías proactivas e inteligentes es un acierto muy grande para mejorar la seguridad de información. Con tantos ataques cibernéticos sucediendo día con día se exige analizar y defender casi en tiempo real a los especialistas de ciberseguridad, es prácticamente imposible el que un humano reaccione a tiempo real a las amenazas, por esta razón se toman medidas inteligentes, la inteligencia de amenazas se encarga de desarrollar nuevas tecnologías y metodologías que ayuden a prevenir los ataques antes de que sucedan, teniendo una visión amplia del panorama, sabiendo como se comportan los criminales y cuales son las tácticas, técnicas y procedimientos que utilizan. [126]

El sandboxing permite generar nueva inteligencia de amenazas para mejorar la seguridad, al ser una tecnología proactiva, inteligente y segura, dependiendo del fabricante y del método de

implementación del sandboxing se puede llegar a obtener grandes funcionalidades y beneficios, tener una infraestructura coordinada de detección y respuesta a la cual se le agregue análisis y detección de malware utilizando tecnología de sandboxing puede incrementar mucho el nivel de seguridad y reducir los tiempos respuesta, al detectar algún equipo posiblemente infectado, aislarlo y ponerlo en cuarentena puede ser una respuesta sumamente efectiva que evite un problema mayor en la red.

Existen diversas formas de implementar un sistema de sandboxing dependiendo de las necesidades de la organización o del usuario, tres variantes de implementación de sandbox serian [127]:
Emulación completa de sistema: El sandbox simula el hardware físico de la maquina anfitriona incluyendo todos sus componentes y sistema operativo.

- **Emulación de sistema operativo:** El sandbox emula únicamente el sistema operativo de la maquina anfitriona.

- **Virtualización:** El sandbox se basa en una máquina virtual con características y recursos asignados por el administrador.

Dependerá del proveedor de la solución y, de la forma de implementación de la tecnología sandboxing, las funcionalidades que ofrezca la herramienta, algunas funcionalidades que presentadas en las distintas soluciones de seguridad de sandboxing serian [128] [129]:

- **Análisis hibrido:** Combinación de análisis previo estático y análisis posterior dinámico, implementación de volcado de memoria.

- **Tecnología de anti-evasión:** Detección anti-sandbox de última generación, monitorización de archivos ejecutados en kernel, agente sigiloso difícilmente detectable.

- **Personalización del entorno:** Toma de control del sistema para evitar que el malware se esconda del análisis del sandbox.

- **Análisis de malware potenciado por IA:** Sandboxing basado en IA en dos pasos, primera detección estática y luego detección dinámica con aprendizaje automatizado de comportamientos y amenazas.

- **Protección automatizada de brechas:** Al integrar varios productos de un mismo fabricante automatiza la estrategia de protección contra amenazas.

- **Herramientas de información e investigación basadas en MITRE ATT&CK:** Informe de análisis detallado que mapea técnicas de malware descubiertas en base al marco MITRE ATT&CK con potentes herramientas de investigación.

Las antes mencionadas son solo un ejemplo de la diversidad de funcionalidades con las que puedan contar las soluciones de seguridad de Sandbox, para hacer una selección oportuna de alguna

solución habría que llevar a cabo un análisis de la organización para ver cuales funcionalidades se aplican mejor a las necesidades de esta.

En la actualidad hay muchos fabricantes que ofrecen soluciones de sandboxing para distintos mercados, es importante realizar un análisis previo a la selección de alguna solución, revisar cuidadosamente cual es la que mejor se adapte a las necesidades de la organización y que presente los mejores beneficios, algunas opciones serían las siguientes:

- **Falcon Sandbox** [130] es una herramienta que realiza un análisis exhaustivo de amenazas evasivas y desconocidas, enriqueciendo los resultados con inteligencia de amenazas. Proporciona **indicadores de compromiso (IOC)** procesables, lo que permite a los equipos de seguridad obtener una comprensión más profunda de los ataques de malware sofisticados y reforzar sus defensas en consecuencia. Esta capacidad para analizar malware avanzado ofrece a las organizaciones una ventaja en la identificación y mitigación de amenazas cibernéticas complejas.

- **FortiSandbox** [129], impulsado por tecnología de IA, es parte de la solución de protección contra infracciones de **Fortinet**. Se integra con la plataforma **Security Fabric** de Fortinet para abordar amenazas dirigidas en constante evolución, como **ransomware**, cripto-malware y otros tipos de malware que afectan a una amplia superficie de ataque digital. Esta integración permite una respuesta coordinada y optimizada frente a las amenazas más avanzadas, mejorando la capacidad de detección y mitigación en un entorno de seguridad integral.

- **Advanced Threat Defense** [129] permite a las organizaciones detectar malware avanzado y evasivo, y convertir la información sobre amenazas en acciones y protección inmediatas. A diferencia de los **sandbox** tradicionales, esta solución incorpora funciones de inspección adicionales que amplían su capacidad de detección y exponen amenazas que podrían pasar desapercibidas por otros medios. Estas características mejoradas permiten a las organizaciones identificar y mitigar amenazas cibernéticas de manera más eficaz, reforzando la seguridad de sus sistemas frente a ataques sofisticados.

- **Cuckoo Sandbox** [131] es un sistema de análisis automatizado de malware de código abierto líder en su categoría. Permite analizar cualquier archivo sospechoso y, en cuestión de minutos, genera un informe detallado sobre el comportamiento del archivo cuando se ejecuta en un entorno realista pero aislado. Esta capacidad de **sandboxing** proporciona a los analistas de seguridad información crucial sobre el comportamiento del malware, facilitando la identificación de amenazas sin comprometer la seguridad de los sistemas reales.

El sandboxing permite detectar amenazas más recientes, criticas e incluso desconocidas, fomenta una mayor colaboración entre los equipos de analistas ofreciendo facilidades de procesos y generación de inteligencia de amenazas.

El desarrollo de nuevas amenazas y el descubrimiento constante de amenazas de día cero, para las cuales no se cuenta con alguna firma para la detección o parche de seguridad, presentan un grave peligro para las organizaciones en la actualidad, es necesario implementar nuevos modelos de análisis de malware para hacer frente a este tipo de ataques, implementar inteligencia de amenazas apoyándose de análisis de malware utilizando sandboxing es una medida muy eficiente para repeler ataques avanzados, así mismo, comprender las tácticas, técnicas y procedimientos de los ataques e implementando marcos de trabajo de inteligencia de amenazas como MITRE ATT&CK resulta altamente efectivo. Es importante mantenerse actualizado con las soluciones de seguridad, aunque el sandboxing es una tecnología que lleva mucho tiempo existiendo, es una de las que se ha mantenido mas fuerte y hace mejor frente a amenazas desconocidas, contar con una solución de este estilo es vital para cualquier organización que quiera estar bien protegida frente a las nuevas amenazas.

2.4.6 Plataformas de Orquestacion y Automatiacion de Seguridad (SOAR)

Como hemos mencionado a lo lardo de este documento, la creciente evolución y desarrollo de amenazas constantes, así como los nuevos vectores y técnicas de ataque, han traído consigo muchas soluciones, cambios y sobre todo, técnicas de mitigación reactivas a los defensores de las organizaciones. Por lo tanto, esta gran cantidad de actualizaciones, herramientas y programas que se necesitan implementar para poder defenderse de dichas amenazas, demanda una gran cantidad de recursos que las consuma, implementen y monitoreen, siendo esta, una de las grandes preocupaciones de las organizaciones y sus equipos defensivos, ya que muchos de estos equipos defensivos cuentan con pocos recursos disponibles para poder implementar dichas contramedidas.

En los últimos cuatro a cinco años, las organizaciones han optado por implementar estrategias y soluciones de automatización, las cuales les permiten poder optimizar acciones de investigación, detecciones, mitigación y respuesta a incidentes de seguridad, la cual se ha convertido en un área específica y demandada por muchos negocios y gobiernos. Esta área, se centra en las bases de operaciones de seguridad y se programas para la capacidad de los analistas para alertar sobre la eliminación y comenzar las reparaciones. La tecnología de automatización y orquestación ayuda a resolver la vida diaria; recopilar y enriquecer las advertencias así pudiendo resolver cualquier caso inesperado y predecir a futuro incidentes.

Gartner define SOAR [132] como una tecnología que permite a las organizaciones llevar inputs de una variedad de fuentes (en su mayoría SIEM) and aplicar flujos de trabajo alineado a proceso sy procedimientos definidos. Por sus siglas se puede definir como lo siguiente:

- S = Security
- O = Orchestration
- A = Automation
- R = Response

SOAR es la tecnología que puede automatizar datos, enriquecerlos con inteligencia de fuentes externas para poder detectar y responder incidentes en una sola plataforma. El objetivo principal

de esta plataforma es poder incrementar la capacidad y la eficiencia dentro de las compañías y departamentos de seguridad, reduciendo el tiempo que ocupan los analistas para trabajar en incidentes y aumentando su capacidad de cobertura por medio de acciones automatizadas.

La tecnología SOAR como sus iniciales indican, orquestan una variedad de programas compatibles, recopilando los eventos detectados y correlacionando los datos de estos, para poder generar reportes automatizados con información accionable. Esto ataca directamente el problema de las organizaciones relacionado al tiempo en que un equipo de seguridad realiza una investigación, así como su falta de personal capacitado [133]. La automatización de la seguridad consiste en implementar iniciativas de seguridad capaces de ser programadas para detectar, analizar y corregir ciberataques reconociendo amenazas potenciales y clasificando las alertas a medida que surgen y que suceden, y luego actuando a su debido tiempo. La automatización y orquestación del SOAR funciona de manera eficiente para el equipo de seguridad de forma que no tengan que pasar manualmente perdiendo tiempo. También se puede clasificar vulnerabilidades y riesgos mediante un proceso paso a paso completamente automático, la toma de decisiones de parte de los profesionales para evaluar el incidente y determinar si se trata de un problema son facilitadas y simplificadas. Gracias a la adopción de las soluciones SOAR, muchas organizaciones están implementando una estrategia de automatización, la cual les ha traído ciertos beneficios:

- Aumentar la productividad de los ingenieros de seguridad.
- Reducir el tiempo medio de resolución.
- Incorporar los productos necesarios para proteger contra amenazas ágiles.

Esto está comenzando a evolucionar al aumentar la inteligencia de amenazas de modo que podamos inferir con mayor precisión la decisión correcta y la mejor acción en un escenario particular. En lugar de simplemente recopilar y presentar datos, se agrega análisis y cognición dando como resultados inteligencia artificial efectiva y educación informática que se utilizan para ayudar a los analistas a mejorar en función de mejor información a su disposición.

Las empresas que buscan soluciones SOAR tienen normalmente entre 20 o 30 proveedores de soluciones de TI, lo cual representa un reto en la operación, mantenimiento y monitoreo de dichas soluciones. Cabe mencionar, que algunas automatizaciones pueden implementarse rápidamente, reduciendo significativamente el tiempo requerido para integrarse en sus soluciones existentes y de terceros. Existen diferentes enfoques para la implementación también, algunos proveedores facilitan la replicación de una implementación de flujo de trabajo, para iniciar y ejecutar sus planes a futuro con las empresas. La disposición de la empresa para conectar productos con terceros los productos a través de sus API’s deben ser abierta para tener también una buena experiencia hacia los consumidores. Y suele ser un reto el implementar todas las arquitecturas de las diferentes compañías de terceros con las que se interactúa esto también siendo unas de las varias funciones de los SOAR.

Además, es necesario contar con especialistas de ciberseguridad que puedan conducir el conocimiento desde la primera línea de defensa hacia el resto de sus compañeros e implementar las mejores prácticas. Aunque la implementación de un sistema de orquestación no es algo rápido,

el apresurarse no es una manera excelente para comenzar, y el desarrollar manuales de usuario y protocolos que puedan quedar con los objetivos y cultura de la empresa. Muchos comienzan con las implementaciones de análisis y filtración de correos electrónicos para la detección de archivos adjuntos malignos y otro tipo de engaños. Por ejemplo, algunos analistas de seguridad como un esfuerzo paralelo deben examinar las URL dentro de sitios web sospechosos y los archivos descargados que llegan por correo electrónico para ver si son maliciosos o no. Esto es fácil de manejar para herramientas de automatización. Para optimizar los recursos también es recomendable el Mapear los procesos que se necesita automatizar durante los primeros doce a veinticuatro meses, con un enfoque en los casos de bajo esfuerzo, bajo precio y poco ahorro de tiempo.

Es necesario proteger las soluciones adoptadas además de seleccionar el caso adecuado para su uso y desarrollo. La integración y las credenciales protegidas en las diversas tecnologías de terceros en automatización y orquestación instrumentos será la única forma en que realmente puedan organizar. Al final se puede tener una estrategia de automatización e inteligencia artificial auto responsiva. Una ves teniendo en cuenta las funciones y ventajas del SOAR, se puede analizar su composición interna y sus funciones. Recorriendo las siglas de estas plataformas nos encontramos primero con la orquestación de seguridad.

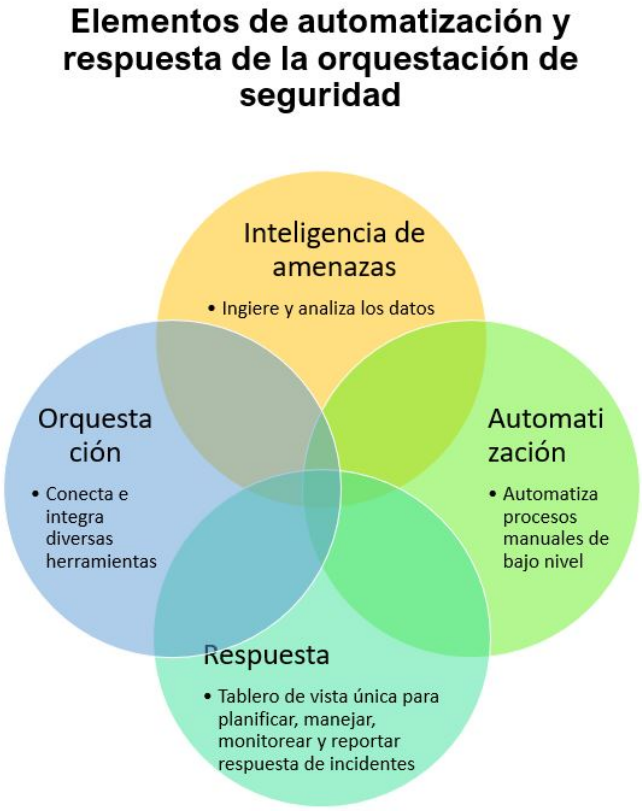


Figura 8. Los elementos de SOAR

Los sistemas interconectados pueden incluir como se describe anteriormente como escáneres de

vulnerabilidades, antivirus, productos de protección de punto a punto, analizadores de comportamiento de usuarios, “firewalls”, así como varios programas de detección de intrusos y monitoreo de incidentes; también incluyendo herramientas de terceros y otras plataformas de inteligencia de riesgos. Con los datos procesados se pueden detectar actitudes anormales y los riesgos que pueden estar interactuando con el sistema, esto puede traer mucha información para analizar, pero con los filtros de las herramientas se pude facilitar su procesamiento. Seguido de la orquestación viene la automatización. Esta herramienta recolecta las alertas y advertencias que ha recibido la parte de orquestación y las analiza para ser procesadas en reportes automáticos y periódicos que pueden remplazar a los reportes manuales de los administradores que necesitan enfocarse en cosas prioritarias. Todas las actividades desempeñadas por el equipo de seguridad, o al menos la mayoría pueden ser ejecutadas por los equipos SOAR y sus inteligencias artificiales haciendo que la plataforma arroje incluso recomendaciones personalizadas y expresar claramente cuando se necesita el involucramiento de un humano. Por último, tenemos la sigla de la respuesta a incidentes y riesgos. Este proceso ofrece una guía de acción unificada para las planeaciones, administraciones y monitoreos de los analistas y sus acciones de contención en caso de incidente. también esto incluye actividades de respuestas después del incidente, así como investigación y reportes de inteligencia para la empresa.

Contar con las plataformas SOAR trae beneficios excelentes a las empresas y a los equipos de seguridad empresarial. Los tiempos de reacción y detección de incidentes más rápidos y pueden ser procesados con mayor efectividad. El volumen y la velocidad de la detección de amenazas y los monitoreos a amenazas a la seguridad aumentan constantemente. El procesador de datos mejorado de SOAR, combinado con puede reducir el tiempo promedio de descubrimiento y el tiempo promedio de respuesta. Al detectar y responder más rápidamente a las amenazas, se puede reducir el impacto y los costos. Con este mejor procesamiento de amenazas. Al integrar más datos de una amplia gama de herramientas y sistemas, las plataformas SOAR pueden tener un contexto digerible para los administradores, mejores análisis e inteligencia de amenazas actualizada con inteligencia artificial.

La gestión simplificada junto con la administración sencilla otorga facilidad de uso incluso para usuarios nuevos, unificando todas las herramientas sobre una interfaz amigable. Esto ayuda a los equipos de operaciones de seguridad y otros equipos al centralizar el manejo de información y datos, simplificar la administración y ahorrar tiempo. Además, con la escalabilidad de los procesos manuales que consumen mucho tiempo puede ser una carga para los empleados e incluso imposible de seguir a medida que aumenta el volumen de eventos de seguridad. La orquestación, automatización y flujos de trabajo de SOAR pueden satisfacer las demandas de crecimiento fácilmente e impulsan la productividad de los analistas.

2.5 Retos de CTI

El reto principal en la ejecución de una estrategia de CTI, se centra en la calidad de la inteligencia obtenida a través del análisis de los datos y radica principalmente en poder transformar toda esta gran cantidad de información en algo accionable que pueda utilizarse para tomar decisiones para la alta dirección [134], por ejemplo, el poder priorizar actividades, asignar presupuesto o personal

en base a los impactos que se pueden llegar a tener basado en los datos recolectados. Esto requiere no solo de tiempo y/o esfuerzo del equipo de TI o ciberseguridad, sino también de organización, colaboración entre las distintas áreas, experiencia y recursos asignados por la alta dirección para realizar estas investigaciones con éxito. Si bien, la comercialización de productos y servicios relacionados con CTI de distintos desarrolladores y fabricantes han ayudado a automatizar muchas de las tareas relacionadas con la extracción, detección, actualización de amenazas y sobre todo la automatización de respuestas a incidentes [135].

Para poder interrumpir o impedir significativamente el ataque o intrusión del adversario, es necesario tener una estrategia defensiva y preparar la infraestructura para tener en cuenta las necesidades de seguridad, controles, procesos y recursos con los que se debe de contar. Con el conocimiento de las tácticas y objetivos del adversario, los defensores deben preparar su infraestructura para contrarrestar ataques en la gama más amplia posible para cubrir todos los posibles vectores de ataque de los adversarios. Sin embargo, existen algunas investigaciones que mencionan esto como un gran reto, ya que se menciona que el campo de CTI carece de una metodología madura, la cual puede afectar el análisis de las amenazas y adversarios por parte de los defensores [136]. A pesar de sus desafíos, la CTI no debe descartarse aún, ya que es un campo emergente que tiene mucho potencial y constante desarrollo por la comunidad de analistas de ciberseguridad, teniendo como objetivo el poder aplicar estrategias y controles de defensa contra los adversarios que buscan comprometer a una organización.

3 Metodología

El flujo seleccionado para la implementación del método propuesto se basa en el Ciclo de vida de la Inteligencia de Amenazas:

3.1 Selección de Eventos de ciberseguridad reales ocurridos en México para el método propuesto

Una de las fases más relevantes del ciclo de vida de Inteligencia [65], se enfoca en poder recabar la información relacionada a amenazas de interés de acuerdo con la población que se desea proteger para así entender los riesgos, amenazas y requerimientos necesarios a investigar, por lo tanto, en esta sección mencionaremos algunas de las plataformas que pueden ser utilizadas para recolectar información relevante para México.

Por lo tanto, la clave para poder realizar un buen proceso de CTI es la defincion de fuentes y recopilación de información, es decir, una vez identificados los requisitos, el siguiente paso es identificar cómo obtener acceso a la información que ayudará a responder a los requisitos. Dichas fuentes de información se les denominan Feeds de inteligencia o Feeds de CTI, los cuales emiten información relevante para los analistas que pueden consumir de distintas formas. Esta definición puede explicarse con un ejemplo desde la perspectiva del análisis de incidentes cibernéticos de tal manera que los datos pueden ser tales como la IP, el dominio, la URL o el correo electrónico que se pueden recopilar de los sistemas o fuentes de información abiertas en internet como Google. Además, la información puede describirse como la URL explotada para el phishing, el dominio que difunde el código malicioso y la IP que establece la comunicación C&C con el código malicioso [67]. La inteligencia de amenazas cibernéticas es el resultado del análisis integral que informa que un grupo de ciberdelincuentes tiene como objetivo vulnerar principalmente a entidades financieras, y recientemente se descubrió que el código malicioso era una variante de alguna amenaza antes vista. Por lo tanto, se requieren acciones para bloquear la dirección IP del servidor de C&C frecuentemente utilizado por el código malicioso.

SANS [65] muestra cuales son las fuentes de inteligencia que más consumen las organizaciones para poder realizar CTI:

Sources for Gathering Intelligence	2020
Open source or public CTI feeds (DNS, MalwareDomainList.com)	74.30%
Threat feeds from CTI-specific vendors	68.90%
Threat feeds from general security vendors	68.50%
Community or industry groups such as information sharing and analysis centers (ISACs) and Computer Emergency Readiness Teams (CERTs)	68.20%
Security data gathered from our IDS, firewall, endpoint and other security systems	63.40%
External sources such as media reports and news	63.10%
Incident response and live forensics	63.10%
SIEM platform	62.00%
Vulnerability data	60.60%
Network traffic analysis (packet and flow data)	57.00%
Forensics (postmortem)	56.40%
CTI service provider	45.90%
Application logs	44.40%
Other formal and informal groups with a shared interest	43.30%
Closed or dark web sources	42.10%
Honey pot data	29.90%
Shared spreadsheets and/or email	21.00%
Other	1.50%

Sources for Gathering Intelligence [65]**.**

Como se mencionó anteriormente, existen diversas plataformas y/o servicios disponibles para poder recolectar información relevante sobre tendencias de amenazas, una amenaza en específico, así como las técnicas que utilizan. Ante esto, surge la primera pregunta de investigación:

¿Existen set de datos disponibles que brinden información de eventos de ciberseguridad ocurridos en el sector mexicano?

En esta sección, se tiene como contribución mostrar algunas de las plataformas que brindan información sobre las amenazas cibernéticas que ocurren en México y que pueden ser utilizadas para generar información relevante y accionable en una organización, es decir, utilizando como punto de partida la información recolectada de alguna tendencia de un malware o ciber amenaza ocurrida o que tenga como objetivo México, categorizándolas en 5 secciones (Phishing, Firewall/IPS, Honeypots, Vulnerability/Scanners and Social Newtrok data) para que así las organizaciones puedan realizar una investigación sobre dicha ciber amenaza para entender su objetivo, técnicas y procedimientos para poder medir su impacto al negocio, con el objetivo principal de convertir dicha información en una estrategia de ciberseguridad para disminuir el riesgo de alguna incidencia a la organización.

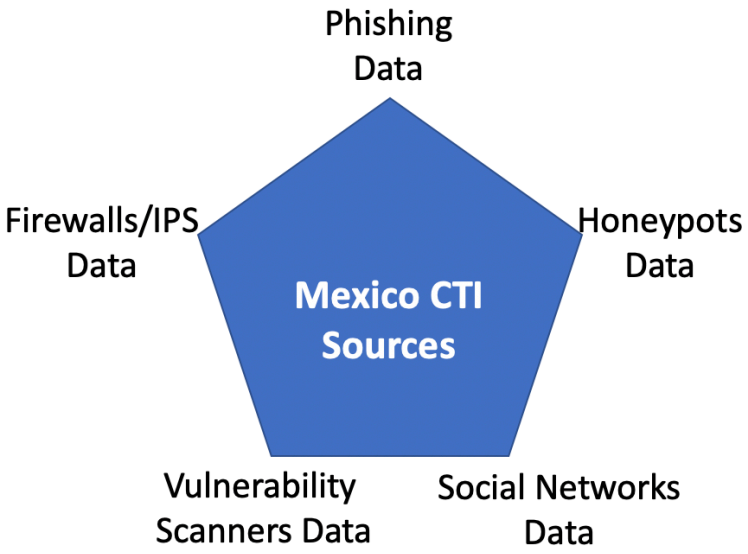


Figura 5. Fuentes de CTI de México.

Para esto, cubriremos algunas de las principales áreas de interés de inteligencia, entre ellas existen plataformas de tendencias de ciberamenazas basadas en detecciones de eventos de ciberseguridad de dispositivos perimetrales (Firewalls, IPS, EPP, etc.), tales como Fortinet Threat Intelligence Insider Latin America [137], una herramienta de tendencias de amenazas trimestrales por FortiGuard Labs [68] para 10 países de la región de Latinoamérica, entre ellos, México, que cuenta con datos recopilados y analizados de millones de eventos de ciberseguridad diarios detectados por los sensores desplegados en la región, además ofrece datos de tendencias de ciberamenazas por país e información sobre los diez principales ciberataques para los países de la región, en la

categoría de malware, exploits y botnets, así como resúmenes ejecutivos regionales de las principales áreas de riesgo y vulnerabilidades identificadas, así como consejos de seguridad y hallazgos clave, además se tiene la posibilidad de descargar dicha información en formato PDF, la cual se actualiza trimestralmente en los 3 idiomas principales de la región (ingles, portugués y español). Otra fuente de CTI que ofrece información de vulnerabilidades y visibilidad de dispositivos expuestos a internet en sector Mexicano, es el motor de búsqueda Shodan [138], es decir, si un dispositivo está conectado directamente a internet (desde computadoras de escritorio pequeñas hasta plantas de energía nuclear, etc.), Shodan lo consulta para obtener la información pública disponible de dicho dispositivo, en el cual se han realizado diversos estudios de los riesgos que existen sobre los dispositivos expuestos a internet [139]. Recientemente Shodan agrego paneles de exposición de dispositivos de internet para ciertos países, entre ellos uno para México [140], en el cual se muestran la cantidad de Sistemas de Control Industriales expuestos en el país, así como las vulnerabilidades más relevantes. Además, se realizó una búsqueda general en esta herramienta utilizando el filtro "country:"MX"", e cual nos arrojó un resultado total de 4,880,789 dispositivos expuestos a internet [88], de los cuales destacaban ciudades como CDMX (616,591), Zapopan (212,236), Guadalajara (189,331), Monterrey (180,109), San Luis Potosí (88,374). Por otro lado, existen diversas plataformas compuestas por una red de Honeypots, que no son más que dispositivos expuestos a internet que fungen como señuelos para atraer ciberamenazas y poder monitorear las técnicas utilizadas por dichas ciber amenazas, tales como Bad Packets Cyber Threat Intelligence [141], el cual cuenta con una red global de Honeypots que detectan las actividades de botnets activas, que están escaneando internet y/o participando en actividades maliciosas, además cuentan con Honeypots desplegados en México [142], los cuales pueden brindar información de las ciberamenazas que tienen como objetivo a nuestro país, en el cual dicha herramienta ha sido utilizada para distintos estudios para monitorear el tráfico de campañas de botnet escaneando los dispositivos expuestos a internet [143] y el perfilamiento de sistemas industriales críticos (ICS) expuestos en la web [144]. Así mismo, también se encontraron plataformas que brindan feeds de inteligencia relacionadas a sitios web fraudulentos, mejor conocidos como Phishing, tales como APWG [145] quienes mencionan en su reporte de Actividades y tendencias de Phishing para el primer trimestre del 2020 que los dominios de código de país (ccTLD), como .UK para el Reino Unido y .MX para México eran aproximadamente el 44% de los dominios en el mundo a principios del primer trimestre, pero solo el 27% de los dominios en la muestra del primer trimestre. Otra plataforma de la cual se puede descargar información de Phishing es OpenPhish [146], el cual brinda distintos planes para el uso de su plataforma, desde la descarga de URL's de manera gratuita, hasta información detallada de cada sitio. Cabe recalcar que utilizando la descarga de sitios de Phishing gratuita que ofrece la plataforma [147], se encontraron al menos 15 sitios con dominio ".mx" y 2 con la palabra "México" en la URL que han sido detectados con alguna actividad maliciosa. Otra herramienta que pude brindar inteligencia sobre sitios maliciosos para México es Urlhause, la cual ofrece feeds de sitios maliciosos que se pueden descargar y para México se encontraron 291 URL´s catalogadas como Phishing o maliciosas [148].

Las plataformas de redes sociales permiten a los usuarios y organizaciones comunicarse y compartir información. Para los profesionales de seguridad, podría ser más que una simple herramienta de red, es decir, puede ser una fuente adicional de información valiosa sobre temas desde vulnerabilidades, exploits y malware hasta actores de amenazas y actividades cibernéticas

anómalas. Por ejemplo, Twitter y Facebook no son solo una plataforma para compartir contenido, promoción o redes sociales. Existen herramientas de inteligencia de código abierto (por ejemplo, TWINT [149] y ThreatExchange [150]) que pueden raspar datos o interfaces de programación de aplicaciones (API) de transmisión de Twitter disponibles públicamente que pueden recopilar datos de muestra para su análisis. También vimos que los bots compartían los indicadores de compromiso (IoC) más recientes e incluso las reglas de detección de amenazas. De hecho, hay información disponible públicamente sobre cómo los bots de Twitter pueden usarse para monitorear dispositivos de Internet de las cosas (IoT). También hay Honeypots de código abierto que pueden registrar datos en Twitter.

Existen plataformas de inteligencia de amenazas basada en la nube, tales como IBM X-Force Exchange [151] es que le permite utilizar, compartir y actuar en base a la inteligencia de amenazas. Esta plataforma permite investigar rápidamente las ciberamenazas más recientes en la industria basado en etiquetas, hashes o indicadores, así como añadir inteligencia accionable, así como colaborar con otros analistas de ciberseguridad y además nos muestra distintas opciones de malware, análisis, perfiles, etc. En esta plataforma se encontraron 35 resultados de ciberamenazas realizando una búsqueda con la etiqueta "México" la cual nos permitió realizar una búsqueda de 35 ciberamenazas documentadas en esta plataforma, de las cuales tan solo 12 estaban relacionadas con México en 2020. Por otro lado, las organizaciones de ciberseguridad han creado mapas de ciberamenazas en tiempo real, para proporcionar una vista general de los ataques y su relación entre países, por ejemplo, Live Cyber Threat Map es una página de Check Point gratuita que muestra en tiempo real los ataques de Malware, Phishing y Exploit en el mundo, así como estadísticas. Al enfocar a México (haciendo clic en el mapa) [152], nos muestra las tendencias de ciberamenazas en los últimos 30 días: Banking Trojans 1.2%, Botnet 6.2%, Cryptominer 3.6%, Mobile 6.5%, Ransomware 0.3%. Otro mapa de amenazas que puede brindar información relevante para México es el mapa de DDoS de la empresa A10 [153], la cual señala que en México existen más de 115,000 dispositivos que pueden utilizarse como armas para llevar a cabo una ataque de denegación de servicios distribuido (DDoS), tales como 21,097 hosts identificados e infectados con malware de DDoS (denominados como Drones), así como 2,884 hosts identificados que están llevando a cabo actividad maliciosa (denominados como Abuse), 5,760 servidores de DNS públicamente expuestos y vulnerables para ser explotados por un ataque de amplificación, así como servidores de NTP (1,608), SSDP (26,421), SNMP (27,375), TFTP (28.527), entre otros. Adicional se encontró servicio que su principal función es ser un motor de búsqueda de servidores y servicios es su soporte para IPv6 generando inteligencia, con esta información obtiene un análisis y evalúa la exposición al riesgo de las organizaciones en tiempo real [154] [155]. Las herramientas y las fuentes de datos siempre serán vitales para el proceso, pero el mundo del análisis de inteligencia está intrínsecamente dirigido por analistas y un enfoque se ubica allí con razón. Compartir no solo IoC y TTP adversarios, sino también procesos y procesos analíticos, ayudará a la comunidad a continuar madurando. Algunos procesos para compartir incluyen estrategias para medir la efectividad de un programa CTI. [65]

Ante esto, pudimos encontrar diferentes fuentes de inteligencia relacionadas con informacion para México, las cuales seran analizadas para dictaminar la capacidad de generar un modelo de deteccion de amenazas basado en la evidencia recolectada de las fuentes descritas en esta sección

siendo FortiGuard Labs [156] la más completa disponible, ya que cuenta con datos de Firewalls de Siguiente Generación con motores de Sistemas de Prevención de Intrusos para detección de técnicas de explotación, un motor de detección Malware y detección de comunicación de campañas de Botnet el cual puede utilizarse en esta investigación ya que un Firewall típicamente es la primera línea de defensa y puede ser utilizado como un sensor que recolecte datos de todo el ciberespacio mexicano.

3.1.1 Conjunto de Datos Seleccionados y Tipos de Amenazas

El conjunto de datos seleccionado para este proyecto se originó a través de la colaboración con uno de los socios industriales de la Universidad Autónoma de Nuevo León, Fortinet. La fuente de datos es parte de la iniciativa de investigación de inteligencia de amenazas de FortiGuard Labs (FortiGuard Labs, 2021), asegurando un conjunto robusto y actualizado de información relevante para el análisis de ciberseguridad en México.

3.1.1.1 Descripción de Tipos de Amenazas

Los datos se recopilaron de una red mundial de productos de seguridad Fortinet, implementados por diversas empresas, desde pequeñas y medianas hasta grandes corporativos. Dos sensores principales fueron utilizados: el firewall "next generation" FortiGate, una solución de red avanzada, y el producto de software de endpoint FortiClient. Los tipos de amenazas detectadas por FortiGate incluyen Botnet, Sistema de Prevención de Intrusiones (IPS), y Virus/Malware.

- **Botnet:** La detección de actividades de botnet es fundamental para comprender las amenazas que se originan desde redes de dispositivos comprometidos. Este análisis se centrará en la identificación de patrones de comportamiento y características específicas asociadas con botnets.
- **Sistema de Prevención de Intrusiones (IPS):** La utilización de IPS amplía la capa de seguridad, identificando y bloqueando comportamientos maliciosos a través del análisis de firmas de tráfico. Este componente permitirá un enfoque más proactivo para la detección y prevención de intrusiones.
- **Virus/Malware:** La inspección avanzada de paquetes de datos por parte del firewall FortiGate permite la identificación de malware y virus, proporcionando una comprensión más profunda de las amenazas que pueden afectar la seguridad de la red.
- **Endpoint:** La detección de amenazas en el nivel de los puntos finales es crucial en un entorno cibernético en constante evolución. El análisis de las amenazas en los endpoints proporciona información sobre las tácticas y técnicas específicas utilizadas por actores maliciosos.

3.1.1.2 Utilización del Conjunto de Datos en la Tesis

Este conjunto de datos permitirá un análisis exhaustivo del panorama de amenazas cibernéticas en México. Al aprovechar la información recopilada por los firewalls perimetrales, se pueden lograr los siguientes objetivos:

- **Identificación de Patrones de Ataque:** El análisis de los datos revelará patrones de ataque específicos, permitiendo la identificación temprana de amenazas recurrentes y la adopción de medidas preventivas efectivas.
- **Evaluación de Vulnerabilidades:** La comprensión de los tipos de amenazas y sus métodos proporcionará información crucial para evaluar las vulnerabilidades en las redes y sistemas de las organizaciones mexicanas.
- **Análisis de Tendencias de Ciberseguridad:** La recopilación de datos a lo largo del tiempo permitirá un análisis de tendencias, proporcionando información valiosa sobre la evolución de las amenazas cibernéticas en el contexto mexicano

3.1.2 Beneficios de Utilizar un Conjunto de Datos de Firewalls Perimetrales

La elección de un conjunto de datos basado en firewalls perimetrales con amplia cobertura y diversidad de sensores ofrece varios beneficios para la investigación:

- **Amplitud de Datos:** El conjunto de datos abarca múltiples tipos de amenazas, proporcionando una visión integral de las posibles vulnerabilidades y ataques que enfrentan las organizaciones mexicanas.
- **Actualización Continua:** Al provenir de FortiGuard Labs, se garantiza la actualización constante del conjunto de datos, reflejando las amenazas más recientes y relevantes en el panorama cibernético.
- **Diversidad de Fuentes:** La inclusión de datos de firewalls perimetrales y endpoints brinda una perspectiva completa, permitiendo la identificación de amenazas tanto en la red como en dispositivos individuales.
- **Aplicabilidad Práctica:** La información recopilada se relaciona directamente con el entorno de seguridad de las organizaciones, brindando una base sólida para implementar estrategias de ciberseguridad efectivas.

En resumen, la utilización de este conjunto de datos fortalecerá la investigación al proporcionar una comprensión detallada de las amenazas cibernéticas en México, permitiendo la identificación de patrones, evaluación de vulnerabilidades y análisis de tendencias para mejorar las prácticas de ciberseguridad en el país.

3.2 Selección de Plataformas para el modelado de los datos

En esta sección se pretende evaluar 2 diferentes plataformas de CTI y 3 herramientas de Análisis y Visualización de datos con el objetivo principal de poder comprender y documentar:

- Procesos de Instalación
- Recursos Necesarios
- Casos de Uso

3.2.1 Caso de Estudio: Instalación plataforma de CTI T-Pot

Para realizar este experimento, se decidió utilizar la infraestructura de la nube publica de AWS, la cual permite desplegar servicios, aplicaciones en un ambiente expuesto a internet con una IP publica, lo cual permite que la plataforma sea un blanco expuesto para los atacantes. Los recursos utilizados en la nube de AWS fueron los siguientes:

T-Pot Resources	
RAM	t2.xlarge (16Gbps)
vCPUs	4
OS	Linux/Debian 10
Days Active	20
Public Ip	Yes

Tabla 7. Recursos asignados en AWS para T-Pot

Para desplegar la plataforma T-Pot en AWS, se realizaron las siguientes configuraciones dentro de la plataforma de AWS, utilizando sus servicios de EC2:

Paso 1. Iniciar sesión en AWS e ingresar a la consola de administración
Paso 2. Dar click en Servicios
Paso 3. Seleccionar EC2

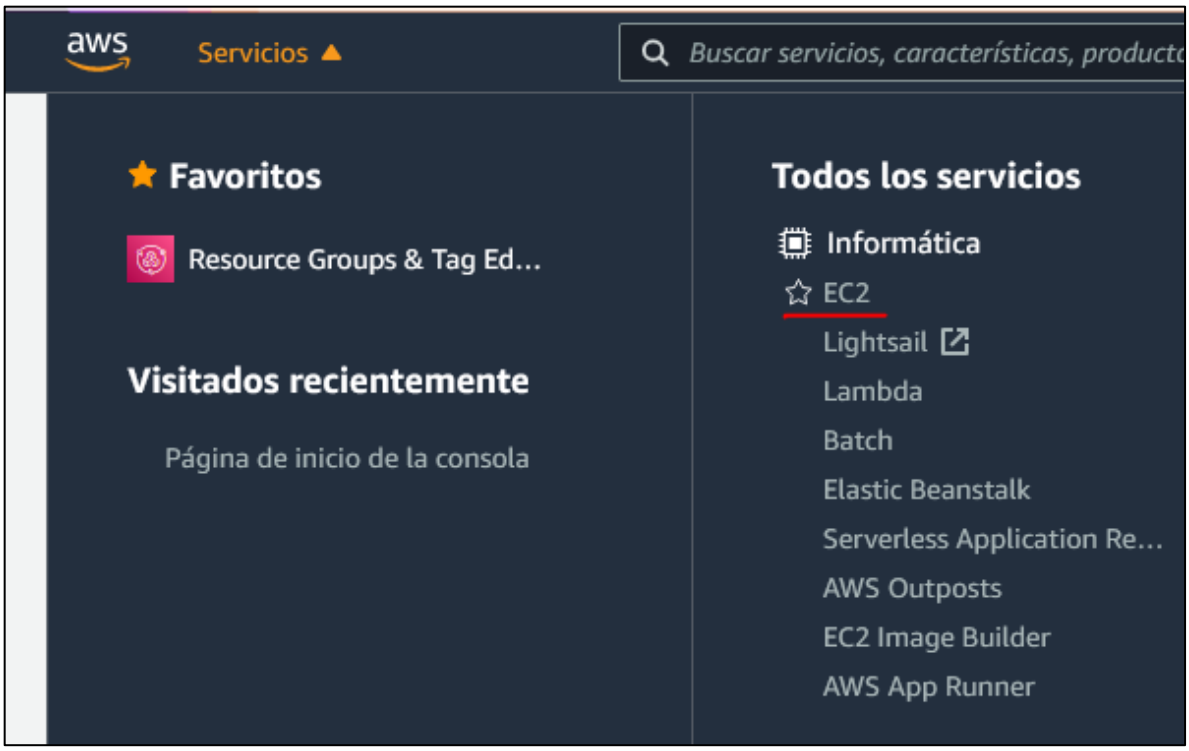


Figura 10. Amazon Web Services

Paso 4. Dar click en "Launch instance"

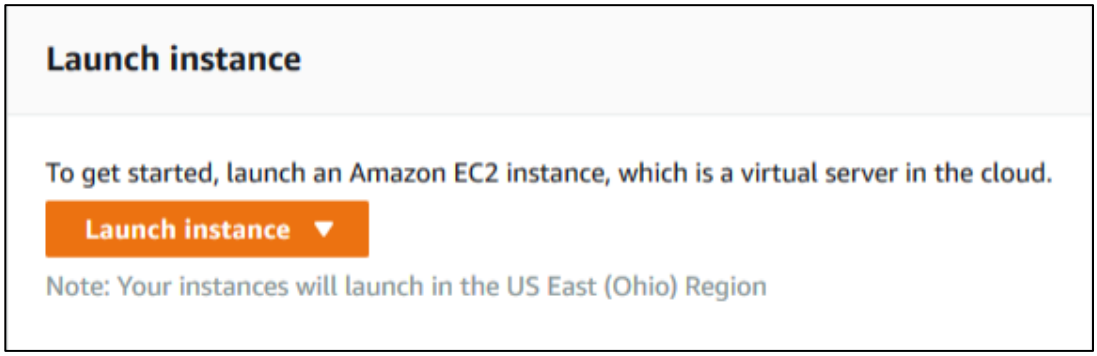


Figura 11. Iniciar Instancia en la nube de AWS.

Paso 5. En esta parte se debe seleccionar una Amazon Machine Image (AMI), la cual es básicamente la imagen del ambiente virtual donde estará corriendo la instancia. En la barra de búsqueda ingresa "Debian 10" y seleccionar AWS Marketplace:

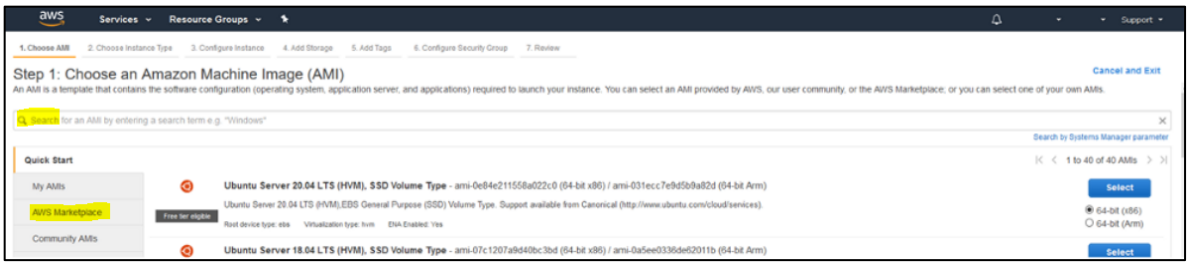


Figura 12. Selección de Ambiente de la Instancia.

Paso 6. Elegir Debian10 Buster y continuar.

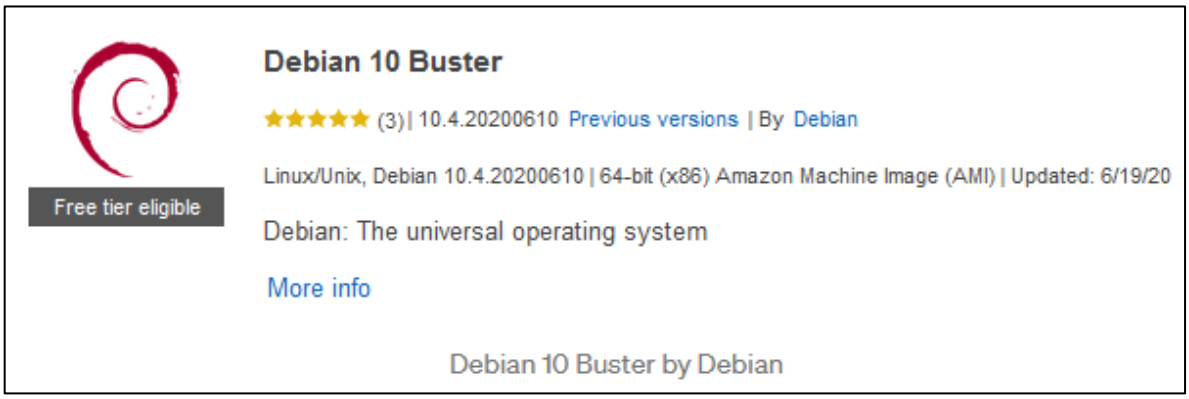


Figura 13. Selección de Sistema Operativo.

Paso 7. Elegir tipo de instancia: se refiere a los recursos que se le asignarán al ambiente virtual. Para este caso, T-Pot honeypot correrá bien en un tipo de instancia “t2.large”

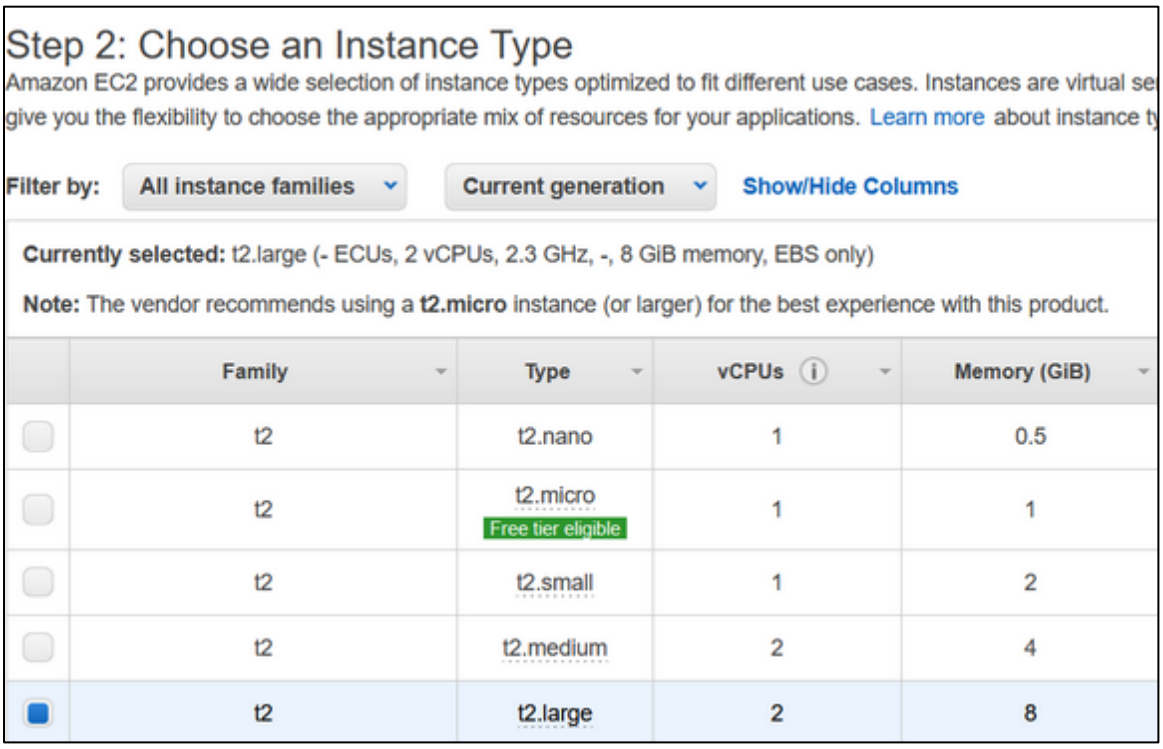


Figura 14. Selección de performance de la instancia.

Paso 8. En "Configure Instance Details" no es necesario configurar nada distinto, por lo tanto, dejarlo como está por defecto.

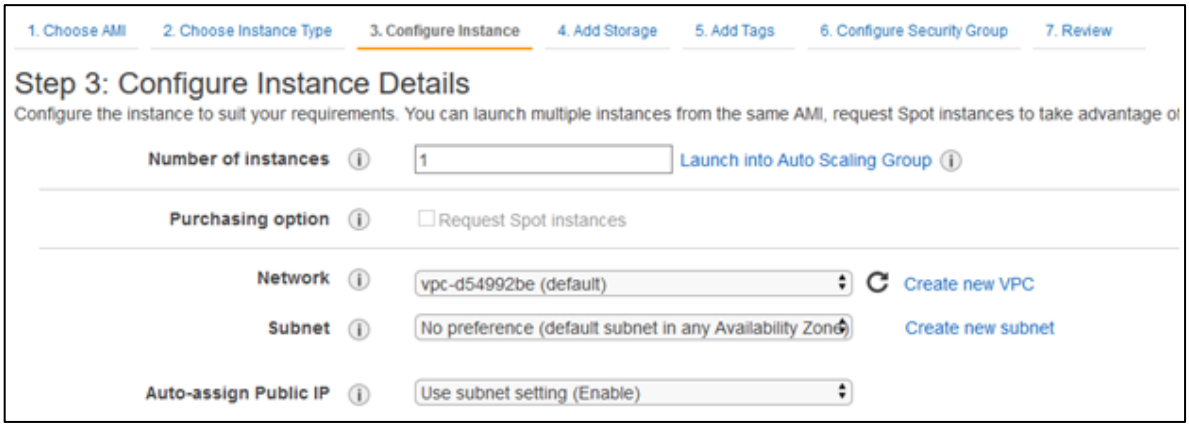


Figura 15. Detalles de configuración.

Paso 9. Capacidad de almacenamiento: La documentación de T-Pot recomienda 128 GB, por lo tanto, ingresar este mismo dato en la configuración.

Figura 16. Selección de almacenamiento de la instancia

Paso 10. La siguiente pantalla en AWS sugiere agregar Tags o etiquetas, no es necesario hacerlo para este proyecto. Dar click en Next

Paso 11. Configurar Grupo de Seguridad: en esta sección se configuran las reglas de firewall que controlan el tráfico hacia la instancia. Por defecto, la regla permite a cualquier IP conectarse a la instancia mediante SSH, lo cual no es seguro. Por lo tanto, cambiar la fuente a "My IP"

Figura 17. Configuración de Firewall perimetral.

Paso 12. Dar click en el botón de "Review and Launch"
Paso 13. Revisar las configuraciones, posteriormente dar click en Launch.
Paso 14. Se abrirá una ventana diciendo que se necesita crear una "Key Pair", la cual es la llave que permitirá conexiones seguras mediante SSH a la instancia. Seleccionar "create new key pair" e ingresar un nombre para esta llave. Después, click en Download Key Pair.
Paso 15. Seleccionar Launch Instances
Paso 16. Una vez que la instancia aparezca en status "Running", dar click en el botón de Connect

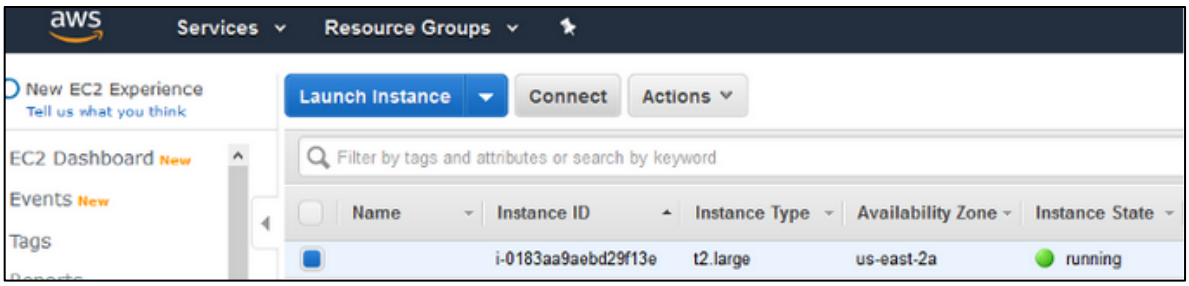


Figura 18. Iniciar Instancia.

Paso 17. Iniciar la aplicación de PuTTygen. Click en “Load” y seleccionar el archivo con la llave (.pem). Ingresar una passphrase y confirmarla. Luego dar click en Save Key y guardarla.

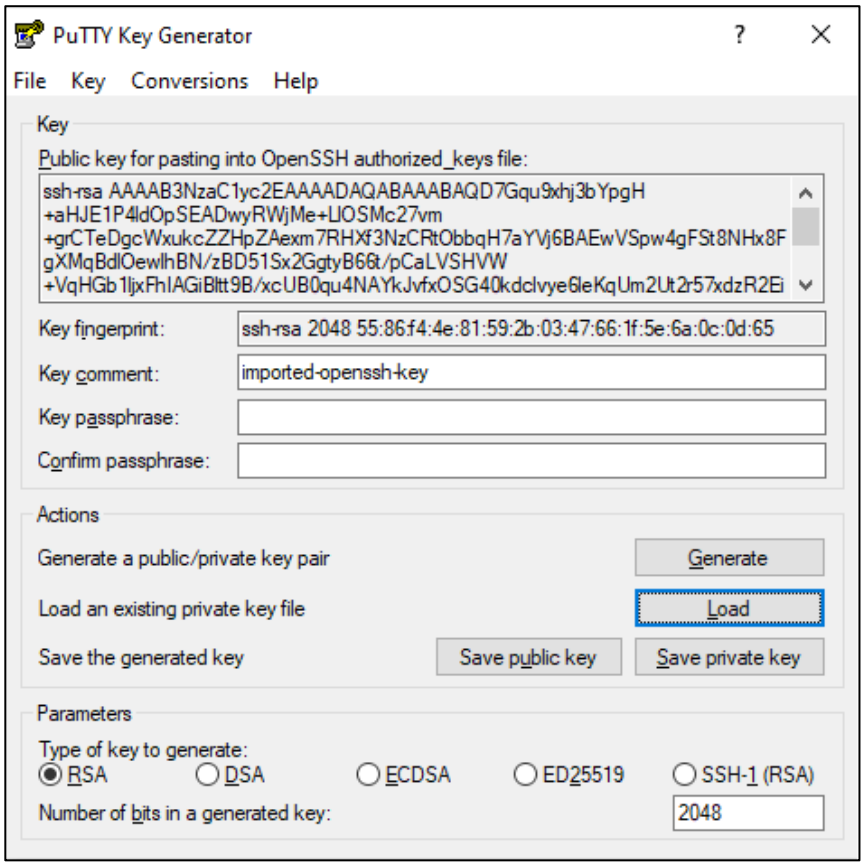


Figura 19. Llave de la Instancia.

Paso 18. Iniciar la aplicación de PuTTy. Ingresar la dirección IP de la instancia y dejar el puerto en 22.
Paso 19. En PuTTy, ir a Connections, SSH, Auth in PuTTY. Dar click en el botón de Browse y seleccionar el archivo creado con PuTTYgen (.ppk)
Paso 20. Dar click en Connect y luego en “Yes” al aparecer la alerta de seguridad de PuTTY.
Paso 21. Login como “admin” e ingresar el passphrase creado con PuTTYgen.
Hasta este punto, ya se logró una sesión exitosa a la instancia de EC2. Ahora hay que instalar T-Pot
Paso 22. Siempre es recomendable actualizar el sistema operativo en su primer uso. Para hacer esto, ingresar los comandos de “sudo apt update” y posterior “sudo apt upgrade”
Paso 23. Instalar Git. Para ello, ingresar el comando de “sudo apt-get install git -y”. Al terminar, ingresar “which git” para confirmar, debería salir información como en esta pantalla:

Paso 24. Para la instalación de T-Pot es necesario clonar el repositorio donde se encuentra y correr el instalador. Para ello, ingresar los siguientes comandos

- git clone https://github.com/dtag-dev-sec/tpotce
- cd tpotce/iso/installer/
- sudo ./install.sh — type=user

Paso 25. El script de instalación comenzará a correr y en cierto punto pregunta si debería continuar, en ese caso ingresar "y"

Figura 20. Script de Instalación.

Paso 26. Al momento de preguntar el tipo de edición de T-Pot a instalar, seleccionar STANDARD y con enter seleccionar OK
Paso 27. En la ventana para ingresar un nombre de usuario, ingresar el username que será utilizado para la interfaz web
Paso 28. Elegir Yes para confirmar el nombre de usuario
Paso 29. Teclear una contraseña segura y posteriormente confirmarla. Esperar a que termine la instalación. Una vez terminada, la instancia se reiniciará automáticamente.
Paso 30. T-Pot cambia el puerto de conexión al 64295, ya no es el puerto 22. Así que la siguiente vez que se necesite iniciar una sesión SSH a la instancia, se debe cambiar el puerto al 64295.
Conectándonos a la interfaz web de T-Pot
Paso 31. En un navegador web ahora es posible conectarse a la interfaz web de T-Pot, simplemente ingresando lo siguiente

- https://ip-de-la-instancia:64297

Y después ingresar el username y password creados durante la instalación de T-Pot. El primer dashboard de la lista luce como en la siguiente pantalla

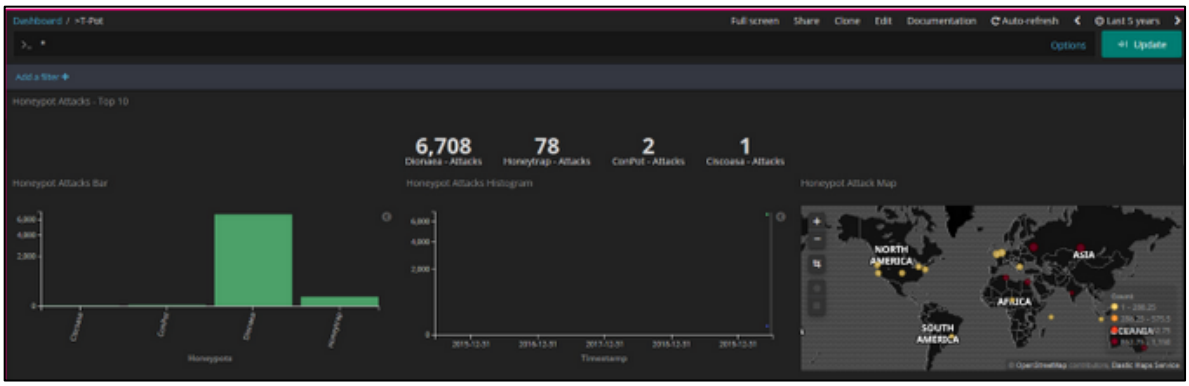


Figura 20. Instalación del Honeypot completada.

Y listo, con esto damos por exitosa la instalación completa de T-Pot honeypot. A continuación, se presentan los datos recopilados por la plataforma durante 20 días las características y recursos utilizados para desplegar la plataforma T-Pot en AWS:

Figura 27. Eventos detectados en T-Pot Honeypots sobre AWS después de 20 días.

3.2.2 Caso de Estudio: Instalación plataforma de CTI MISP

Para la implementación de esta Plataforma [157], fue necesario utilizar un ambiente de nube privada, con un hipervistor VMWARe ESXi [158], el cual es un sistema operativo que permite virtualizar otros sistemas operativos, a diferencia de virtualizadores más convencionales como podrían ser VMware Workstation Player o VirtualBox que se instalan dentro de otro sistema operativo base, VMware ESXi se instala directamente en un servidor físico como sistema operativo principal. Cabe mencionar, que MISP se despliega en una plataforma Ubuntu 20.04.1.

Una vez que se haya desplegado un Sistema Operativo Ubuntu 20.04.1, hay que realizar una

búsqueda de actualizaciones e instalarlas en el sistema utilizando los siguientes comandos:

- sudo apt-get update -y && sudo apt-get upgrade -y

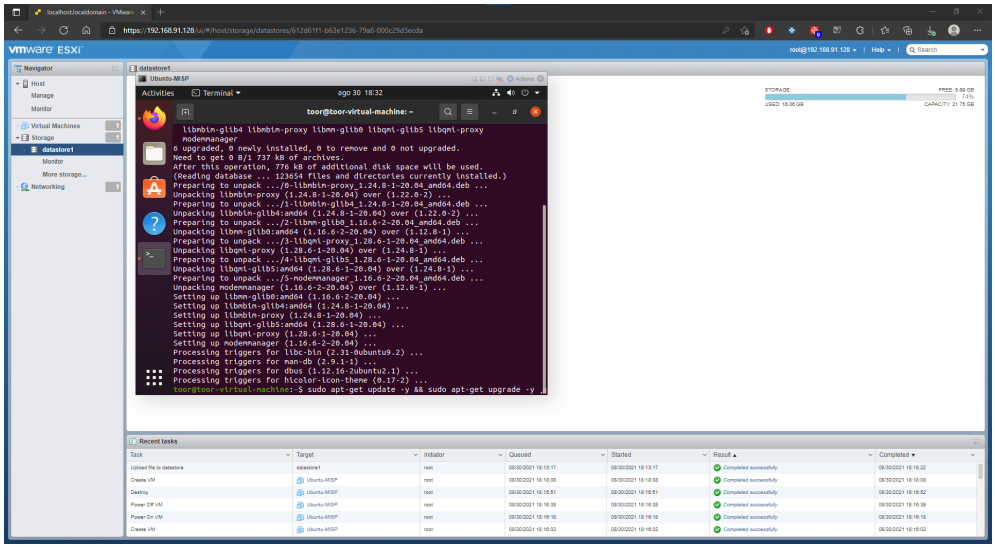


Figura 21. Actualización de Sistema Operativo Linux.

Para seguir con la instalación es necesario contar con el cliente de MySQL en el sistema, cual puede ser instalado de manera automática ejecutando los siguientes comandos en nuestra sitema Ubuntu:

- sudo apt-get install mysql-client -y

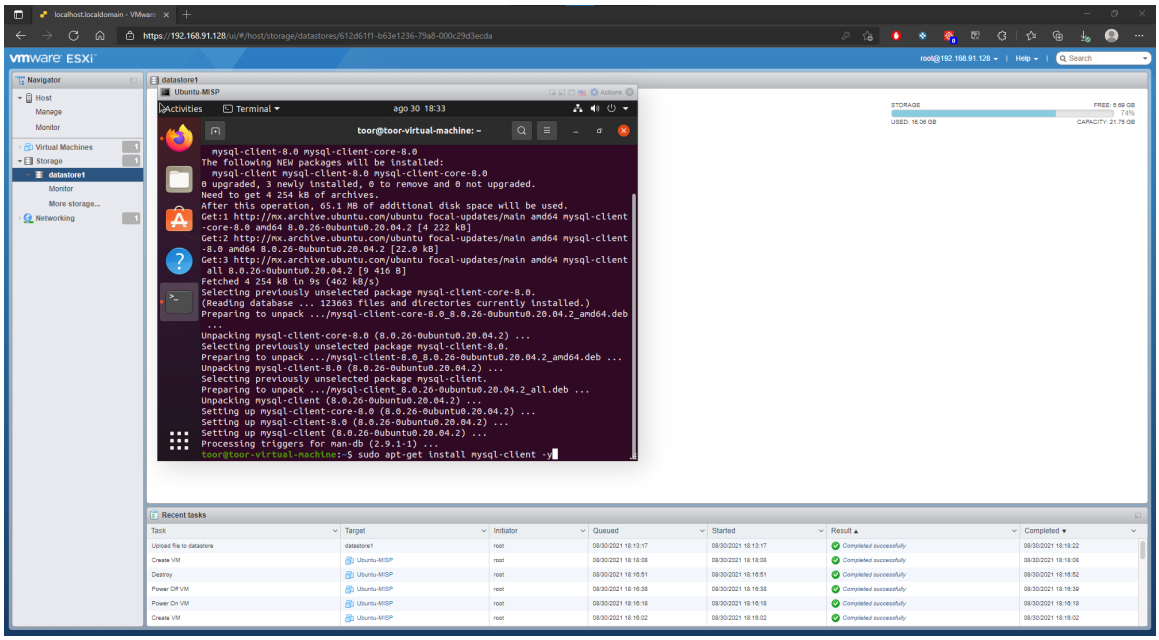


Figura 22. Instalación de cliente de SQL.

El siguiente paso, es la descarga del instalador de MISP, el siguiente script bash automatizado no

se puede ejecutar con privilegios de root, por lo tanto, se ejecutó este script con un usuario sin privilegios (No root):

- curl https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh -o misp_install.sh

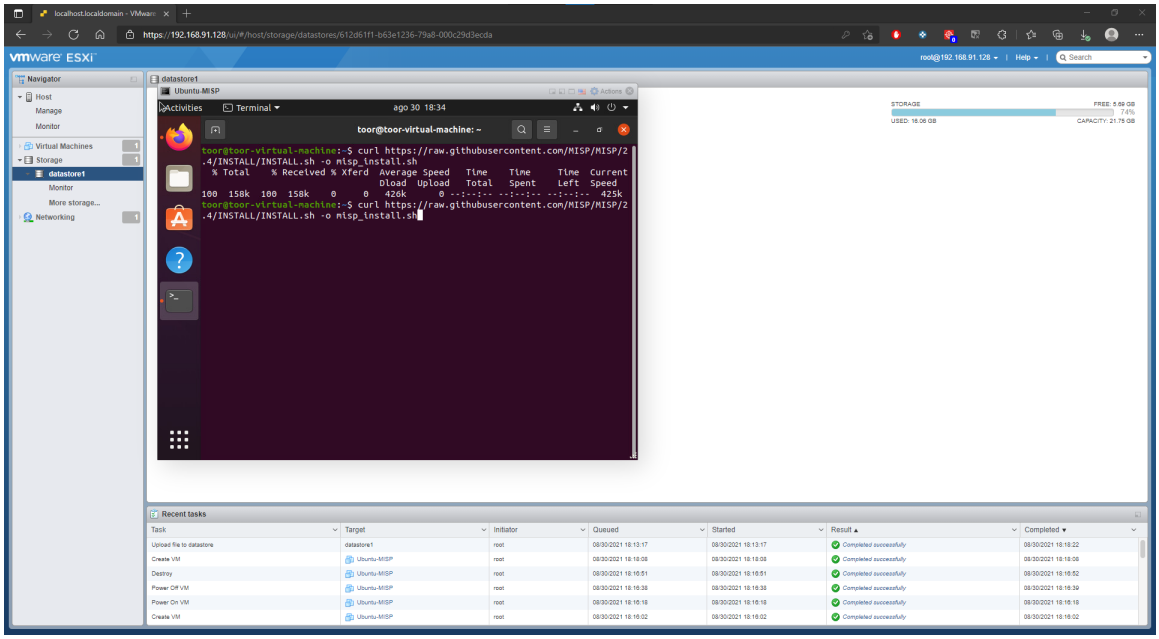


Figura 23. Descarga de MISP.

Adicional, en necesario cambiar el permiso del archivo misp_install.sh y hacerlo ejecutable:

- chmod +x misp_install.sh
- ./misp_install.sh -A

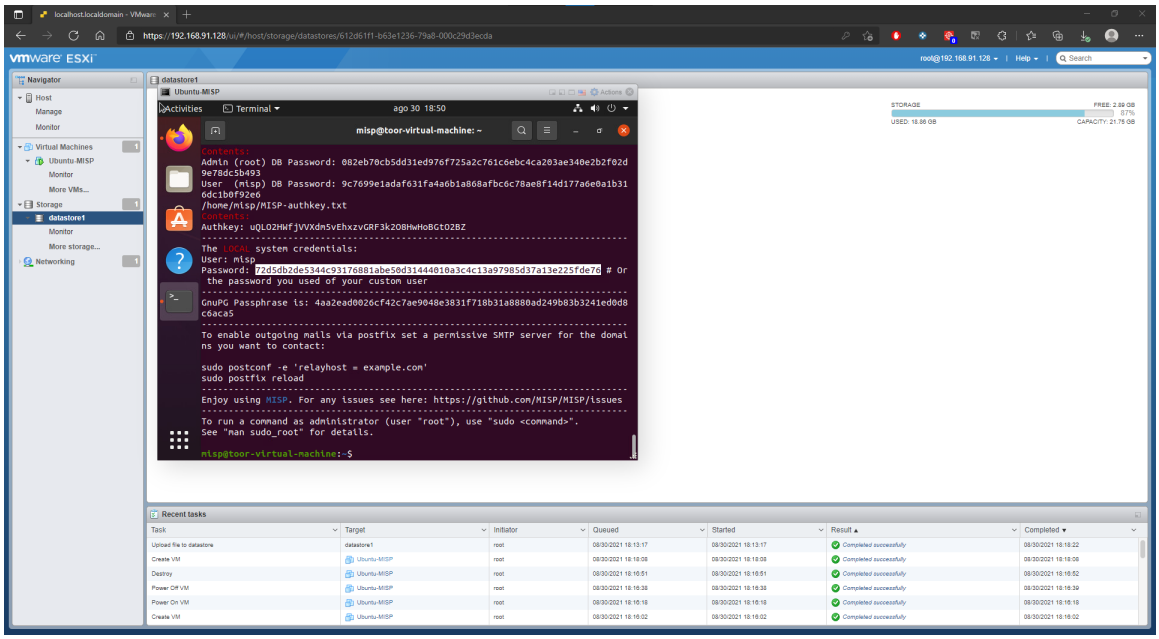


Figura 24. Elevación de permisos.

Cabe mencionar, que una de las mejores prácticas y recomendaciones al desplegar MISP, es poder asegurar el acceso mediante reglas de firewall correspondientes para permitir los puertos 80/tcp y 443/tcp:

- sudo ufw allow 80/tcp
- sudo ufw allow 443/tcp

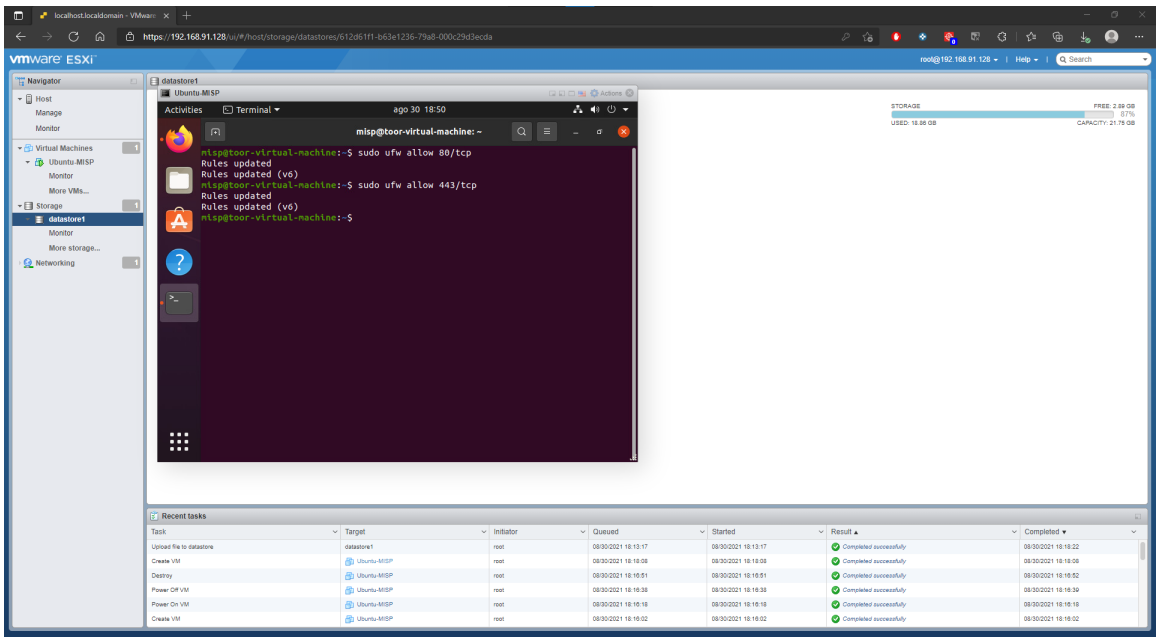


Figura 25. Configuración de Firewall local.

Una vez terminada la instalación hay que acceder a la dirección 127.0.0.1 desde el navegador web

y autenticarse con las credenciales de usuario por defecto o bien, acceder a la dirección IP del sistema Ubuntu por los puertos previamente permitidos.

- Usuario: admin@admin.test
- Contraseña: admin

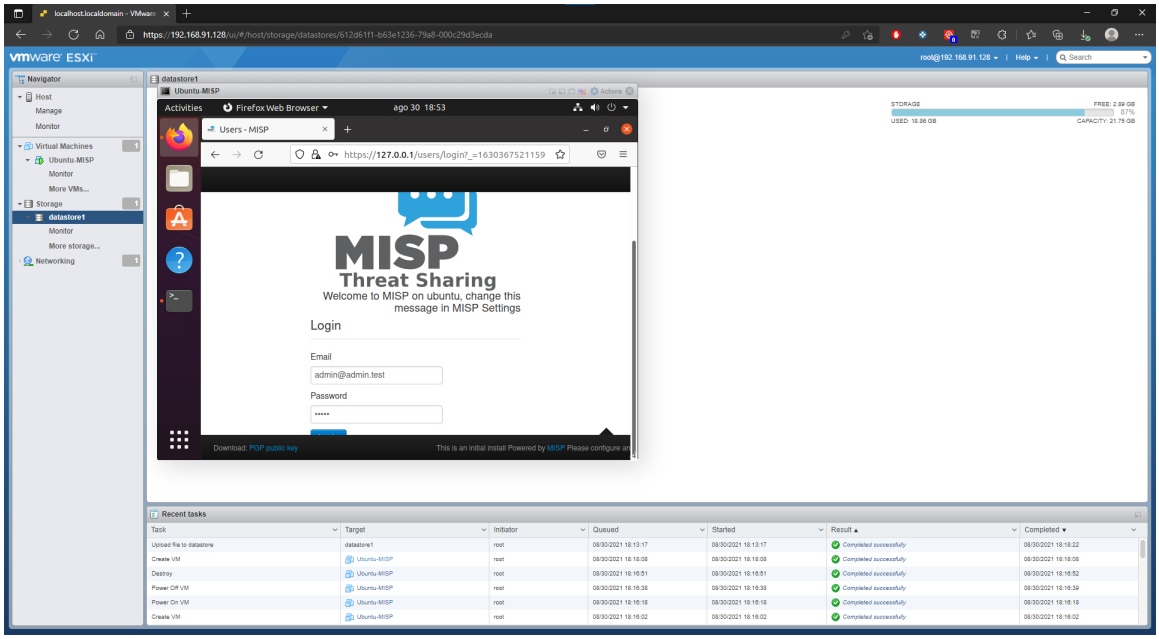


Figura 26. Instalación completa.

Al entrar a la plataforma por primera vez, es necesario realizar un cambio de contraseña la primera vez que se inicie sesión, debe ser de al menos 12 caracteres, contener una mayúscula, una minúscula, carácter especial y un número. De esta forma se logra tener una instancia de la plataforma de MISP lista para utilizarse en una máquina virtual con sistema operativo Ubuntu levantada en el Hypervisor de VMware ESXi.

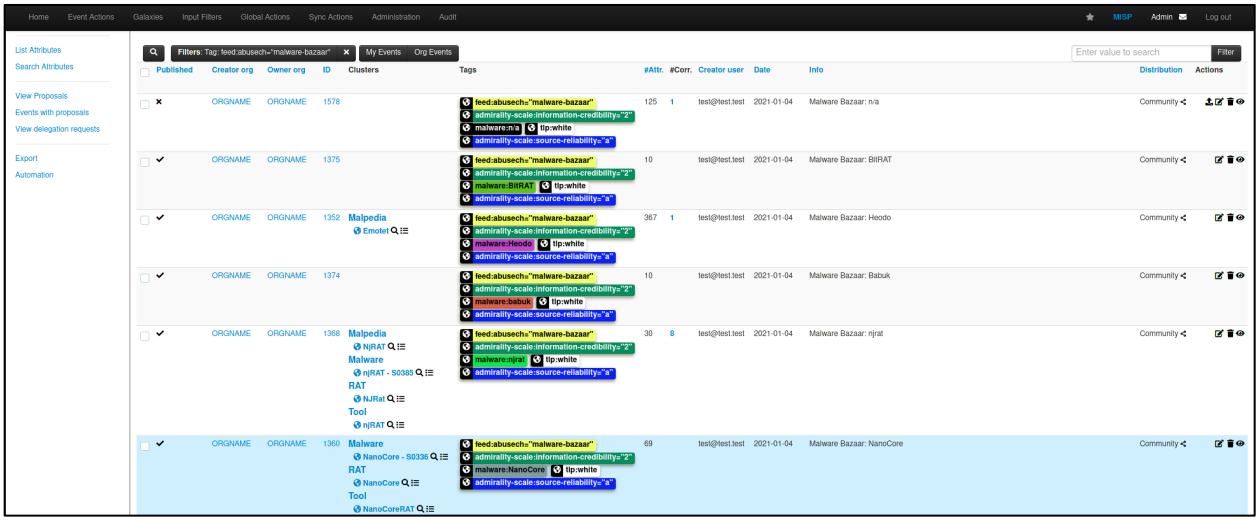


Figura 27. MISP dashboard

3.2.3 Python for Data Science, Exploration and Visualization

En el ámbito académico, Python ha experimentado un notorio aumento en su popularidad, destacándose como un lenguaje versátil y poderoso, especialmente en el contexto de la ciencia de datos (McKinney, 2016). Este incremento se traduce en una herramienta valiosa para la investigación científica y el análisis de datos.

3.2.3.1 Características y Contribuciones en la Investigación Científica:

Versatilidad y Flexibilidad: Python sirve como un "pegamento" que integra códigos heredados, facilitando la incorporación de bibliotecas especializadas en álgebra lineal, optimización y transformadas rápidas de Fourier (McKinney, 2017).

Ecosistema Abundante: La comunidad de Python se beneficia de un extenso conjunto de paquetes y bibliotecas de terceros, como Numpy, Pandas, Matplotlib y otros, que fortalecen su utilidad en la investigación científica (VanderPlas, 2016).

Entorno de Desarrollo Unificado: Python, con herramientas como Jupyter Notebook, permite a los investigadores trabajar desde la etapa de investigación y prototipado hasta la producción, eliminando la necesidad de múltiples entornos de desarrollo (McKinney, 2017).
En el contexto de esta tesis, se utilizará Jupyter Notebook para las etapas de exploración de datos, aprovechando su flujo de trabajo interactivo para un análisis detallado.

3.2.4 Tableau Software

Tableau, originado en investigaciones académicas, se destaca como una herramienta poderosa para la visualización de datos, desarrollada a partir de disertaciones doctorales (MacEachran, 2019). La tecnología VizQL, desarrollada durante estos estudios, ha llevado la visualización de datos a una nueva dimensión al combinar consulta, análisis y visualización en un solo marco.

3.2.4.1 Contribuciones Académicas:

Innovación Visual: La implementación de las variables visuales de Bertin y la tecnología VizQL han ampliado los horizontes de la visualización de datos, convirtiendo a Tableau en una herramienta esencial en la representación gráfica de información compleja (Jock Mackinlay | Tableau Research, 2021).
La implementación de Tableau en la investigación proporciona una capacidad excepcional para explorar y comunicar hallazgos de manera efectiva.

3.2.5 Power BI

Power BI, una herramienta de Microsoft, se ha convertido en un componente integral en el ámbito académico y empresarial para el análisis y visualización de datos.

3.2.5.1 Características Destacadas:

Integración con Ecosistema Microsoft: Power BI se integra sin problemas con otras herramientas de Microsoft, proporcionando una sinergia eficiente con aplicaciones como Excel y Azure.

Capacidades de Visualización Interactiva: Ofrece opciones avanzadas de visualización, tableros interactivos y capacidades de generación de informes para presentar datos de manera impactante. Su implementación en la investigación permitirá una exploración detallada y una presentación efectiva de los resultados obtenidos en el análisis de amenazas cibernéticas en México.

3.2.6 Plataforma de procesamiento y visualización de datos seleccionada

Power BI, una herramienta integral de Microsoft, se posiciona como la elección principal para la visualización de datos en esta tesis, basándonos en varias consideraciones clave. La elección de Power BI se alinea estratégicamente con el entorno tecnológico existente y proporciona las herramientas necesarias para presentar hallazgos de manera efectiva, contribuyendo así al éxito general de la investigación sobre amenazas cibernéticas en México.

3.2.6.1 Razones para Seleccionar Power BI:

Integración con Ecosistema Microsoft:
Dada la prevalencia de soluciones Microsoft en el entorno empresarial y académico, Power BI ofrece una integración perfecta con herramientas como Excel y Azure. Esto garantiza la coherencia en el flujo de trabajo y la compatibilidad con otras plataformas utilizadas en el proyecto.

Facilidad de Uso y Aprendizaje:
Power BI se destaca por su interfaz intuitiva y fácil de aprender, lo que facilita su adopción tanto para usuarios principiantes como para aquellos con experiencia. Esto resulta crucial para optimizar el tiempo de aprendizaje y maximizar la eficiencia en la creación de visualizaciones complejas.

Capacidades de Visualización Interactiva:
Power BI ofrece una amplia gama de opciones avanzadas de visualización, permitiendo la creación de tableros interactivos y presentaciones dinámicas de datos. Esto es esencial para comunicar de manera efectiva los resultados del análisis de amenazas cibernéticas de una manera visualmente impactante.

Conectividad Versátil:
La capacidad de Power BI para conectarse a diversas fuentes de datos, incluidas bases de datos locales, servicios en la nube y archivos planos, facilita la integración de datos recopilados de múltiples fuentes, un aspecto clave en la investigación.

Actualizaciones en Tiempo Real:
Power BI permite la configuración de actualizaciones en tiempo real, lo que garantiza que las visualizaciones reflejen los datos más recientes. Esto es esencial para mantener la vigencia de los

resultados a medida que se analizan eventos en constante evolución.
La elección de Power BI se alinea estratégicamente con el entorno tecnológico existente y proporciona las herramientas necesarias para presentar hallazgos de manera efectiva, contribuyendo así al éxito general de la investigación sobre amenazas cibernéticas en México.

3.3 Selección de metodologías de CTI para el método propuesto

El objetivo principal de esta sección se basa en la recopilación e investigación de los esquemas, herramientas y conjuntos de metodologías de CTI para contestar la siguiente pregunta de investigación:

¿Qué marcos y/o metodologías existentes Inteligencia contra Amenazas (CTI) se pueden utilizar para comprender el panorama de ciber amenazas de México?

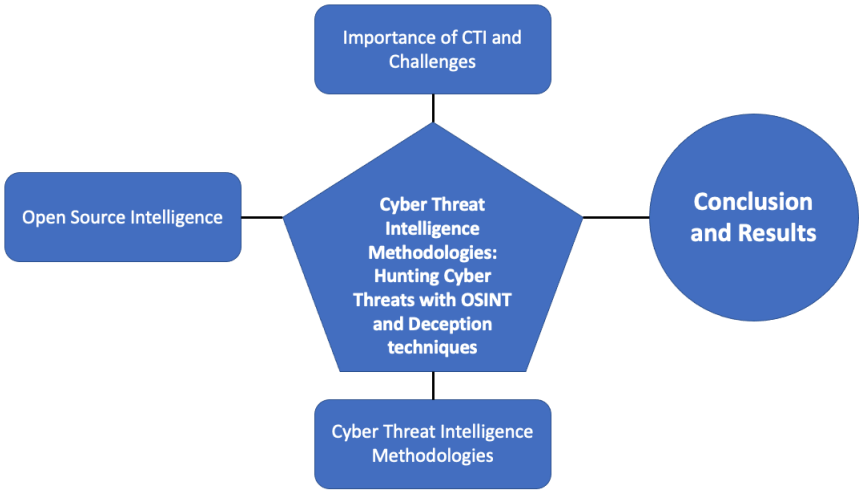


Figura 28. Contribuciones y estructura de investigación.

En esta sección, analizamos los datos recolectados por los Honeypots expuestos a internet para analizar los modelos de Cyber Kill Chain, ATT&CK, Shield y Diamond Model, para poder comprender algunas de las fases y TTP's realizadas por los adversarios para lograr sus objetivos dentro de la infraestructura desplegada.

3.3.1 Caso de Estudio

En esta investigación desplegamos T-Pot en la nube publica de Amazon Web Services (AWS), con el objetivo principal de exponer los Honeypots disponibles de la plataforma T-Pot a internet, con la finalidad de poder recolectar amenazas reales que mayormente son automatizadas en el ciberespacio, lo cual nos permitirá recopilar algunas de las TTP's de los adversarios y nos permitirá analizar la información para modelarla con las metodologías descritas en el documento por medio de casos de estudio, con el propósito de poder identificar cómo se implementan cada uno de los modelos ante un ciberataque real y como se complementan entre ellos.

A continuación, se presentan los datos recopilados por la plataforma durante 20 días las características y recursos utilizados para desplegar la plataforma T-Pot en AWS:

Figura 29. Eventos detectados en T-Pot Honeypots sobre AWS después de 20 días.

El caso de estudio que se plantea envuelve una víctima que desplego un servicio con un acceso de SSH expuesto a internet. Los adversarios utilizaron técnicas de escaneo masivo, para detectar vulnerabilidades conocidas de los sistemas expuestos. Adicional, los adversarios realizaron la creación de correos electrónicos utilizando técnicas como ingeniera social y Phishing basados en los escaneos GeoIP anteriores para decidir el idioma a utilizar. Además, los adversarios generaron un exploit para ejecutar un webshell como un malware desde un sitio web infectado previamente. Se detectaron distintos intentos de accesos a las plataformas por protocolos como SSH y RDP desde IP's catalogadas como maliciosas. Algunas de estas IPs lograron acceder a los sistemas mediante el uso de técnicas como Fuerza Bruta y ataques de diccionario. Una vez que el adversario entro al sitio, se detectaron ejecuciones de comandos para la descarga de archivos por medio de una shellcode a una URL catalogada como maliciosas por contenido de Malware. Después de realizar la descarga, se detectaron ejecuciones de comandos para la descarga de archivos de malware de una IP catalogada como maliciosa. Una vez detectadas los dominios/IPs maliciosos y el malware descargado por el adversario, se procedió a revisar fuentes de inteligencia abiertas como Virus Total, para buscar las IP's o dominios relacionados con el malware instalado.

Una vez recopilada esta información, se presentan los resultados de las investigaciones realizadas con las metodologías descritas en el documento. El Cyber Kill Chain Model, nos ayuda a entender cada una de las fases de la cadena de ataque realizada por los adversarios y nos guía para poder

empezar a realizar una búsqueda de los eventos relevantes en cada una de las fases.

Fase	Procedimiento	Indicadores
Reconocimiento	ip_rep.keyword: mass scanner	**Suricata Signature:** ET SCAN NMAP -sS window 1024 ET POLICY RDP connection request ET DOS Microsoft RDP Syn then Reset 30 Second DoS Attempt ET SCAN Potential SSH Scan
Preparación	Webshell creation Previous Infected URL data: password data: covid	SSH Dictionary Attack detected Phishing emails detected
Entrega	message: login message: success eventid: cowrie.login.success src_port: 22	**Attacker IP:** 206[.]189[.]50[.]126, 46[.]101[.]156[.]22, 185[.]153[.]199[.]182 **Message Log:** login attempt / succeeded
Explotación	message: download input: wget	**Downstream URL:** http://104[.]168[.]195[.]213/Thorbins.sh http://212[.]73[.]150[.]134/NoHomobins.sh **Exploited vulnerabilities:** CVE-2001-0540, CVE-2012-0152, CVE-2019-0708
Instalación	eventid: cowrie.command.input input: wget input: run input: 104[.]168[.]195[.]213	**Malware/Trojan:** 48251b805670802373821564eb9c7056703a6822d4e025c790d3acce0776c7fa **Malware/Downloader:** a2ef7e6b666d570dd6e26cddf4d4fd7f **Executed commands:** cd /tmp || cd /run || cd /; wget http:// 104[.]168[.]195[.]213/Thorbins.sh; chmod 777 Thorbins.sh; sh Thorbins.sh; tftp 104[.]168[.]195[.]213-c get Thortftp1.sh; chmod 777 Thortftp1.sh; sh Thortftp1.sh; tftp -r Thortftp2.sh -g 104[.]168[.]195[.]213; chmod 777 Thortftp2.sh; sh Thortftp2.sh; rm -rf Thorbins.sh Thortftp1.sh Thortftp2.sh; rm -rf *
Comando y Control	Se realizaron búsquedas en Virus Total y Spiderfoot con los hashes del malware y las IP's encontradas	23[.]47[.]207[.]24:80 (TCP) 184[.]28[.]221[.]115:80 (TCP) 23[.]47[.]206[.]49:443 (TCP) 17[.]249[.]25[.]246:443 (TCP) 17[.]142[.]169[.]200:443 (TCP) 17[.]253[.]21[.]208:443 (TCP)
Acciones en los Objetivos	N/A	N/A

Tabla 8. Resultados obtenidos mediante Cyber Kill Chain Model

Con la información recolectada por la plataforma de Honeypots y el Cyber Kill Chain Model, se puede ahondar mucho más en las tácticas y técnicas utilizadas por los adversarios para entender sus objetivos y operaciones mediante el uso de MITRE ATT&CK.

Figura 30. Resultados Obtenidos mediante MITRE ATT&CK

Una vez que se modelan las TTP's de los adversarios en ATT&CK, podemos utilizar MITRE Shield para realizar un mapeo de las TTP's encontradas en ATT&CK utilizadas por los adversarios para realizar una estrategia de defensa activa. Por ejemplo, el acceso inicial a los sistemas expuestos se realizó a través de un sistema remoto expuesto a través de una cuenta valida. Ante esto, Shield nos da la posibilidad de generar una estrategia de defensa activa con la oportunidad de validar si el adversario ya cuenta con credenciales de una o más cuentas validad para algún sistema de la red mediante el uso de uno señuelo o honeypot para poder recolectar más información de las TTP's utilizadas por el adversario como lo hemos estado haciendo durante esta investigación.

Channel	Collect	Contain	Detect	Disrupt	Facilitate	Legitimize	Test
Admin Access	API Monitoring	Admin Access	API Monitoring	Admin Access	Admin Access	Application Diversity	Admin Access
API Monitoring	Application Diversity	Baseline	Application Diversity	Application Diversity	Application Diversity	Burn-In	API Monitoring
Application Diversity	Backup and Recovery	Decoy Account	Behavioral Analytics	Backup and Recovery	Behavioral Analytics	Decoy Account	Application Diversity
Decoy Account	Decoy Account	Decoy Network	Decoy Account	Baseline	Burn-In	Decoy Content	Backup and Recovery
Decoy Content	Decoy Content	Detonate Malware	Decoy Content	Behavioral Analytics	Decoy Account	Decoy Credentials	Decoy Account
Decoy Credentials	Decoy Credentials	Hardware Manipulation	Decoy Credentials	Decoy Content	Decoy Content	Decoy Diversity	Decoy Content
Decoy Network	Decoy Network	Isolation	Decoy Network	Decoy Credentials	Decoy Credentials	Decoy Network	Decoy Credentials
Decoy Persona	Decoy System	Migrate Attack Vector	Decoy System	Decoy Network	Decoy Diversity	Decoy Persona	Decoy Diversity
Decoy Process	Detonate Malware	Network Manipulation	Email Manipulation	Email Manipulation	Decoy Persona	Decoy Process	Decoy Network
Decoy System	Email Manipulation	Security Controls	Hunting	Hardware Manipulation	Decoy System	Decoy System	Decoy Persona
Detonate Malware	Network Diversity	Software Manipulation	Isolation	Isolation	Network Diversity	Network Diversity	Decoy System
Migrate Attack Vector	Network Monitoring		Network Manipulation	Network Manipulation	Network Manipulation	Pocket Litter	Detonate Malware
Network Diversity	PCAP Collection		Network Monitoring	Security Controls	Peripheral Management		Migrate Attack Vector
Network Manipulation	Peripheral Management		PCAP Collection	Standard Operating Procedure	Pocket Litter		Network Diversity
Peripheral Management	Protocol Decoder		Pocket Litter	User Training	Security Controls		Network Manipulation
Pocket Litter	Security Controls		Protocol Decoder	Software Manipulation	Software Manipulation		Peripheral Management
Security Controls	System Activity Monitoring		Standard Operating Procedure				Pocket Litter
Software Manipulation	Software Manipulation		System Activity Monitoring				Security Controls
			User Training				Software Manipulation
			Software Manipulation				

Figura 31. Resultados Obtenidos mediante MITRE Shield/Engage

En Modelo de Diamante, utilizamos un enfoque centrado en la victima (Honeypots) para poder revelar la conexión entre los elementos relacionados del adversario, tales como la infraestructura y capacidades organizadas en eventos.

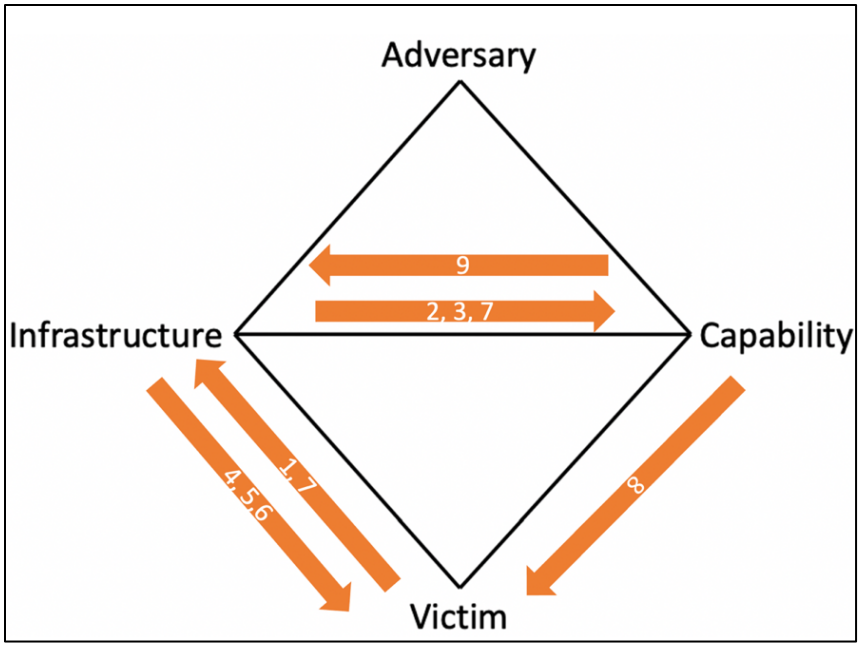


Figura 32. Resultados Obtenidos mediante el Diamond Model

Id	Descripción	Fase	Metodología	Infraestructura	Capacidad
1	Los adversarios utilizaron tecnicas de escaneo masivo, para detectar vulnerabilidades conocidias de los sitemas expuestos.	Reconnaissance	Active Scanning	Bad IPs reputations	Massive scanners tools
2	Creation of Phishing Emails based on the previous GeoIP scans to decide the language to use.	Resource development	Spearphishing service	N/A	Email
3	the adversaries could create or obtain a malicious payload or exploit to execute a webshell as a downloader/trojan malware	Resource development	Compromise Infraestructure Obtain Capabilities	N/A	Malicious payload/malware
4	Se detectaron distintos intentos de accesos a las plataformas por protocolos como RDP desde IP's catalogadas como maliciosas.	Initial Acces	External Remote Access	206[.]189[.]50[.]126 46[.]101[.]156[.]22	Automated scripts/tools
5	Se detectaron distintos intentos de accesos a las plataformas por protocolos como SSH desde IP's catalogadas como maliciosas.	Initial Acces	External Remote Access Valid Accounts	206[.]189[.]50[.]126 46[.]101[.]156[.]22 185[.]153[.]199[.]182	Automated scripts/tools and dictionaries
6	Algunas de estas IP's lograron acceder a los sistemas mediante el uso de tecnicas como Fuerza Bruta y ataques de diccionario	Credential Acess	External Remote Access Valid Accounts	46[.]101[.]156[.]22	Brute Force Attack
7	Una ves que el adversario entro al sistema, se detectaron ejecuciones de comandos para la descarga de archivos por medio de una shellcode a una URL catalogada como maliciosas por contenido de Malware.	Execution	Malicious Link	http://104[.]168[.]195[.]213/Thorbins.sh http://212[.]73[.]150[.]134/NoHomobins.sh	Service execution Vulnerable exposed Server
8	Se detectaron comando para agregar, modificar y dar permisos de ejecuciony borrado de eventos para las descragas de los archivos maliciosos	Persistence	Web shell	http://104[.]168[.]195[.]213/Thorbins.sh	Web Shell Malicious payload/malware
9	Una ves detectadas los dominios/IPs maliciosos y el malware descargado por el adversario, se procedio a revisar fuentes de inteligencia abiertas como Virus Total, para buscar las IP's o dominios relacionados con el malware instalado	Command and Control	Web Service	23[.]47[.]207[.]24:80 184[.]28[.]221[.]115:80 23[.]47[.]206[.]49:443 17[.]249[.]25[.]246:443 17[.]142[.]169[.]200:443 17[.]253[.]21[.]208:443	Vulnerable exposed Server

Tabla 9. Resultados Obtenidos mediante with Diamond Model

3.3.2 Metodologías de Inteligencia contra Amenazas (CTI) Seleccionadas

En el desarrollo de la metodología para este proyecto, se seleccionaron dos marcos de trabajo ampliamente reconocidos en el campo de la Inteligencia contra Amenazas (CTI): Cyber Kill Chain y MITRE ATT&CK. Estas metodologías ofrecen enfoques complementarios para analizar y comprender las tácticas, técnicas y procedimientos (TTP) de los adversarios en el ciberespacio.

3.3.2.1 Cyber Kill Chain

Cyber Kill Chain, desarrollada por Lockheed Martin, proporciona un marco estructurado para entender y contrarrestar las fases de un ataque cibernético, desde la fase inicial de reconocimiento hasta la fase final de acciones en el objetivo. La selección de Cyber Kill Chain en esta tesis permitirá:

- **Visualización del Ciclo de Ataque:** Cyber Kill Chain ofrece una representación gráfica del ciclo de vida de un ataque, facilitando la identificación de puntos críticos y la comprensión de las etapas del adversario.
- **Focalización en la Prevención:** Al identificar las fases específicas de un ataque, se puede centrar la atención en medidas preventivas y de mitigación adaptadas a cada etapa.
- **Mejora de la Postura de Seguridad:** El análisis basado en Cyber Kill Chain permitirá

mejorar la postura de seguridad al identificar debilidades en las defensas existentes y proponer contramedidas efectivas en las fases específicas de un ataque.

3.3.2.2 MITRE ATT&CK

MITRE ATT&CK es un marco de trabajo que describe las acciones que los adversarios toman en diferentes etapas de su operación en el ciberespacio. A diferencia de la Cyber Kill Chain, que se centra en el ciclo de vida del ataque, MITRE ATT&CK se enfoca en las tácticas y técnicas utilizadas por los adversarios. La inclusión de MITRE ATT&CK en la metodología aportará:

- **Identificación de Tácticas Específicas:** Permite una comprensión detallada de las tácticas específicas utilizadas por los adversarios, proporcionando información valiosa para la detección y respuesta.
- **Adaptabilidad a Diversas Amenazas:** MITRE ATT&CK es un marco amplio que abarca una variedad de amenazas, lo que permite adaptarse a diferentes escenarios y actores maliciosos.
- **Enfoque en la Defensa Activa:** Facilita la adopción de una postura de seguridad activa al entender las tácticas y técnicas que pueden ser empleadas contra la infraestructura de la organización.

3.3.2.3 Exclusión del "The Diamond Model"

Aunque "The Diamond Model" es otra metodología valiosa en el ámbito de la CTI, no fue seleccionada para este proyecto debido a las siguientes consideraciones:

- **Enfoque en la Atribución:** "The Diamond Model" se centra en la atribución de amenazas, mientras que el enfoque preferido para esta investigación se orienta hacia la comprensión de tácticas y técnicas, sin asignar necesariamente la autoría de los ataques.
- **Complejidad para Datos de Logs:** La implementación de "The Diamond Model" puede ser más compleja cuando se trabaja con datos de logs de firewalls perimetrales, ya que requiere una variedad de información que puede no estar directamente disponible en este contexto específico.

3.3.2.4 Beneficios de las Metodologías de CTI Seleccionadas en la Tesis

La combinación de Cyber Kill Chain y MITRE ATT&CK proporciona una perspectiva integral de las tácticas y técnicas utilizadas por los adversarios. Estas metodologías se alinean con el objetivo de entender y contrarrestar amenazas cibernéticas, permitiendo una modelización detallada de los eventos en cada fase del ataque.

La exclusión del Modelo Diamond se basa en la necesidad de una aproximación más detallada y técnica. Mientras que el Modelo Diamond se enfoca en actores, tácticas, técnicas y procedimientos, Cyber Kill Chain y MITRE ATT&CK ofrecen una granularidad adicional, lo que resulta esencial para la investigación detallada y el análisis de amenazas específicas en el ciberespacio.

4 Experimentación

En esta sección se describe el entorno en el cual fue realizado el experimento para el método propuesto.

4.1 Diseño Experimental

En esta sección se presenta una guía del Diseño Experimental. Como se mencionó en la sección 3, el diseño y planificación del experimento para el método propuesto se llevará acabo siguiendo el ciclo de vida de Inteligencia contra Amenazas (CTI):

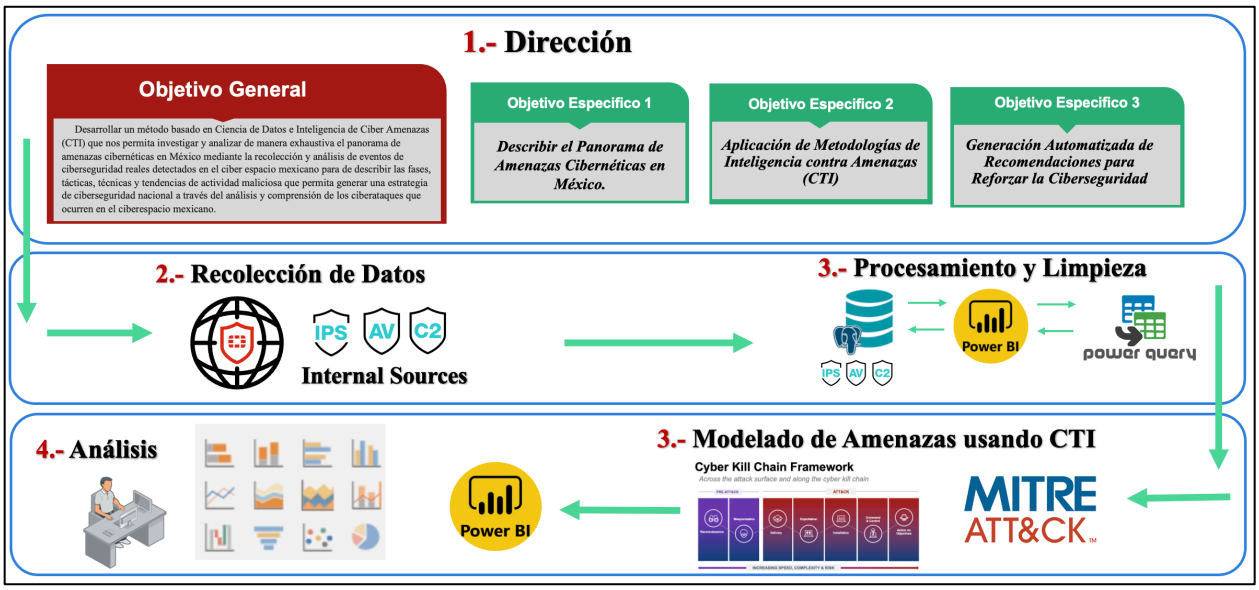


Figura 33. Ciclo de Vida de CTI para el método propuesto

4.1.1 Fase 1. Dirección (Objetivos)

La dirección de este experimento está relacionada directamente con los objetivos de la investigación como se mencionó en la sección 1.6

Desarrollar un método basado en Ciencia de Datos e Inteligencia de Ciber Amenazas (CTI) que nos permita investigar y analizar de manera exhaustiva el panorama de amenazas cibernéticas en México mediante la recolección y análisis de eventos de ciberseguridad reales detectados en el ciber espacio mexicano para de describir las fases, tácticas, técnicas y tendencias de actividad maliciosa que permita generar una estrategia de ciberseguridad nacional a través del análisis y comprensión de los ciberataques que ocurren en el ciberespacio mexicano.

- ***Objetivo Específico 1 - Describir el Panorama de Amenazas Cibernéticas en México.***
- ***Objetivo Específico 2 - Aplicación de Metodologías de Inteligencia contra Amenazas (CTI)***
- ***Objetivo Específico 3 - Generación Automatizada de Recomendaciones para Reforzar la Ciberseguridad***

4.1.2 Fase 2. Recolección y Análisis de Eventos de Ciberseguridad

Se realizo un análisis exhaustivo de eventos reales de ciberseguridad detectados en organizaciones mexicanas disponibles.

4.1.2.1 Conjunto de Datos Recolectados y Tipos de Amenazas

El conjunto de datos utilizado para este proyecto se originó a través de la colaboración con uno de los socios industriales y académicos de la Universidad Autónoma de Nuevo León, Fortinet. La fuente de datos es parte de la iniciativa de investigación de inteligencia de amenazas de FortiGuard Labs asegurando un conjunto robusto y actualizado de información relevante para el análisis de ciberseguridad en México.

Además, dicho conjunto de datos utilizado fue recopilado de una flota de productos de seguridad de Fortinet desplegados globalmente, utilizados por una amplia base de clientes que van desde pequeñas y medianas empresas hasta grandes empresas. Los sensores incluyen el dispositivo de red de próxima generación, el firewall FortiGate. Los tipos de amenazas detectados por el firewall FortiGate a través de la actividad de la red son:

- Botnet
- Sistema de Prevención de Intrusiones (IPS)
- Virus/Malware

4.1.3 Fase 3. Procesamiento (Implementación de metodologías de CTI)

Se seleccionarán, adaptarán e implementarán las metodologías de CTI para categorizar y analizar las fases específicas de los ciberataques en el contexto mexicano. Esto incluirá la identificación de tácticas, técnicas y procedimientos (TTP) empleados por adversarios ayudando a cumplir el ***Objetivo Específico 2 - Aplicación de Metodologías de Inteligencia contra Amenazas (CTI)***

4.1.4 Fase 4. Análisis

Esto implicará la revisión detallada de la información recopilada en esta investigación para identificar patrones, tácticas y técnicas utilizadas por adversarios lo cual nos ayudará a cumplir el ***Objetivo Específico 1 - Describir el Panorama de Amenazas Cibernéticas en México.***

4.1.4.1 Plataforma de procesamiento y visualización de datos seleccionada

Power BI, una herramienta integral de Microsoft, se posiciona como la elección principal para la visualización de datos en esta tesis, basándonos en varias consideraciones clave. La elección de Power BI se alinea estratégicamente con el entorno tecnológico existente y proporciona las herramientas necesarias para presentar hallazgos de manera efectiva, contribuyendo así al éxito general de la investigación sobre amenazas cibernéticas en México.

4.1.5 Fase 5. Diseminación

Al finalizar el análisis, se integrarán los resultados obtenidos de los objetivos anteriores. Las lecciones aprendidas se utilizarán para generar recomendaciones específicas, aprovechando técnicas de aprendizaje automático y análisis predictivo, cumpliendo el ***Objetivo Específico 3 - Generación Automatizada de Recomendaciones para Reforzar la Ciberseguridad***

4.2 Configuración del entorno experimental

Para llevar a cabo los experimentos necesarios en esta tesis, se utilizó Power BI Desktop como la herramienta principal de visualización de datos. Power BI Desktop permite construir consultas avanzadas, modelos y reportes que visualizan datos de manera efectiva. Con esta herramienta, se pueden construir modelos de datos, crear reportes y compartir el trabajo mediante la publicación en el servicio de Power BI. A continuación se detalla la configuración del entorno experimental utilizado, incluyendo la instalación y los requisitos mínimos de Power BI Desktop.

4.2.1 Instalación de Power BI Desktop

Power BI Desktop se puede obtener de dos maneras, cada una descrita en las siguientes secciones:

- **Instalación como una aplicación desde la Microsoft Store**: Este método facilita la instalación y actualización automática del software.
- **Descarga directa como un ejecutable**: Se puede descargar e instalar directamente en el equipo desde el sitio oficial de Microsoft. Este método permite un control más directo sobre el proceso de instalación y la versión del software utilizada.

Ambos métodos permiten obtener la última versión de Power BI Desktop en el equipo, pero existen algunas diferencias a tener en cuenta:

- **Microsoft Store**: Proporciona actualizaciones automáticas y una instalación más sencilla.
- **Descarga directa**: Ofrece mayor control sobre la instalación y permite mantener versiones específicas del software.

4.2.2 Requisitos Mínimos

Para ejecutar Power BI Desktop, se deben cumplir los siguientes requisitos mínimos:

- **Sistema Operativo**: Windows 7 / Windows Server 2008 R2, o versiones posteriores.
- **.NET Framework**: Versión 4.6.2 o superior.
- **Navegador**: Internet Explorer 10 o versiones posteriores.
- **Memoria (RAM)**: Al menos 1 GB disponible, siendo recomendable 1.5 GB o más.
- **Pantalla**: Resolución mínima de 1440x900 o 1600x900 (16:9). Resoluciones más bajas como 1024x768 o 1280x800 no son compatibles, ya que ciertos controles (como el cierre de la pantalla de inicio) se visualizan fuera de esas resoluciones.

- **Configuración de Pantalla en Windows**: Si se configura la pantalla para cambiar el tamaño del texto, aplicaciones y otros elementos a más del 100%, es posible que no se puedan ver ciertos diálogos necesarios para continuar usando Power BI Desktop. En caso de encontrarse con este problema, se debe verificar la configuración de pantalla en Windows y ajustar el tamaño al 100%.
- **CPU**: Se recomienda un procesador de 1 gigaherzio (GHz) de 64 bits (x64).

4.2.3 Configuración Específica del Entorno

En este proyecto, Power BI Desktop se instaló como una aplicación desde la Microsoft Store, asegurando que el software estuviera siempre actualizado. La configuración del entorno se realizó en un equipo con las siguientes especificaciones:

- **Sistema Operativo**: Windows 10 Pro
- **Procesador**: Intel Core i7 de 64 bits (x64)
- **Memoria (RAM)**: 16 GB
- **Disco Duro**: 512 GB SSD
- **Pantalla**: Resolución de 1920x1080 (Full HD)

4.2.4 Uso de Power BI Desktop en la Experimentación

Power BI Desktop se utilizó para la creación y visualización de los modelos de datos necesarios para el análisis de ciberseguridad. Las principales funcionalidades empleadas incluyeron:

- **Conexión a fuentes de datos**: Integración con bases de datos y archivos CSV proporcionados por Fortinet.
- **Modelado de datos**: Construcción de relaciones entre tablas de datos y creación de medidas calculadas.
- **Visualización de datos**: Creación de gráficos, tablas y dashboards interactivos para analizar la prevalencia de amenazas cibernéticas.
- **Publicación de reportes**: Compartición de los reportes a través del servicio de Power BI, facilitando la colaboración y revisión por parte de los stakeholders del proyecto.

Esta configuración del entorno experimental permitió un análisis detallado y visualización efectiva de los datos de amenazas cibernéticas, contribuyendo significativamente a los hallazgos y conclusiones de esta tesis doctoral.

4.2.5 Exploración de los Datos seleccionados

La exploración de datos es un proceso fundamental en cualquier análisis de datos, ya que permite comprender mejor la estructura, características y calidad del conjunto de datos. En este proyecto, la exploración de los datos se realizó utilizando Power BI Desktop, aprovechando sus capacidades de análisis y visualización interactiva. A continuación, se describen los pasos y hallazgos principales de esta fase.

El conjunto de datos utilizado en esta investigación consta de datos totales mensuales agregados

de la prevalencia y volumen de amenazas de los tres tipos de amenazas detectadas mencionados anteriormente en el territorio mexicano. El conjunto de datos utilizado en este proyecto está dedicado a la medida de prevalencia y volumen de conteo de amenazas, donde el valor del conteo es el número total de dispositivos que detectan amenazas y el volumen de detecciones por dichos dispositivos. Se eligió la medida de prevalencia y volumen para capturar la amplitud del panorama de amenazas.

Es importante diferenciar entre la prevalencia de amenazas y el volumen de amenazas. La prevalencia se refiere al número total de dispositivos que detectan al menos una amenaza en un periodo determinado, mientras que el volumen de amenazas es el número total de detecciones dentro de ese mismo periodo. Por ejemplo, un volumen de 100 detecciones de amenazas podría registrarse bajo diferentes niveles de prevalencia: 10 dispositivos que detectan 10 conexiones maliciosas cada uno, lo que da como resultado un volumen de 100 y una prevalencia de 10, o 100 dispositivos que detectan 1 conexión de amenaza cada uno, generando también un volumen de 100 pero con una prevalencia de 100.

Donde la prevalencia de amenazas es el valor medido, los operadores comunes como suma, promedio, desviación estándar, mínimo y máximo no se pueden usar para resumir los datos. Para ilustrar esto, se consideran los siguientes escenarios.

Escenario 1:

- El día 1, los dispositivos a y b detectan al menos una amenaza, lo que da una prevalencia de 2.
- El día 2, los dispositivos c y d detectan al menos una amenaza, lo que da una prevalencia de 2.
- La suma de prevalencia en este escenario es 4.

Escenario 2:

- El día 1, los dispositivos a y b detectan al menos una amenaza, lo que da una prevalencia de 2.
- El día 2, los mismos dispositivos a y b detectan al menos una amenaza, lo que da una prevalencia de 2.
- La suma de prevalencia en este escenario es 2.

A partir de los dos escenarios anteriores, es evidente que el operador de suma no se puede aplicar consistentemente a la medida de prevalencia. Lo mismo ocurre para los operadores de mínimo y máximo como se muestra en el escenario 3 a continuación.

Escenario 3:

- El día 1, los dispositivos a y b detectan al menos una amenaza, lo que da una prevalencia de 2.
- El día 2, los dispositivos c y d detectan al menos una amenaza, lo que da una prevalencia de 2.

- El día 3, los dispositivos e y f detectan al menos una amenaza, lo que da una prevalencia de 2.
- Aplicando los operadores de mínimo y máximo para este intervalo de 3 días, obtenemos un mínimo de 2 y un máximo de 2. Sin embargo, en realidad, el número mínimo de dispositivos para este intervalo de 3 días es 6 y el máximo también es 6.

4.3 Procedimientos de experimentación

En esta sección se detallan los procedimientos experimentales llevados a cabo en el desarrollo de esta tesis doctoral. La metodología seguida se estructura en varias fases, desde la recolección de datos hasta la generación de recomendaciones basadas en el análisis de ciberamenazas en México.

4.3.1 Recolección de Datos

La recolección de datos se realizó a través de la colaboración con Fortinet, específicamente utilizando los datos proporcionados por FortiGuard Labs. Los datos recopilados incluyen registros de amenazas cibernéticas detectadas por dispositivos de seguridad Fortinet, tales como firewalls FortiGate y el software de endpoint FortiClient. Los tipos de amenazas consideradas en este estudio son botnets, intrusiones detectadas por el sistema de prevención de intrusiones (IPS) y virus/malware.

4.3.1.1 Cómo Cargar los Datos

En esta sección se describe el proceso para crear un dashboard para el análisis de los datos proporcionados por el equipo de Ciencia de Datos en formato JSON.

1. Primero, se debe importar los datos a la plataforma haciendo clic en "Obtener Datos" como se muestra en la Figura 34.

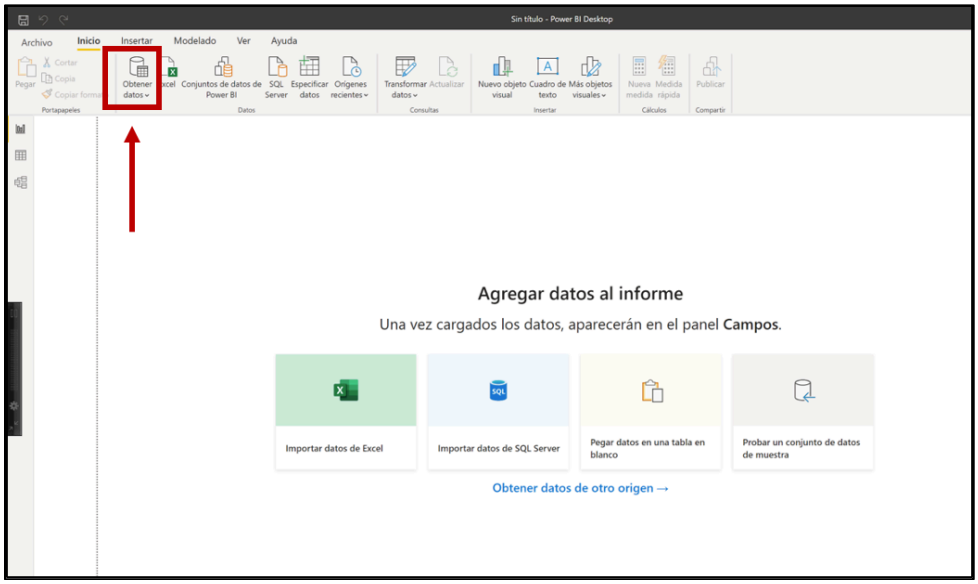


Figura 34. Obtener Dato en Power BI.

2. A continuación, seleccionamos el tipo de datos con los que vamos a trabajar. En este caso, seleccionamos JSON, Web o el formato deseado como se muestra en la Figura 35.

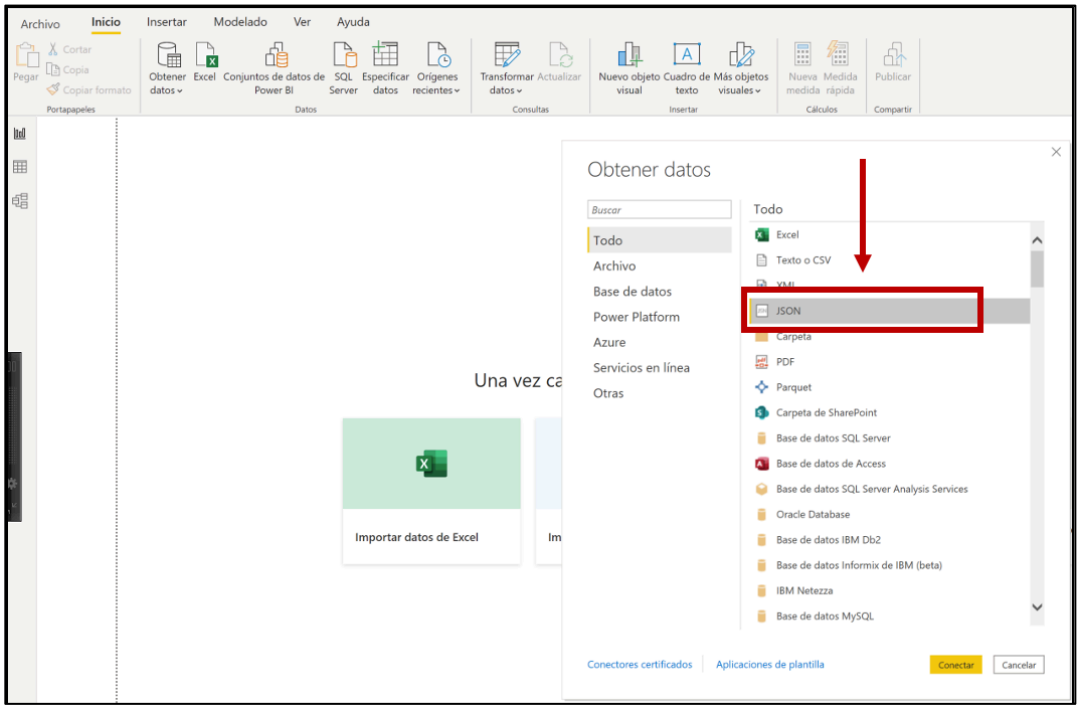


Figura 35. Selección de tipo de Datos.

3. En este punto, importamos los datos del archivo de datos a Power BI. Sin embargo, debido al tipo de formato que tiene este archivo, es necesario convertirlo en una tabla y luego expandir los datos. En la pestaña Archivo, hacemos clic en "Convertir a Tabla" como se muestra en la Figura 3.

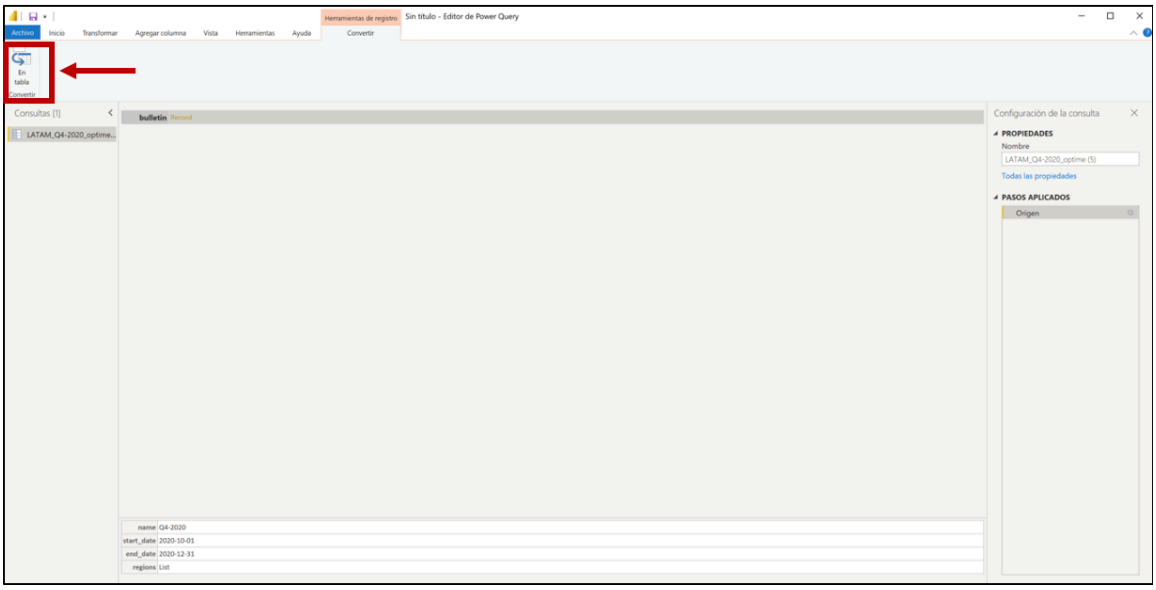


Figura 36. Conversion de Datos a Tabla.

4. Ahora, hemos visto que el formato de los datos ha cambiado, pero aún no muestra toda la información. Para ello, debemos extraer los datos de las columnas.

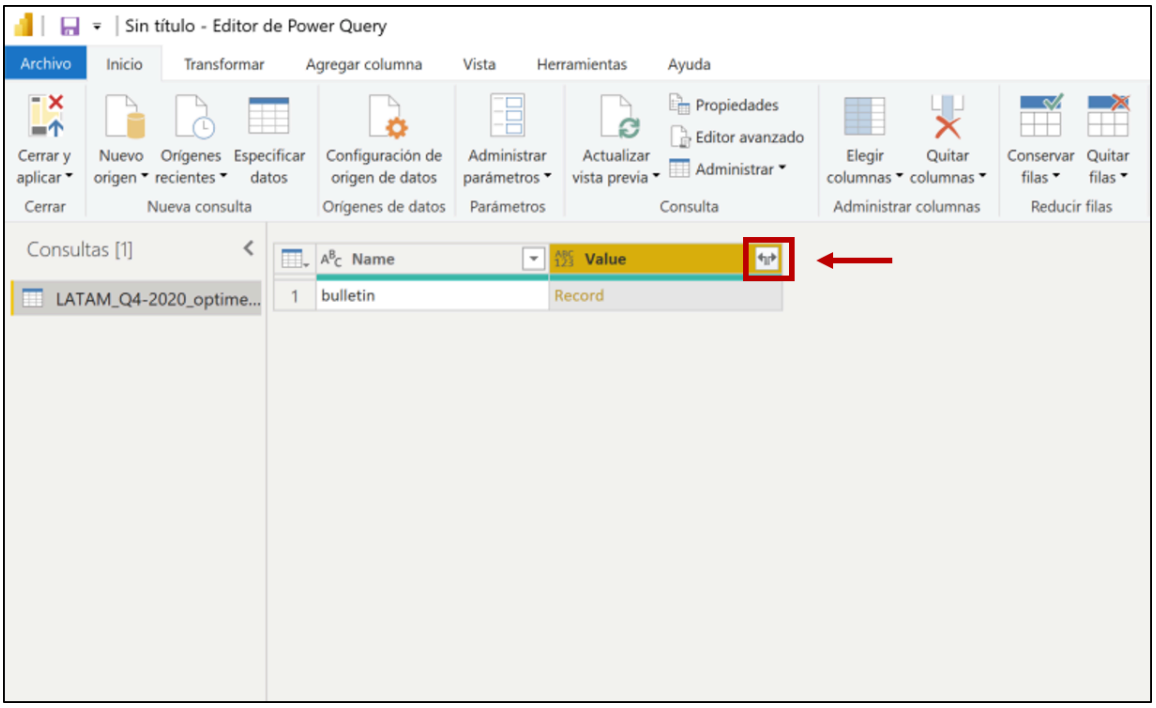


Figura 37. Extraccion de Datos.

5. La Figura 5 muestra el tipo de datos que contiene la columna "Value". Para poder extraerlos, hacemos clic en el botón "Aceptar".

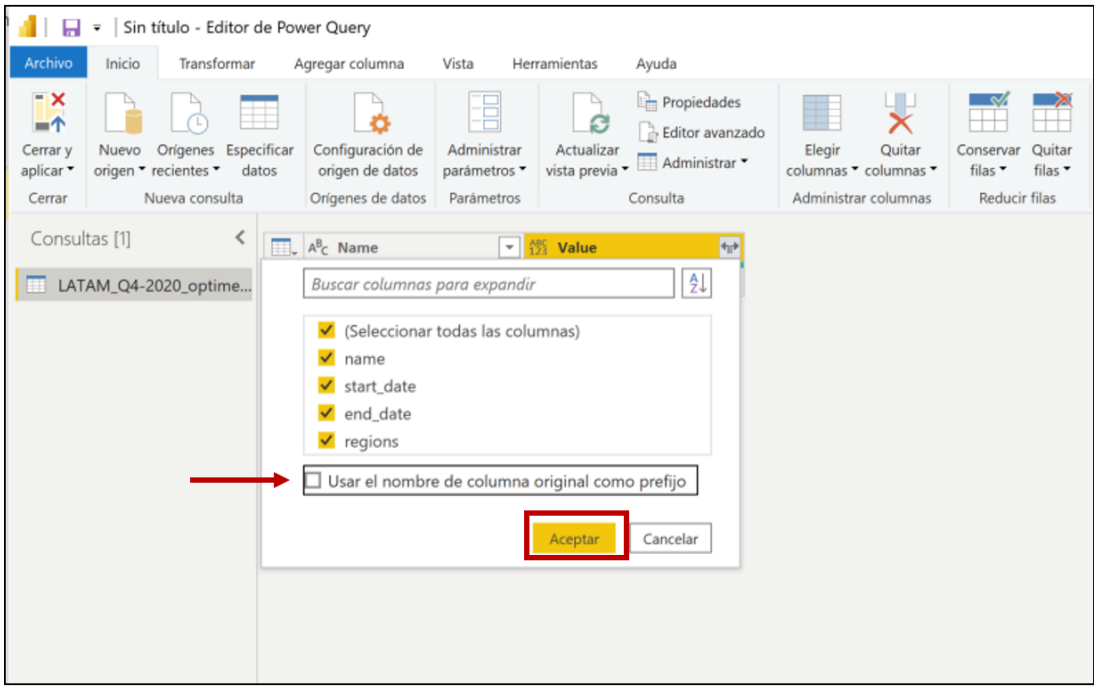


Figura 38. Selección de Columna.

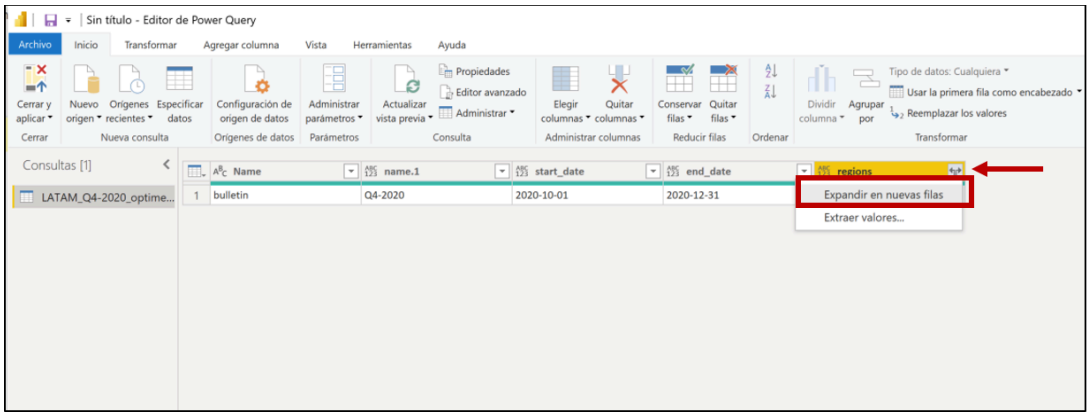


Figura 39. Expandir Nuevas Filas

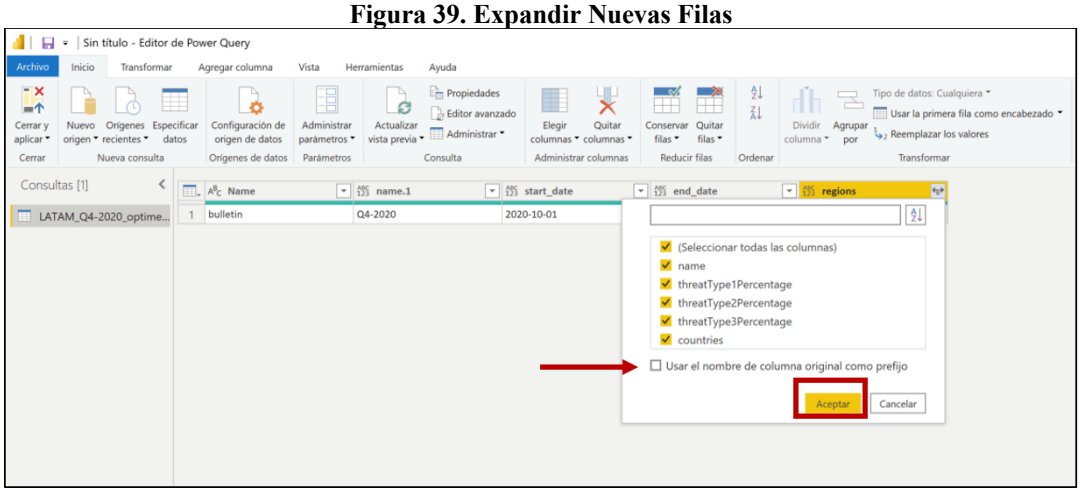


Figura 40. Selección de Nombre de Columna.

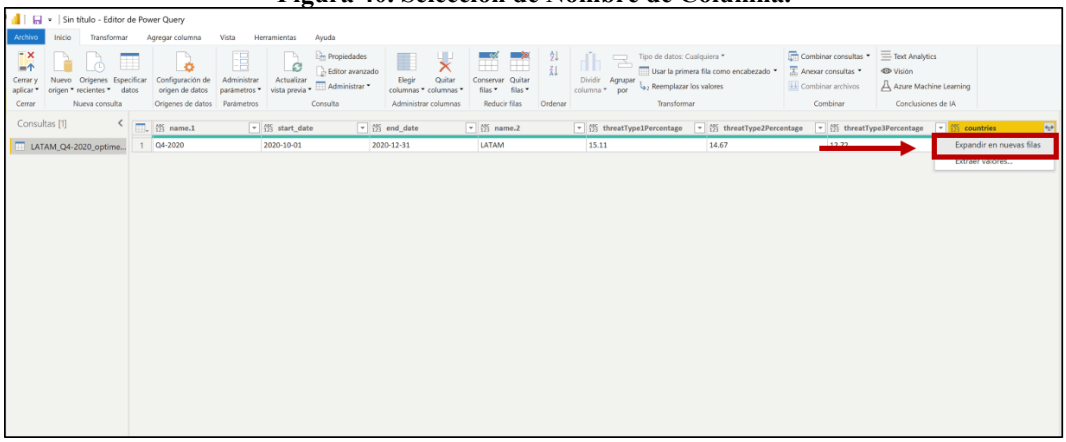


Figura 41. Expandir nuevas Filas.

6. En este punto, vemos que se han añadido más filas y columnas a nuestra tabla, ya que hemos llegado a la columna con los datos de los países, como se muestra en la Figura 42.

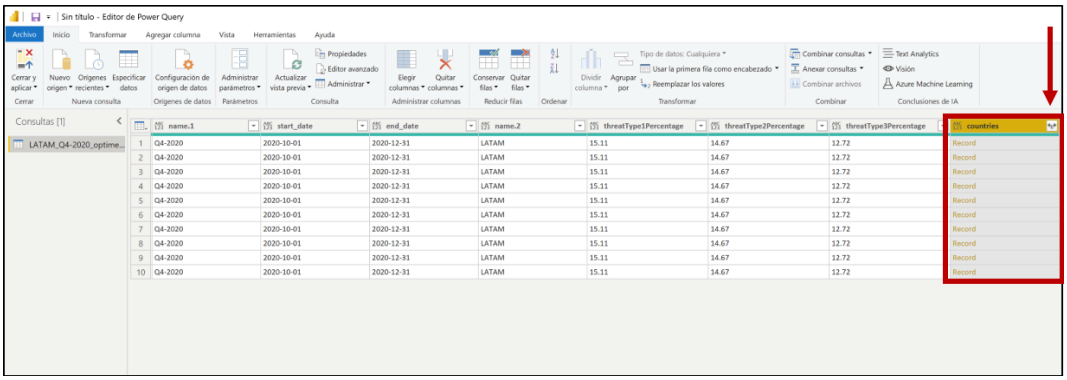


Figura 42. Expandir Tablas.

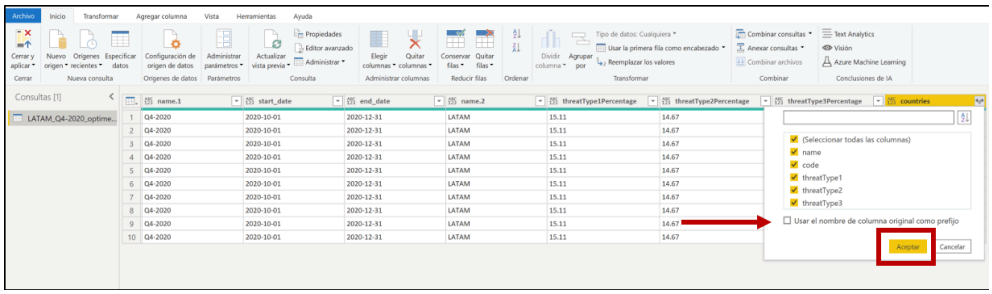


Figura 43. Selección de Nombre de Columna.

7. Como se muestra en la Figura 11, Power BI muestra los diferentes tipos de amenazas que tenemos, donde ThreatType1 corresponde a firmas de malware, ThreatType2 corresponde a firmas de botnets y ThreatType3 corresponde a firmas de IPS. Por lo tanto, debemos duplicar la lista para tener una tabla con cada una de las amenazas, ya que Power BI tiene un límite de 1,000 filas.

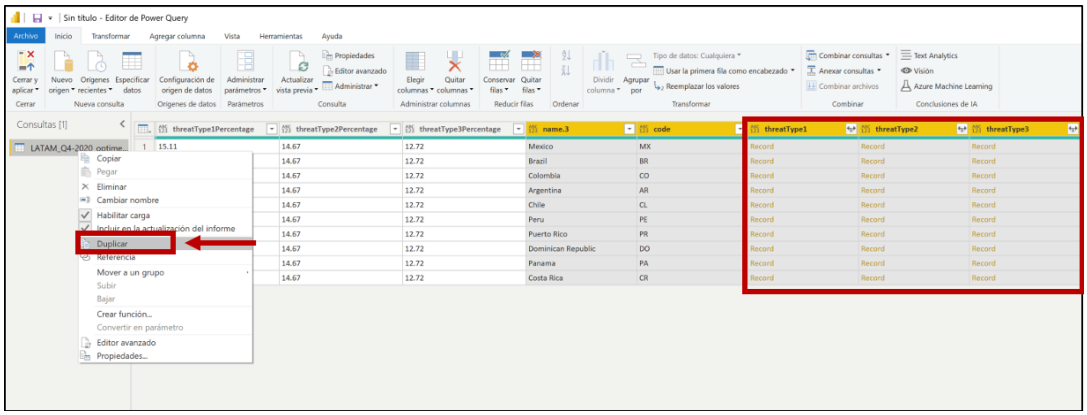


Figura 44. Tipo de Datos.

8. Una vez que copiamos las tablas, podemos eliminar las columnas que no necesitamos. En este caso, para la tabla de firmas de malware, podemos eliminar las columnas ThreatType2 y ThreatType3. Es recomendable nombrarlas según la información a analizar.

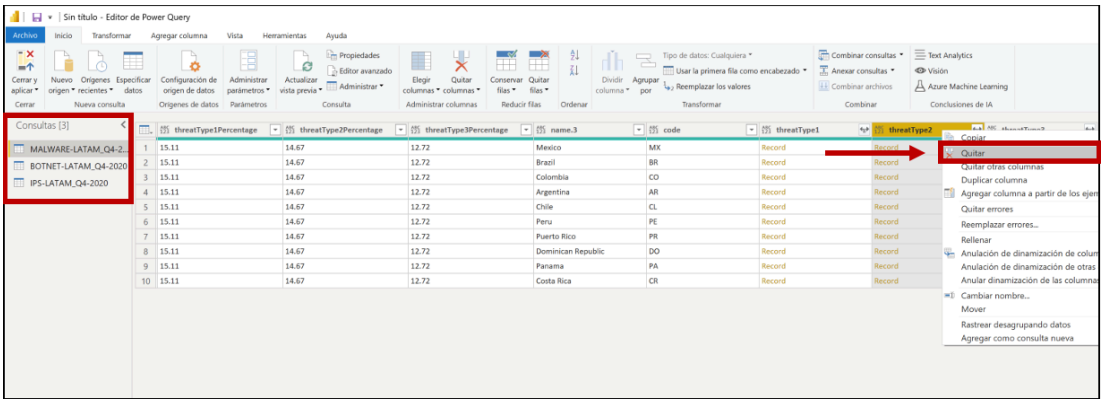


Figura 45. Remover Columnas.

9. Ahora, repetimos el procedimiento para obtener todos los datos.

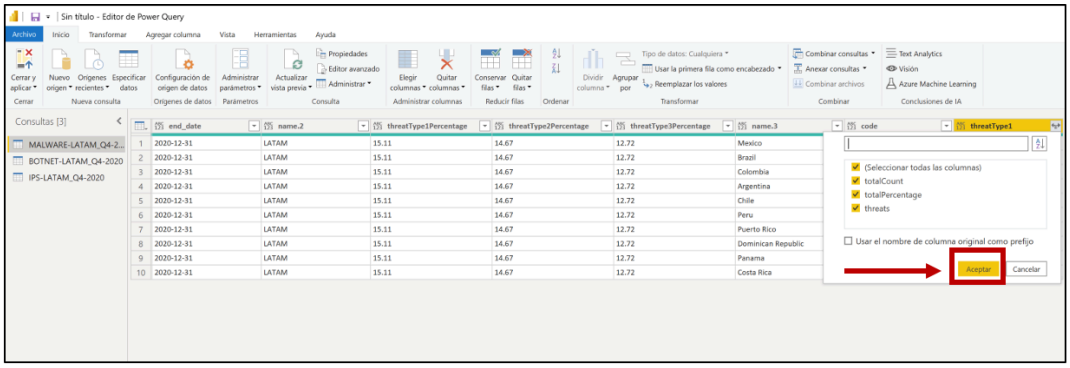


Figura 46. Selección de Nombre Columnas.

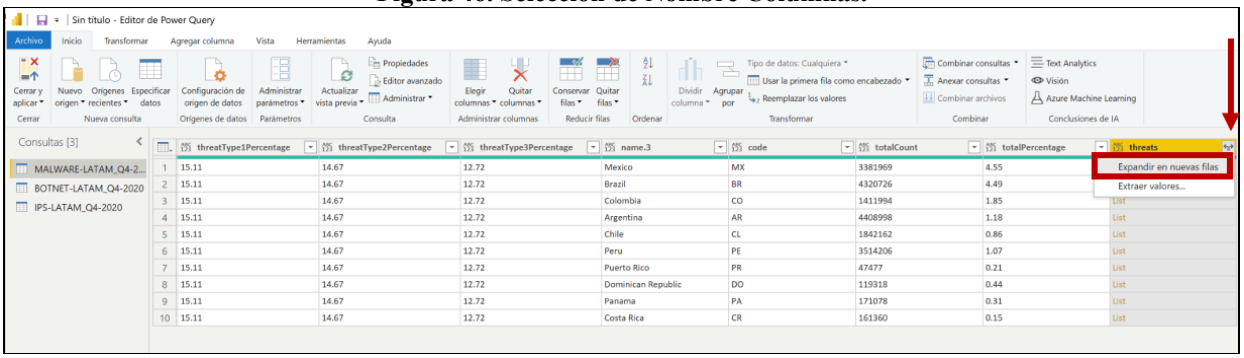


Figura 47. Expandir nuevas Filas.

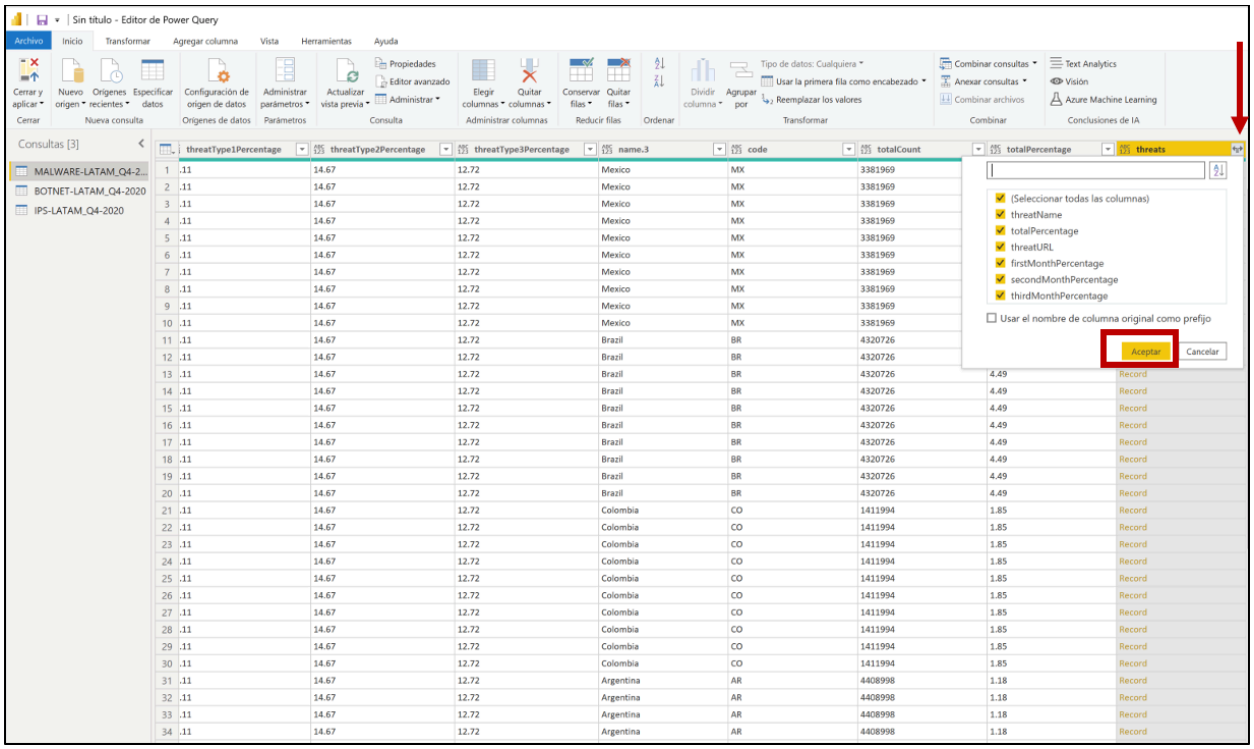


Figura 48. Selección de Datos.

10. En la Figura 49 podemos ver que ya se muestran los datos de las amenazas listadas para malware.

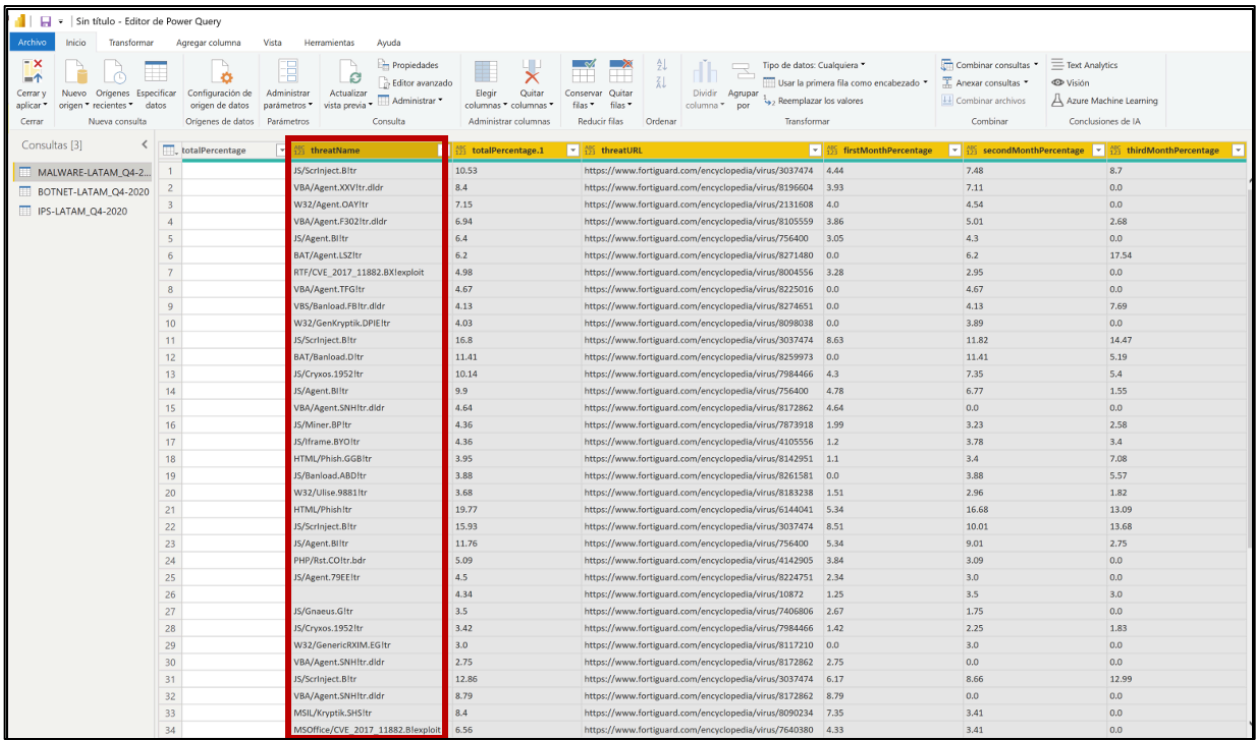
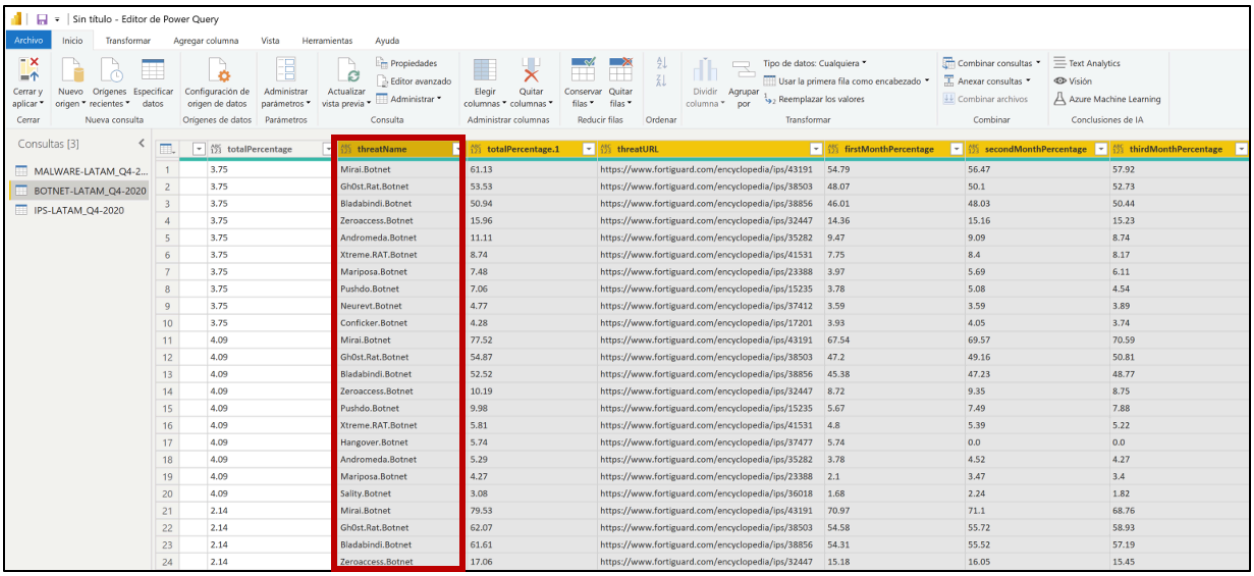


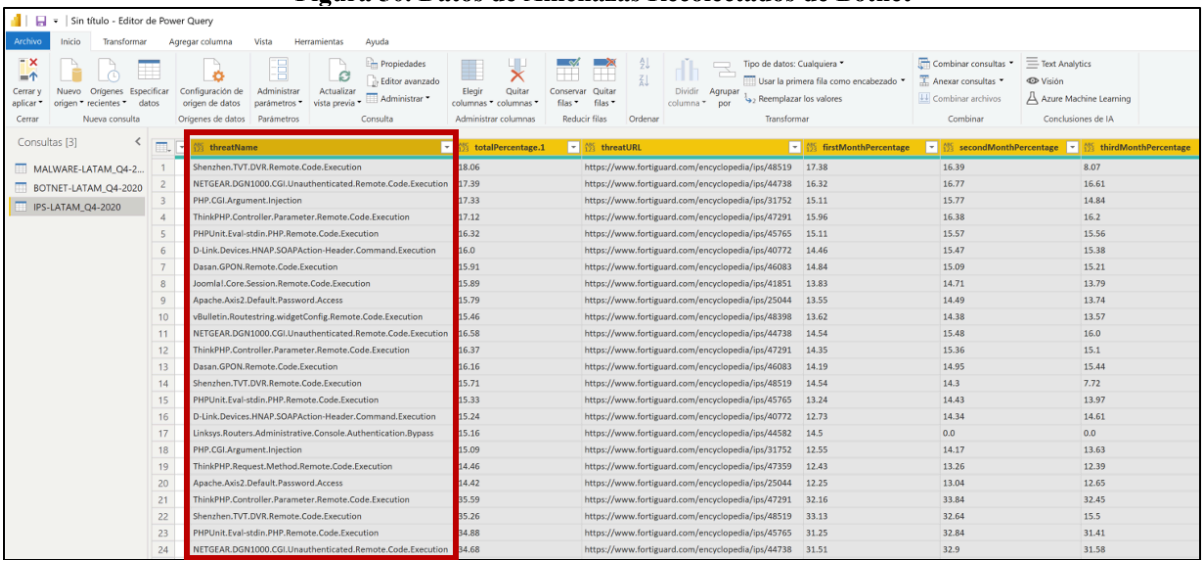
Figura 49. Datos de Amenazas Recolectados de Virus

11. El siguiente paso es repetir el procedimiento para las otras tablas.



	totalPercentage	threatName	totalPercentage.1	threatURL	firstMonthPercentage	secondMonthPercentage	thirdMonthPercentage
1	3.75	Mirai.Botnet	61.13	https://www.fortiguard.com/encyclopedia/ips/43191	54.79	56.47	57.92
2	3.75	Gh0st.Rat.Botnet	53.53	https://www.fortiguard.com/encyclopedia/ips/38503	48.07	50.1	52.73
3	3.75	Bladabindi.Botnet	50.94	https://www.fortiguard.com/encyclopedia/ips/38856	46.01	48.03	50.44
4	3.75	Zeroaccess.Botnet	15.96	https://www.fortiguard.com/encyclopedia/ips/32447	14.36	15.16	15.23
5	3.75	Andromeda.Botnet	11.11	https://www.fortiguard.com/encyclopedia/ips/35282	9.47	9.09	8.74
6	3.75	Xtreme.RAT.Botnet	8.74	https://www.fortiguard.com/encyclopedia/ips/41531	7.75	8.4	8.17
7	3.75	Mariposa.Botnet	7.48	https://www.fortiguard.com/encyclopedia/ips/23388	3.97	5.69	6.11
8	3.75	Pushdo.Botnet	7.06	https://www.fortiguard.com/encyclopedia/ips/15235	3.78	5.08	4.54
9	3.75	Neurevt.Botnet	4.77	https://www.fortiguard.com/encyclopedia/ips/37412	3.59	3.59	3.89
10	3.75	Conficker.Botnet	4.28	https://www.fortiguard.com/encyclopedia/ips/17201	3.93	4.05	3.74
11	4.09	Mirai.Botnet	77.52	https://www.fortiguard.com/encyclopedia/ips/43191	67.54	69.57	70.59
12	4.09	Gh0st.Rat.Botnet	54.87	https://www.fortiguard.com/encyclopedia/ips/38503	47.2	49.16	50.81
13	4.09	Bladabindi.Botnet	52.52	https://www.fortiguard.com/encyclopedia/ips/38856	45.38	47.23	48.77
14	4.09	Zeroaccess.Botnet	10.19	https://www.fortiguard.com/encyclopedia/ips/32447	8.72	9.35	8.75
15	4.09	Pushdo.Botnet	9.98	https://www.fortiguard.com/encyclopedia/ips/15235	5.67	7.49	7.88
16	4.09	Xtreme.RAT.Botnet	5.81	https://www.fortiguard.com/encyclopedia/ips/41531	4.8	5.39	5.22
17	4.09	Hangover.Botnet	5.74	https://www.fortiguard.com/encyclopedia/ips/37477	5.74	0.0	0.0
18	4.09	Andromeda.Botnet	5.29	https://www.fortiguard.com/encyclopedia/ips/35282	3.78	4.52	4.27
19	4.09	Mariposa.Botnet	4.27	https://www.fortiguard.com/encyclopedia/ips/23388	2.1	3.47	3.4
20	4.09	Sality.Botnet	3.08	https://www.fortiguard.com/encyclopedia/ips/36018	1.68	2.24	1.82
21	2.14	Mirai.Botnet	79.53	https://www.fortiguard.com/encyclopedia/ips/43191	70.97	71.1	68.76
22	2.14	Gh0st.Rat.Botnet	62.07	https://www.fortiguard.com/encyclopedia/ips/38503	54.58	55.72	58.93
23	2.14	Bladabindi.Botnet	61.61	https://www.fortiguard.com/encyclopedia/ips/38856	54.31	55.52	57.19
24	2.14	Zeroaccess.Botnet	17.06	https://www.fortiguard.com/encyclopedia/ips/32447	15.18	16.05	15.45

Figura 50. Datos de Amenazas Recolectados de Botnet



	threatName	totalPercentage.1	threatURL	firstMonthPercentage	secondMonthPercentage	thirdMonthPercentage
1	Shenzhen.TVT.DVR.Remote.Code.Execution	18.06	https://www.fortiguard.com/encyclopedia/ips/48519	17.38	16.39	8.07
2	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	17.39	https://www.fortiguard.com/encyclopedia/ips/44738	16.32	16.77	16.61
3	PHP.CGI.Argument.Injection	17.33	https://www.fortiguard.com/encyclopedia/ips/31752	15.11	15.77	14.84
4	ThinkPHP.Controller.Parameter.Remote.Code.Execution	17.12	https://www.fortiguard.com/encyclopedia/ips/47291	15.96	16.38	16.2
5	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	16.32	https://www.fortiguard.com/encyclopedia/ips/45765	15.11	15.57	15.56
6	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	16.0	https://www.fortiguard.com/encyclopedia/ips/40772	14.46	15.47	15.38
7	Dasan.GPON.Remote.Code.Execution	15.91	https://www.fortiguard.com/encyclopedia/ips/46083	14.84	15.09	15.21
8	Joomla!.Core.Session.Remote.Code.Execution	15.89	https://www.fortiguard.com/encyclopedia/ips/41851	13.83	14.71	13.79
9	Apache.Axis2.Default.Password.Access	15.79	https://www.fortiguard.com/encyclopedia/ips/25044	13.55	14.49	13.74
10	vBulletin.Routestring.widgetConfig.Remote.Code.Execution	15.46	https://www.fortiguard.com/encyclopedia/ips/48398	13.62	14.38	13.57
11	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	16.58	https://www.fortiguard.com/encyclopedia/ips/44738	14.54	15.48	16.0
12	ThinkPHP.Controller.Parameter.Remote.Code.Execution	16.37	https://www.fortiguard.com/encyclopedia/ips/47291	14.35	15.36	15.1
13	Dasan.GPON.Remote.Code.Execution	16.16	https://www.fortiguard.com/encyclopedia/ips/46083	14.19	14.95	15.44
14	Shenzhen.TVT.DVR.Remote.Code.Execution	15.71	https://www.fortiguard.com/encyclopedia/ips/48519	14.54	14.3	7.72
15	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	15.33	https://www.fortiguard.com/encyclopedia/ips/45765	13.24	14.43	13.97
16	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	15.24	https://www.fortiguard.com/encyclopedia/ips/40772	12.73	14.34	14.61
17	Linksys.Routers.Administrative.Console.Authentication.Bypass	15.16	https://www.fortiguard.com/encyclopedia/ips/44582	14.5	0.0	0.0
18	PHP.CGI.Argument.Injection	15.09	https://www.fortiguard.com/encyclopedia/ips/31752	12.55	14.17	13.63
19	ThinkPHP.Request.Method.Remote.Code.Execution	14.46	https://www.fortiguard.com/encyclopedia/ips/47359	12.43	13.26	12.39
20	Apache.Axis2.Default.Password.Access	14.42	https://www.fortiguard.com/encyclopedia/ips/25044	12.25	13.04	12.65
21	ThinkPHP.Controller.Parameter.Remote.Code.Execution	35.59	https://www.fortiguard.com/encyclopedia/ips/47291	32.16	33.84	32.45
22	Shenzhen.TVT.DVR.Remote.Code.Execution	35.26	https://www.fortiguard.com/encyclopedia/ips/48519	33.13	32.64	15.5
23	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	34.88	https://www.fortiguard.com/encyclopedia/ips/45765	31.25	32.84	31.41
24	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	34.68	https://www.fortiguard.com/encyclopedia/ips/44738	31.51	32.9	31.58

Figura 51. Datos de Amenazas Recolectados de IPS

12. Es importante mencionar que, una vez que tenemos las tablas completas con toda la información, debemos formatear los datos. Para esto, es necesario seleccionar todas las tablas (ctrl + a) y luego ir a la pestaña "Transformar" y hacer clic en "Detectar tipo de datos".

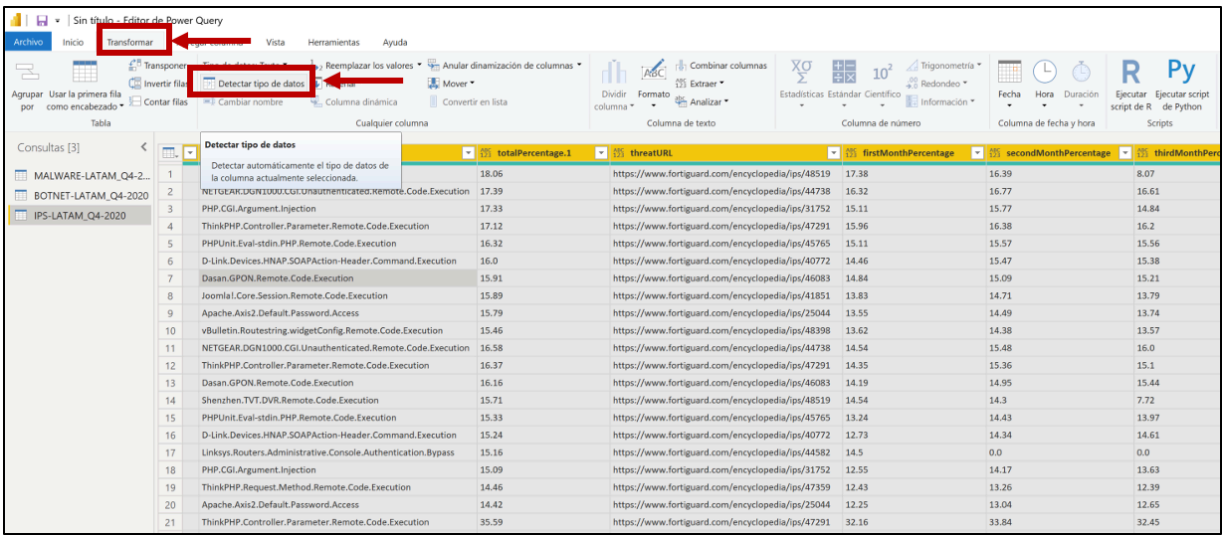


Figura 52. Detectar tipo de Datos.

13. Una vez aplicado, Power BI detectará qué tipo de datos contiene cada tabla, y esto nos ayudará cuando estemos creando nuestro dashboard.

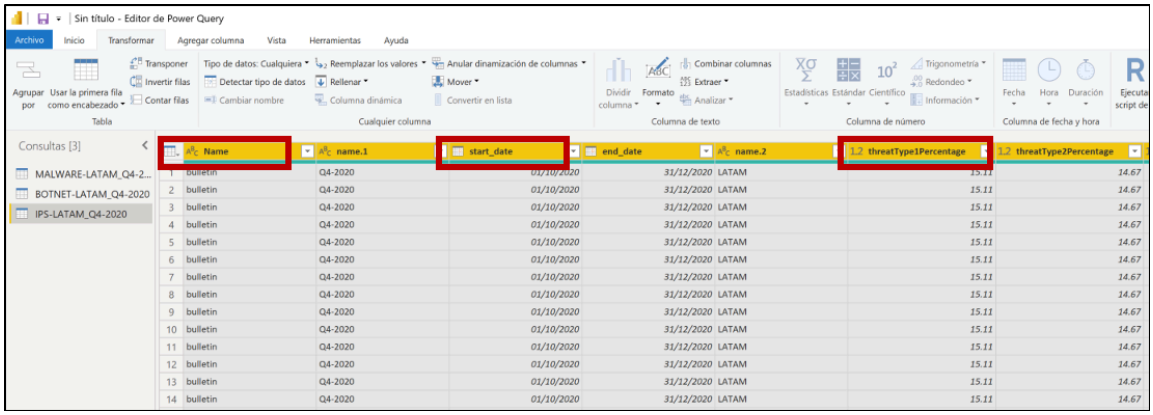
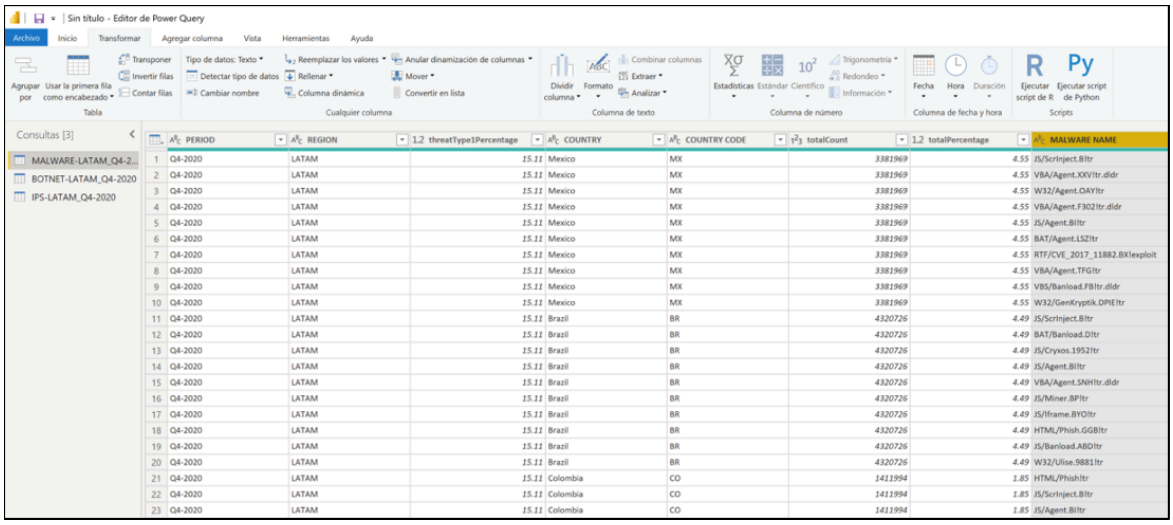


Figura 53. Datos Detectados.

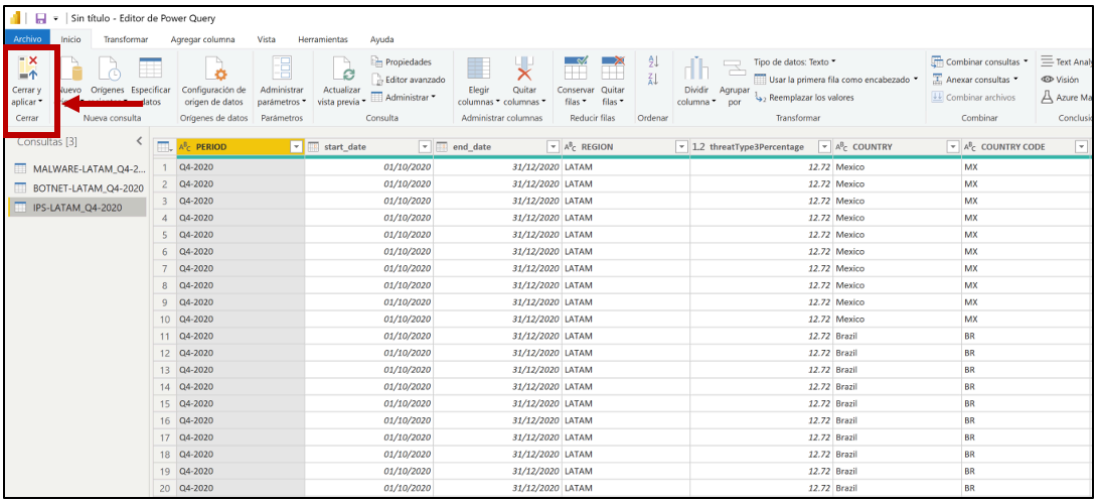
14. También, podemos renombrar cualquier columna y eliminar cualquier columna que no necesitemos.



	PERIOD	REGION	threatType1Percentage	COUNTRY	COUNTRY CODE	totalCount	totalPercentage	MALWARE NAME
1	Q4-2020	LATAM	15.11	Mexico	MX	3381969	4.55	JS/ScrInject.BItr
2	Q4-2020	LATAM	15.11	Mexico	MX	3381969	4.55	VBA/Agent.XXVItr.dldr
3	Q4-2020	LATAM	15.11	Mexico	MX	3381969	4.55	W32/Agent.OAYItr
4	Q4-2020	LATAM	15.11	Mexico	MX	3381969	4.55	VBA/Agent.F302Itr.dldr
5	Q4-2020	LATAM	15.11	Mexico	MX	3381969	4.55	JS/Agent.BIItr
6	Q4-2020	LATAM	15.11	Mexico	MX	3381969	4.55	BAT/Agent.LSZItr
7	Q4-2020	LATAM	15.11	Mexico	MX	3381969	4.55	RTF/CVE_2017_11882.BXIexploit
8	Q4-2020	LATAM	15.11	Mexico	MX	3381969	4.55	VBA/Agent.TFGItr
9	Q4-2020	LATAM	15.11	Mexico	MX	3381969	4.55	VBS/Banload.FBItr.dldr
10	Q4-2020	LATAM	15.11	Mexico	MX	3381969	4.55	W32/GenKryptik.DPIEItr
11	Q4-2020	LATAM	15.11	Brazil	BR	4320726	4.49	JS/ScrInject.BItr
12	Q4-2020	LATAM	15.11	Brazil	BR	4320726	4.49	BAT/Banload.DItr
13	Q4-2020	LATAM	15.11	Brazil	BR	4320726	4.49	JS/Cryxos.1952Itr
14	Q4-2020	LATAM	15.11	Brazil	BR	4320726	4.49	JS/Agent.BIItr
15	Q4-2020	LATAM	15.11	Brazil	BR	4320726	4.49	VBA/Agent.SNHItr.dldr
16	Q4-2020	LATAM	15.11	Brazil	BR	4320726	4.49	JS/Miner.BPItr
17	Q4-2020	LATAM	15.11	Brazil	BR	4320726	4.49	JS/Iframe.BYOItr
18	Q4-2020	LATAM	15.11	Brazil	BR	4320726	4.49	HTML/Phish.GGBItr
19	Q4-2020	LATAM	15.11	Brazil	BR	4320726	4.49	JS/Banload.ABDItr
20	Q4-2020	LATAM	15.11	Brazil	BR	4320726	4.49	W32/Ulise.9881Itr
21	Q4-2020	LATAM	15.11	Colombia	CO	1411994	1.85	HTML/PhishItr
22	Q4-2020	LATAM	15.11	Colombia	CO	1411994	1.85	JS/ScrInject.BItr
23	Q4-2020	LATAM	15.11	Colombia	CO	1411994	1.85	JS/Agent.BIItr

Figura 54. Renombrar columnas.

15. Ahora, estamos listos para ir a nuestro dashboard. En la pestaña "Inicio" hacemos clic en "Cerrar y aplicar".



	PERIOD	start_date	end_date	REGION	threatType3Percentage	COUNTRY	COUNTRY CODE
1	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Mexico	MX
2	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Mexico	MX
3	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Mexico	MX
4	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Mexico	MX
5	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Mexico	MX
6	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Mexico	MX
7	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Mexico	MX
8	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Mexico	MX
9	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Mexico	MX
10	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Mexico	MX
11	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Brazil	BR
12	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Brazil	BR
13	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Brazil	BR
14	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Brazil	BR
15	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Brazil	BR
16	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Brazil	BR
17	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Brazil	BR
18	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Brazil	BR
19	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Brazil	BR
20	Q4-2020	01/10/2020	31/12/2020	LATAM	12.72	Brazil	BR

Figura 55. Guardar y Aplicar Cambios.

16. Ahora que tenemos los datos cargados, podemos comenzar a usarlos y generar nuestro dashboard.

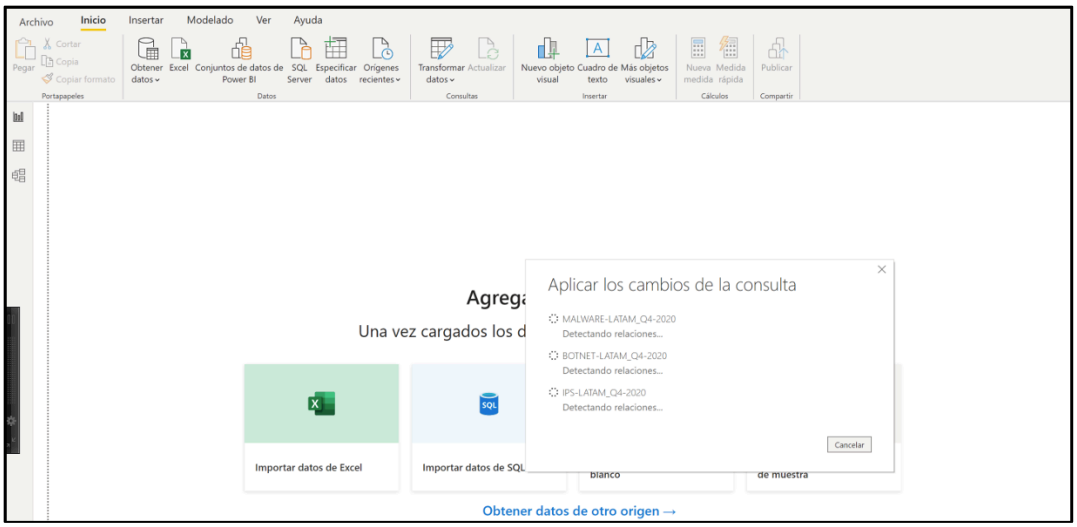


Figura 56. Aplicación y Carga de Datos.

Figura 57. Datos Cargados.

4.3.1.2 Resumen Tabular del set de datos

En esta sección proporciona un resumen tabular simple mostrando las amenazas detectadas junto sus detecciones totales, así como a la cantidad de registros recolectados durante el experimento divididos en Volumen y Prevalencia:

En la tabla 10 podemos observar que el set de datos cuenta con 3,529 registros de la categoría volumen, los cuales cuentan con más de 84 mil millones de detecciones de eventos de ciberseguridad. Siendo IPS el motor de detección que mayores detecciones registro el periodo del 2023.

Motor de Detección	Categoria	Detecciones Totales	Eventos Registrados
botnet	Volume	118,649,993	600
ips	Volume	84,011,059,641	542
ransomware	Volume	91,025	1819
virus	Volume	93,122,749	568
Total		**84,222,923,408**	**3529**

Tabla 10. Resumen Tabular del Volumen del set de datos

En la tabla 11 podemos observar que el set de datos cuenta con 4,130 registros de la categoría Prevalencia, los cuales cuentan con más de 1 Millón de detecciones de amenazas de ciberseguridad. Siendo IPS el motor de detección que mayores detecciones registro en el periodo del 2023.

Motor de Detección	Categoria	Detecciones Totales	Eventos Registrados
botnet	Prevalence	236,910	1200
ips	Prevalence	672,967	585
ransomware	Prevalence	2,541	1780
virus	Prevalence	102,890	565
Total		**1,015,308**	**4130**

Tabla 11. Resumen Tabular del Prevalencia del set de datos

4.3.2 Preprocesamiento de Datos

El preprocesamiento de datos es una etapa crucial para garantizar la calidad y coherencia de los datos antes de su análisis. Las actividades incluidas en esta fase son:

- **Limpieza de Datos**
- **Normalización**
- **Enriquecimiento de Datos**

4.3.2.1 Limpieza de Datos

La limpieza de datos es una fase crucial en cualquier análisis de datos, ya que garantiza la integridad y calidad de los datos utilizados para la experimentación. En este proyecto, se siguieron varios pasos para limpiar y preparar los datos antes de su análisis detallado. A continuación, se describen los procedimientos implementados:

4.3.2.1.1 Eliminación de Duplicados

Los datos duplicados pueden distorsionar los resultados del análisis, llevando a conclusiones incorrectas. Por lo tanto, la primera tarea fue identificar y eliminar cualquier registro duplicado en

el conjunto de datos. Este proceso se realizó utilizando las funciones de Power BI Desktop que permiten detectar y eliminar duplicados automáticamente.

Procedimiento:

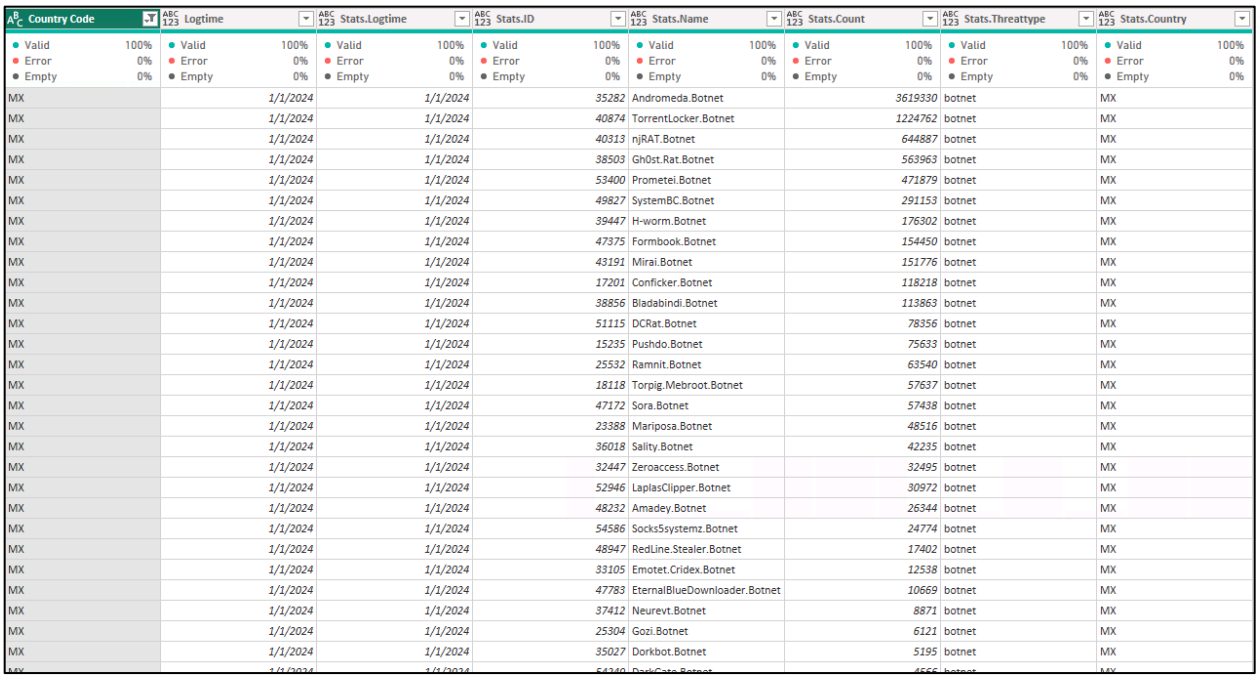
1. **Detección de Duplicados**: Utilizando la herramienta de transformación de datos en Power BI, se aplicó el filtro de "Eliminar duplicados" sobre las columnas clave que identifican de manera única cada registro.
2. **Verificación**: Después de la eliminación, se verificó manualmente una muestra aleatoria de los datos para asegurarse de que los duplicados se habían eliminado correctamente.

4.3.2.1.2 Corrección de Errores

La presencia de errores en los datos, como valores faltantes o incorrectos, puede afectar negativamente el análisis. Se implementaron varios métodos para identificar y corregir estos errores:

Procedimiento:

1. **Identificación de Valores Faltantes**: Se utilizaron visualizaciones de Power BI para detectar valores nulos o faltantes en las columnas críticas. Las tablas de resumen y los gráficos de dispersión ayudaron a visualizar las áreas problemáticas.
2. **Imputación de Datos Faltantes**: Dependiendo de la naturaleza de los datos, los valores faltantes se imputaron utilizando métodos como la media, la mediana, o el valor más frecuente. En algunos casos, se optó por eliminar los registros incompletos si la imputación no era viable.
3. **Corrección de Valores Incorrectos**: Se buscaron valores atípicos o inconsistentes que podrían indicar errores en la entrada de datos. Estos valores se corrigieron o eliminaron según fuera necesario. Por ejemplo, se revisaron las fechas para asegurarse de que estuvieran en un rango razonable y se corrigieron formatos inconsistentes.



Country Code	Logtime	Stats.Logtime	Stats.ID	Stats.Name	Stats.Count	Stats.Threattype	Stats.Country
Valid 100% Error 0% Empty 0%	Valid 100% Error 0% Empty 0%	Valid 100% Error 0% Empty 0%	Valid 100% Error 0% Empty 0%	Valid 100% Error 0% Empty 0%	Valid 100% Error 0% Empty 0%	Valid 100% Error 0% Empty 0%	Valid 100% Error 0% Empty 0%
MX	1/1/2024	1/1/2024	35282	Andromeda.Botnet	3619330	botnet	MX
MX	1/1/2024	1/1/2024	40874	TorrentLocker.Botnet	1224762	botnet	MX
MX	1/1/2024	1/1/2024	40313	njRAT.Botnet	644887	botnet	MX
MX	1/1/2024	1/1/2024	38503	Gh0st.Rat.Botnet	563963	botnet	MX
MX	1/1/2024	1/1/2024	53400	Prometei.Botnet	471879	botnet	MX
MX	1/1/2024	1/1/2024	49827	SystemBC.Botnet	291153	botnet	MX
MX	1/1/2024	1/1/2024	39447	H-worm.Botnet	176302	botnet	MX
MX	1/1/2024	1/1/2024	47375	Formbook.Botnet	154450	botnet	MX
MX	1/1/2024	1/1/2024	43191	Mirai.Botnet	151776	botnet	MX
MX	1/1/2024	1/1/2024	17201	Conficker.Botnet	118218	botnet	MX
MX	1/1/2024	1/1/2024	38856	Bladabindi.Botnet	113863	botnet	MX
MX	1/1/2024	1/1/2024	51115	DCRat.Botnet	78356	botnet	MX
MX	1/1/2024	1/1/2024	15235	Pushdo.Botnet	75633	botnet	MX
MX	1/1/2024	1/1/2024	25532	Ramnit.Botnet	63540	botnet	MX
MX	1/1/2024	1/1/2024	18118	Torpig.Mebroot.Botnet	57637	botnet	MX
MX	1/1/2024	1/1/2024	47172	Sora.Botnet	57438	botnet	MX
MX	1/1/2024	1/1/2024	23388	Mariposa.Botnet	48516	botnet	MX
MX	1/1/2024	1/1/2024	36018	Sality.Botnet	42235	botnet	MX
MX	1/1/2024	1/1/2024	32447	Zeroaccess.Botnet	32495	botnet	MX
MX	1/1/2024	1/1/2024	52946	LaplasClipper.Botnet	30972	botnet	MX
MX	1/1/2024	1/1/2024	48232	Amadey.Botnet	26344	botnet	MX
MX	1/1/2024	1/1/2024	54586	Socks5systemz.Botnet	24774	botnet	MX
MX	1/1/2024	1/1/2024	48947	RedLine.Stealer.Botnet	17402	botnet	MX
MX	1/1/2024	1/1/2024	33105	Emotet.Cridex.Botnet	12538	botnet	MX
MX	1/1/2024	1/1/2024	47783	EternalBlueDownloader.Botnet	10669	botnet	MX
MX	1/1/2024	1/1/2024	37412	Neurevt.Botnet	8871	botnet	MX
MX	1/1/2024	1/1/2024	25304	Gozi.Botnet	6121	botnet	MX
MX	1/1/2024	1/1/2024	35027	Dorkbot.Botnet	5195	botnet	MX

Figura 58. Corrección de Errores

4.3.2.2 Normalización y Estandarización

Para asegurar la coherencia en el análisis, se normalizaron y estandarizaron los datos según fuera necesario. Esto incluyó la conversión de unidades, la normalización de nombres de variables y la estandarización de formatos de fecha y hora. Agregar la columna de clasificación de amenaza (botnet, ips, virus y ransomware)

Procedimiento:

1. **Conversión de Unidades**: Donde fue necesario, se convirtieron las unidades de medida a un estándar común. Por ejemplo, todas las medidas de tiempo se unificaron en el mismo formato (por ejemplo, horas a minutos).
2. **Estandarización de Formatos**: Las fechas se convirtieron a un formato estándar (DD/MM/AAAA) para facilitar la comparación y el análisis. Los nombres de las variables se revisaron para asegurar que fueran consistentes y descriptivos.

Country Code	Date	Sig ID	Signature Name	Volume	Stats.Threattype	Data.Type	Tactic
MX	Sunday, January 1, 2023	8289142	W32/VHD.OBF!tr.ransom	155	ransomware		
MX	Sunday, January 1, 2023	8289138	W32/VHD.A4D6!tr.ransom	48	ransomware		
MX	Sunday, January 1, 2023	8279374	MSIL/Filecoder.AEJ!tr.ransom	51	ransomware		
MX	Sunday, January 1, 2023	8273597	W32/Conti.F!tr.ransom	343	ransomware		
MX	Sunday, January 1, 2023	8272254	W32/Filecoder.FC!tr.ransom	53	ransomware		
MX	Sunday, January 1, 2023	8270915	W32/Filecoder.EEF8!tr.ransom	52	ransomware		
MX	Sunday, January 1, 2023	8270905	W32/Filecoder.56F4!tr.ransom	52	ransomware		
MX	Sunday, January 1, 2023	8265481	W32/Kryptik.FBCK!tr.ransom	53	ransomware		
MX	Sunday, January 1, 2023	8264162	W32/Filecoder.EF15!tr.ransom	53	ransomware		
MX	Sunday, January 1, 2023	8256519	W32/Zudochka.CI!tr.ransom	53	ransomware		
MX	Sunday, January 1, 2023	8256512	W32/Locky.2FF2!tr.ransom	205	ransomware		
MX	Sunday, January 1, 2023	8255875	W64/Filecoder.B1A4!tr.ransom	53	ransomware		
MX	Sunday, January 1, 2023	8255856	W32/Filecoder.ODN!tr.ransom	53	ransomware		
MX	Sunday, January 1, 2023	8253717	W32/Filecoder.ODE!tr.ransom	365	ransomware		
MX	Sunday, January 1, 2023	8252089	W32/Zudochka.EVG!tr.ransom	53	ransomware		
MX	Sunday, January 1, 2023	8251600	W32/Gen.ODE!tr.ransom	52	ransomware		

Sort ascending
Sort descending
Clear sort
Clear filter
Clear all filters
Text filters
Search
(Select all)
botnet
endpoint
ips
ransomware
virus
virus_fsa

Figura 59. Normalización y Estandarización de Datos.

4.3.2.3 Enriquecimiento de Datos

Durante esta fase, se realizaron tareas de incorporación de información adicional relevante, como categorización por amenaza, tipo de ataque y tipo de detección. Para ello, se llevaron distintas acciones como:

- Agregar la columna de Data.Type para clasificar si el evento registrado es Volumen o Prevalence
- Agregar la columna de Tactic para clasificar el evento de seguridad usando MITRE ATT&CK

Country Code	Date	Sig ID	Signature Name	Volume	Stats.Threattype	Data.Type	Tactic
MX	Sunday, January 1, 2023	8289142	W32/VHD.OBF!tr.ransom	155	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8289138	W32/VHD.A4D6!tr.ransom	48	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8279374	MSIL/Filecoder.AEJ!tr.ransom	51	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8273597	W32/Conti.F!tr.ransom	343	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8272254	W32/Filecoder.FC!tr.ransom	53	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8270915	W32/Filecoder.EEF8!tr.ransom	52	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8270905	W32/Filecoder.56F4!tr.ransom	52	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8265481	W32/Kryptik.FBCK!tr.ransom	53	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8264162	W32/Filecoder.EF15!tr.ransom	53	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8256519	W32/Zudochka.CI!tr.ransom	53	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8256512	W32/Locky.2FF2!tr.ransom	205	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8255875	W64/Filecoder.B1A4!tr.ransom	53	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8255856	W32/Filecoder.ODN!tr.ransom	53	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8253717	W32/Filecoder.ODE!tr.ransom	365	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8252089	W32/Zudochka.EVG!tr.ransom	53	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8251600	W32/Gen.ODE!tr.ransom	52	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8250095	W32/Avaddon.C!tr.ransom	104	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8239338	Python/Filecoder.P!tr.ransom	5	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8234853	MSIL/Thanos.A!tr.ransom	155	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8227633	W32/Kryptik.GAC!tr.ransom	51	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8226398	W32/Snake.A!tr.ransom	48	ransomware	Volume	TA0002
MX	Sunday, January 1, 2023	8225947	W32/Kryptik.FRIA!tr.ransom	52	ransomware	Volume	TA0002

Figura 60. Enriquecimiento de Datos.

4.3.2.4 Validación de Datos

Finalmente, se realizó una validación exhaustiva de los datos para asegurar su calidad antes de proceder con el análisis. Esto incluyó verificaciones cruzadas y comparaciones con fuentes de datos externas para confirmar la precisión de los datos.

Procedimiento:

1. **Verificación Cruzada**: Se compararon los datos con fuentes externas o bases de datos previas para asegurar que los valores fueran consistentes y precisos.
2. **Revisión Manual**: Se realizó una revisión manual de una muestra de los datos para identificar cualquier error que pudiera haber pasado desapercibido durante los procesos automatizados.

Al seguir estos procedimientos, se garantizó que el conjunto de datos estuviera limpio, consistente y listo para el análisis, proporcionando una base sólida para obtener resultados precisos y confiables en el estudio.

Country Code	Date	Sig ID	Signature Name	Volume	Stats.Threattype	Data.Type	Tactic
Valid 100%	Valid 100%	Valid 100%	Valid 100%	Valid 100%	Valid 100%	Valid 100%	Valid 100%
Error 0%	Error 0%	Error 0%	Error 0%	Error 0%	Error 0%	Error 0%	Error 0%
Empty 0%	Empty 0%	Empty 0%	Empty 0%	Empty 0%	Empty 0%	Empty 0%	Empty 0%
MX	1/1/2024	35282	Andromeda.Botnet	3619330	botnet	Volume	TA0011
MX	1/1/2024	40874	TorrentLocker.Botnet	1224762	botnet	Volume	TA0011
MX	1/1/2024	40313	njRAT.Botnet	644887	botnet	Volume	TA0011
MX	1/1/2024	38503	Gh0st.Rat.Botnet	563963	botnet	Volume	TA0011
MX	1/1/2024	53400	Prometei.Botnet	471879	botnet	Volume	TA0011
MX	1/1/2024	49827	SystemBC.Botnet	291153	botnet	Volume	TA0011
MX	1/1/2024	39447	H-worm.Botnet	176302	botnet	Volume	TA0011
MX	1/1/2024	47375	Formbook.Botnet	154450	botnet	Volume	TA0011
MX	1/1/2024	43191	Mirai.Botnet	151776	botnet	Volume	TA0011
MX	1/1/2024	17201	Conficker.Botnet	118218	botnet	Volume	TA0011
MX	1/1/2024	38856	Bladabindi.Botnet	113863	botnet	Volume	TA0011
MX	1/1/2024	51115	DCRat.Botnet	78356	botnet	Volume	TA0011
MX	1/1/2024	15235	Pushdo.Botnet	75633	botnet	Volume	TA0011
MX	1/1/2024	25532	Ramnit.Botnet	63540	botnet	Volume	TA0011
MX	1/1/2024	18118	Torpig.Mebroot.Botnet	57637	botnet	Volume	TA0011
MX	1/1/2024	47172	Sora.Botnet	57438	botnet	Volume	TA0011
MX	1/1/2024	23388	Mariposa.Botnet	48516	botnet	Volume	TA0011
MX	1/1/2024	36018	Sality.Botnet	42235	botnet	Volume	TA0011
MX	1/1/2024	32447	Zeroaccess.Botnet	32495	botnet	Volume	TA0011
MX	1/1/2024	52946	LaplasClipper.Botnet	30972	botnet	Volume	TA0011
MX	1/1/2024	48232	Amadey.Botnet	26344	botnet	Volume	TA0011
MX	1/1/2024	54586	Socks5systemz.Botnet	24774	botnet	Volume	TA0011
MX	1/1/2024	48947	RedLine.Stealer.Botnet	17402	botnet	Volume	TA0011
MX	1/1/2024	33105	Emotet.Cridex.Botnet	12538	botnet	Volume	TA0011
MX	1/1/2024	47783	EternalBlueDownloader.Botnet	10669	botnet	Volume	TA0011
MX	1/1/2024	37412	Neurevt.Botnet	8871	botnet	Volume	TA0011
MX	1/1/2024	25304	Gozi.Botnet	6121	botnet	Volume	TA0011
MX	1/1/2024	35027	Dorkbot.Botnet	5195	botnet	Volume	TA0011
MX	1/1/2024	54249	DarkGate.Botnet	4566	botnet	Volume	TA0011
MX	1/1/2024	54294	RisePro.Botnet	4324	botnet	Volume	TA0011

Figura 61. Validación de Datos

4.3.3 Implementación en Power Query

Para llevar a cabo los procedimientos de limpieza de datos mencionados, se utilizó el lenguaje de Power Query en Power BI. A continuación, se presenta el código utilizado para eliminar duplicados, corregir errores, y normalizar los datos en las figuras 62, 63, 64 y 65. La documentacion tecnica del codigo puede encontrarse en el Anexo de este documento. Este código

detalla los pasos específicos implementados para preparar los datos para su análisis para cada set de datos recolectado de cada motor de inspección seleccionado para la experimentación.

Figura 62. Power Query Antivirus

Figura 63. Power Query IPS

Figura 64. Power Query Botnet

Figura 65. Power Query Ransomware

Esta estructura asegura que el proceso de limpieza de datos esté documentado de manera clara y comprensible, proporcionando tanto una descripción de alto nivel como detalles técnicos precisos.

4.3.4 Análisis Exploratorio de Datos (EDA)

El Análisis Exploratorio de Datos (EDA, por sus siglas en inglés) es una fase crucial en cualquier proyecto de ciencia de datos. Esta etapa se enfoca en investigar y resumir las principales características de los datos, a menudo empleando métodos visuales y estadísticas descriptivas. El EDA ayuda a descubrir patrones, detectar anomalías, verificar hipótesis y realizar suposiciones. En este proyecto, el EDA se realizó utilizando Power BI Desktop, aprovechando sus capacidades de visualización interactiva y análisis de datos.

Los objetivos principales del Análisis Exploratorio de Datos en este proyecto fueron:

1. **Comprender la distribución de los datos**: Analizar cómo se distribuyen las variables clave, identificar valores atípicos y entender la dispersión de los datos.
2. **Identificar patrones y tendencias**: Detectar patrones temporales, estacionales o cualquier otra tendencia relevante en los datos.
3. **Evaluar la calidad de los datos**: Identificar datos faltantes, inconsistencias, retos y errores potenciales.
4. **Explorar relaciones entre variables**: Investigar posibles correlaciones y relaciones entre las diferentes variables del conjunto de datos.

4.3.4.1 Herramientas y Métodos Utilizados

- **Power BI Desktop**: Utilizado para crear visualizaciones interactivas y realizar análisis descriptivos.
- **Estadísticas Descriptivas**: Se calcularon medidas como la media, mediana, moda, desviación estándar, entre otras, para resumir las características principales de los datos.
- **Visualizaciones Interactivas**: Gráficos y tablas dinámicas que permitieron una exploración detallada y visual de los datos.

4.3.4.2 Proceso de EDA

1. **Visualización de la Distribución de los Datos**

Se crearon gráficos de histograma para visualizar la distribución de las principales variables de interés, como la prevalencia y el volumen de las amenazas. Estos gráficos ayudaron a identificar valores atípicos y entender la dispersión de los datos. Estos, permitieron observar la frecuencia de los valores de las variables clave.

Como podemos observar en la Figura 66, el motor de inspección con mayor cantidad de detecciones maliciosas es el motor de IPS, seguido del motor de detección de Botnets, Antimalware y Ransomware ya sea tanto en Volumen como en Prevalencia. Esto se debe a la naturaleza de los sensores utilizados para la recolección de datos, siendo estos dispositivos que se encargan de la seguridad perimetral de las organizaciones mexicanas, siendo la primer línea de defensa y recibiendo intentos de ciberataques automatizados.

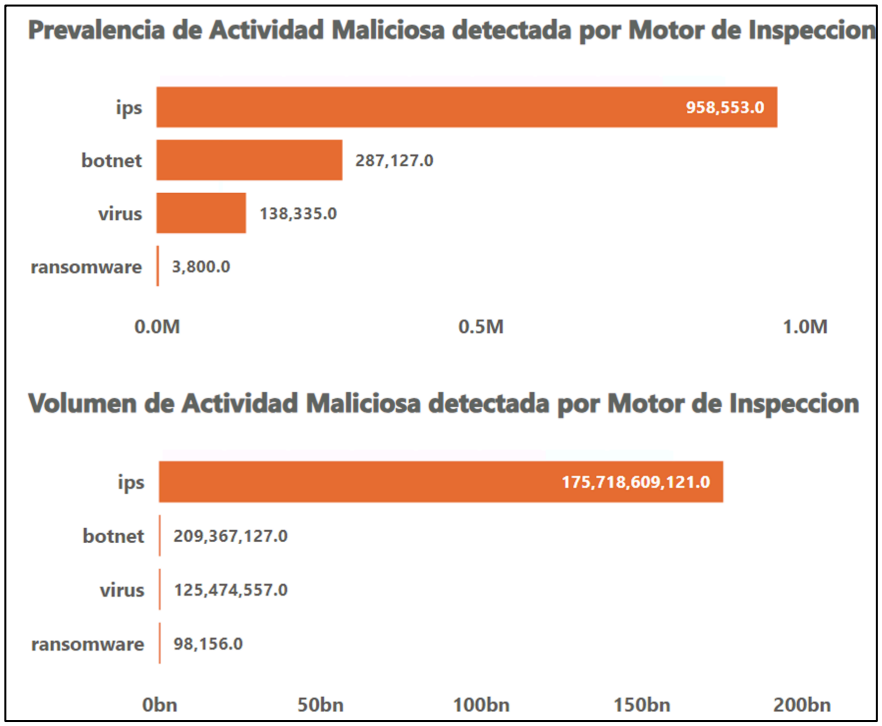


Figura 66. Histograma 1 – Actividad Maliciosa detectada por Motor se Inspección

Por otro lado, se realizó el análisis exploratorio de los datos utilizando CTI. Es decir, se modelo la información recolectada a las fases y técnicas de los frameworks de CTI seleccionados. Esto nos permite poder detectar las fases donde ocurre la mayor cantidad de ataques en el territorio mexicano, siendo la fase de Reconocimiento e Impacto la que presenta mayor cantidad de actividad maliciosa detectada por Volumen. Sin embargo, la Prevalencia de los datos indican que él una mayor cantidad de dispositivos detectaron intentos de Acceso Inicial, así como actividad de botnets activos por medio de canales de Comando y Control durante el periodo de este experimento como se muestra en la Figura 67.

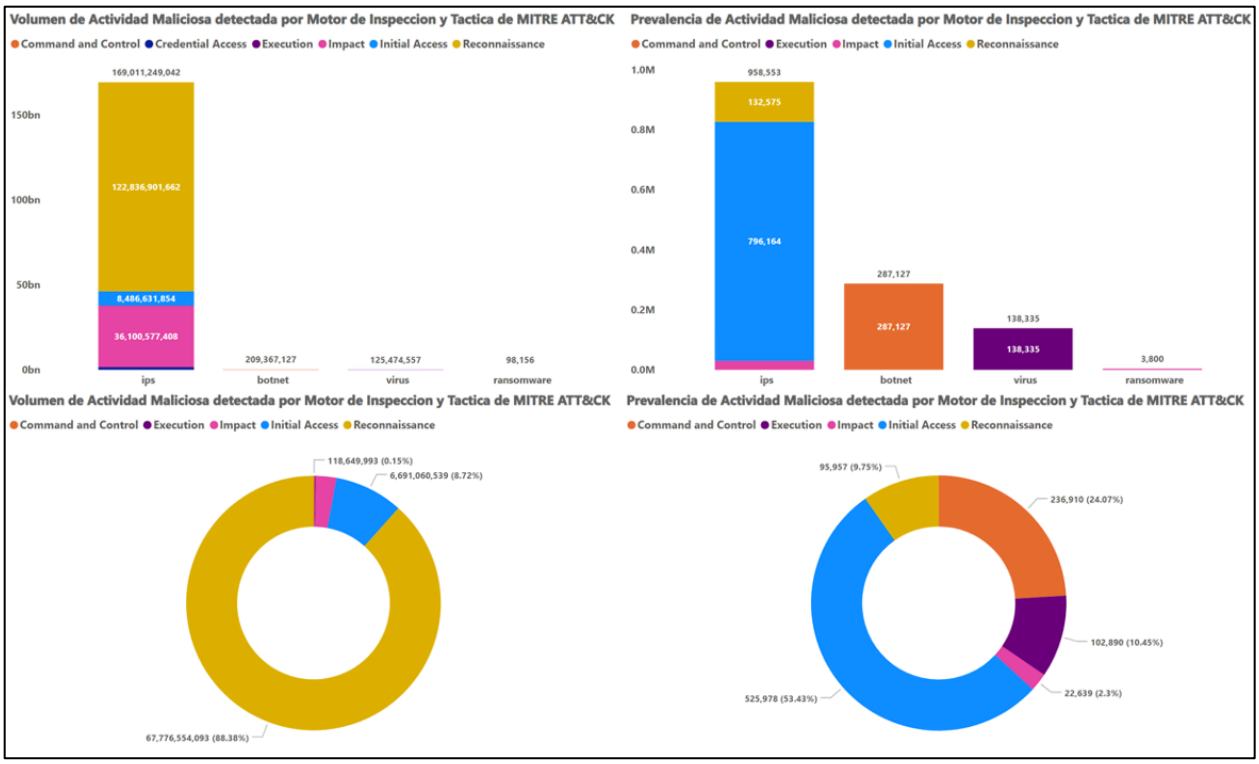


Figura 67. Histograma 2 - Distribución de Actividad Maliciosa detectada por Táctica de MITRE ATTT&CK

Gracias a este análisis, podemos inferir que existe una diferencia notable entre el tipo de datos recolectado, ya que el Volumen de la actividad maliciosa detectada no necesariamente coincide con el valor de Prevalencia. Esto quiere decir que, algunas organizaciones mexicanas pueden recibir ataques más dirigidos (Volumen), mientras que la Prevalencia nos ayuda a verificar cuales son los ataques más comunes que se detectaron en las organizaciones mexicanas durante el periodo de esta investigación (Enero a Diciembre 2023).

Por otro lado la figura 68 nos revela la relación entre volumen y prevalencia con los motores de inspección y las tácticas de MITRE ATT&CK detectadas en este estudio. Es decir, aunque los datos revelan que las técnicas de reconocimiento tienen una mayor cantidad de volumen esto no necesariamente significa que todas las organizaciones mexicanas están siendo afectadas por esta técnica ya que la prevalencia no es tan alta. Por otro lado, los datos revelan que las técnicas de acceso inicial son las que tienen mayor prevalencia en el periodo del estudio. Es decir, las organizaciones mexicanas están experimentando técnicas de acceso inicial en su mayoría. Además, podemos ver que las técnicas de comando y control se encuentran con una prevalencia media y una cantidad de volumen moderada lo que nos dice que existen muchos dispositivos infectados por campañas de botnet en las organizaciones mexicanas de donde se obtuvieron los datos.

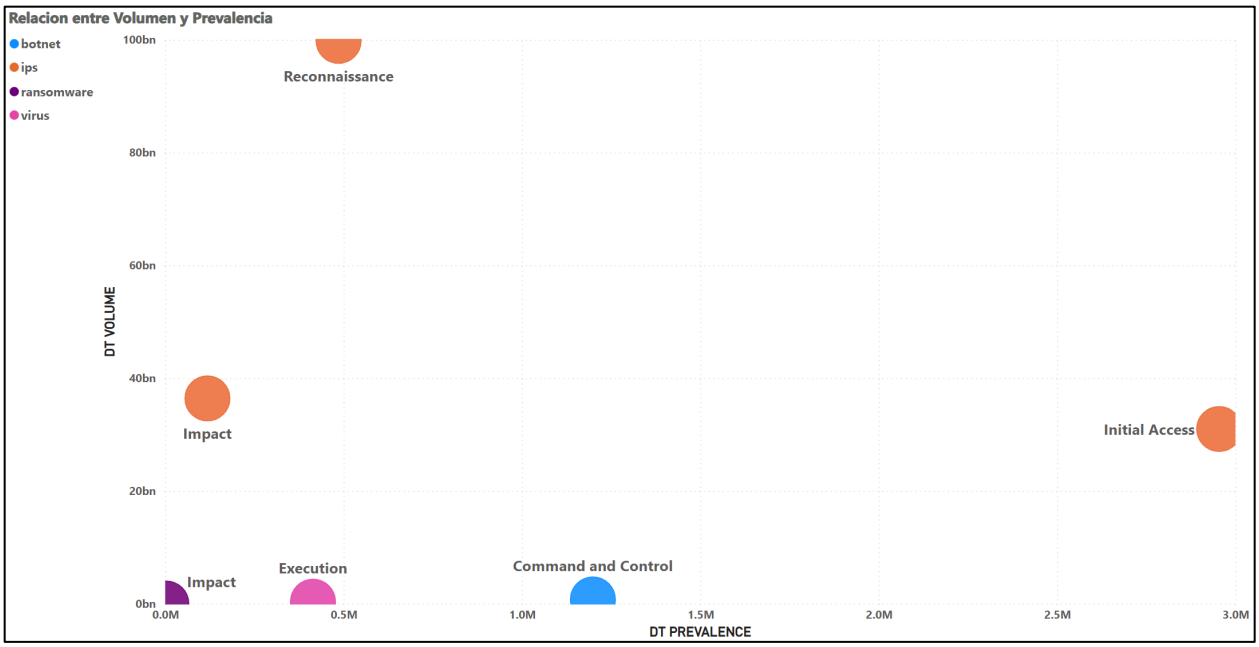


Figura 68. Relación entre motor de inspección y Tácticas de MITRE ATT&CK detectadas por Volumen y Prevalencia

2. Análisis Temporal

Se realizaron gráficos de series temporales para analizar cómo las amenazas evolucionaron a lo largo del tiempo. Se utilizaron para visualizar la evolución de las amenazas a lo largo del período de estudio.

Durante este estudio, se realizó un análisis comparativo entre la actividad maliciosa del 2022 y 2023. El cual revela una disminución considerable de eventos detectados durante el periodo de esta investigación comparando con el año anterior tanto en Volumen como Prevalencia ilustrado en la Figura 69. Sin embargo, podemos observar que la serie temporal nos muestra un aumento de actividad maliciosa detectada a partir de Septiembre.

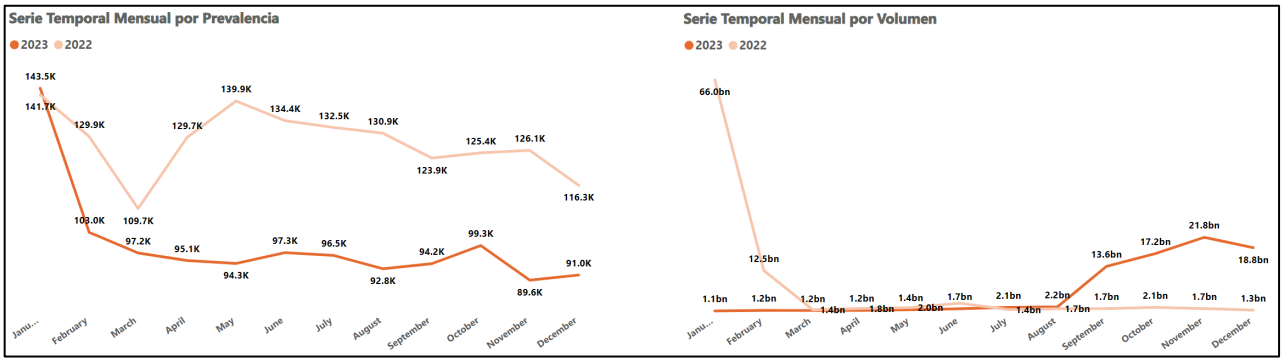


Figura 69. Serie Temporal 1 – Volumen y Prevalencia mensual de actividad maliciosa detectada en México.

Por otro lado, en la Figura 70, podemos notar que el incremento en volumen de actividad maliciosa se debe a tácticas de reconocimiento a partir dl mes de Septiembre. Sin embargo, la prevalencia se

mantiene constante en la mayoría del periodo con un leve aumento de actividad de Acceso Inicial y Comando y Control en Octubre.

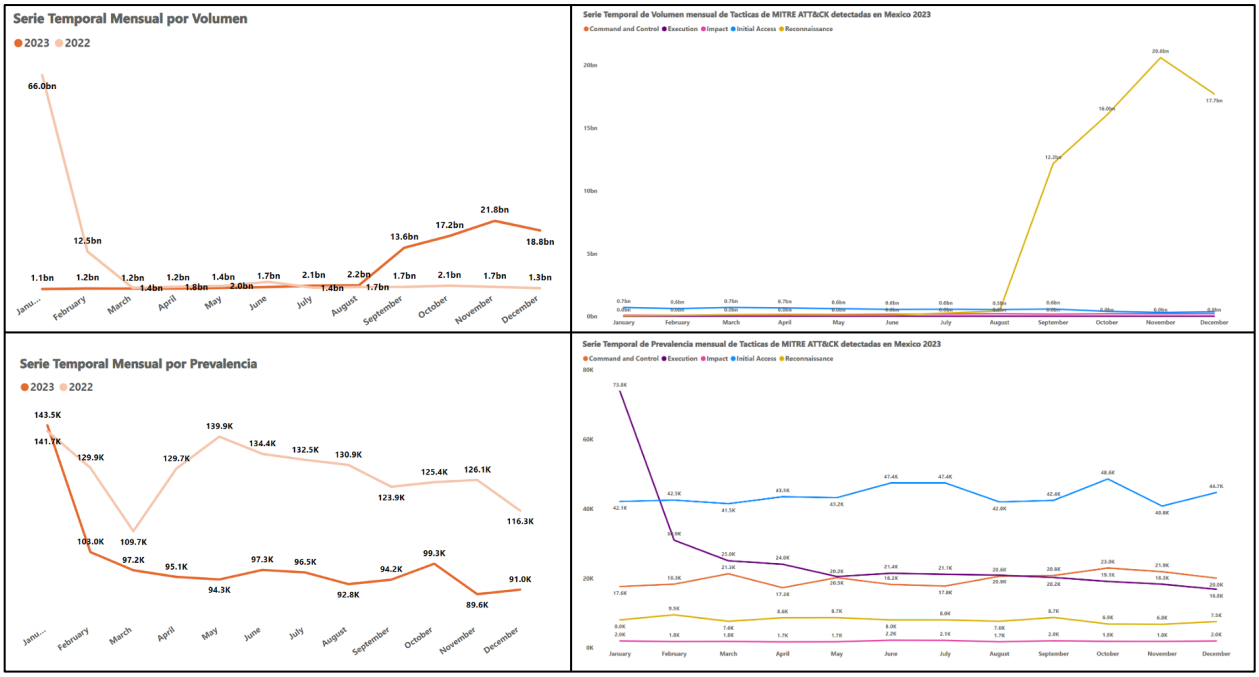


Figura 70. Serie Temporal 2 – Volumen y Prevalencia mensual de actividad maliciosa detectada en México.

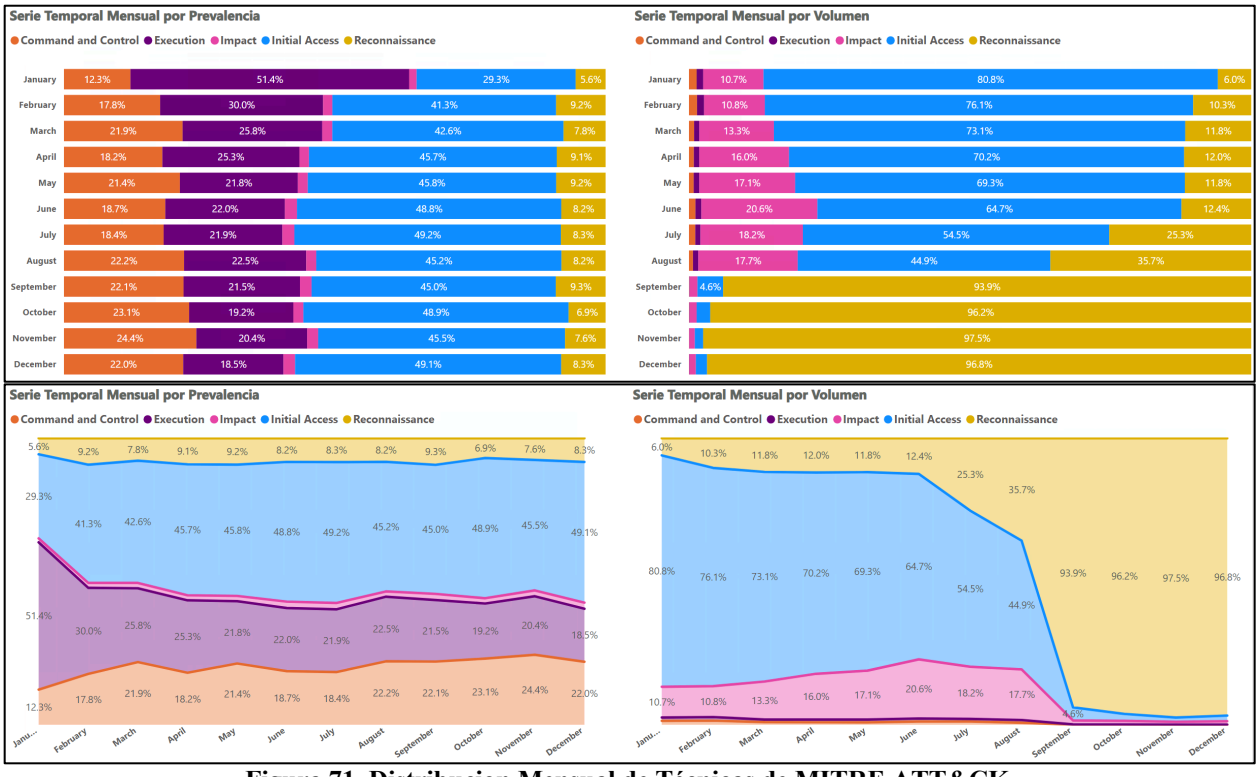


Figura 71. Distribucion Mensual de Técnicas de MITRE ATT&CK

4.3.4.3 Hallazgos Principales del EDA

1. **Distribución de Amenazas**: Gracias a este análisis, podemos inferir que existe una diferencia notable entre el tipo de datos recolectado, ya que el Volumen de la actividad maliciosa detectada no necesariamente coincide con el valor de Prevalencia. Esto quiere decir que, algunas organizaciones mexicanas pueden recibir ataques más dirigidos (Volumen), mientras que la Prevalencia nos ayuda a verificar cuales son los ataques más comunes que se detectaron en las organizaciones mexicanas durante el periodo de esta investigación (Enero a Diciembre 2023).
2. **Tendencias Temporales**: Se identificaron patrones estacionales en la prevalencia y volumen de amenazas, con ciertos tipos de amenazas mostrando picos en meses específicos. Además, se puede notar que tácticas como Acceso Inicial, Comando y Control y Ejecución son predominantes en Prevalencia a diferencia de el volumen considerable de Reconocimiento detectado en el mismo periodo. Esto puede indicar que se realizan técnicas de reconocimiento a organizaciones especificas durante el último trimestre del año.
3. **Correlaciones Significativas**: Se detectaron correlaciones significativas entre ciertos tipos de amenazas y variables contextuales, como protocolos, tipos de vectores de ataque, etc. Por ejemlpo, la figura 68 nos revela la relación entre volumen y prevalencia con los motores de inspección y las tácticas de MITRE ATT&CK detectadas en este estudio. Es decir, aunque los datos revelan que las técnicas de reconocimiento tienen una mayor cantidad de volumen esto no necesariamente significa que todas las organizaciones mexicanas están siendo afectadas por esta técnica ya que la prevalencia no es tan alta. Por otro lado, los datos revelan que las técnicas de acceso inicial son las que tienen mayor prevalencia en el periodo del estudio. Es decir, las organizaciones mexicanas están experimentando técnicas de acceso inicial en su mayoría. Además, podemos ver que las técnicas de comando y control se encuentran con una prevalencia media y una cantidad de volumen moderada lo que nos dice que existen muchos dispositivos infectados por campañas de botnet en las organizaciones mexicanas de donde se obtuvieron los datos.
4. **Ruido y Outliers**: Se identificaron y gestionaron adecuadamente los valores que generan ruido, asegurando la integridad del análisis posterior. Por ejemplo, las Tácticas de reconocimiento generan mucho Volumen, dada la naturaleza de su actividad, al igual que los ataques de Denegación de Servicio. Al ser actividades volumétricas se puede considerar como ruido en este estudio, por lo que se evaluara en trabajos futuros el remover estos datos para realizar un análisis posterior.

En resumen, el Análisis Exploratorio de Datos proporcionó una comprensión profunda de la estructura y características del conjunto de datos, sentando una base sólida para el análisis y la modelización subsecuente. Utilizando Power BI Desktop, se logró una exploración interactiva y visual efectiva, permitiendo identificar patrones y tendencias relevantes que informaron las siguientes etapas del proyecto.

5 Resultados

En esta sección se presentan los resultados obtenidos durante la experimentación y análisis de los datos utilizando Power BI Desktop. Cada apartado está organizado de acuerdo con las fases del Cyber Kill Chain, proporcionando un análisis detallado de cada etapa del ciclo de vida de un ataque cibernético.

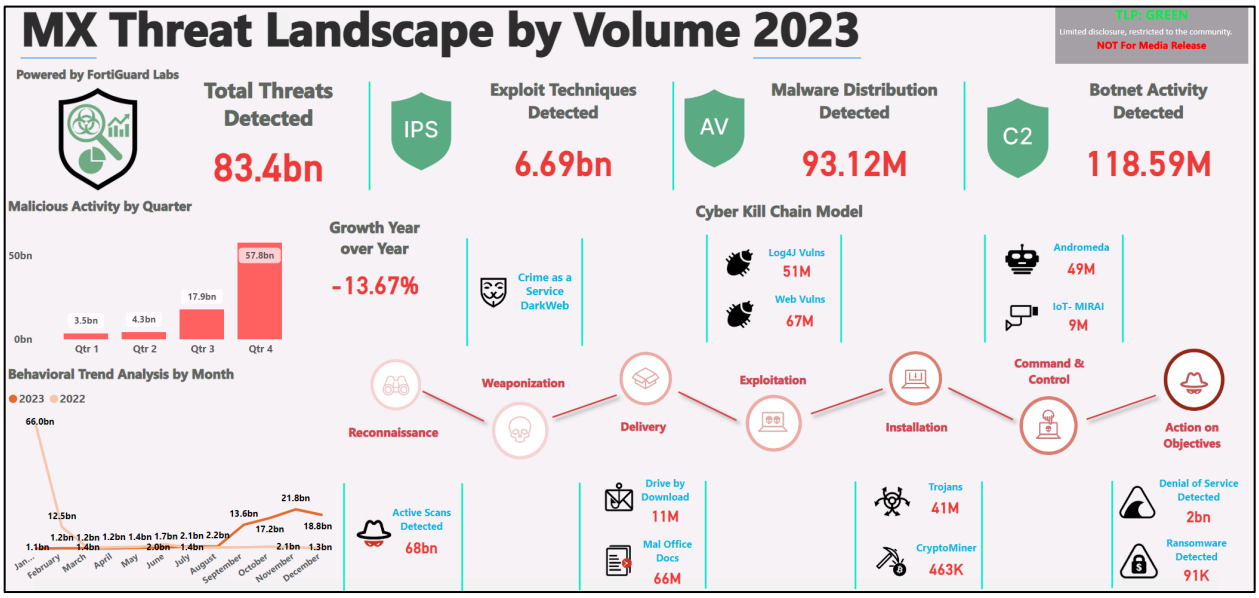


Figura 71. Panoramad de Amenazas Mexico 2023 por Volumen.

En la figura 71 tenemos un resultado de aproximadamente 83000 millones de actividades maliciosas detectadas de las cuales pudimos modelar a nivel trimestral y vimos un aumento considerable en el último trimestre del año del 2023 esto se realizó una comparación con el año anterior del estudio realizado en el cual podemos validar que existe una disminución del 13% en cuestión del año en el que analizamos que es 2023 esta información ha sido modelada en diferentes tipos de frameworks de ciberataques en el cual podemos visualizar el modelo de cyber kitchen el cual consta de 7 fases de un ataque donde podemos visualizar que la mayoría de la actividad maliciosa es detectada en la fase de reconocimiento con más de 68000 millones de eventos detectados en este periodo adicional tenemos diferentes tipos de eventos en la fase de entrega a través de descargas o inclusive a través de archivos de office maliciosos Por otro lado podemos ver que en la fase de explotación las características a resaltar son vulnerabilidades en sistemas operativos e inclusive en servicios web expuestos asimismo en la fase de instalación podemos ver diferentes tipos de malware como troyanos entre otros en las fases finales de la cadena del ataque podemos visualizar campañas de botnet como andrómeda enfocada a dispositivos Windows o mirai que está enfocada a dispositivos de iot tales como cámaras televisores entre otros dispositivos. Para finalizar podemos detectar que los objetivos se pueden dividir en ataques de denegación de servicio y en ataques de ransomware los cuales están muy ligados a la actividad de cibercrimen detectado en México.

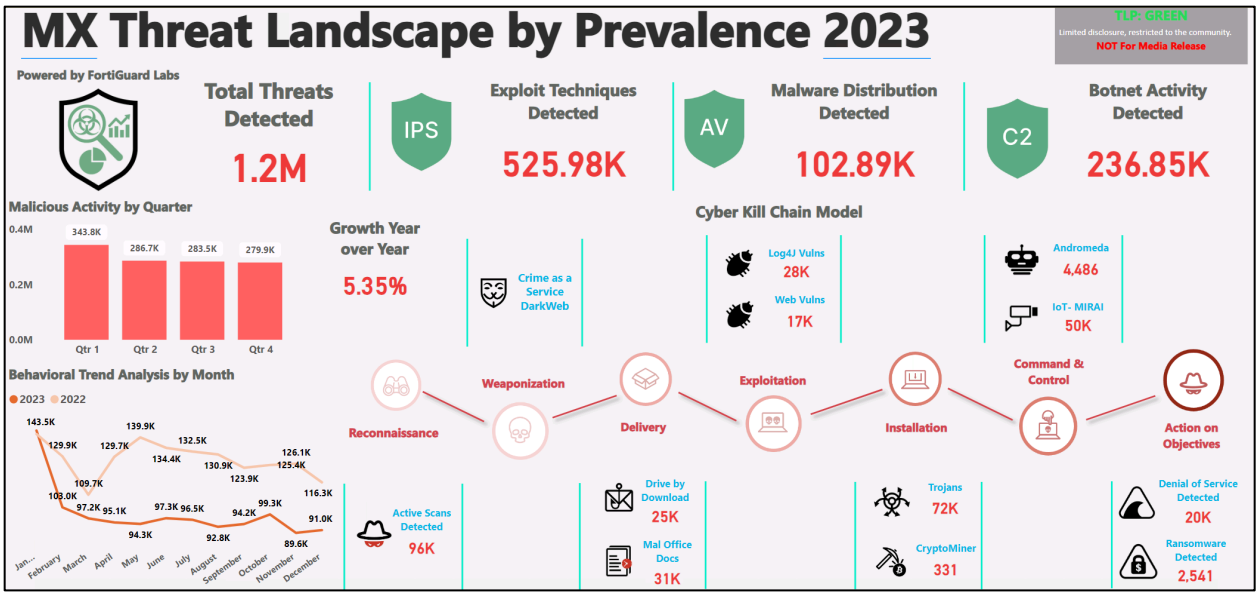


Figura 72. Panorama de Amenazas Mexico 2023 por Prevalencia.

Por otro lado la figura 72 nos muestra la prevalencia de eventos maliciosos detectados en México en el 2023 ddóndepodemos ver un total de un aproximado de 1.2 millones de eventos mmaliciosoregistrados en el ccuálvemos una tendencia en la serie temporal normalizada entre 300 y 200 60 eventos maliciosos por trimestre.

5.1 Panorama de Amenazas usando CTI

En las siguientes secciones se pre presenta el analisis de los datos recolectados modelados en los frameworks de CTI seleccionados para este estudio (MITRE ATT&CK y Cyber Kill Chain).

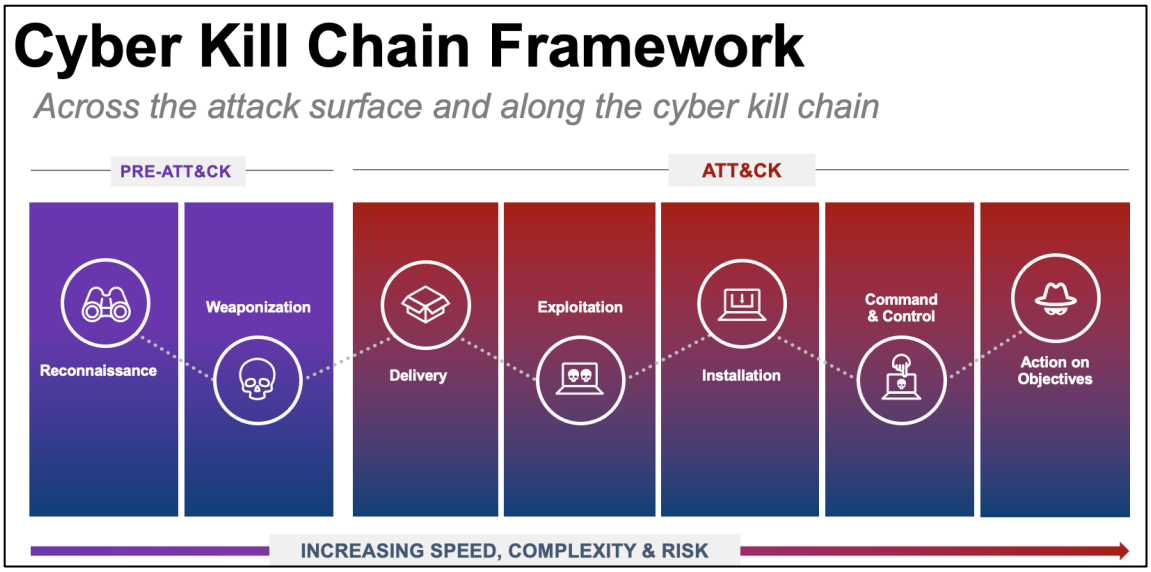


Figura 73. Cyber Kill Chain Framework

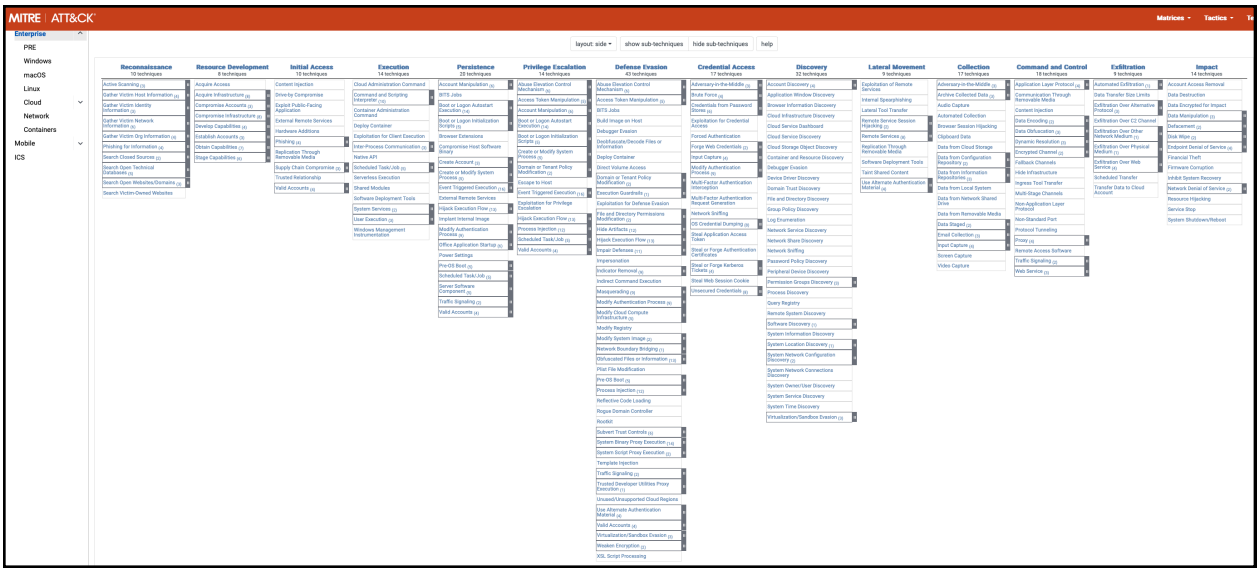


Figura 74. MITRE ATT&CK Framework V15.

5.1.1 Reconocimiento

En la fase de reconocimiento, los atacantes recopilan información sobre sus objetivos. Los datos analizados en esta etapa incluyeron patrones de escaneo de redes y actividades de recopilación de inteligencia.

5.1.1.1 Tácticas y Técnicas de MITRE ATT&CK detectadas en la fase de Reconocimiento

El reconocimiento [159] consiste en técnicas que implican que los adversarios recopilen información de manera activa o pasiva que pueda utilizarse para apoyar la selección de objetivos. Dicha información puede incluir detalles sobre la organización víctima, su infraestructura o su personal. Esta información puede ser aprovechada por el adversario para ayudar en otras fases del ciclo de vida del adversario, como el uso de la información recopilada para planificar y ejecutar el acceso inicial, para definir y priorizar los objetivos posteriores a la intrusión, o para impulsar y guiar otros esfuerzos de reconocimiento.

A continuación se listan las Técnicas y Tácticas de MITRE ATT&CK relacionadas con Reconocimiento detectadas en el experimento:

- **T1595.001 - Active Scanning: Scanning IP Blocks** [160]
- **T1595.002 - Active Scanning: Vulnerability Scanning** [161]
- **T1590.002 – Gather Victim Network Information: DNS** [162]

Estas técnicas reflejan los métodos utilizados por los adversarios para recopilar información clave sobre la infraestructura y el personal de la organización objetivo, lo que les permite planificar y ejecutar ataques más precisos y efectivos.

5.1.1.2 Hallazgos Clave:

Aunque existen diferencias entre la prevalencia y el volumen de eventos detectados en México en el 2023 específicamente en la fase de reconocimiento pudimos de detectar ciertas similitudes gracias al método propuesto. Por ejemplo que existen herramientas utilizadas para poder estar haciendo reconocimiento constante de todo lo que está expuesto en el territorio mexicano tales como emma sentis mascan cuáles openvas dir buster, nessus entre otras. Además, pudimos detectar cuáles son los protocolos que más están escaneando en el ciberespacio mexicano tales como protocolos sip de DNS, PHP, SIP, SMB entre otros.

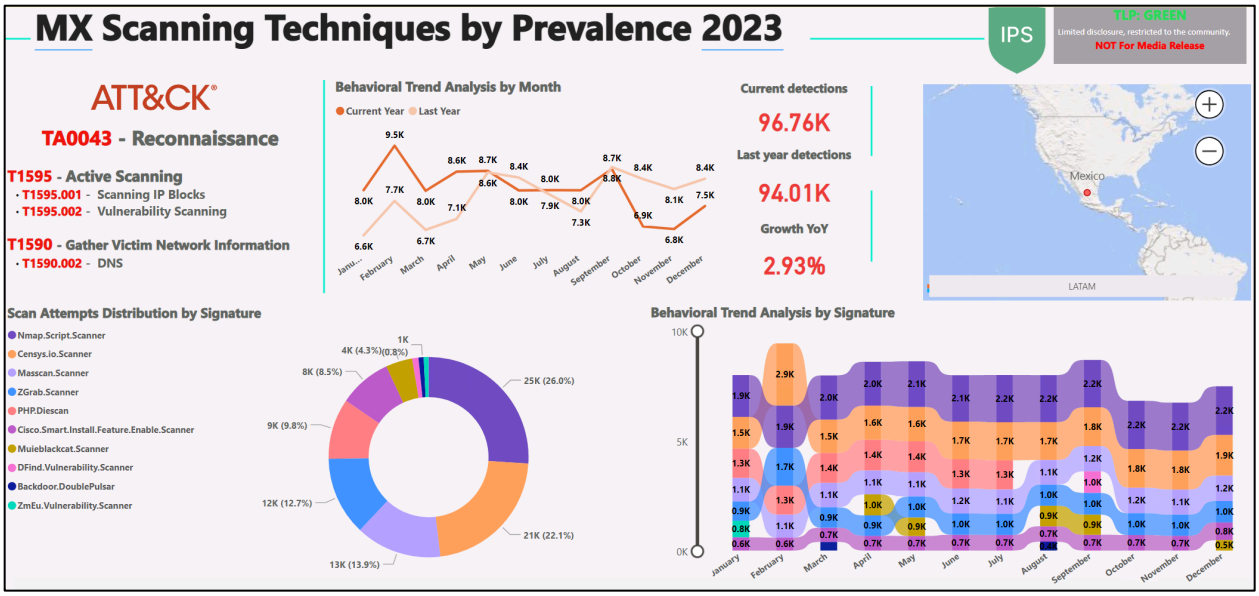


Figura 75. Reconocimiento y Tecnicas de escaneo detectadas en Mexico 2023 por Prevalencia

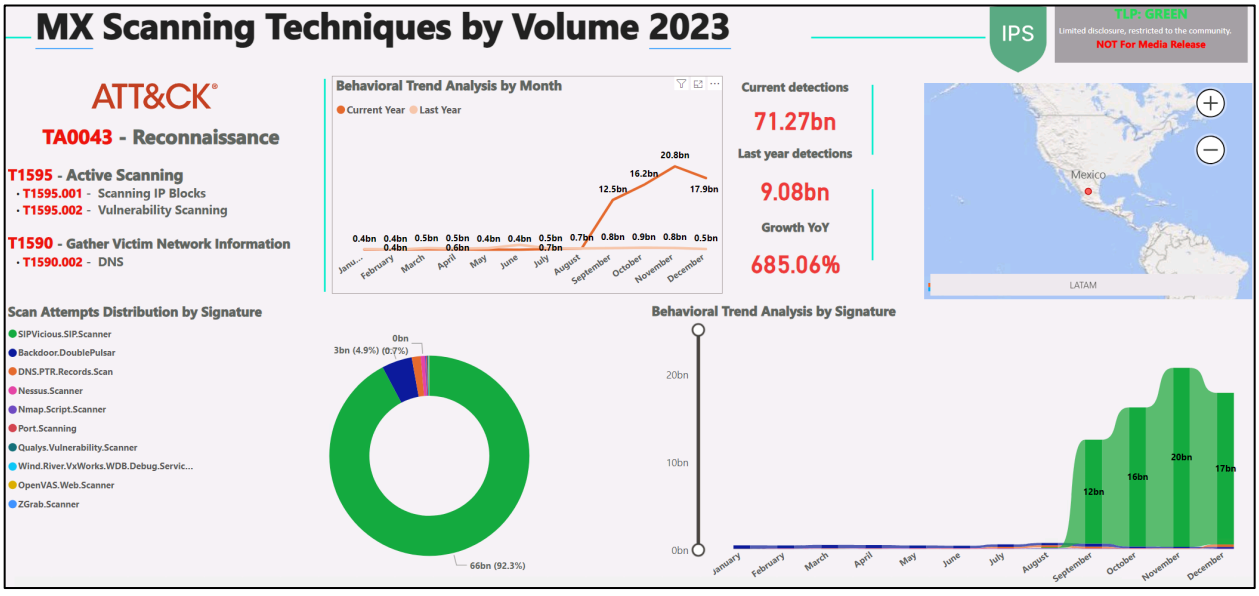


Figura 76. Reconocimiento y Tecnicas de escaneo detectadas en Mexico 2023 por Volumen

Para poder comprender mejor esta relación decidimos generar una gráfica de dispersión (Figura 77) para poder correlacionar la información entre los datos de volumen y prevalencia mostrados en la figura x. Esto nos quiere decir que algunas organizaciones mexicanas están siendo escaneadas constantemente para buscar vulnerabilidades en sistemas Windows en el protocolo SMB dada la firma Backdoor Double Pulsar Para obtener un acceso inicial. Por otro lado herramientas como en Nmap, Censys y mascan son las que mayormente están escaneando el ciberespacio mexicano.

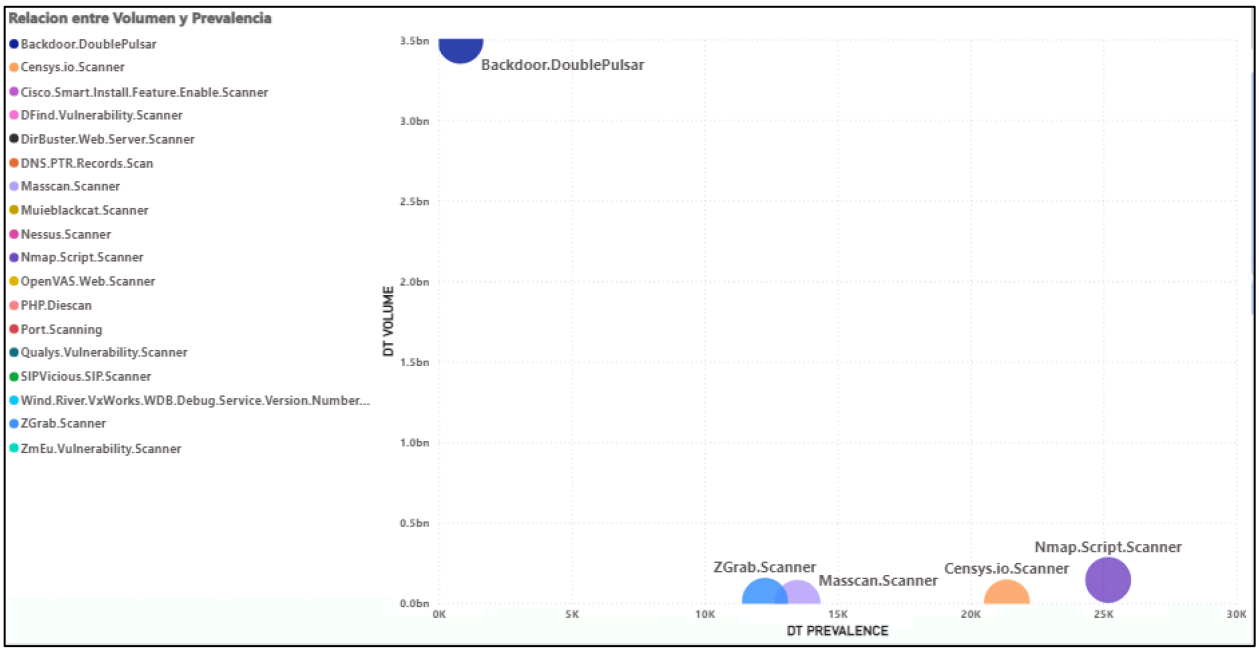


Figura 77. Relacion entre Tecnicas de escaneo detectadas en Mexico 2023 por Volumen y Prevalencia

5.1.2 Explotación

En la fase de explotación, los atacantes aprovechan las vulnerabilidades del sistema para ejecutar su código malicioso. Los datos analizados incluyeron intentos de explotación de vulnerabilidades conocidas.

5.1.2.1 Tácticas y Técnicas de MITRE ATT&CK detectadas en la fase de Explotación y Acceso Inicial

El Acceso Inicial [163]consiste en técnicas que utilizan diversos vectores de entrada para obtener su primer punto de apoyo dentro de una red. Las técnicas empleadas para obtener este punto de apoyo incluyen el spearphishing dirigido y la explotación de vulnerabilidades en servidores web expuestos al público. Los puntos de apoyo obtenidos a través del acceso inicial pueden permitir un acceso continuo, como cuentas válidas y el uso de servicios remotos externos, o pueden ser de uso limitado debido al cambio de contraseñas.

A continuación se listan las Técnicas y Tácticas de MITRE ATT&CK relacionadas con Explotación y Acceso Inicial detectadas en el experimento:

- **T1190 - Exploit Public-Facing Application** [164]

- **T1133 - External Remote Services** [165]
- **T1195.002 - Supply Chain Compromise: Compromise Software Supply Chain** [166]

Estas técnicas muestran cómo los atacantes explotan vulnerabilidades en aplicaciones y servicios para obtener acceso no autorizado y ejecutar código malicioso en sistemas comprometidos, así como los métodos utilizados para el acceso inicial a los sistemas objetivo.

5.1.2.2 Hallazgos Clave:

Se observó un aumento en los intentos de explotación de vulnerabilidades conocidas en sistemas operativos y aplicaciones populares. Los exploits más comunes incluían aquellos dirigidos a vulnerabilidades de día cero y fallos de seguridad no parcheados.

En la Figura 79 podemos apreciar que durante el período estudiado en México 2023 tenemos una cantidad de volumen de 3000 millones de eventos maliciosos detectados lo cual representa una disminución del 46% comparado con el año anterior y en la figuera 78 podemos observar la prevalencia recolccetada con un aproximado de 525000 eventos durante el 2023 en el territorio mexicano, lo cual representa un crecimiento de casi el 7% en comparación al año anterior.

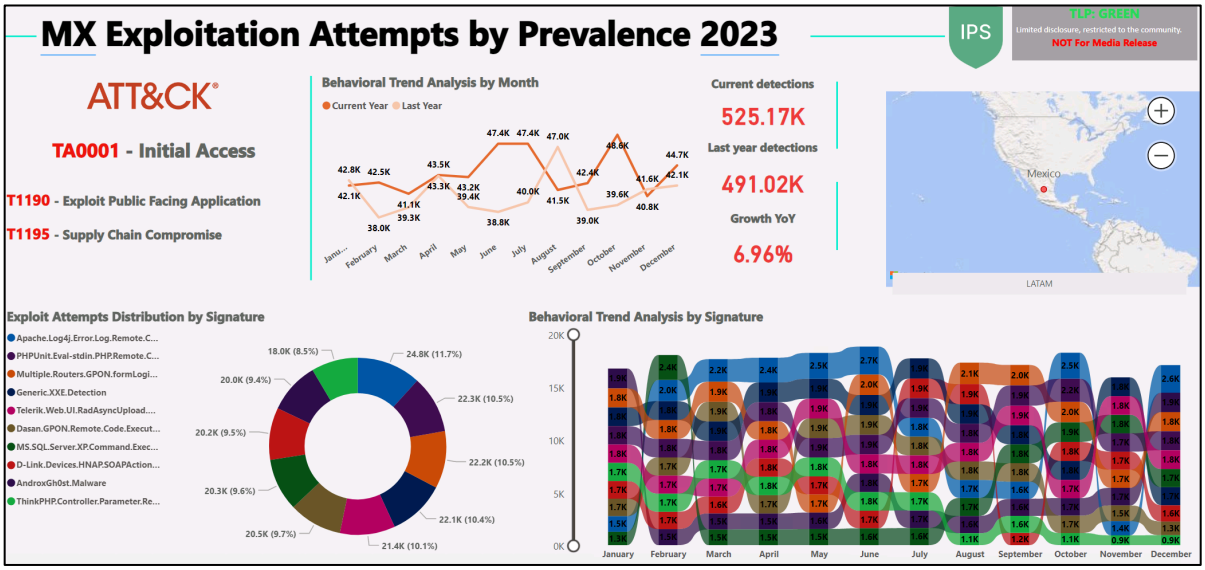


Figura 78. Tecnicas de Explotacion detectadas en Mexico 2023 por Prevalnce.

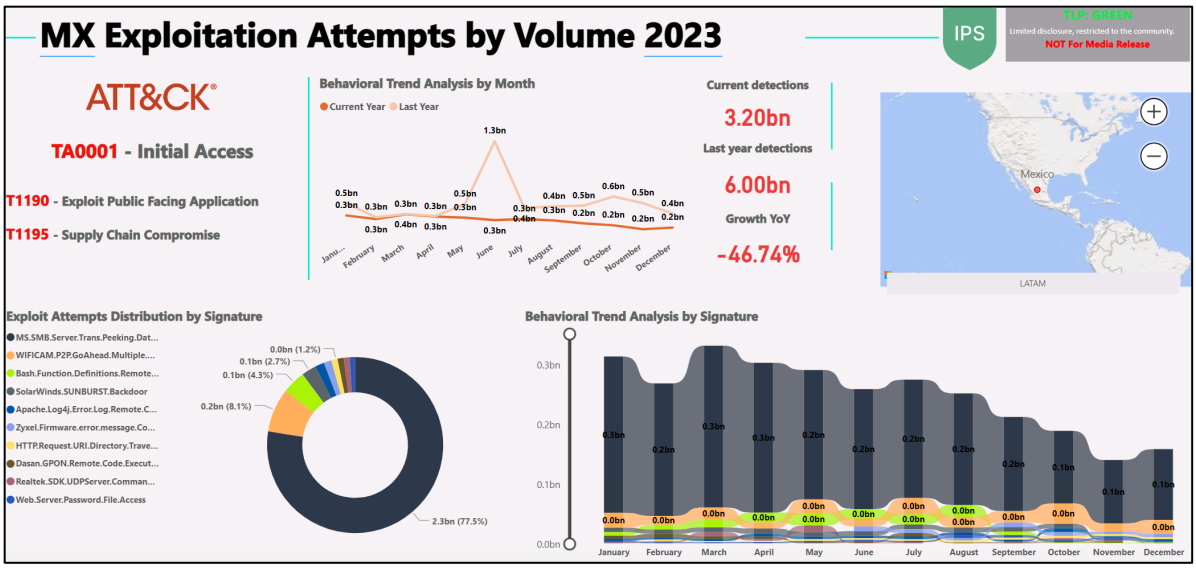


Figura 79. Tecnicas de Explotacion detectadas en Mexico 2023 por Volumen.

Para poder comprender de mejor manera la relación entre los datos de técnicas de explotación por volumen y prevalencia usaremos una gráfica de dispersión (figura 80). En esta gráfica podemos observar Que la ejecución de código remoto para el lenguaje “bash” es la que mayor volumen presenta en el período de los datos recolectados para este estudio sin embargo no necesariamente es la técnica de explotación más vista en todaslas organizaciones mexicanas ya que no presenta una prevalencia alta. Una de las técnicas de explotación con mayor volumen y prevalencia en el territorio mexicano en el 2023 es la de Apache Log4J, así como otras enfocadas a servidores de SQL Microsoft, servidores de PHP, asi como dispositivos GPON y camaras para ejecutar código de manera remota.

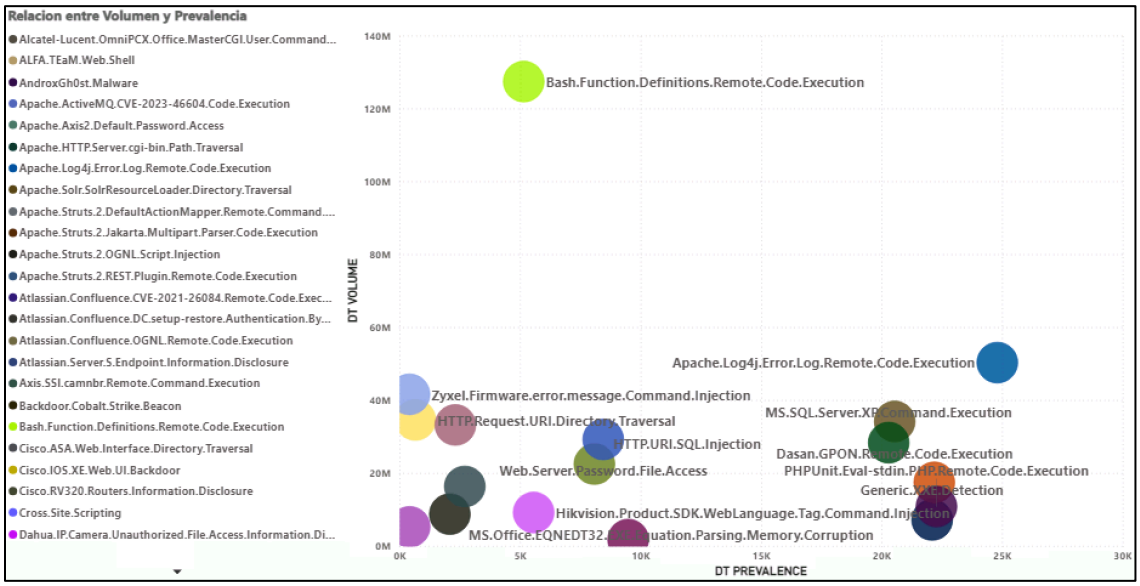


Figura 80. Relacion entre Tecnicas de Explotacion detectadas en Mexico 2023 por Volumen y Prevalencia

Con la información recolectada anteriormente podemos relacionar el volumen y la prevalencia de técnicas de explotación por sistemas operativos como se muestra en la figura 81. Esto nos revela

que los sistemas operativos Windows tienen una mayor cantidad de intentos de explotación de vulnerabilidades específicas. Sin embargo, podemos ver que los sistemas operativos linux están siendo blanco de los ciber atacantes de manera masiva ya que presentan una mayor prevalencia. Por otro lado, podemos observar que existen técnicas de explotación generales que pueden aplicar para más de un sistema operativo esto representa una gran cantidad de prevalencia y un volumen relativamente normal considerando los datos recolectados para este estudio. Por lo tanto, es importante considerar en la estrategia de ciberdefensa una correcta gestión de vulnerabilidades para evitar que en los sistemas de las organizaciones mexicanas se vean afectados y el atacante pueda acceder de manera no autorizada a los sistemas y por ende a la información de las organizaciones mexicanas.

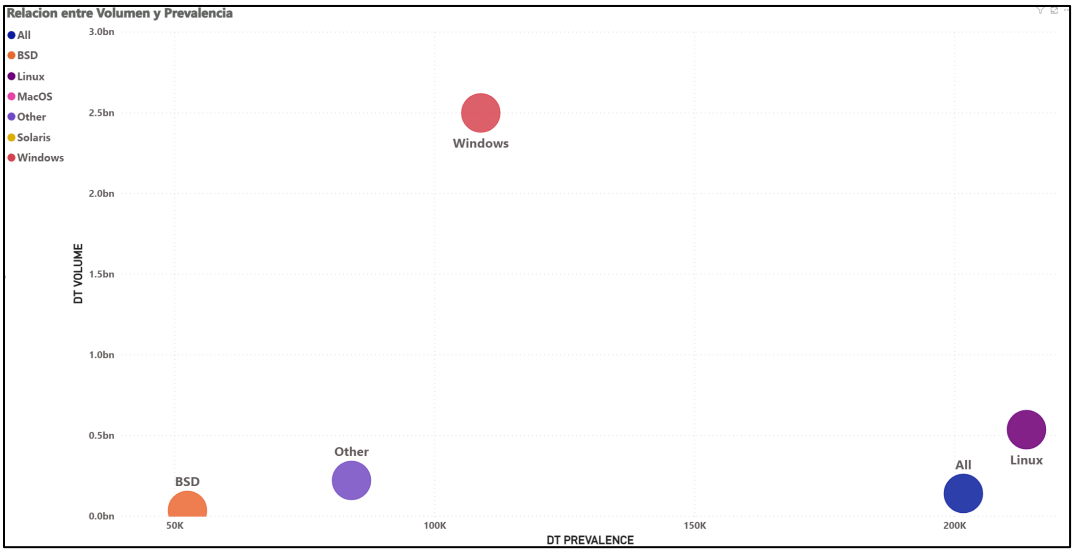


Figura 81. Relacion entre Sistemas Operativos afectados en Mexico 2023 por Volumen y Prevalencia

5.1.3 Instalación, Entrega y Ejecución de Malware

En esta fase, los atacantes instalan puertas traseras u otras herramientas maliciosas en los sistemas comprometidos. Los datos analizados incluyeron la detección de puertas traseras y troyanos. Se identificaron distintas variantes de puertas traseras que los atacantes buscan desplegar en los sistemas comprometidos. Estas puertas traseras permiten a los atacantes obtener acceso remoto y persistente a los sistemas. Además, se detectaron múltiples troyanos que están diseñados para robar información sensible y enviar los datos a servidores controlados por los atacantes.

Por otro lado, la fase de entrega implica el envío de las herramientas maliciosas a las víctimas. Los métodos comunes incluyen correos electrónicos de phishing, sitios web comprometidos y dispositivos USB infectados.

5.1.3.1 Técnicas y Tácticas de MITRE ATT&CK relacionadas con Entrega, Instalación Ejecución de Malware

La ejecución [167] consta de técnicas que dan como resultado la ejecución de código controlado por el adversario en un sistema local o remoto. Las técnicas que ejecutan código malicioso a menudo se combinan con técnicas de todas las demás tácticas para lograr objetivos más amplios,

como explorar una red o robar datos. Por ejemplo, un adversario podría utilizar una herramienta de acceso remoto para ejecutar un script de PowerShell que realice el descubrimiento remoto del sistema. A continuación se listan las Técnicas y Tácticas de MITRE ATT&CK relacionadas con Entrega e Instalacion de malware detectadas en el experimento:

- **T1566.001 - Phishing: Spearphishing Attachment** [168]
- **T1566.002 - Phishing: Spearphishing Link** [169]
- **T1203 - Exploitation for Client Execution** [170]

5.1.3.2 Hallazgos Clave:

El volumen de la distribución de malware en el territorio mexicano fue de 93000000 de eventos registrados 49% de disminución de eventos a comparación del año anterior y la prevalencia fue de 102000 detecciones durante el periodo del 2023 con una disminución del 13.82% a comparación del año anterior. Como podemos observar la distribución de malware en su mayoría es a través de archivos y/o documentos de Microsoft office maliciosos.

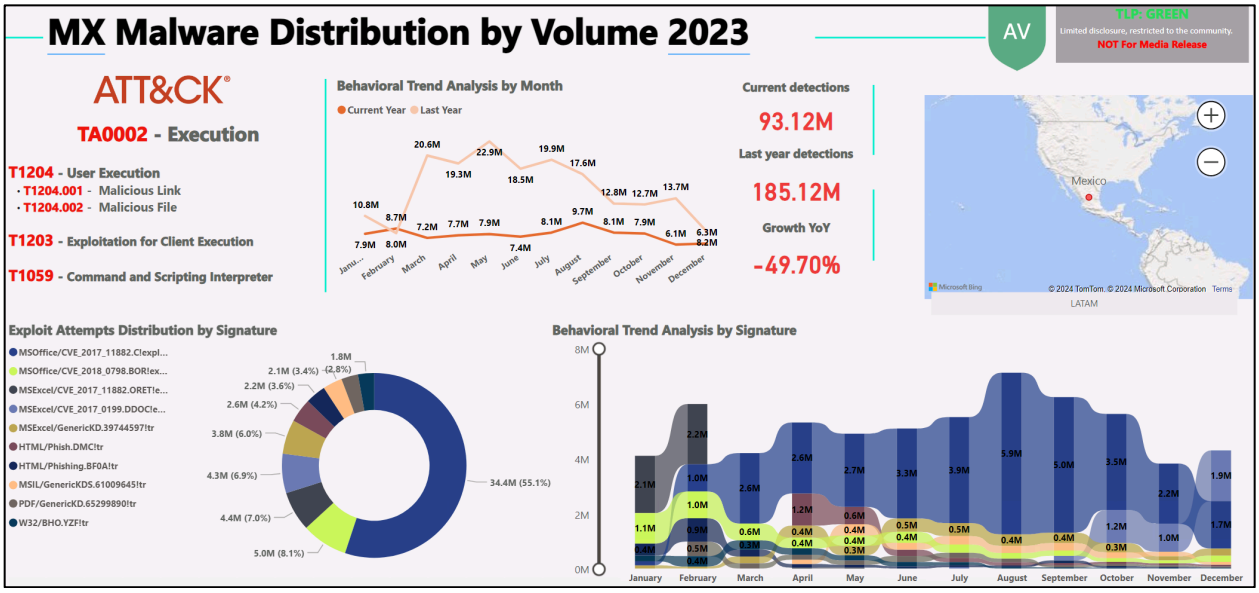


Figura 82. Tecnicas de Distribucion de Malware detectadas en Mexico 2023 por Volumen.

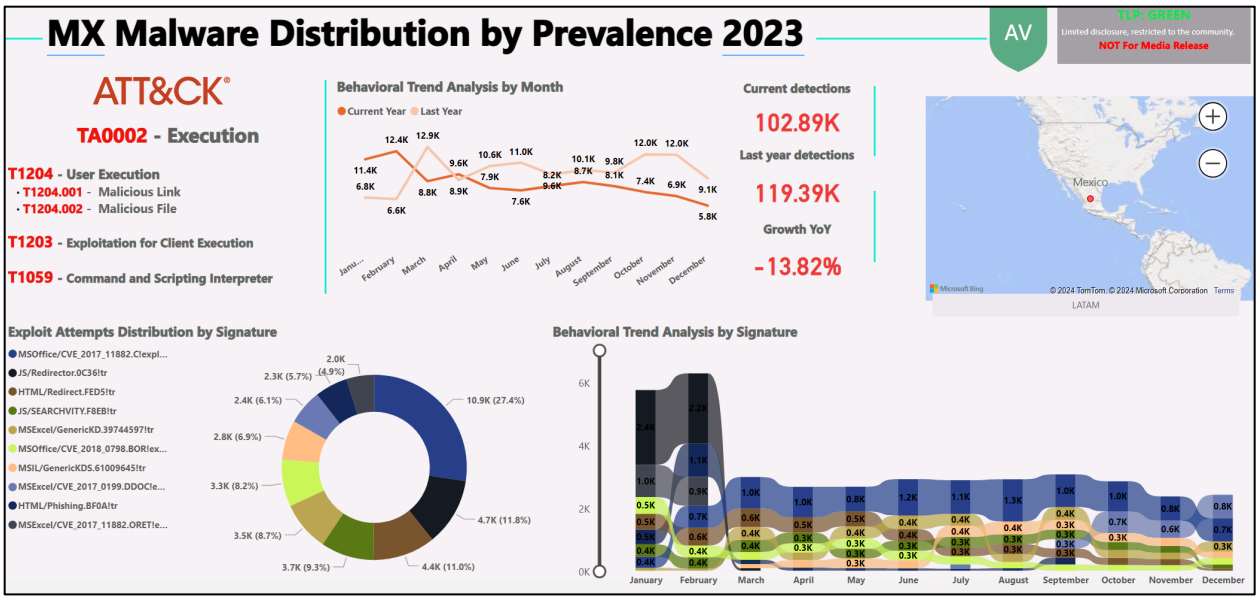


Figura 83. Tecnicas de Distribucion de Malware detectadas en Mexico 2023 por Prevalencia.

En la figura 84 podemos correlacionar que la mayor distribución de malware es a través de una vulnerabilidad del 2017 enfocada archivos de Microsoft office. Así mismo, se detectó que la mayoría de estos archivos maliciosos suelen ser de la plataforma de Microsoft Excel, donde los atacantes buscan explotar vulnerabilidades viejas entre 2017 y 2018. Por lo tanto, es importante tener en cuenta la explotacion mediante software de terceros. Por otro lado, existe distribución de malware a través de redirecciones o protocolos como html y javascript.

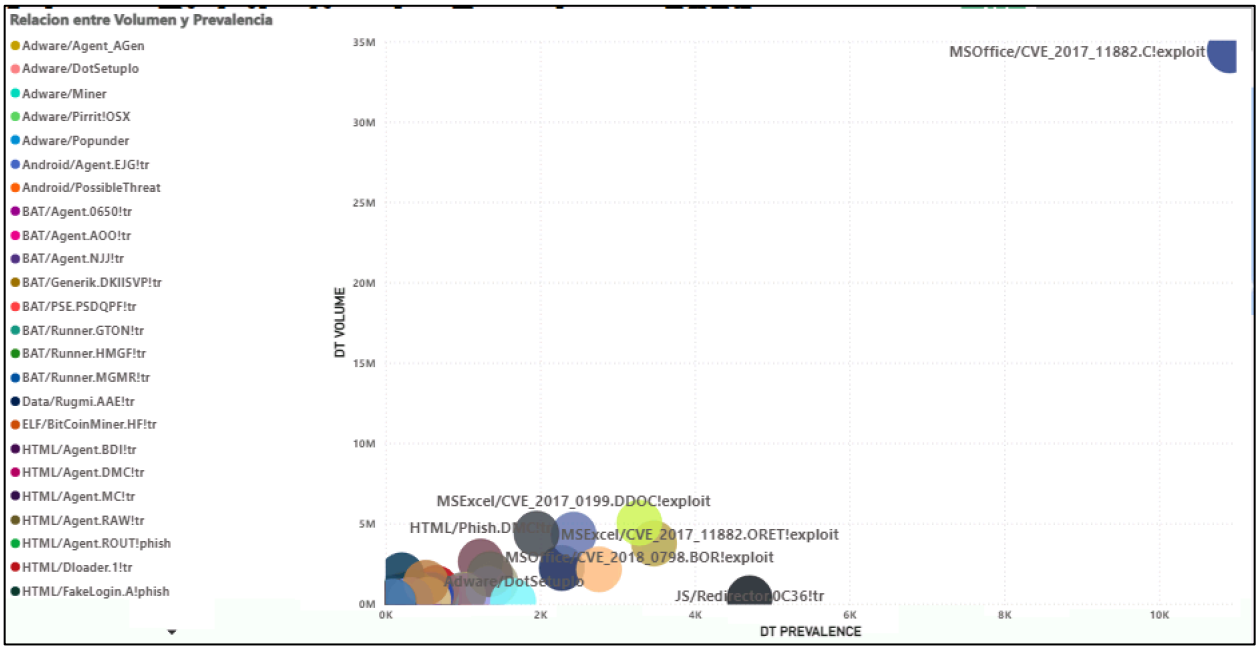


Figura 84. Relacion entre Variantes de Malware en Mexico 2023 por Volumen y Prevalencia

5.1.4 Comando y Control (C2)

En la fase de comando y control, los atacantes establecen canales de comunicación con los sistemas comprometidos para controlarlos de forma remota. Los datos analizados incluyeron el tráfico de red asociado con servidores C2. Se identificaron varios servidores C2 que estaban siendo utilizados para controlar sistemas comprometidos. Estos servidores fueron bloqueados y se implementaron reglas de firewall para prevenir la comunicación con ellos. El análisis del tráfico de red reveló patrones anómalos que indicaban la presencia de comunicación C2. Estos patrones fueron monitoreados continuamente para detectar y responder rápidamente a cualquier actividad maliciosa.

5.1.4.1 Técnicas y Tácticas de MITRE ATT&CK relacionadas con Comando y Control (C2)

Comando y control [168] consiste en técnicas que los adversarios pueden utilizar para comunicarse con los sistemas bajo su control dentro de una red víctima. Los adversarios suelen intentar imitar el tráfico normal y esperado para evitar ser detectados. Hay muchas formas en que un adversario puede establecer comando y control con varios niveles de sigilo dependiendo de la estructura de red y las defensas de la víctima.

- **T1583.005 - Acquire Infrastructure: Botnet** [172]
- **T1585.005 - Compromise Infrastructure: Botnet** [173]
- **T1071.001 - Application Layer Protocol: Web Protocols** [174]
- **T1041 - Exfiltration Over C2 Channel** [175]

Estas técnicas destacan cómo los atacantes establecen y mantienen canales de comunicación con los sistemas comprometidos, permitiéndoles coordinar y controlar sus operaciones de forma remota.

5.1.4.2 Hallazgos Clave

En la figura 86 podemos validar la relación de las campañas de botnet en el territorio mexicano entre volumen y prevalencia en donde las campañas que registran mayor actividad es una campaña enfocada a dispositivos de internet de las cosas IoT por sus siglas en inglés denominada botnet mirai, seguida de la campaña denominada blada bindi así como ghost rat botnet. Por otro lado la campaña con mayor actividad en volumen en el territorio mexicano es la campaña denominada andrómeda la cual curiosamente ya había sido interrumpida en el 2017 por diferentes agencias de la ley.

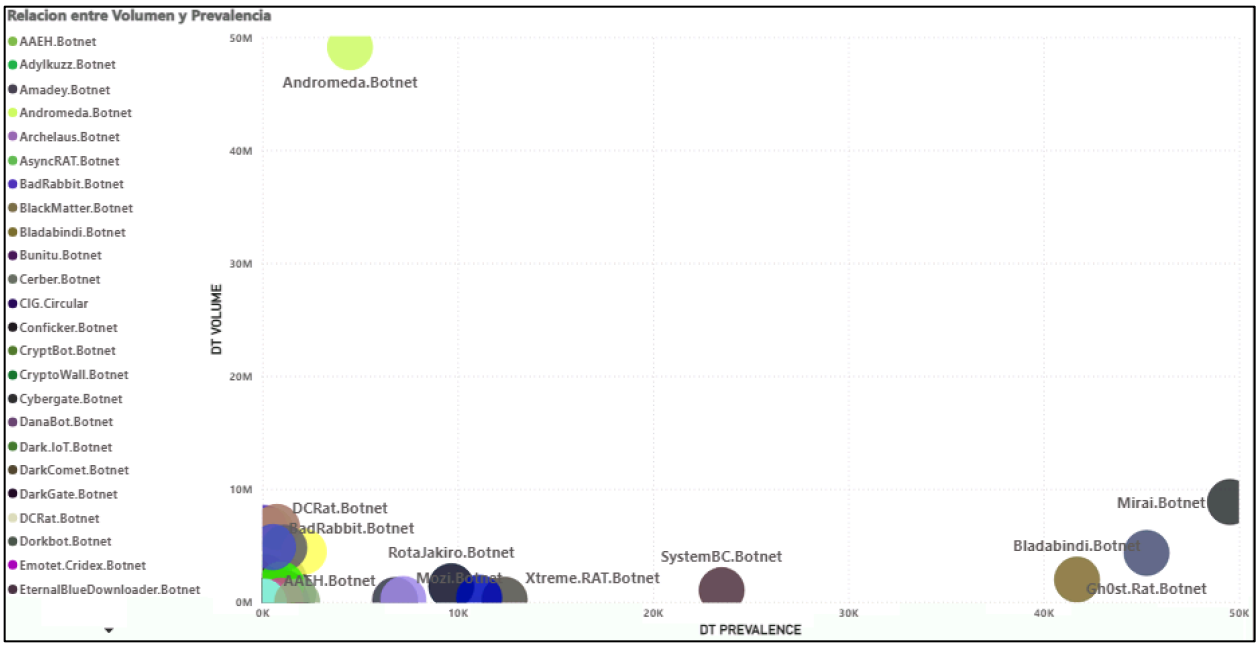


Figura 86. Relacion Campañas de Botnet C2 en Mexico 2023 por Volumen y Prevalencia

Esto nos quiere decir que aunque la campaña de botnet haya sido cesada y sus operaciones hayan sido interrumpidas en el territorio mexicano existen muchos dispositivos que aún siguen infectados con este tipo de botnet y siguen tratando de comunicarse a los servidores de comando y control previamente destruidos. Esto genera un riesgo potencial ya que un atacante podría comprar estos dominios o estos servidores de comando y control y obtener el acceso y control de los dispositivos previamente infectados que se encuentran en las organizaciones mexicanas es decir se puede obtener un acceso inicial por estas campañas de botnet que aunque ya fueron derrocadas los dominios podrían estar siendo disponibles o podrían ser redirigidos y algún atacante pudiera tomar control o obtener acceso a las organizaciones mexicanas que cuente con estos dispositivos infectados.

5.1.5 Acciones en el Objetivo

En esta última fase, los atacantes llevan a cabo sus objetivos finales, como el robo de datos, la destrucción de sistemas o la interrupción de servicios. Los datos analizados incluyeron incidentes de robo de información y ataques de denegación de servicio. Se detectaron varios incidentes de exfiltración de datos, donde los atacantes intentaron robar información confidencial por medio de variantes de Ransomware.

5.1.5.1 Técnicas y Tácticas de MITRE ATT&CK Relacionadas con Impacto (Ransomware):

1. **Cifrado de Datos (T1486)**
    - Los adversarios cifran archivos y datos importantes en los sistemas de la víctima para luego exigir un rescate a cambio de la clave de descifrado. Esta es la técnica central del ransomware y afecta gravemente la disponibilidad de la información.
2. **Destrucción de Datos (T1485)**

- En algunos casos, además de cifrar los datos, los adversarios pueden destruir copias de seguridad y otros datos importantes para asegurarse de que la víctima no pueda recuperar la información sin pagar el rescate.

3. **Manipulación de Datos (T1565)**
   - Los adversarios pueden manipular o alterar datos en un sistema para comprometer la integridad de la información y causar efectos adversos en los procesos de negocio, aumentando la presión sobre la víctima para que pague el rescate.
4. **Interrupción de Servicios (T1499)**
   - Los ataques de ransomware a menudo interrumpen servicios críticos al cifrar datos esenciales para la operación de la organización, afectando la disponibilidad de recursos críticos y paralizando las operaciones.
5. **Deshabilitación de Infraestructura Crítica (T1529)**
   - Los adversarios pueden deshabilitar componentes críticos de la infraestructura, como servidores de respaldo o servicios de recuperación, para maximizar el impacto del ataque de ransomware y dificultar la recuperación sin pagar el rescate.

Estas técnicas de impacto son empleadas por los adversarios para asegurar que sus ataques de ransomware tengan un efecto devastador en la organización, forzando a las víctimas a considerar el pago del rescate para restaurar sus operaciones y acceder a sus datos críticos.

5.1.5.2 Hallazgos Clave

En la figura 84, podemos observar que las variantes de Ransomware en México tienen una distribución muy similar, ya que este tipo de amenazas no son tan comunes y van mutando con el tiempo. Aun así, podemos observar una variante denominada Nemucode con mayor volumen en las organizaciones mexicanas. Sin embargo, la variante Filecoder, la cual se considera una variante de Ransomware genérico, es decir, que no pertenece a una banda de cibercriminales en especifica es la que mayores detecciones obtuvo por Prevalencia en el set de datos utilizado en este estudio.

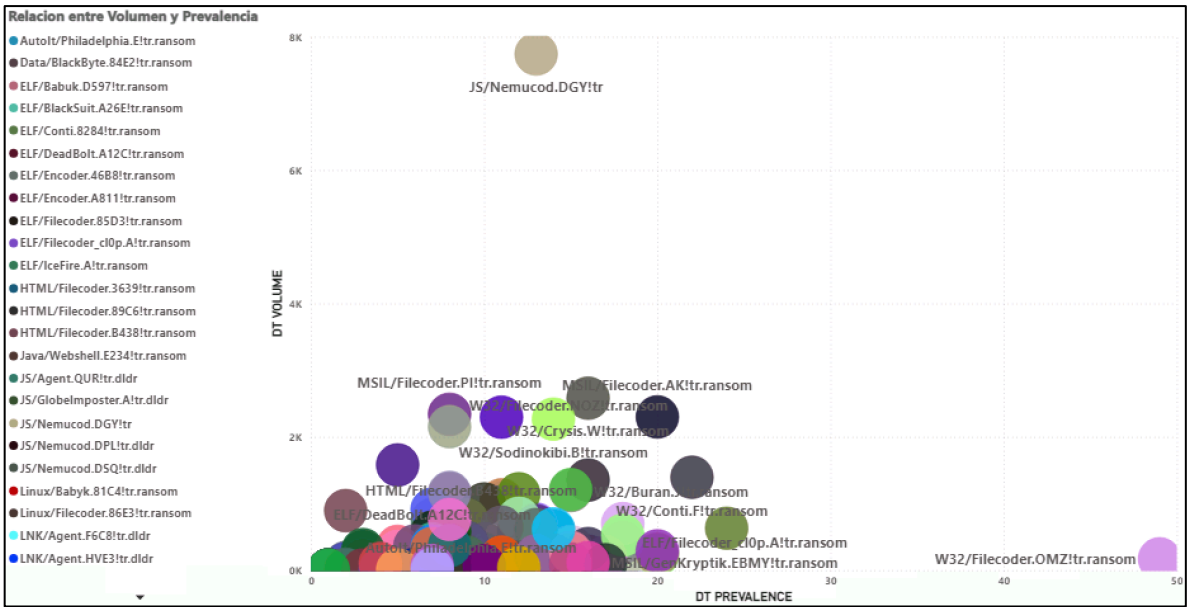


Figura 84. Relacion Varianres de Ransomware en Mexico 2023 por Volumen y Prevalencia

Es importante mencionar que se incluyó una descripción de las variantes de Ransomware detectadas en este estudio en el Anexo de este documento.

5.2 Matriz de MITRE ATT&CK basada en los resultados

Gracias a la investigación y método propuesto podemos generar una matriz de Tácticas y Técnicas utilizando el framework de CTI MITRE TTA&CK como se muestra en la figura 85. Dicha matriz nos permitirá abordar de una manera más profunda los eventos recolectados darles contexto y generar recomendaciones.

about

2023 Mexico Threat Landcaspe

Panorama de Amenazas
de Mexico en 2023 basado en l recolección
de eventos de NGFW (IPs, AV, C2)

domain

Enterprise ATT&CK v15

platforms

Windows, Linux, macOS,
Network, PRE, Containers, Office 365,
SaaS, Google Workspace, IaaS, Azure AD

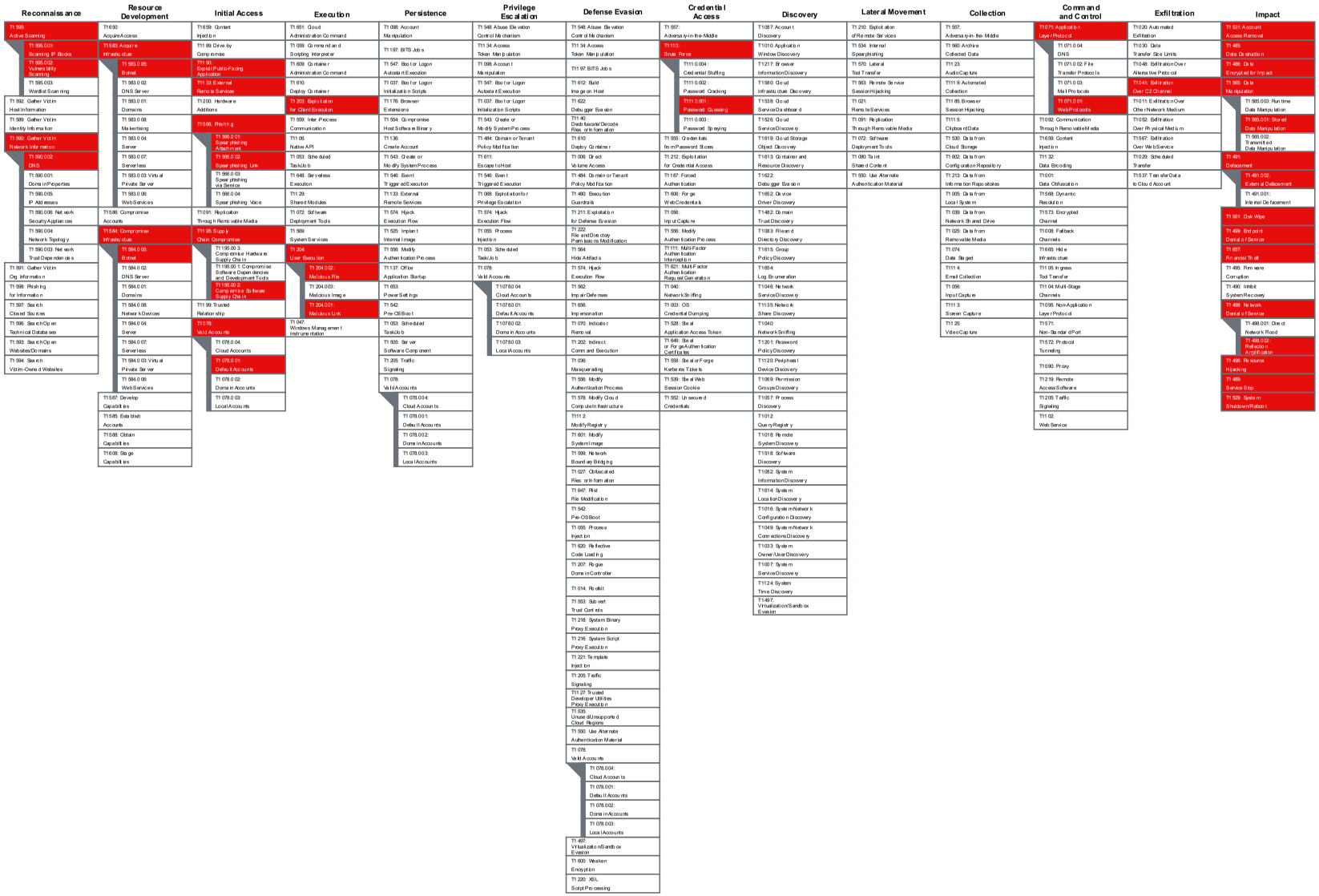


Figura 85. Matriz de MITRE AT&CK V15 Mexico 2023.

Tacticas y Tecnicas de MITRE ATT&CK V15	Descripcion
TA0043: Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
T1595: Active Scanning	Adversarios realizan escaneos activos para identificar información sobre los sistemas de la víctima, como servicios abiertos y configuraciones.
T1595.001: Scanning IP Blocks	El escaneo de bloques de IP consiste en identificar rangos de direcciones IP para encontrar sistemas activos dentro de un rango específico.
T1595.002: Vulnerability Scanning	Escaneo para detectar vulnerabilidades específicas en los sistemas de la víctima que podrían ser explotadas.
T1590: Gather Victim Network Information	Recopilación de información sobre la red de la víctima, incluyendo la topología, servicios y configuraciones.
T1590.002: DNS	Uso del DNS para recolectar información sobre la infraestructura de red de la víctima.
TA0042: Resource Development	The adversary is trying to establish resources they can use to support operations.
T1583: Acquire Infrastructure	Adquisición de infraestructura necesaria para llevar a cabo ataques, como servidores y dominios.
T1583.005: Botnet	Creación o adquisición de una botnet para utilizar en ataques distribuidos o de gran escala.
T1584: Compromise Infrastructure	Compromiso de infraestructuras existentes para su uso en actividades maliciosas.
T1584.005: Botnet	Utilización de botnets comprometidas para realizar ataques.
TA0001: Initial Access	The adversary is trying to get into your network.
T1190: Exploit Public-Facing Application	Explotación de aplicaciones accesibles públicamente para obtener acceso inicial a la red de la víctima.
T1133: External Remote Services	Abuso de servicios remotos externos para obtener acceso a la red interna de la víctima.
T1566: Phishing	Envío de correos electrónicos fraudulentos para engañar a los usuarios y obtener información sensible o acceso.
T1566.001: Spearphishing Attachment	Envío de correos electrónicos con archivos adjuntos maliciosos dirigidos específicamente a individuos u organizaciones.
T1566.002: Spearphishing Link	Envío de correos electrónicos con enlaces maliciosos diseñados para engañar a los usuarios.
T1195: Supply Chain Compromise	Compromiso de la cadena de suministro para introducir software o hardware malicioso.
T1195.002: Compromise Software Supply Chain	Compromiso de la cadena de suministro de software para insertar código malicioso en aplicaciones legítimas.
T1078: Valid Accounts	Uso de cuentas válidas y legítimas para acceder a la red de la víctima.
T1078.001: Default Accounts	Explotación de cuentas predeterminadas que no han sido deshabilitadas o modificadas.
TA0002: Execution	The adversary is trying to run malicious code.
T1203: Exploitation for Client Execution	Explotación de vulnerabilidades en software cliente para ejecutar código malicioso.
T1204: User Execution	Ejecutar código malicioso convenciendo a los usuarios para que lo hagan.
T1204.002: Malicious File	Uso de archivos maliciosos que los usuarios ejecutan sin darse cuenta.
T1204.001: Malicious Link	Enlaces maliciosos que llevan a los usuarios a ejecutar código malicioso.
TA0006: Credential Access	The adversary is trying to steal account names and passwords.
T1110: Brute Force	Intentos de fuerza bruta para adivinar contraseñas y obtener acceso a cuent
T1110.001: Password Guessing	Adivinanza de contraseñas utilizando técnicas de fuerza bruta.
TA0011: Command and Control	The adversary is trying to communicate with compromised systems to control them.
T1071: Application Layer Protocol	Uso de protocolos de capa de aplicación para comunicarse con infraestructura de comando y control (C2).
T1071.001: Web Protocols	Uso de protocolos web para establecer comunicaciones C2. (HTTP o HTTPS)
TA0010: Exfiltration	The adversary is trying to steal data.
T1041: Exfiltration Over C2 Channel	Exfiltración de datos utilizando canales de comando y control.
TA0040: Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.
T1531: Account Access Removal	Eliminación del acceso a cuentas legítimas para interrumpir las operaciones de la víctima.
T1485: Data Destruction	Destrucción de datos para interrumpir la disponibilidad y la integridad de la información.
T1486: Data Encrypted for Impact	Cifrado de datos para causar un impacto, como en ataques de ransomware.
T1565: Data Manipulation	Manipulación de datos para causar daño o confusión.
T1565.001: Stored Data Manipulation	Manipulación de datos almacenados para alterar la integridad de la información.
T1491: Defacement	Desfiguración de sitios web para dañar la reputación de la víctima.
T1491.002: External Defacement	Desfiguración de sitios web externos para causar un impacto visual y reputacional.
T1561: Disk Wipe	Borrado de discos para destruir datos y causar interrupciones.
T1499: Endpoint Denial of Service	Ataques de denegación de servicio dirigidos a puntos finales para interrumpir su funcionamiento.
T1657: Financial Theft	Robo financiero a través de la manipulación de sistemas y transacciones.
T1498: Network Denial of Service	Denegación de servicio a nivel de red para interrumpir el acceso y la disponibilidad de servicios.

T1498.002: Reflection Amplification	Uso de técnicas de amplificación de reflexión para lanzar ataques de denegación de servicio.
T1496: Resource Hijacking	Secuestro de recursos para utilizarlos en actividades maliciosas, como el minado de criptomonedas.
T1489: Service Stop	Detención de servicios críticos para causar interrupciones.
T1529: System Shutdown/Reboot	Apagado o reinicio de sistemas para interrumpir las operaciones.

Tabla12. Descripción de Tácticas y Técnicas de MITRE ATT&CK detectadas

Tacticas y Tecnicas de MITRE ATT&CK V15	Mitigacion
TA0043: Reconnaissance	M1056: Pre-compromise
T1595: Active Scanning	
T1595.001: Scanning IP Blocks	
T1595.002: Vulnerability Scanning	
T1590: Gather Victim Network Information	
T1590.002: DNS	
TA0042: Resource Development	
T1583: Acquire Infrastructure	
T1583.005: Botnet	
T1584: Compromise Infrastructure	
T1584.005: Botnet	
TA0001: Initial Access	M1048 Application Isolation and Sandboxing M1050 Exploit Protection M1030 Network Segmentation M1026 Privileged Account Management M1051 Update Software M1016 Vulnerability Scanning
T1190: Exploit Public-Facing Application	
T1133: External Remote Services	M1042 Disable or Remove Feature or Program M1035 Limit Access to Resource Over Network M1032 Multi-factor Authentication M1030 Network Segmentation
T1566: Phishing	M1049 Antivirus/Antimalware M1047 Audit M1031 Network Intrusion Prevention M1021 Restrict Web-Based Content M1054 Software Configuration M1017 User Training
T1566.001: Spearphishing Attachment	
T1566.002: Spearphishing Link	
T1195: Supply Chain Compromise	M1013 Application Developer Guidance M1046 Boot Integrity M1033 Limit Software Installation M1051 Update Software M1016 Vulnerability Scanning
T1195.002: Compromise Software Supply Chain	
T1078: Valid Accounts	M1036 Account Use Policies M1015 Active Directory Configuration M1013 Application Developer Guidance M1027 Password Policies M1026 Privileged Account Management M1018 User Account Management M1017 User Training
T1078.001: Default Accounts	
TA0002: Execution	M1047 Audit M1040 Behavior Prevention on Endpoint M1045 Code Signing M1038 Execution Prevention M1031 Network Intrusion Prevention M1021 Restrict Web-Based Content M1017 User Training M1048 Application Isolation and Sandboxing M1050 Exploit Protection
T1203: Exploitation for Client Execution	
T1204: User Execution	
T1204.002: Malicious File	
T1204.001: Malicious Link	
TA0006: Credential Access	M1032 Multi-factor Authentication M1027 Password Policies M1051 Update Software M1018 User Account Management
T1110: Brute Force	
T1110.001: Password Guessing	
TA0011: Command and Control	M1031 Network Intrusion Prevention M1031 Network Intrusion Prevention
T1071: Application Layer Protocol	
T1071.001: Web Protocols	
TA0010: Exfiltration	M1057 Data Loss Prevention M1031 Network Intrusion Prevention
T1041: Exfiltration Over C2 Channel	
TA0040: Impact	
T1531: Account Access Removal	N/A

T1485: Data Destruction	M1053 Data Backup
T1486: Data Encrypted for Impact	M1040 Behavior Prevention on Endpoint M1053 Data Backup
T1565: Data Manipulation	M1041 Encrypt Sensitive Information
T1565.001: Stored Data Manipulation	M1030 Network Segmentation M1029 Remote Data Storage M1022 Restrict File and Directory Permissions
T1491: Defacement	M1053 Data Backup
T1491.002: External Defacement	
T1561: Disk Wipe	
T1499: Endpoint Denial of Service	M1037 Filter Network Traffic
T1498: Network Denial of Service	
T1498.002: Reflection Amplification	
T1496: Resource Hijacking	N/A
T1489: Service Stop	M1030 Network Segmentation M1022 Restrict File and Directory Permissions M1024 Restrict Registry Permissions M1018 User Account Management
T1529: System Shutdown/Reboot	N/A
T1657: Financial Theft	M1018 User Account Management M1017 User Training

Tabla13. Descripción de Mitigaciones de MITRE ATT&CK detectadas

Cabe mencionar que en el anexo de este documento se encuentra una tabla con mayor detalle que incluye las descripciones de cada Tactica y Tecnica detectada, asi como de la mitigacion correspondiente

6 Discusión

La actividad del IPS capturada por nuestros sensores revela cómo el adversario realiza el reconocimiento e intenta comprometer sistemas vulnerables. El disparo de una de estas firmas de detección no significa necesariamente que el ataque haya tenido éxito, pero proporciona información valiosa sobre qué tipos de vulnerabilidades y sistemas están siendo activamente apuntados. Las tendencias de malware reflejan la intención y capacidad del adversario. Similar a las detecciones de IPS, el malware detectado por nuestros sensores no siempre indica infecciones confirmadas, sino más bien la creación y/o distribución de código malicioso. Las detecciones pueden ocurrir a nivel de red, aplicación y host en una variedad de dispositivos. Mientras que las tendencias de explotación y malware generalmente muestran el lado previo al compromiso de los ataques, los botnets proporcionan una perspectiva posterior al compromiso. Una vez infectados, los sistemas a menudo se comunican con hosts remotos, haciendo que este tráfico sea una parte importante de la monitorización del alcance completo de la actividad maliciosa.

El análisis de datos basado en el Cyber Kill Chain permitió una comprensión profunda de las tácticas y técnicas utilizadas por los atacantes. Cada fase del ciclo de vida del ataque fue minuciosamente analizada, proporcionando información valiosa para mejorar las estrategias de defensa y mitigación de ciberamenazas. El uso de Power BI Desktop facilitó la visualización y el análisis de los datos, permitiendo una respuesta rápida y efectiva a los incidentes de seguridad detectados.

Los resultados de esta investigación revelan patrones significativos en la actividad de amenazas cibernéticas, específicamente en las fases de la cadena de eliminación de ciberataques y las técnicas de MITRE ATT&CK. A continuación, se detallan los principales hallazgos y su relevancia:

1. **Fase de Reconocimiento**
    - La detección de actividades de reconocimiento por parte de los adversarios mostró una alta prevalencia de técnicas pasivas y activas, como el escaneo de puertos y la recopilación de información sobre el personal y la infraestructura de la organización. Esto subraya la necesidad de mejorar las medidas de monitoreo y detección temprana para mitigar la exposición de información sensible.
2. **Fase de Explotación**
    - Las técnicas de acceso inicial identificadas, como la explotación de vulnerabilidades en servidores web públicos y el spearphishing, fueron prevalentes. Esto indica que las organizaciones deben reforzar sus defensas perimetrales y educar a sus empleados sobre la importancia de la ciberhigiene y el reconocimiento de intentos de phishing.
3. **Fase de Instalación**
    - La instalación de malware, detectada a través de firmas específicas y análisis de comportamiento, resaltó la adaptabilidad de los adversarios en el desarrollo y distribución de código malicioso. Los sistemas de detección de intrusiones (IPS) y los firewalls de próxima generación demostraron ser efectivos en la identificación de estas amenazas, aunque es necesario un enfoque más proactivo para bloquear la entrada de malware.
4. **Fase de Control y Comando (C2)**
    - La actividad de los botnets evidenció la capacidad de los adversarios para mantener el control de los sistemas comprometidos y ejecutar comandos remotos. Las detecciones de tráfico C2 son cruciales para identificar y desmantelar estas redes maliciosas, destacando la importancia de las soluciones de monitoreo continuo y análisis de tráfico.
5. **Fase de Acción sobre el Objetivo**
    - Los ataques de ransomware, como principal técnica de impacto, demostraron ser devastadores al cifrar datos críticos y exigir rescates. Las organizaciones deben implementar estrategias de respuesta a incidentes y mantener copias de seguridad robustas y aisladas para recuperar los datos sin necesidad de pagar rescates.

6.1 Limitaciones del Estudio

Este estudio presenta ciertas limitaciones que deben ser consideradas al interpretar los resultados:

- **Limitaciones de los Datos**: Los datos analizados se basan en detecciones específicas de sensores y sistemas de seguridad. Es posible que algunas amenazas no hayan sido capturadas debido a la naturaleza evasiva de los adversarios y las limitaciones tecnológicas.
- **Alcance Geográfico**: La investigación se centró en amenazas detectadas en el territorio mexicano, lo que puede no reflejar completamente las tendencias globales en ciberseguridad.
- **Temporalidad de los Datos**: Los datos recopilados cubren un periodo específico y los patrones de amenazas pueden evolucionar con el tiempo. Es importante realizar estudios continuos para mantenerse al día con las nuevas tácticas y técnicas de los adversarios.

6.2 Implicaciones para la Práctica de la Ciberseguridad

Los hallazgos de esta investigación tienen varias implicaciones importantes para la práctica de la ciberseguridad:

- **Mejora de la Detección Temprana**: Las organizaciones deben invertir en tecnologías avanzadas de detección y monitoreo para identificar actividades de reconocimiento y explotación en las primeras fases del ciclo de vida del ataque.
- **Capacitación y Concientización**: La educación continua de los empleados en prácticas de ciberseguridad y la concientización sobre las tácticas de los adversarios son cruciales para reducir la efectividad de técnicas como el spearphishing.
- **Resiliencia y Recuperación**: Desarrollar planes de respuesta a incidentes robustos y mantener sistemas de respaldo seguros son esenciales para mitigar el impacto de ataques de ransomware y otros incidentes críticos.

6.3 Diseminacion del estudio y metodo propuesto

EAI
EUROPEAN ALLIANCE FOR INNOVATION

ACCEPTANCE LETTER

Hereby we confirm that the article with the title „**Cyber Threat Intelligence Methodologies: Hunting Cyber Threats with Threat Intelligence Platforms and Deception techniques**“ by Arturo Torres Cavazos et.al. has been accepted for inclusion and will be published in the EAI/Springer Innovations in Communication and Computing series (**ISSN:** 2522-8595).

Date: 15 Nov 2021

Martin Karbovanec
Ing. Martin Karbovanec
Head of the Publication Department
European Alliance for Innovations

Cyber Threat Intelligence Methodologies: Hunting Cyber Threats with Threat Intelligence Platforms and Deception techniques

M.A Arturo E. Torres, Dr. Francisco Torres, Dr. Arturo Torres Budgud.

Universidad Autonoma de Nuevo Leon
Pedro de Alba S/N, Niños Héroes, Ciudad Universitaria, San Nicolás de los Garza, N.L.
arturo.torrescv@uanl.edu.mx, francisco.torresgrr@uanl.edu.mx, arturo.torresbg@uanl.edu.mx

Abstract - Faced with the great wave of cyber threats, as well as the considerable increase in cybercrime in recent years, organizations have been forced to redefine their digital defense strategies to protect their information assets, infrastructure and reputation from different people. malicious adversaries. Given this, the IT cybersecurity community has chosen to use intelligence techniques to prepare for emerging cyber threats. Therefore, the field of Cyber Threat Intelligence (CTI) has had significant growth in recent years, given the growth and evolution of cyber threats, as well as the complexity of the techniques used by adversaries. However, the CTI field has different challenges for companies that don't have a big budget or lack the experience to implement a CTI plan. The main contribution of this research is based on the compilation and investigation of the schemes, tools, challenges and sets of methodologies most used for the execution of an CTI program, as well as the deployment of a CTI platform based on deception techniques (honeypots) for data collection and cyber threat events. This enables organizations with smaller budgets to use the CTI platform and the methodologies described in this document to stay secure.

Keywords: Cyber Threat Intelligence (CTI), information technology, cyber security events, cyber threats, intelligence sources, cyber security, deception techniques, honeypots, etc.

EAI
EUROPEAN ALLIANCE FOR INNOVATION

ACCEPTANCE LETTER

Hereby we confirm that the article with the title „**Data-Driven Cyber Threat Intelligence: a survey of Mexican territory**" by Arturo Torres Cavazos et.al. has been accepted for inclusion and will be published in the EAI/Springer Innovations in Communication and Computing series (**ISSN:** 2522-8595).

Date: 15 Nov 2021

Martin Karbovanec

Ing. Martin Karbovanec
Head of the Publication Department
European Alliance for Innovations

Data-Driven Cyber Threat Intelligence: a survey of Mexican territory

M.A Arturo E. Torres, Dr. Francisco Torres, Dra. Leticia Neira - UANL

***Abstract*— Las tecnologias de la informacion , asi como la informacion digital y activos de informacion, juegan un papel muy importante en la actualidad a nivel global, por lo cual hemos sido testigos de como publicaciones relacionadas a incidentes de ciberseguridad se incrementan dia a dia, por ello y ante el gran crecimiento de las amenazas cibernetica, diversos investigadores han dedicado gran parte de sus esfuerzos para proteger dichos activos de informacion utilizando fuentes de inteligencia para desarrollar diversas tecnicas para la comprension, evolucion, deteccion y respuestas proactivas contra las amenazas cibernetica que se enfrentan. Por su parte, las empresas, gobiernos y especialistas de ciberseguridad han mostrado un gran interes en el consumo de estas fuentes de inteligncia denominadas como Inteligencia contra Amenazas (CTI), la cual consiste en el conocimiento basado en evidencia, que incluye contexto, mecanismos, indicadores, implicaciones y consejos accionables, sobre una amenaza o peligro existente o emergente para los activos que se pueden usar para informar las decisiones con respecto a la respuesta del sujeto a esa amenaza o peligro. Con un enfoque al territorio Mexicano, este trabajo tiene como objetivo analizar los datos obtenidos de fuentes de CTI utilizando las detecciones de dispositivos de ciberseguridad perimetrales (Firewalls, Intrusion Preventions System, Antivirus, Honeypots, etc.), así como el estudio de trabajos de investigacion relacionados con predicciones de ciberseguridad para señalar la importancia de contar con un modelo capaz de realizar una posible prediccion de amenazas cibernetica en Mexico. También se discuten los desafios y las direcciones futuras en este campo.**

***Index Terms*— tecnologias de la informacion, incidentes de ciberseguridad, amenazas cibernetica, fuentes de inteligencia, ciberseguridad, Inteligencia contra Amenazas (CTI), Firewalls, Intrusion Preventions System, Antivirus, Honeypots, prediccion de amenazas cibrneticas**

el comercio global de todas las principales drogas ilegales combinadas [1]. Asi mismo, en el reporte anual de riesgos 2020 [2] publicado por el "World Economic Forum" se cataloga a los Ciberataques como un riesgo latente de el que hay que estar preparados, ya que la probabilidad e impacto a la economia causado por este fenomeno estan solo por debajo de riesgos como Desastres Naturales, Crisis por falta de agua, Climas extremos, seguidos de riesgos como Enferemedades Infecciosas, Desastres ambientales creados por los humanos, Crisis por alimentos, etc. En el mismo estudio [2] se habla sobre "Los peligros de la evolucion digital" y de como el IoT también está amplificando el potencial de la superficie de ciberataque, estimando que el dia de hoy existen mas de 21 mil millones de dispositivos inteligentes o Internet de las Cosas (IoT) en todo el mundo y se espera que se duplique para el 2025 [3], los cuales han se han convertido en herramientas utlizadas por cibercriminales, caso ocurido a finales de 2016, en el cual lanzaron un ataque importante conocido Denegacion de Servicio Distribuido (DDoS), causando una interrupción en los servicios de Internet que afectó a muchas empresas, incluidas Amazon, PayPal, Netflix, Spotify y Twitter [4]. Asi mismo, la revista Forbes publico [5] que investigadores de la empresa de ciberseguridad F-Secure detectaron un aumento de mas del 300% en los ataques a dispositivos IoT en la primera mitad de 2019 [6], mientras que en septiembre de 2019, dichos dispositivos fueron utilizados para derribar los servicios de paginas como Wikipedia a través de un ataque de Denegación de Servicio Distribuida (DDoS) [7] y se estima que existira un aumento sobre el uso de los dispositivos IoT como intermediarios entre los atacantes y sus víctimas.

Ante estos incidentes y la gran cantidad de amenazas cibernetica rondando el internet afectando a los diferentes sectores de la industria, se han realizado investigaciones en sectores tales como en el sector salud [8] el cual los autores señalan este el sector salud como un objetivo principal de los ciber atacantes para el robo de informacion personal, critica y

CERTIFICADO DE PARTICIPACIÓN

El Registro de Direcciones de Internet para América Latina y Caribe certifica que

Arturo Torres

ha participado en

LACNIC 40 LACNOG 2023

evento realizado del 2 al 6 de octubre de 2023 en Fortaleza, Brasil.

lacnic 40
lacnog 2023
2 - 6 Octubre / Fortaleza, Brasil

FIRST
Improving Security Together

lacnic

https://www.first.org/events/symposium/fortaleza2023/program

7 Conclusiones

En esta sección, se revisan y analizan los resultados obtenidos durante la investigación en relación con las hipótesis planteadas. Se evalúa si se han cumplido los objetivos y se discuten las implicaciones de los hallazgos para la práctica de la ciberseguridad en México.

7.1 Evaluación de la Hipótesis Principal

La hipótesis principal de esta investigación proponía que al analizar eventos reales de ciberseguridad en organizaciones mexicanas, se podría obtener una visión detallada y actualizada del panorama de amenazas cibernéticas en el país. Además, se esperaba que esto permitiera desarrollar una estrategia de ciberseguridad nacional basada en los ciberataques analizados.

7.1.1 Cumplimiento de la Hipótesis Principal:

1. **Visión Detallada y Actualizada del Panorama de Amenazas:**
    - Los resultados de esta investigación confirmaron que el análisis de eventos reales de ciberseguridad permitió obtener una comprensión profunda y precisa de las amenazas cibernéticas que enfrentan las organizaciones mexicanas. Se identificaron patrones de ataque, vectores de amenaza y técnicas empleadas por los adversarios, lo que proporcionó una visión completa del entorno de amenazas.
2. **Desarrollo de una Estrategia de Ciberseguridad Nacional:**
    - Basándose en los hallazgos del análisis, se generaron recomendaciones y estrategias específicas para fortalecer la ciberseguridad a nivel nacional. Estas recomendaciones se enfocaron en mejorar la detección temprana, la respuesta a incidentes y la resiliencia de las organizaciones mexicanas frente a ciberataques.

7.1.2 Evaluación de la Hipótesis 2 Relacionada a la Aplicación de Metodologías de CTI

La segunda hipótesis sugería que la selección y aplicación de metodologías de Inteligencia contra Amenazas (CTI) en el análisis de eventos de ciberseguridad permitiría identificar y categorizar las fases específicas de los ciberataques, así como analizar y modelar tácticas, técnicas y procedimientos (TTP) de ciberataques en el ciberespacio mexicano.

7.1.3 Cumplimiento de la Hipótesis 2:

1. **Identificación y Categorización de Fases de Ciberataques:**
    - La aplicación de metodologías de CTI permitió clasificar los eventos de ciberseguridad en las diferentes fases de la cadena de eliminación de ciberataques (Cyber Kill Chain). Se identificaron técnicas específicas utilizadas por los adversarios en cada fase, proporcionando una visión estructurada de los ciberataques.
2. **Análisis y Modelado de TTPs:**
    - El uso de la matriz MITRE ATT&CK facilitó el análisis detallado de las tácticas, técnicas y procedimientos (TTP) empleados por los atacantes. Esto permitió

modelar los comportamientos adversarios y desarrollar estrategias de defensa más efectivas basadas en un entendimiento profundo de las amenazas.

7.1.4 Evaluación de la Hipótesis 3 Relacionada a la Generación Automatizada de Recomendaciones

La tercera hipótesis proponía que al finalizar el análisis, sería posible generar recomendaciones específicas para reforzar las medidas de ciberseguridad en las organizaciones mexicanas, utilizando las lecciones aprendidas del análisis de amenazas y datos recopilados durante la investigación.

7.1.5 Cumplimiento de la Hipótesis 3:

1. **Generación de Recomendaciones Específicas:**
   - A partir del análisis de los eventos de ciberseguridad, se lograron identificar vulnerabilidades comunes y patrones de ataque recurrentes. Esto permitió formular recomendaciones específicas y accionables para mejorar las defensas de las organizaciones. Estas recomendaciones incluyeron mejoras en la infraestructura de seguridad, capacitación del personal y adopción de nuevas tecnologías de detección y respuesta.
2. **Utilización de Lecciones Aprendidas:**
   - Las lecciones aprendidas durante la investigación fueron fundamentales para desarrollar estrategias de mitigación y respuesta a incidentes. Se promovió la adopción de prácticas proactivas de ciberseguridad y la implementación de controles técnicos y organizativos basados en las tendencias observadas en el análisis.

7.2 Respuesta a las Preguntas de Investigación

Pregunta 1: ¿Existen set de datos disponibles que brinden información de eventos de ciberseguridad ocurridos en el sector mexicano?

- **Respuesta:** Sí, se identificaron y utilizaron conjuntos de datos que brindan información detallada sobre eventos de ciberseguridad en organizaciones mexicanas. Estos datos permitieron describir el panorama de amenazas cibernéticas en México, cumpliendo así con el Objetivo Específico 1. Los datos analizados provenían de diferentes fuentes, incluyendo sistemas de detección de intrusiones (IPS), registros de malware y botnets, proporcionando una visión integral de las amenazas enfrentadas por las organizaciones en el país.

Pregunta 2: ¿Cuáles son los patrones predominantes en los eventos de ciberseguridad detectados en organizaciones mexicanas?

- **Respuesta:** Los patrones predominantes identificados en los eventos de ciberseguridad incluyeron técnicas de reconocimiento, explotación de vulnerabilidades, uso de malware y

comunicación post-compromiso a través de botnets. La aplicación de metodologías de Inteligencia contra Amenazas (CTI), como MITRE ATT&CK, permitió identificar y categorizar las fases específicas de los ciberataques en el contexto mexicano, cumpliendo con el Objetivo Específico 2. Se observaron tendencias significativas en el uso de ciertos tipos de malware y técnicas de explotación que proporcionaron información valiosa para el desarrollo de estrategias de mitigación.

Pregunta 3: ¿Cuáles son las herramientas y técnicas más efectivas para la recolección, análisis y visualización de los eventos de seguridad recolectados para esta investigación en un entorno experimental avanzado?

- **Respuesta:** Las herramientas y técnicas más efectivas identificadas para la recolección, análisis y visualización de eventos de ciberseguridad incluyeron el uso de Power BI para el análisis y visualización interactiva de datos, así como la aplicación de metodologías de Inteligencia contra Amenazas (CTI) para estructurar y analizar los eventos. Estas herramientas permitieron un enfoque sistemático y científico para el análisis de datos de ciberseguridad, facilitando la identificación de patrones y tendencias relevantes. Este enfoque cumplió con el Objetivo Específico 3, proporcionando una base sólida para el desarrollo de un entorno experimental integral.

Pregunta 4: ¿Cómo se pueden integrar los resultados obtenidos de la investigación para generar recomendaciones específicas y automatizadas destinadas a reforzar las medidas de ciberseguridad en las organizaciones mexicanas?

- **Respuesta:** Los resultados de la investigación se integraron de manera efectiva para generar recomendaciones específicas y automatizadas. Estas recomendaciones se basaron en el análisis detallado de eventos de ciberseguridad y las lecciones aprendidas durante la investigación. Las recomendaciones incluyeron mejoras en la infraestructura de seguridad, la adopción de nuevas tecnologías de detección y respuesta, y la implementación de prácticas proactivas de ciberseguridad. Este enfoque cumplió con el Objetivo Específico 3, proporcionando estrategias prácticas y accionables para fortalecer las defensas de las organizaciones mexicanas.

7.3 Cumplimiento de los Objetivos de la Tesis

7.3.1 Objetivo General

Desarrollar un método basado en Ciencia de Datos e Inteligencia de Ciber Amenazas (CTI) que nos permita investigar y analizar de manera exhaustiva el panorama de amenazas cibernéticas en México mediante la recolección y análisis de eventos de ciberseguridad reales detectados en el ciberespacio mexicano para describir las fases, tácticas, técnicas y tendencias de actividad maliciosa que permita generar una estrategia de ciberseguridad nacional a través del análisis y comprensión de los ciberataques que ocurren en el ciberespacio mexicano.

El objetivo general de esta tesis ha sido plenamente alcanzado. Mediante el uso de técnicas avanzadas de Ciencia de Datos e Inteligencia de Ciber Amenazas (CTI), se logró investigar y analizar exhaustivamente el panorama de amenazas cibernéticas en México. La recolección y análisis de eventos reales de ciberseguridad proporcionaron una comprensión detallada de las fases, tácticas, técnicas y tendencias de actividad maliciosa, permitiendo así la formulación de una estrategia de ciberseguridad nacional basada en evidencia concreta.

7.3.1.1 Objetivos Específicos

Objetivo Específico 1 - Describir el Panorama de Amenazas Cibernéticas en México Este objetivo busca proporcionar una visión detallada y actualizada del panorama de amenazas cibernéticas en México, basándose en el análisis de eventos reales de ciberseguridad detectados en organizaciones mexicanas.

- **Cumplimiento:** Se logró proporcionar una visión detallada del panorama de amenazas cibernéticas en México. El análisis de datos recolectados permitió identificar las principales amenazas que enfrentan las organizaciones mexicanas, así como las técnicas y tácticas empleadas por los adversarios. Este análisis incluyó la detección de patrones de actividad maliciosa y la identificación de las vulnerabilidades más explotadas.

Objetivo Específico 2 – Aplicación de Metodologías de Inteligencia contra Amenazas (CTI) Seleccionar y aplicar metodologías de CTI en el análisis de los eventos de ciberseguridad recolectados para identificar y categorizar las fases específicas de los ciberataques para analizar y modelar tácticas, técnicas y procedimientos (TTP) de adversarios en el contexto mexicano.

- **Cumplimiento:** Se aplicaron con éxito metodologías de CTI, como MITRE ATT&CK, para analizar los eventos de ciberseguridad recolectados. Esto permitió identificar y categorizar las fases específicas de los ciberataques, así como modelar las tácticas, técnicas y procedimientos (TTP) utilizados por los adversarios en el contexto mexicano. Este enfoque sistemático y basado en inteligencia contra amenazas facilitó una comprensión profunda de las estrategias de los atacantes y sus patrones de comportamiento.

Objetivo Específico 3 – Generación Automatizada de Recomendaciones para Reforzar la Ciberseguridad Nacional Al finalizar el análisis, la tesis se propone proporcionar recomendaciones específicas para reforzar las medidas de ciberseguridad en las organizaciones mexicanas, basadas en las lecciones aprendidas del análisis de amenazas.

- **Cumplimiento:** Se generaron recomendaciones específicas y automatizadas basadas en el análisis de los datos de ciberseguridad. Estas recomendaciones se enfocaron en reforzar las medidas de ciberseguridad en las organizaciones mexicanas, abarcando desde mejoras en la infraestructura de seguridad hasta la adopción de nuevas tecnologías de detección y respuesta. Las recomendaciones también incluyeron estrategias proactivas para la gestión de riesgos y la mitigación de amenazas, basadas en las lecciones aprendidas durante la investigación.

7.4 Resolución del Problema

A lo largo de esta investigación, se ha logrado abordar y resolver el problema planteado mediante el cumplimiento de los objetivos y la validación de las hipótesis formuladas. A continuación, se detallan los logros que han contribuido a la resolución del problema:

1. **Desarrollo de un Método Basado en Ciencia de Datos e Inteligencia de Ciber Amenazas (CTI)**:
    - Se desarrolló un método robusto que permitió la recolección y análisis exhaustivo de eventos reales de ciberseguridad en México. Este método proporcionó una visión detallada de las fases, tácticas, técnicas y tendencias de actividad maliciosa en el ciberespacio mexicano.
2. **Descripción del Panorama de Amenazas Cibernéticas en México**:
    - Se describió de manera detallada el panorama de amenazas cibernéticas en México, identificando las principales amenazas que enfrentan las organizaciones mexicanas y las técnicas empleadas por los adversarios.
3. **Aplicación de Metodologías de Inteligencia contra Amenazas (CTI)**:
    - Se aplicaron metodologías de CTI, como MITRE ATT&CK, para identificar y categorizar las fases específicas de los ciberataques. Esto facilitó el análisis y modelado de las tácticas, técnicas y procedimientos (TTP) utilizados por los adversarios en el contexto mexicano.
4. **Generación Automatizada de Recomendaciones para Reforzar la Ciberseguridad**:
    - Se generaron recomendaciones específicas y automatizadas basadas en el análisis de los datos de ciberseguridad. Estas recomendaciones están orientadas a reforzar las medidas de ciberseguridad en las organizaciones mexicanas, abarcando desde mejoras en la infraestructura de seguridad hasta la adopción de nuevas tecnologías de detección y respuesta.

En conclusión, la investigación ha logrado resolver el problema planteado al proporcionar un método efectivo y basado en evidencia para analizar el panorama de amenazas cibernéticas en México. La integración de inteligencia de ciber amenazas y la generación de recomendaciones específicas contribuyen significativamente a la formulación de una estrategia nacional de ciberseguridad, abordando así la necesidad de una defensa integral y coordinada contra las ciberamenazas.

7.5 Conclusión Final

De acuerdo con la investigación publicada por SANS [65], podemos concordar que la CTI se enfoca en poder recabar la información relacionada a amenazas de interés de acuerdo con la población que se desea proteger para así entender los riesgos, amenazas y requerimientos necesarios a investigar. Por lo tanto, comprender cómo un ataque informático puede beneficiar a un equipo de seguridad de nuestra organización puede beneficiar a la comunidad de ciberseguridad impulsar que los defensores recopilen datos sobre los adversarios para aumentar la base de conocimientos de TTP’s, facilitando la selección de medidas de defensa. Si los defensores

implementan contramedidas más rápido de lo que evolucionan sus adversarios, mantienen una ventaja táctica.

En esta investigación, hemos demostrado el uso efectivo de las metodologías más utilizadas del campo de CTI para la detección, mitigación y generación de CTI durante el proceso de análisis e investigación de TTP's reales recolectadas por sensores de ciberseguridad con motores de inspección en las organizaciones mexicanas, donde se pudo encontrar que cada de estas metodologías se complementan mutuamente. En el cual, el Cyber Kill Chain Model nos ayuda a entender las fases del ataque de un adversario, por lo tanto, obtenemos una guía inicial para los defensores de donde enfocar sus recursos y a su vez, ayuda a alimentar el modelo MITRE ATT&CK, el cual nos da la oportunidad de enumerar y entender que TTP's utilizan los adversarios en cada una de sus fases de ataque y proveer información necesaria para la generación de una estrategia de defensa. activa.

En resumen, la investigación realizada no solo validó las hipótesis planteadas, sino que también cumplió con los objetivos específicos de manera efectiva. La aplicación de Ciencia de Datos e Inteligencia de Ciber Amenazas permitió obtener una comprensión detallada y actualizada del panorama de amenazas cibernéticas en México. Además, se lograron identificar y modelar las tácticas, técnicas y procedimientos de los adversarios, y se generaron recomendaciones prácticas para mejorar la ciberseguridad en las organizaciones mexicanas. Estos logros destacan la importancia de un enfoque basado en datos y en inteligencia contra amenazas para enfrentar los desafíos de ciberseguridad en el entorno mexicano.

8 Trabajo Futuro

Los próximos pasos en esta y futuras investigaciones incluyen identificar las fuentes de inteligencia necesarias para realizar un modelo predicativo basado en datos y evidencia recolectadas para el sector mexicano, incluso se pueden planificar ajustes específicos identificando las circunstancias de los datos recolectados. Además, se realizarán estudios sobre la tecnología de procesamiento de grandes cantidades de datos e información de ciberamenazas, así como las técnicas de análisis de minería de datos, el análisis de correlación entre los datos con el objetivo principal de procesar la información de CTI recolectada para estimar un pronóstico de incidentes cibernéticos basado en la evidencia de las fuentes de inteligencia.

9 ANEXO

9.1 GLOSARIO

Termino	Definición
AI	Inteligencia artificial, rama de la informática que investiga procesos que imiten la inteligencia de los seres vivos.
Antivirus	Programas cuyo objetivo es detectar y eliminar virus informáticos.

Termino	Definición
APT	Una amenaza persistente avanzada, también conocida por sus siglas en inglés, APT, es un conjunto de procesos informáticos sigilosos orquestados por un tercero con la intención y la capacidad de atacar de forma avanzada y continuada en el tiempo, un objetivo determinado.
Autoridad Certificada	Entidad de confianza, responsable de emitir y revocar los certificados, utilizando en ellos la firma electrónica, para lo cual se emplea la criptografía de clave pública.
Beacon	Son pequeños dispositivos basados en tecnología Bluetooth de bajo consumo (BTT), los cuales emiten una señal que los identifica de forma única. Dicha señal puede ser recibida e interpretada por otros dispositivos, e información que censan, como temperatura, distancia, acciones, entre otras.
BI	*Business Intelligence* es transformar los datos e información en conocimiento, de manera que se pueda optimizar el proceso de toma de decisiones en los negocios.
Big Data	Es un término que hace referencia a conjuntos de datos tan grandes y complejos que precisan de aplicaciones informáticas no tradicionales de procesamiento de datos para tratarlos adecuadamente
Botnet	Es un término que hace referencia a una red de dispositivos, ordenadores y servidores infectados, que son controlados de manera remota, autónoma y automática.
Bug	Un error de software o fallo es un problema en un sistema que desencadena un resultado indeseado.
Control de Acceso	Sistema de verificación de identidad que solicita acceso a un recurso físico o lógico.
Crypto jacking	Robar recursos del sistema de la víctima con el fin de minar criptomonedas.
Cyber Warfare	Desplazamiento de un conflicto, que toma el ciberespacio y las tecnologías de comunicación e información como campo de operaciones.
Dark web	La *dark web* o internet oscura es el contenido de la *World Wide Web* que existe en "la oscuridad", redes que se superponen a la internet pública y requieren de software específico y configuraciones o autorización para acceder.
DDoS	Ataque de denegación de servicio (DoS) para degradar o bloquear la disponibilidad de servicios para los usuarios
ETL	*Extract, Transform and Load* es el proceso que permite a las organizaciones mover datos desde múltiples fuentes, reformatearlos, limpiarlos, y cargarlos en otra base de datos, llamada *DataMart*, universo o *data warehouse* para su posterior análisis.
Exploit	Programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema, de forma que un atacante podría usarla en su beneficio.
Firewall	Es un sistema cuya función es prevenir y proteger una red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso.

Termino	Definición
Fuzzing Testing	técnica de pruebas de software, automatizada o semiautomatizada, que implica proporcionar datos inválidos, inesperados o aleatorios a las entradas de un sistema.
Hacktivista	Es un ataque a medios electrónicos como por ejemplo una página web y que tiene un fin político.
Hash	El hash o función hash, es una función criptográfica especial que es utilizada para generar identificadores únicos e irrepetibles.
Honeypot	Es una herramienta de la seguridad informática dispuesto en una red o sistema informático para ser el objetivo de un posible ataque informático, y así poder detectarlo y obtener información del mismo y del atacante.
IPS	Sistema de prevención de intrusos es un dispositivo de seguridad, fundamentalmente para redes, que se encarga de monitorear actividades a nivel de la capa 3 (red) y/o a nivel de la capa 7 (aplicación) del Modelo OSI, con el fin de identificar comportamientos maliciosos, sospechosos e indebidos, a fin de reaccionar ante ellos en tiempo real.
Malware	El software malintencionado o malware puede incluir cargas útiles, goteros, herramientas posteriores al compromiso, puertas traseras, empaquetadores y protocolos C2. Los adversarios pueden adquirir malware para respaldar sus operaciones, obteniendo un medio para mantener el control de máquinas remotas, evadiendo defensas y ejecutando comportamientos posteriores al compromiso.
MCA	Es una persona o grupo que se caracteriza por intención de hacer daño utilizando computadoras, dispositivos, sistemas o redes.
Minería de Datos	Es un campo de la estadística y las ciencias de la computación referido al proceso que intenta descubrir patrones en grandes volúmenes de datos. Utiliza los métodos de la inteligencia artificial, aprendizaje automático, estadística y sistemas de bases de datos.
ML	*Machine Learning* es una disciplina científica del ámbito de la Inteligencia Artificial que crea sistemas que aprenden automáticamente.
Phishing	Técnica de ingeniería social que busca engañar a una víctima, ganándose su confianza y haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.
PoS Malware	Software malintencionado (*malware*) que utilizan los ciberdelincuentes para apuntar a puntos de venta (POS) y terminales de pago con la intención de obtener información de tarjetas de crédito y débito.
Ransomware	Secuestro de la información de la víctima, con el propósito de recibir un pago por el rescate de la misma.
Scamware	Malware para estafar con cargas maliciosas, o con limitados o ningún beneficio, que son vendidos a los consumidores vía ciertas prácticas no éticas de comercialización.

Termino	Definición
SCRUM	Scrum es un marco ligero que ayuda a las personas, los equipos y las organizaciones a generar valor a través de soluciones adaptativas para problemas complejos.
SDLC	El ciclo de vida de desarrollo seguro de sistemas es el proceso de creación o modificación de los sistemas, modelos y metodologías que la gente usa para desarrollar estos sistemas de software.
SHA-2	Es un conjunto de funciones hash criptográficas diseñadas por la Agencia de Seguridad Nacional (NSA).
Sprint	Es un evento SCRUM que es un periodo de tiempo de un mes o menor, que sirve de contenedor para los otros eventos y actividades de SCRUM. Los Sprints son ejecutados consecutivamente, sin interrupciones.
Spyware	Malware espía, utilizado para recopilar información de un dispositivo víctima y transmitir dicha información a una entidad externa sin el permiso de la víctima.
SQL Injection	Método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.
Targeted Attack	Las amenazas dirigidas son una clase de malware destinado a una organización o industria específica, están diseñadas para robar información confidencial.
Trojan	*Malware* que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo.
Worm	Es un *malware* que tiene la capacidad de copiarse a sí mismo de una máquina a otra.
XSS	*Cross-site* scripting es un vector de ataque que puede ser utilizado para robar información delicada, secuestrar sesiones de usuario, y comprometer el navegador, subyugando la integridad del sistema, a través de la inyección de código en la página vulnerable.

9.2 Codigo de Power Query

Este código de Power Query está diseñado para importar y transformar datos de un archivo de Excel almacenado en una biblioteca de documentos de SharePoint. El proceso incluye varias etapas de filtrado, renombrado y eliminación de columnas, así como la invocación de una función personalizada para enriquecer los datos.

A continuación, se expande una columna para obtener datos detallados, se ajustan los tipos de datos y se agregan columnas personalizadas basadas en ciertas transformaciones de texto. Este flujo de trabajo asegura que los datos finales estén limpios, estructurados y listos para su análisis en Power BI.

9.2.1 Explicación del código utilizado

```
let
  // Conecta a la biblioteca de archivos de SharePoint del sitio especificado
  Source = SharePoint.Files("https://fortinet.sharepoint.com/sites/FG-POWERBI", [ApiVersion = 15]),

  // Filtra las filas para obtener solo los archivos en la carpeta especificada
  #"Filtered Rows" = Table.SelectRows(Source, each ([Folder Path] = "https://fortinet.sharepoint.com/sites/FG-POWERBI/Shared Documents/General/GEOLOCATIONS/")),

  // Selecciona el contenido del archivo "Geolocation.xlsx" en la carpeta especificada
  #"Geolocation xlsx_https://fortinet sharepoint com/sites/FG-POWERBI/Shared Documents/General/GEOLOCATIONS/" = #"Filtered Rows"{[Name="Geolocation.xlsx",#"Folder Path"="https://fortinet.sharepoint.com/sites/FG-POWERBI/Shared Documents/General/GEOLOCATIONS/"]}[Content],

  // Importa el libro de Excel seleccionado
  #"Imported Excel Workbook" = Excel.Workbook(#"Geolocation xlsx_https://fortinet sharepoint com/sites/FG-POWERBI/Shared Documents/General/GEOLOCATIONS/"),

  // Selecciona la tabla "Geolocation" del libro de Excel importado
  Geolocation_Table = #"Imported Excel Workbook"{[Item="Geolocation",Kind="Table"]}[Data],

  // Filtra las filas donde la columna "FG-Regions" no sea nula
  #"Filtered Rows1" = Table.SelectRows(Geolocation_Table, each ([#"FG-Regions"] <> null)),

  // Renombra la columna "name" a "Country Name"
  #"Renamed Columns" = Table.RenameColumns(#"Filtered Rows1",{{"name", "Country Name"}}),

  // Elimina la columna "alpha-3"
  #"Removed Columns" = Table.RemoveColumns(#"Renamed Columns",{"alpha-3"}),

  // Renombra la columna "alpha-2" a "Country Code"
  #"Renamed Columns1" = Table.RenameColumns(#"Removed Columns",{{"alpha-2", "Country Code"}}),

  // Elimina la columna "country-code"
  #"Removed Columns1" = Table.RemoveColumns(#"Renamed Columns1",{"country-code"}),

  // Renombra las columnas "region" y "FG-Regions" a "Original Region" y "Region" respectivamente
  #"Renamed Columns2" = Table.RenameColumns(#"Removed Columns1",{{"region", "Original Region"}, {"FG-Regions", "Region"}}),

  // Elimina la columna "intermediate-region"
  #"Removed Columns2" = Table.RemoveColumns(#"Renamed Columns2",{"intermediate-region"}),

  // Elimina varias columnas: "Country Name", "Original Region", "sub-region", "Region"
  #"Removed Columns3" = Table.RemoveColumns(#"Removed Columns2",{"Country Name", "Original Region", "sub-region", "Region"}),

  // Invoca una función personalizada "V-AV by Country Code" y agrega los resultados como una nueva columna "AV by Country Code"
  #"Invoked Custom Function" = Table.AddColumn(#"Removed Columns3", "AV by Country Code", each #"V-AV by Country Code"([Country Code])),

  // Elimina las filas que tienen errores en la columna "AV by Country Code"
  #"Removed Errors" = Table.RemoveRowsWithErrors(#"Invoked Custom Function", {"AV by Country Code"}),

  // Expande la columna "AV by Country Code" para incluir las columnas especificadas
  #"Expanded AV by Country Code" = Table.ExpandTableColumn(#"Removed Errors", "AV by Country Code", {"Logtime", "Stats.Logtime", "Stats.ID", "Stats.Name", "Stats.Count", "Stats.Threattype", "Stats.Country"}, {"Logtime", "Stats.Logtime", "Stats.ID", "Stats.Name", "Stats.Count", "Stats.Threattype", "Stats.Country"}),

  // Renombra la columna "Logtime" a "Date"
```

```
    #"Renamed Columns3" = Table.RenameColumns(#"Expanded AV by Country Code",{{"Logtime", "Date"}}),

    // Elimina la columna "Stats.Logtime"
    #"Removed Columns4" = Table.RemoveColumns(#"Renamed Columns3",{"Stats.Logtime"}),

    // Cambia el tipo de varias columnas a los tipos especificados
    #"Changed Type" = Table.TransformColumnTypes(#"Removed Columns4",{{"Stats.Count", Int64.Type}, {"Date", type date}, {"Stats.ID", type text}, {"Stats.Name", type text}, {"Stats.Country", type text}, {"Stats.Threattype", type text}}),

    // Renombra varias columnas: "Stats.Name" a "Signature Name", "Stats.ID" a "Sig ID", "Stats.Count" a "Volume"
    #"Renamed Columns4" = Table.RenameColumns(#"Changed Type",{{"Stats.Name", "Signature Name"}, {"Stats.ID", "Sig ID"}, {"Stats.Count", "Volume"}}),

    // Elimina la columna "Stats.Country"
    #"Removed Columns5" = Table.RemoveColumns(#"Renamed Columns4",{"Stats.Country"}),

    // Filtra las filas donde la columna "Signature Name" no esté vacía
    #"Filtered Rows2" = Table.SelectRows(#"Removed Columns5", each ([Signature Name] <> "")),

    // Agrega una columna personalizada "Data.Type" reemplazando "virus" por "Volume" en la columna "Stats.Threattype"
    #"Added Custom" = Table.AddColumn(#"Filtered Rows2", "Data.Type", each Text.Replace([Stats.Threattype], "virus", "Volume")),

    // Agrega una columna personalizada "Tactic" reemplazando "virus" por "TA0002" en la columna "Stats.Threattype"
    #"Added Custom1" = Table.AddColumn(#"Added Custom", "Tactic", each Text.Replace([Stats.Threattype], "virus", "TA0002"))
in
    #"Added Custom1"
```

Esta estructura asegura que el proceso de limpieza de datos esté documentado de manera clara y comprensible, proporcionando tanto una descripción de alto nivel como detalles técnicos precisos.

9.3 Descripción de Campañas de Ransomware detectadas

9.3.1 KlopRansom.S!tr.ransom

KlopRansom, también conocido como Clop, es operado por un grupo de cibercriminales sofisticados conocido como TA505. Este grupo ha sido responsable de numerosos ataques de alto perfil y ha sido muy activo en la escena del ransomware. TA505 es conocido por su capacidad para adaptarse y evolucionar rápidamente sus tácticas, técnicas y procedimientos (TTPs).

9.3.1.1 Sistemas Operativos Objetivo

KlopRansom.S!tr.ransom está diseñado principalmente para infectar sistemas operativos Windows. Sin embargo, sus operadores han demostrado la capacidad de apuntar a diversos sistemas dentro de las redes corporativas para maximizar el daño.

9.3.1.2 Vulnerabilidades

Clop se propaga utilizando una variedad de métodos, incluyendo:

- **Explotación de Vulnerabilidades de Software**: Utiliza vulnerabilidades conocidas en aplicaciones y servicios sin parchear.
- **Fuerza Bruta en Servicios RDP**: Obtienen acceso utilizando credenciales débiles o comprometidas.
- **Campañas de Phishing**: Correos electrónicos con archivos adjuntos maliciosos o enlaces que descargan el ransomware.
- **Uso de Malware Previo**: Como el troyano FlawedAmmyy y otros RATs (Remote Access Trojans) para obtener acceso inicial.

9.3.1.3 Sector de Industria

Clop ha afectado a una amplia gama de sectores industriales, incluyendo:

- Servicios Financieros
- Salud
- Educación
- Manufactura
- Tecnología
- Energía
- Gobierno
- Pequeñas y medianas empresas

9.3.1.4 Historia

Clop apareció por primera vez alrededor de 2019 y rápidamente se hizo conocido por su enfoque en grandes organizaciones y su uso de técnicas de doble extorsión. Los ataques de Clop no solo cifran los datos, sino que también exfiltran información sensible y amenazan con publicarla si no se paga el rescate. TA505, el grupo detrás de Clop, ha sido activo desde al menos 2014 y es responsable de una serie de campañas de malware y ransomware previas.

9.3.1.5 Relaciones

Clop ha mostrado conexiones con otras familias de ransomware y herramientas de cibercrimen. Su código y métodos de distribución han sido comparados con Dridex y otras herramientas utilizadas por TA505. Además, la técnica de doble extorsión ha sido adoptada por otros grupos de ransomware que operan de manera similar.

9.3.2 Comportamiento Post-Explotación e Impacto

Una vez que KlopRansom.S!tr.ransom ha comprometido un sistema, sigue generalmente los siguientes pasos:

1. **Acceso Inicial**: Obtención de acceso a través de RDP, phishing, o explotando vulnerabilidades.
2. **Movilidad Lateral**: Exploración y compromiso de otros sistemas en la red para maximizar el impacto.

3. **Cifrado de Archivos**: Utiliza algoritmos de cifrado robustos como AES-256 combinado con RSA para cifrar archivos críticos.
4. **Exfiltración de Datos**: Antes de cifrar los datos, el ransomware exfiltra datos sensibles a servidores controlados por los atacantes.
5. **Nota de Rescate**: Deja una nota de rescate en el sistema afectado, instruyendo al usuario sobre cómo pagar el rescate en criptomonedas (generalmente Bitcoin).
6. **Comunicación con el Servidor C&C**: Puede comunicarse con un servidor de comando y control para recibir instrucciones adicionales y enviar información sobre el sistema comprometido.

9.3.3 W32/Conti.F!tr.ransom

Conti es operado por un grupo de cibercriminales altamente sofisticados, conocido por sus ataques dirigidos a grandes organizaciones y corporaciones en todo el mundo. Conti es un ransomware-as-a-service (RaaS), lo que significa que el grupo central desarrolla y gestiona el ransomware mientras que los afiliados realizan los ataques a cambio de una parte del rescate.

9.3.3.1 Sistemas Operativos Objetivo

W32/Conti.F!tr.ransom está diseñado principalmente para infectar sistemas operativos Windows. Los atacantes buscan vulnerabilidades en servidores y estaciones de trabajo dentro de las redes corporativas para maximizar el impacto.

9.3.3.2 Vulnerabilidades

Conti se propaga utilizando una variedad de métodos, incluyendo:

- **Explotación de Vulnerabilidades de Software**: Las vulnerabilidades en aplicaciones y servicios no actualizados pueden ser explotadas para ganar acceso inicial.
- **Fuerza Bruta en Servicios RDP**: Los atacantes intentan obtener acceso utilizando credenciales débiles o comprometidas.
- **Campañas de Phishing**: Correos electrónicos con archivos adjuntos maliciosos o enlaces que descargan el ransomware.
- **Kits de Explotación**: Utilizan kits de explotación para aprovechar vulnerabilidades en navegadores web y plugins desactualizados.

9.3.3.3 Sector de Industria

Conti ha afectado a una amplia gama de sectores industriales, incluyendo:

- Servicios Financieros
- Salud
- Educación
- Manufactura
- Tecnología
- Energía

- Gobierno
- Pequeñas y medianas empresas

9.3.3.4 Historia

Conti apareció por primera vez a principios de 2020 y rápidamente se hizo conocido por sus ataques devastadores y la alta velocidad de cifrado que utiliza. El grupo detrás de Conti ha demostrado ser muy organizado y profesional, operando como un negocio con un modelo de afiliación. Conti también se destaca por su doble extorsión, donde no solo cifran los archivos, sino que también amenazan con publicar datos robados si no se paga el rescate.

9.3.3.5 Relaciones

Conti ha mostrado conexiones con otras familias de ransomware y herramientas de cibercrimen. Su código y métodos de distribución han sido comparados con Ryuk, y se ha especulado que los operadores de Conti podrían tener vínculos con los grupos detrás de este ransomware.

9.3.4 Comportamiento Post-Explotación e Impacto

Una vez que W32/Conti.F!tr.ransom ha comprometido un sistema, sigue generalmente los siguientes pasos:

1. **Acceso Inicial**: Obtención de acceso a través de RDP, phishing o vulnerabilidades explotadas.
2. **Movilidad Lateral**: Exploración y compromiso de otros sistemas en la red para maximizar el impacto.
3. **Cifrado de Archivos**: Utiliza algoritmos de cifrado robustos como AES-256 combinado con RSA para cifrar archivos críticos.
4. **Exfiltración de Datos**: Antes de cifrar los datos, el ransomware exfiltra datos sensibles a servidores controlados por los atacantes.
5. **Nota de Rescate**: Deja una nota de rescate en el sistema afectado, instruyendo al usuario sobre cómo pagar el rescate en criptomonedas (generalmente Bitcoin).
6. **Comunicación con el Servidor C&C**: Puede comunicarse con un servidor de comando y control para recibir instrucciones adicionales y enviar información sobre el sistema comprometido.

9.3.5 Mitigación y Prevención

Para mitigar el riesgo de infecciones por W32/Conti.F!tr.ransom y otras variantes de ransomware, se recomiendan las siguientes acciones:

1. **Capacitación en Concienciación de Seguridad**: Educar a los empleados sobre los riesgos del phishing y cómo identificar correos electrónicos maliciosos.
2. **Actualización y Parches**: Mantener todos los sistemas operativos y aplicaciones actualizados con los últimos parches de seguridad.

3. **Restricción de RDP**: Deshabilitar RDP si no es necesario y, si es necesario, usar VPNs y autenticación de dos factores.
4. **Uso de Software de Seguridad**: Implementar soluciones de seguridad robustas, como antivirus, firewalls y sistemas de detección de intrusiones (IDS).
5. **Copias de Seguridad**: Realizar copias de seguridad regulares y almacenarlas en ubicaciones seguras y desconectadas de la red.
6. **Segregación de Redes**: Segmentar las redes internas para limitar la propagación del ransomware.
7. **Monitoreo y Detección**: Utilizar herramientas de monitoreo y detección de amenazas para identificar actividades sospechosas.

9.3.6 JS/Nemucod.DGY!tr

JS/Nemucod.DGY!tr es una variante del ransomware Nemucod, que es conocido por ser distribuido principalmente por cibercriminales que se especializan en ataques de phishing y correos electrónicos maliciosos. El grupo detrás de Nemucod ha sido difícil de identificar con precisión, pero se sabe que operan principalmente en la darknet y en foros de hacking.

9.3.6.1 Sistemas Operativos Objetivo

JS/Nemucod.DGY!tr se enfoca principalmente en sistemas operativos Windows. Utiliza scripts JavaScript maliciosos para descargar y ejecutar su payload, que generalmente está diseñado para afectar a diferentes versiones de Windows, desde Windows XP hasta las versiones más recientes.

9.3.6.2 Vulnerabilidades

Nemucod y sus variantes, incluyendo JS/Nemucod.DGY!tr, no dependen necesariamente de vulnerabilidades específicas del sistema operativo para infectar a los usuarios. En su lugar, se propagan a través de correos electrónicos de phishing que contienen archivos adjuntos maliciosos (por ejemplo, archivos JavaScript, archivos comprimidos o documentos de Office con macros). Una vez que el usuario abre el archivo adjunto, el script se ejecuta y descarga el ransomware desde un servidor remoto.

Sin embargo, Nemucod ha sido conocido por aprovecharse de vulnerabilidades en aplicaciones de terceros, como navegadores web y plugins no actualizados, para facilitar su distribución y ejecución.

9.3.6.3 Sector de Industria

Nemucod y sus variantes no discriminan por sector y han afectado a una amplia gama de industrias, incluyendo:

- Servicios financieros
- Salud
- Educación
- Gobierno

- Tecnología
- Manufactura
- Pequeñas y medianas empresas

9.3.6.4 Historia

Nemucod apareció por primera vez alrededor de 2015 y rápidamente ganó notoriedad por su método de propagación a través de correos electrónicos de phishing. Originalmente, Nemucod se utilizaba principalmente como un downloader, descargando otros tipos de malware, incluyendo troyanos bancarios y ransomware. A lo largo de los años, se han desarrollado múltiples variantes, incluyendo JS/Nemucod.DGY!tr, que es específicamente una variante diseñada para cifrar archivos y exigir un rescate.

9.3.6.5 Relaciones

Nemucod tiene una relación con varias familias de malware debido a su capacidad como downloader. Ha sido conocido por descargar y ejecutar otros tipos de ransomware, como Locky y TeslaCrypt, además de sus propias variantes de ransomware.

9.3.7 Comportamiento Post-Explotación e Impacto

Una vez que JS/Nemucod.DGY!tr ha comprometido un sistema, sigue generalmente los siguientes pasos:

1. **Descarga y Ejecución del Payload**: El script malicioso descargado se conecta a un servidor C&C (Comando y Control) para obtener el payload del ransomware.
2. **Cifrado de Archivos**: El ransomware cifra archivos en el sistema infectado utilizando algoritmos de cifrado robustos (como AES-256).
3. **Nota de Rescate**: Deja una nota de rescate en el escritorio y en los directorios afectados, instruyendo al usuario a pagar un rescate en Bitcoin para recuperar sus archivos.
4. **Comunicación con el Servidor C&C**: El ransomware puede enviar información sobre el sistema infectado de vuelta a los operadores y recibir más instrucciones.

9.3.8 Mitigación y Prevención

Para mitigar el riesgo de infecciones por JS/Nemucod.DGY!tr y otras variantes de ransomware, se recomiendan las siguientes acciones:

1. **Capacitación en Concienciación de Seguridad**: Educar a los empleados sobre los riesgos del phishing y cómo identificar correos electrónicos maliciosos.
2. **Actualización y Parches**: Mantener todos los sistemas operativos y aplicaciones actualizados con los últimos parches de seguridad.
3. **Uso de Software de Seguridad**: Implementar soluciones de seguridad robustas, como antivirus, firewalls y sistemas de detección de intrusiones (IDS).
4. **Copias de Seguridad**: Realizar copias de seguridad regulares y almacenarlas en ubicaciones seguras y desconectadas de la red.

5. **Restricción de Macros**: Configurar las aplicaciones de Office para deshabilitar macros de forma predeterminada y permitirlas solo cuando sea absolutamente necesario.

9.3.9 W32/Crysis.W!tr.ransom

El ransomware Crysis (también conocido como Dharma) es operado por un grupo de cibercriminales que se especializan en ataques de ransomware dirigidos a organizaciones de diversos sectores. Este grupo es conocido por sus técnicas de distribución agresivas y su capacidad para actualizar rápidamente sus herramientas para evadir las defensas de seguridad.

9.3.9.1 Sistemas Operativos Objetivo

W32/Crysis.W!tr.ransom está diseñado para infectar sistemas operativos Windows. Puede comprometer una amplia gama de versiones de Windows, desde las más antiguas hasta las más recientes, aprovechando debilidades en la configuración de seguridad y prácticas operativas inadecuadas.

9.3.9.2 Vulnerabilidades

El ransomware Crysis/Dharma típicamente no se basa en vulnerabilidades específicas del sistema operativo para propagarse. En cambio, utiliza una variedad de vectores de ataque, incluyendo:

- **Correos Electrónicos de Phishing**: Con archivos adjuntos maliciosos o enlaces que descargan el ransomware.
- **Protocolo de Escritorio Remoto (RDP)**: Los atacantes escanean en busca de sistemas con RDP habilitado y utilizan técnicas de fuerza bruta para obtener acceso.
- **Explotación de Servicios y Software Sin Parches**: Aprovechando aplicaciones y servicios desactualizados y sin parches.

9.3.9.3 Sector de Industria

Crysis/Dharma ha afectado a una amplia gama de sectores industriales, incluyendo pero no limitado a:

- Salud
- Educación
- Finanzas
- Gobierno
- Manufactura
- Pequeñas y medianas empresas

9.3.9.4 Historia

Crysis apareció por primera vez en 2016 y rápidamente ganó notoriedad debido a su efectividad y la rapidez con la que los operadores actualizan sus técnicas y variantes. Ha evolucionado en múltiples versiones, siendo una de las familias de ransomware más persistentes y difíciles de

erradicar. Se destaca por su capacidad para cifrar una amplia gama de tipos de archivos y por su uso de algoritmos de cifrado robustos como AES y RSA.

9.3.9.5 Relaciones

Crysis/Dharma ha mostrado conexiones con otras familias de ransomware y herramientas de cibercrimen. Su código y métodos de distribución han sido comparados con otros ransomware como Locky y Cerber, y ha compartido técnicas comunes utilizadas por grupos de cibercriminales que operan en foros de hacking y la darknet.

9.3.10 Comportamiento Post-Explotación e Impacto

Una vez que W32/Crysis.W!tr.ransom ha comprometido un sistema, sigue generalmente los siguientes pasos:

1. **Acceso Inicial**: Utiliza técnicas de phishing o fuerza bruta para obtener acceso inicial al sistema.
2. **Descarga y Ejecución del Payload**: El ransomware se descarga y ejecuta, comenzando el proceso de cifrado.
3. **Cifrado de Archivos**: Utiliza algoritmos de cifrado robustos para cifrar una amplia variedad de tipos de archivos en el sistema.
4. **Nota de Rescate**: Deja una nota de rescate en el sistema afectado, generalmente en el escritorio y en cada carpeta con archivos cifrados, instruyendo al usuario sobre cómo pagar el rescate en Bitcoin.
5. **Comunicación con el Servidor C&C**: Puede comunicarse con un servidor de comando y control para enviar información sobre el sistema comprometido y recibir instrucciones adicionales.

9.3.11 Mitigación y Prevención

Para mitigar el riesgo de infecciones por W32/Crysis.W!tr.ransom y otras variantes de ransomware, se recomiendan las siguientes acciones:

1. **Capacitación en Concienciación de Seguridad**: Educar a los empleados sobre los riesgos del phishing y cómo identificar correos electrónicos maliciosos.
2. **Actualización y Parches**: Mantener todos los sistemas operativos y aplicaciones actualizados con los últimos parches de seguridad.
3. **Restricción de RDP**: Deshabilitar RDP si no es necesario y, si es necesario, usar VPNs y autenticación de dos factores.
4. **Uso de Software de Seguridad**: Implementar soluciones de seguridad robustas, como antivirus, firewalls y sistemas de detección de intrusiones (IDS).
5. **Copias de Seguridad**: Realizar copias de seguridad regulares y almacenarlas en ubicaciones seguras y desconectadas de la red.
6. **Segregación de Redes**: Segmentar las redes internas para limitar la propagación del ransomware.

9.3.12 W32/Sodinokibi.N!tr.ransom

Sodinokibi, también conocido como REvil, es operado por un grupo de cibercriminales altamente sofisticados. Este grupo es conocido por utilizar un modelo de Ransomware-as-a-Service (RaaS), donde afiliados pueden utilizar el ransomware a cambio de una parte del rescate pagado. El grupo REvil ha sido muy activo y notorio, llevando a cabo ataques de alto perfil contra grandes corporaciones y organizaciones en todo el mundo.

9.3.12.1 Sistemas Operativos Objetivo

W32/Sodinokibi.N!tr.ransom está diseñado principalmente para infectar sistemas operativos Windows, aunque también puede afectar a sistemas basados en Linux en algunos casos específicos. Los atacantes buscan vulnerabilidades en servidores, estaciones de trabajo y otros dispositivos conectados a la red.

9.3.12.2 Vulnerabilidades

Sodinokibi se propaga utilizando una variedad de métodos, incluyendo:

- **Explotación de Vulnerabilidades de Software**: Como CVE-2019-2725 en Oracle WebLogic y CVE-2019-19781 en Citrix ADC, entre otras.
- **Fuerza Bruta en Servicios RDP**: Los atacantes intentan obtener acceso utilizando credenciales débiles.
- **Campañas de Phishing**: Correos electrónicos con archivos adjuntos maliciosos o enlaces que descargan el ransomware.
- **Kits de Explotación**: Aprovechando vulnerabilidades en navegadores web y plugins no actualizados.

9.3.12.3 Sector de Industria

REvil/Sodinokibi ha afectado a una amplia gama de sectores industriales, incluyendo:

- Servicios Financieros
- Salud
- Educación
- Manufactura
- Tecnología
- Energía
- Gobierno
- Pequeñas y medianas empresas

9.3.12.4 Historia

Sodinokibi apareció por primera vez a principios de 2019 y rápidamente se hizo conocido por sus ataques devastadores y por el alto valor de los rescates exigidos. El grupo detrás de REvil ha demostrado ser muy profesional y organizado, operando como un negocio con un modelo de

afiliación. Los ataques de REvil han incluido tanto el cifrado de datos como la exfiltración y amenaza de publicar datos sensibles si no se paga el rescate.

9.3.12.5 Relaciones

Sodinokibi tiene conexiones con otras familias de ransomware y herramientas de cibercrimen. Se ha especulado que los operadores de REvil podrían tener vínculos con los grupos detrás de GandCrab, otro ransomware notorio. Además, el uso de servicios de RaaS implica una amplia red de afiliados que utilizan y distribuyen el ransomware.

9.3.13 Comportamiento Post-Explotación e Impacto

Una vez que W32/Sodinokibi.N!tr.ransom ha comprometido un sistema, sigue generalmente los siguientes pasos:

1. **Acceso Inicial**: Obtención de acceso a través de RDP, phishing o vulnerabilidades explotadas.
2. **Movilidad Lateral**: Exploración y compromiso de otros sistemas en la red para maximizar el impacto.
3. **Cifrado de Archivos**: Utiliza algoritmos de cifrado robustos como AES-256 combinado con RSA para cifrar archivos críticos.
4. **Exfiltración de Datos**: A menudo, antes de cifrar los datos, el ransomware exfiltra datos sensibles a servidores controlados por los atacantes.
5. **Nota de Rescate**: Deja una nota de rescate en el sistema afectado, instruyendo al usuario sobre cómo pagar el rescate en criptomonedas (generalmente Bitcoin o Monero).
6. **Comunicación con el Servidor C&C**: Puede comunicarse con un servidor de comando y control para recibir instrucciones adicionales y enviar información sobre el sistema comprometido.

9.3.14 Mitigación y Prevención

Para mitigar el riesgo de infecciones por W32/Sodinokibi.N!tr.ransom y otras variantes de ransomware, se recomiendan las siguientes acciones:

1. **Capacitación en Concienciación de Seguridad**: Educar a los empleados sobre los riesgos del phishing y cómo identificar correos electrónicos maliciosos.
2. **Actualización y Parches**: Mantener todos los sistemas operativos y aplicaciones actualizados con los últimos parches de seguridad.
3. **Restricción de RDP**: Deshabilitar RDP si no es necesario y, si es necesario, usar VPNs y autenticación de dos factores.
4. **Uso de Software de Seguridad**: Implementar soluciones de seguridad robustas, como antivirus, firewalls y sistemas de detección de intrusiones (IDS).
5. **Copias de Seguridad**: Realizar copias de seguridad regulares y almacenarlas en ubicaciones seguras y desconectadas de la red.
6. **Segregación de Redes**: Segmentar las redes internas para limitar la propagación del ransomware.

7. **Monitoreo y Detección**: Utilizar herramientas de monitoreo y detección de amenazas para identificar actividades sospechosas.

9.3.15 Impacto

- **Pérdida de Datos**: Los archivos cifrados son inaccesibles sin la clave de descifrado.
- **Interrupción de Operaciones**: La incapacidad de acceder a datos críticos puede interrumpir las operaciones comerciales.
- **Costo Financiero**: Además del posible pago de rescate, hay costos asociados con la recuperación y restauración de sistemas, así como posibles sanciones regulatorias.
- **Daño a la Reputación**: Un ataque exitoso puede dañar la reputación de una organización, afectando la confianza de los clientes y socios.
- **Fuga de Información**: La exfiltración de datos puede llevar a la exposición pública de información confidencial.

9.4 Tabla de TTPS y Mitigaciones de MITRE ATT&CK

Tacticas y Tecnicas de MITRE ATT&CK V15	Description	Mitigacion	Descripcion
TA0043: Reconnaissance	**The adversary is trying to gather information they can use to plan future operations.**	M1056: Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.
T1595: Active Scanning	Adversarios realizan escaneos activos para identificar información sobre los sistemas de la víctima, como servicios abiertos y configuraciones.		
T1595.001: Scanning IP Blocks	El escaneo de bloques de IP consiste en identificar rangos de direcciones IP para encontrar sistemas activos dentro de un rango específico.		
T1595.002: Vulnerability Scanning	Escaneo para detectar vulnerabilidades específicas en los sistemas de la víctima que podrían ser explotadas.		
T1590: Gather Victim Network Information	Recopilación de información sobre la red de la víctima, incluyendo la topología, servicios y configuraciones.		
T1590.002: DNS	Uso del DNS para recolectar información sobre la infraestructura de red de la víctima.		
TA0042: Resource Development	**The adversary is trying to establish resources they can use to support operations.**		
T1583: Acquire Infrastructure	Adquisición de infraestructura necesaria para llevar a cabo ataques, como servidores y dominios.		
T1583.005: Botnet	Creación o adquisición de una botnet para utilizar en ataques distribuidos o de gran escala.		
T1584: Compromise Infrastructure	Compromiso de infraestructuras existentes para su uso en actividades maliciosas.		
T1584.005: Botnet	Utilización de botnets comprometidas para realizar ataques.		
TA0001: Initial Access	**The adversary is trying to get into your network.**	M1048 Application Isolation and Sandboxing M1050 Exploit Protection M1030 Network Segmentation M1026 Privileged Account Management M1051 Update Software M1016 Vulnerability Scanning	Application isolation will limit what other processes and system features the exploited target can access. Web Application Firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application. Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure. Use least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system. Update software regularly by employing patch management for externally exposed applications. Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.(Citation: OWASP Top 10)
T1190: Exploit Public-Facing Application	Explotación de aplicaciones accesibles públicamente para obtener acceso inicial a la red de la víctima.		
T1133: External Remote Services	Abuso de servicios remotos externos para obtener acceso a la red interna de la víctima.	M1042 Disable or Remove Feature or Program M1035 Limit Access to Resource Over Network M1032 Multi-factor Authentication M1030 Network Segmentation	Disable or block remotely available services that may be unnecessary. Limit access to remote services through centrally managed concentrators such as VPNs and other managed remote access systems. Use strong two-factor or multi-factor

			authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials, but be aware of [Multi-Factor Authentication Interception](https://attack.mitre.org/techniques/T1111) techniques for some two-factor authentication implementations. Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls.
T1566: Phishing	Envío de correos electrónicos fraudulentos para engañar a los usuarios y obtener información sensible o acceso.	M1049 Antivirus/Antimalware M1047 Audit M1031 Network Intrusion Prevention M1021 Restrict Web-Based Content M1054 Software Configuration M1017 User Training	Anti-virus can automatically quarantine suspicious files. Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses. Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to block activity. Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk. Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.(Citation: Microsoft Anti Spoofing)(Citation: ACSC Email Spoofing) Users can be trained to identify social engineering techniques and phishing emails.
T1566.001: Spearphishing Attachment	Envío de correos electrónicos con archivos adjuntos maliciosos dirigidos específicamente a individuos u organizaciones.		
T1566.002: Spearphishing Link	Envío de correos electrónicos con enlaces maliciosos diseñados para engañar a los usuarios.		
T1195: Supply Chain Compromise	Compromiso de la cadena de suministro para introducir software o hardware malicioso.	M1013 Application Developer Guidance M1046 Boot Integrity M1033 Limit Software Installation M1051 Update Software M1016 Vulnerability Scanning	Application developers should be cautious when selecting third-party libraries to integrate into their application. Additionally, where possible, developers should lock software dependencies to specific versions rather than pulling the latest version on build.(Citation: Cider Security Top 10 CICD Security Risks) Use secure methods to boot a system and verify the integrity of the operating system and loading mechanisms. Where possible, consider requiring developers to pull from internal repositories containing verified and approved packages rather than from external ones.(Citation: Cider Security Top 10 CICD Security Risks) A patch management process should be implemented to check unused dependencies, unmaintained and/or previously vulnerable dependencies, unnecessary features, components, files, and documentation. Continuous monitoring of vulnerability sources and the use of automatic and manual code review tools should also be implemented as well.(Citation: OWASP Top 10)
T1195.002: Compromise Software Supply Chain	Compromiso de la cadena de suministro de software para insertar código malicioso en aplicaciones legítimas.		
T1078: Valid Accounts	Uso de cuentas válidas y legítimas para acceder a la red de la víctima.	M1036 Account Use Policies M1015 Active Directory Configuration M1013 Application Developer Guidance M1027 Password Policies M1026 Privileged Account Management M1018 User Account Management M1017 User Training	Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges.(Citation: Microsoft Common Conditional Access Policies) Disable legacy authentication, which does not support MFA, and require the use of modern authentication protocols instead. Ensure that applications do not store sensitive data or credentials insecurely. (e.g. plaintext credentials in code, published credentials in repositories, or credentials in public cloud storage). "Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment.(Citation: US-CERT Alert TA13-175A Risks of Default Passwords on the Internet) When possible, applications that use SSH keys should be updated periodically and properly secured. Policies should minimize (if not eliminate) reuse of passwords between different user accounts, especially employees using the same credentials for personal accounts that may not be defended by enterprise security resources." Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account. (Citation: TechNet Credential Theft) (Citation: TechNet Least Privilege) These audits should also
T1078.001: Default Accounts	Explotación de cuentas predeterminadas que no han sido deshabilitadas o modificadas.		

			include if default accounts have been enabled, or if new local accounts are created that have not be authorized. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers. (Citation: Microsoft Securing Privileged Access) Regularly audit user accounts for activity and deactivate or remove any that are no longer needed. Applications may send push notifications to verify a login as a form of multi-factor authentication (MFA). Train users to only accept valid push notifications and to report suspicious push notifications.
TA0002: Execution	**The adversary is trying to run malicious code.**	M1047 Audit M1040 Behavior Prevention on Endpoint M1045 Code Signing M1038 Execution Prevention M1031 Network Intrusion Prevention M1021 Restrict Web-Based Content M1017 User Training M1048 Application Isolation and Sandboxing M1050 Exploit Protection	Audit images deployed within the environment to ensure they do not contain any malicious components. On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent executable files from running unless they meet a prevalence, age, or trusted list criteria and to prevent Office applications from creating potentially malicious executable content by blocking malicious code from being written to disk. Note: cloud-delivered protection must be enabled to use certain rules. (Citation: win10_asr) Utilize a trust model such as Docker Content Trust with digital signatures to ensure runtime verification of the integrity and publisher of specific image tags.(Citation: Content trust in Docker)(Citation: Content trust in Azure Container Registry) Application control may be able to prevent the running of executables masquerading as other files. Network prevention intrusion systems and systems designed to scan and remove malicious downloads can be used to block activity. If a link is being visited by a user, block unknown or unused files in transit by default that should not be downloaded or by policy from suspicious sites as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some download scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious files. Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events.
T1203: Exploitation for Client Execution	Explotación de vulnerabilidades en software cliente para ejecutar código malicioso.		
T1204: User Execution	Ejecutar código malicioso convenciendo a los usuarios para que lo hagan.		
T1204.002: Malicious File	Uso de archivos maliciosos que los usuarios ejecutan sin darse cuenta.		
T1204.001: Malicious Link	Enlaces maliciosos que llevan a los usuarios a ejecutar código malicioso.		
TA0006: Credential Access	**The adversary is trying to steal account names and passwords.**	M1032 Multi-factor Authentication M1027 Password Policies M1051 Update Software M1018 User Account Management	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services. Refer to NIST guidelines when creating password policies. (Citation: NIST 800-63-3) Upgrade management services to the latest supported and compatible version. Specifically, any version providing increased password complexity or policy enforcement preventing default or weak passwords. Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts.
T1110: Brute Force	Intentos de fuerza bruta para adivinar contraseñas y obtener acceso a cuenta		
T1110.001: Password Guessing	Adivinanza de contraseñas utilizando técnicas de fuerza bruta.		
TA0011: Command and Control	**The adversary is trying to communicate with compromised systems to control them.**	M1031 Network Intrusion Prevention M1031 Network Intrusion Prevention	Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic. Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level.
T1071: Application Layer Protocol	Uso de protocolos de capa de aplicación para comunicarse con infraestructura de comando y control (C2).		
T1071.001: Web Protocols	Uso de protocolos web para establecer comunicaciones C2. (HTTP o HTTPS)		
TA0010: Exfiltration	**The adversary is trying to steal data.**	M1057 Data Loss Prevention M1031 Network Intrusion Prevention	Data loss prevention can detect and block sensitive data being sent over unencrypted protocols. Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools. (Citation: University of Birmingham C2)
T1041: Exfiltration Over C2 Channel	Exfiltración de datos utilizando canales de comando y control.		
TA0040: Impact	**The adversary is trying to manipulate, interrupt, or destroy your systems and data.**		

T1531: Account Access Removal	Eliminación del acceso a cuentas legítimas para interrumpir las operaciones de la víctima.	N/A	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
T1485: Data Destruction	Destrucción de datos para interrumpir la disponibilidad y la integridad de la información.	M1053 Data Backup	Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.(Citation: Ready.gov IT DRP) Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.
T1486: Data Encrypted for Impact	Cifrado de datos para causar un impacto, como en ataques de ransomware.	M1040 Behavior Prevention on Endpoint M1053 Data Backup	On Windows 10, enable cloud-delivered protection and Attack Surface Reduction (ASR) rules to block the execution of files that resemble ransomware. (Citation: win10_asr)
T1565: Data Manipulation	Manipulación de datos para causar daño o confusión.	M1041 Encrypt Sensitive Information M1030 Network Segmentation M1029 Remote Data Storage M1022 Restrict File and Directory Permissions	Consider encrypting important information to reduce an adversary's ability to perform tailored data modifications. Identify critical business and system processes that may be targeted by adversaries and work to isolate and secure those systems against unauthorized access and tampering. Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.(Citation: Ready.gov IT DRP) Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and manipulate backups. Ensure least privilege principles are applied to important information resources to reduce exposure to data manipulation risk.
T1565.001: Stored Data Manipulation	Manipulación de datos almacenados para alterar la integridad de la información.		
T1491: Defacement	Desfiguración de sitios web para dañar la reputación de la víctima.	M1053 Data Backup	Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.(Citation: Ready.gov IT DRP) Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.
T1491.002: External Defacement	Desfiguración de sitios web externos para causar un impacto visual y reputacional.		
T1561: Disk Wipe	Borrado de discos para destruir datos y causar interrupciones.		
T1499: Endpoint Denial of Service	Ataques de denegación de servicio dirigidos a puntos finales para interrumpir su funcionamiento.	M1037 Filter Network Traffic	Leverage services provided by Content Delivery Networks (CDN) or providers specializing in DoS mitigations to filter traffic upstream from services.(Citation: CERT-EU DDoS March 2017) Filter boundary traffic by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport. When flood volumes exceed the capacity of the network connection being targeted, it is typically necessary to intercept the incoming traffic upstream to filter out the attack traffic from the legitimate traffic. Such defenses can be provided by the hosting Internet Service Provider (ISP) or by a 3rd party such as a Content Delivery Network (CDN) or providers specializing in DoS mitigations.(Citation: CERT-EU DDoS March 2017) Depending on flood volume, on-premises filtering may be possible by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.(Citation: CERT-EU DDoS March 2017) As immediate response may require rapid engagement of 3rd parties, analyze the risk associated to critical resources being affected by Network DoS attacks and create a disaster recovery plan/business continuity plan to respond to incidents.(Citation: CERT-EU DDoS March 2017)
T1498: Network Denial of Service	Denegación de servicio a nivel de red para interrumpir el acceso y la disponibilidad de servicios.		
T1498.002: Reflection Amplification	Uso de técnicas de amplificación de reflexión para lanzar ataques de denegación de servicio.		
T1496: Resource Hijacking	Secuestro de recursos para utilizarlos en actividades maliciosas, como el minado de criptomonedas.	N/A	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
T1489: Service Stop	Detención de servicios críticos para causar interrupciones.	M1030 Network Segmentation M1022 Restrict File and Directory Permissions M1024 Restrict Registry Permissions M1018 User Account Management	Operate intrusion detection, analysis, and response systems on a separate network from the production environment to lessen the chances that an adversary can see and interfere with critical response functions. Ensure proper process and file permissions are in place to inhibit adversaries from disabling or interfering with critical services. Ensure proper registry permissions are in place to inhibit adversaries from disabling or interfering with critical services. Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations.
T1529: System Shutdown/Reboot	Apagado o reinicio de sistemas para interrumpir las operaciones.	N/A	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
T1657: Financial Theft	Robo financiero a través de la manipulación de sistemas y transacciones.	M1018 User Account Management M1017 User Training	Limit access/authority to execute sensitive transactions, and switch to systems and procedures designed to authenticate/approve

			payments and purchase requests outside of insecure communication lines such as email. Train and encourage users to identify social engineering techniques used to enable financial theft. Also consider training users on procedures to prevent and respond to swatting and doxing, acts increasingly deployed by financially motivated groups to further coerce victims into satisfying ransom/extortion demands.(Citation: Cyber Safety Review Board: Lapsus)(Citation: SWAT-hospital)

9.5 Tabla de TTPS y Mitigaciones de MITRE D3FEND

ATT&CK ID	ATT&CK Name	Related D3FEND Techniques					
T1595	Active Scanning	no defensive relations yet					
T1595.001	Scanning IP Blocks						
T1595.002	Vulnerability Scanning						
T1590	Gather Victim Network Information						
T1590.002	DNS						
T1583	Acquire Infrastructure						
T1583.005	Botnet						
T1584	Compromise Infrastructure						
T1584.005	Botnet						
T1190	Exploit Public-Facing Application	produces	Inbound Internet Network Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		produces	Inbound Internet Network Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		produces	Inbound Internet Network Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		produces	Inbound Internet Network Traffic	Detect	Inbound Session Volume Analysis	analyzes	Inbound Internet Network Traffic
		produces	Inbound Internet Network Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		produces	Inbound Internet Network Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		produces	Inbound Internet Network Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		produces	Inbound Internet Network Traffic	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		modifies	Process Segment	Harden	Process Segment Execution Prevention	neutralizes	Process Segment
		modifies	Process Segment	Harden	Segment Address Offset Randomization	obfuscates	Process Segment
		injects	Database Query	Detect	Database Query String Analysis	analyzes	Database Query
		produces	Inbound Internet Network Traffic	Isolate	Network Traffic Filtering	filters	Network Traffic
		produces	Inbound Internet Network Traffic	Isolate	Inbound Traffic Filtering	filters	Inbound Network Traffic
T1133	External Remote Services	produces	Authentication	Detect	Resource Access Pattern Analysis	analyzes	Authentication
		produces	Authentication	Detect	Session Duration Analysis	analyzes	Authentication
		produces	Authentication	Detect	Authentication Event Thresholding	analyzes	Authentication
		produces	Network Session	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		produces	Authorization	Detect	Job Function Access Pattern Analysis	analyzes	Authorization

		produces	Authorization	Detect	Authorization Event Thresholding	analyzes	Authorization
		produces	Network Session	Isolate	Network Traffic Filtering	filters	Network Traffic
		produces	Network Session	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		produces	Network Session	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		produces	Network Session	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		produces	Network Session	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		produces	Network Session	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		produces	Network Session	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
T1566	Phishing	produces	File	Deceive	Decoy File	spoofs	File
		produces	Email	Detect	Emulated File Analysis	analyzes	Document File
		produces	Email	Detect	Dynamic Analysis	analyzes	Document File
		produces	Inbound Internet Mail Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Inbound Session Volume Analysis	analyzes	Inbound Internet Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		produces	URL	Detect	URL Analysis	analyzes	URL
		produces	URL	Detect	Identifier Activity Analysis	analyzes	Identifier
		produces	Email	Detect	Homoglyph Detection	analyzes	Email
		produces	Inbound Internet Mail Traffic	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		produces	Email	Detect	Sender Reputation Analysis	analyzes	Email
		produces	Email	Detect	Sender MTA Reputation Analysis	analyzes	Email
		produces	File	Detect	File Integrity Monitoring	analyzes	File
		produces	Email	Evict	File Removal	deletes	File
		produces	Email	Harden	File Encryption	encrypts	File
		produces	File	Harden	Local File Permissions	restricts	File
		produces	Email	Model	Data Inventory	inventories	Document File
		produces	Inbound Internet Mail Traffic	Isolate	Network Traffic Filtering	filters	Network Traffic
		produces	File	Restore	Restore File	restores	File
		produces	File	Detect	File Analysis	analyzes	File
		produces	URL	Detect	URL Reputation Analysis	analyzes	URL
		produces	Email	Evict	Email Removal	deletes	Email
		produces	Inbound Internet Mail Traffic	Isolate	Inbound Traffic Filtering	filters	Inbound Network Traffic
		produces	Email	Isolate	Email Filtering	filters	Email
		produces	Email	Restore	Restore Email	restores	Email
T1566.001	Spearphishing Attachment	produces	Email	Detect	Emulated File Analysis	analyzes	Document File
		produces	Email	Detect	Dynamic Analysis	analyzes	Document File
		produces	Email	Deceive	Decoy File	spoofs	File
		produces	Inbound Internet Mail Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic

		produces	Inbound Internet Mail Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Inbound Session Volume Analysis	analyzes	Inbound Internet Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		produces	Email	Detect	File Integrity Monitoring	analyzes	File
		produces	Email	Detect	Homoglyph Detection	analyzes	Email
		produces	Email	Detect	Sender MTA Reputation Analysis	analyzes	Email
		produces	Email	Detect	Sender Reputation Analysis	analyzes	Email
		produces	Inbound Internet Mail Traffic	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		produces	Email	Harden	Local File Permissions	restricts	File
		produces	Email	Harden	File Encryption	encrypts	File
		produces	Inbound Internet Mail Traffic	Isolate	Network Traffic Filtering	filters	Network Traffic
		produces	Email	Evict	File Removal	deletes	File
		produces	Email	Model	Data Inventory	inventories	Document File
		produces	Email	Restore	Restore File	restores	File
		produces	Email	Detect	File Analysis	analyzes	File
		produces	Inbound Internet Mail Traffic	Isolate	Inbound Traffic Filtering	filters	Inbound Network Traffic
		produces	Email	Restore	Restore Email	restores	Email
		produces	Email	Evict	Email Removal	deletes	Email
		produces	Email	Isolate	Email Filtering	filters	Email
T1566.002	Spearphishing Link	produces	Email	Deceive	Decoy File	spoofs	File
		produces	Email	Detect	Dynamic Analysis	analyzes	Document File
		produces	Email	Detect	Emulated File Analysis	analyzes	Document File
		produces	Inbound Internet Mail Traffic	Detect	Inbound Session Volume Analysis	analyzes	Inbound Internet Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		produces	Inbound Internet Mail Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		produces	URL	Detect	Homoglyph Detection	analyzes	URL
		produces	URL	Detect	URL Analysis	analyzes	URL
		produces	URL	Detect	Identifier Activity Analysis	analyzes	Identifier
		produces	Email	Detect	Sender Reputation Analysis	analyzes	Email
		produces	Email	Detect	Sender MTA Reputation Analysis	analyzes	Email
		produces	Inbound Internet Mail Traffic	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		produces	Email	Detect	File Integrity Monitoring	analyzes	File
		produces	Email	Evict	File Removal	deletes	File
		produces	Email	Harden	File Encryption	encrypts	File

		produces	Email	Harden	Local File Permissions	restricts	File
		produces	Inbound Internet Mail Traffic	Isolate	Network Traffic Filtering	filters	Network Traffic
		produces	Email	Model	Data Inventory	inventories	Document File
		produces	Email	Detect	File Analysis	analyzes	File
		produces	Email	Restore	Restore File	restores	File
		produces	URL	Detect	URL Reputation Analysis	analyzes	URL
		produces	Email	Evict	Email Removal	deletes	Email
		produces	Email	Restore	Restore Email	restores	Email
		produces	Inbound Internet Mail Traffic	Isolate	Inbound Traffic Filtering	filters	Inbound Network Traffic
		produces	Email	Isolate	Email Filtering	filters	Email
T1195	Supply Chain Compromise	modifies	Software	Model	Software Inventory	inventories	Software
		modifies	Software	Model	Asset Vulnerability Enumeration	evaluates	Software
		modifies	Hardware Device	Model	Hardware Component Inventory	inventories	Hardware Device
		modifies	Software	Restore	Restore Software	restores	Software
		modifies	Software	Harden	Software Update	updates	Software
T1195.002	Compromise Software Supply Chain	modifies	Software	Harden	Software Update	updates	Software
		modifies	Software	Model	Software Inventory	inventories	Software
		modifies	Software	Model	Asset Vulnerability Enumeration	evaluates	Software
		modifies	Software	Restore	Restore Software	restores	Software
T1078	Valid Accounts	produces	Authentication	Detect	Authentication Event Thresholding	analyzes	Authentication
		produces	Authorization	Detect	Authorization Event Thresholding	analyzes	Authorization
		produces	Authentication	Detect	Session Duration Analysis	analyzes	Authentication
		uses	Domain User Account	Detect	Domain Account Monitoring	monitors	Domain User Account
		produces	Authorization	Detect	Job Function Access Pattern Analysis	analyzes	Authorization
		produces	Authorization	Detect	Resource Access Pattern Analysis	analyzes	Authorization
		uses	Local User Account	Detect	Local Account Monitoring	analyzes	Local User Account
		uses	User Account	Evict	Account Locking	disables	User Account
		uses	Domain User Account	Harden	Biometric Authentication	authenticates	User Account
		uses	User Account	Harden	Multi-factor Authentication	authenticates	User Account
		uses	Domain User Account	Harden	Strong Password Policy	strengthens	User Account
		uses	User Account	Harden	User Account Permissions	restricts	User Account
		uses	Domain User Account	Harden	One-time Password	authenticates	User Account
		uses	Local User Account	Model	Access Modeling	maps	User Account
		uses	Cloud User Account	Restore	Restore User Account Access	restores	User Account
		uses	Domain User Account	Restore	Unlock Account	restores	User Account
T1078.001	Default Accounts	produces	Authentication	Detect	Authentication Event Thresholding	analyzes	Authentication
		produces	Authorization	Detect	Authorization Event Thresholding	analyzes	Authorization
		produces	Authorization	Detect	Job Function Access Pattern Analysis	analyzes	Authorization
		produces	Authentication	Detect	Resource Access Pattern Analysis	analyzes	Authentication
		produces	Authentication	Detect	Session Duration Analysis	analyzes	Authentication
		uses	User Account	Harden	One-time Password	authenticates	User Account

		uses	User Account	Harden	Strong Password Policy	strengthens	User Account
		uses	User Account	Harden	User Account Permissions	restricts	User Account
		uses	User Account	Harden	Biometric Authentication	authenticates	User Account
		uses	User Account	Harden	Multi-factor Authentication	authenticates	User Account
		uses	User Account	Evict	Account Locking	disables	User Account
		uses	User Account	Model	Access Modeling	maps	User Account
		uses	User Account	Restore	Restore User Account Access	restores	User Account
		uses	User Account	Restore	Unlock Account	restores	User Account
T1203	Exploitation for Client Execution	modifies	Process Code Segment	Detect	Process Code Segment Verification	verifies	Process Code Segment
		modifies	Stack Frame	Detect	Shadow Stack Comparisons	analyzes	Stack Frame
		modifies	Process Code Segment	Harden	Process Segment Execution Prevention	neutralizes	Process Segment
		modifies	Process Code Segment	Harden	Segment Address Offset Randomization	obfuscates	Process Segment
		modifies	Stack Frame	Harden	Stack Frame Canary Validation	validates	Stack Frame
		modifies	Process Code Segment	Detect	Memory Boundary Tracking	analyzes	Process Code Segment
T1204	User Execution	produces	Outbound Internet Web Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Relay Pattern Analysis	analyzes	Outbound Internet Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		executes	Executable File	Detect	Emulated File Analysis	analyzes	Executable File
		executes	Executable File	Detect	Dynamic Analysis	analyzes	Executable File
		executes	Executable File	Deceive	Decoy File	spoofs	File
		accesses	URL	Detect	URL Analysis	analyzes	URL
		accesses	URL	Detect	Identifier Activity Analysis	analyzes	Identifier
		accesses	URL	Detect	Homoglyph Detection	analyzes	URL
		executes	Executable File	Detect	File Integrity Monitoring	analyzes	File
		produces	Outbound Internet Web Traffic	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		executes	Executable File	Harden	File Encryption	encrypts	File
		executes	Executable File	Harden	Local File Permissions	restricts	File
		executes	Executable File	Evict	File Removal	deletes	File
		executes	Executable File	Isolate	Executable Allowlisting	blocks	Executable File
		executes	Executable File	Isolate	Executable Denylisting	blocks	Executable File
		produces	Outbound Internet Web Traffic	Isolate	Network Traffic Filtering	filters	Network Traffic
		executes	Executable File	Restore	Restore File	restores	File
		executes	Executable File	Detect	File Analysis	analyzes	File
		accesses	URL	Detect	URL Reputation Analysis	analyzes	URL
		produces	Outbound Internet Web Traffic	Isolate	Outbound Traffic Filtering	filters	Outbound Network Traffic
T1204.002	Malicious File	executes	Executable File	Harden	File Encryption	encrypts	File
		executes	Executable File	Harden	Local File Permissions	restricts	File

		executes	Executable File	Isolate	Executable Allowlisting	blocks	Executable File
		executes	Executable File	Isolate	Executable Denylisting	blocks	Executable File
		executes	Executable File	Detect	File Integrity Monitoring	analyzes	File
		executes	Executable File	Evict	File Removal	deletes	File
		executes	Executable File	Restore	Restore File	restores	File
		executes	Executable File	Detect	Emulated File Analysis	analyzes	Executable File
		executes	Executable File	Detect	Dynamic Analysis	analyzes	Executable File
		executes	Executable File	Deceive	Decoy File	spoofs	File
		executes	Executable File	Detect	File Analysis	analyzes	File
T1204.001	Malicious Link	produces	Outbound Internet Web Traffic	Detect	Relay Pattern Analysis	analyzes	Outbound Internet Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		accesses	URL	Detect	Identifier Activity Analysis	analyzes	Identifier
		accesses	URL	Detect	Homoglyph Detection	analyzes	URL
		accesses	URL	Detect	URL Analysis	analyzes	URL
		produces	Outbound Internet Web Traffic	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Isolate	Network Traffic Filtering	filters	Network Traffic
		accesses	URL	Detect	URL Reputation Analysis	analyzes	URL
		produces	Outbound Internet Web Traffic	Isolate	Outbound Traffic Filtering	filters	Outbound Network Traffic
T1110	Brute Force	may-create	Intranet Administrative Network Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		may-create	Intranet Administrative Network Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		may-create	Intranet Administrative Network Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		accesses	Password	Deceive	Decoy User Credential	spoofs	Credential
		may-create	Intranet Administrative Network Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		may-create	Intranet Administrative Network Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		may-create	Intranet Administrative Network Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		may-create	Intranet Administrative Network Traffic	Detect	Administrative Network Activity Analysis	analyzes	Intranet Administrative Network Traffic
		may-create	Intranet Administrative Network Traffic	Detect	Connection Attempt Analysis	analyzes	Intranet Network Traffic
		produces	Authentication	Detect	Resource Access Pattern Analysis	analyzes	Authentication
		produces	Authentication	Detect	Session Duration Analysis	analyzes	Authentication
		may-create	Intranet Administrative Network Traffic	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		accesses	Password	Detect	Credential Compromise Scope Analysis	analyzes	Credential
		produces	Authentication	Detect	Authentication Event Thresholding	analyzes	Authentication
		accesses	Password	Evict	Credential Revoking	deletes	Credential
		accesses	Password	Evict	Authentication Cache Invalidation	deletes	Credential
		accesses	Password	Harden	One-time Password	use-limits	Password
		accesses	Password	Harden	Strong Password Policy	strengthens	Password

		accesses	Password	Harden	Credential Transmission Scoping	restricts	Credential
		accesses	Password	Harden	Credential Rotation	regenerates	Credential
		may-create	Intranet Administrative Network Traffic	Isolate	Network Traffic Filtering	filters	Network Traffic
		accesses	Password	Restore	Reissue Credential	restores	Credential
T1110.001	Password Guessing	accesses	Password	Deceive	Decoy User Credential	spoofs	Credential
		produces	Authentication	Detect	Authentication Event Thresholding	analyzes	Authentication
		accesses	Password	Detect	Credential Compromise Scope Analysis	analyzes	Credential
		produces	Authentication	Detect	Resource Access Pattern Analysis	analyzes	Authentication
		accesses	Password	Harden	Credential Rotation	regenerates	Credential
		accesses	Password	Harden	Credential Transmission Scoping	restricts	Credential
		accesses	Password	Restore	Reissue Credential	restores	Credential
		accesses	Password	Harden	One-time Password	use-limits	Password
		accesses	Password	Harden	Strong Password Policy	strengthens	Password
		produces	Authentication	Detect	Session Duration Analysis	analyzes	Authentication
		accesses	Password	Evict	Authentication Cache Invalidation	deletes	Credential
		accesses	Password	Evict	Credential Revoking	deletes	Credential
T1071	Application Layer Protocol	produces	Outbound Internet Network Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Relay Pattern Analysis	analyzes	Outbound Internet Network Traffic
		produces	Outbound Internet File Transfer Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		produces	Outbound Internet File Transfer Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		may-transfer	Certificate File	Detect	Certificate Analysis	analyzes	Certificate File
		produces	Outbound Internet File Transfer Traffic	Detect	File Carving	analyzes	File Transfer Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		produces	Outbound Internet DNS Lookup Traffic	Detect	DNS Traffic Analysis	analyzes	Outbound Internet DNS Lookup Traffic
		produces	Outbound Internet DNS Lookup Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		produces	Outbound Internet Mail Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		may-transfer	Certificate File	Deceive	Decoy File	spoofs	File
		may-transfer	Certificate File	Detect	File Integrity Monitoring	analyzes	File
		produces	Outbound Internet File Transfer Traffic	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		may-transfer	Certificate File	Harden	Local File Permissions	restricts	File
		may-transfer	Certificate File	Evict	File Removal	deletes	File
		may-transfer	Certificate File	Harden	File Encryption	encrypts	File
		produces	Outbound Internet DNS Lookup Traffic	Isolate	DNS Allowlisting	blocks	Outbound Internet DNS Lookup Traffic
		produces	Outbound Internet Web Traffic	Isolate	Network Traffic Filtering	filters	Network Traffic
		produces	Outbound Internet DNS Lookup Traffic	Isolate	DNS Denylisting	blocks	DNS Network Traffic
		may-transfer	Certificate File	Restore	Restore File	restores	File
		may-transfer	Certificate File	Detect	File Analysis	analyzes	File
		produces	Outbound Internet Network Traffic	Isolate	Outbound Traffic Filtering	filters	Outbound Network Traffic
		produces	Outbound Internet DNS Lookup Traffic	Isolate	Forward Resolution Domain Denylisting	blocks	Outbound Internet DNS Lookup Traffic
		produces	Outbound Internet DNS Lookup Traffic	Isolate	Reverse Resolution IP Denylisting	blocks	Outbound Internet DNS Lookup Traffic
T1071.001	Web Protocols	produces	Outbound Internet Web Traffic	Detect	Relay Pattern Analysis	analyzes	Outbound Internet Network Traffic

		produces	Outbound Internet Web Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		may-transfer	Certificate File	Detect	Certificate Analysis	analyzes	Certificate File
		produces	Outbound Internet Web Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		may-transfer	Certificate File	Deceive	Decoy File	spoofs	File
		may-transfer	Certificate File	Detect	File Analysis	analyzes	File
		produces	Outbound Internet Web Traffic	Isolate	Outbound Traffic Filtering	filters	Outbound Network Traffic
		may-transfer	Certificate File	Harden	Local File Permissions	restricts	File
		may-transfer	Certificate File	Harden	File Encryption	encrypts	File
		produces	Outbound Internet Web Traffic	Isolate	Network Traffic Filtering	filters	Network Traffic
		produces	Outbound Internet Web Traffic	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		may-transfer	Certificate File	Detect	File Integrity Monitoring	analyzes	File
		may-transfer	Certificate File	Evict	File Removal	deletes	File
		may-transfer	Certificate File	Restore	Restore File	restores	File
T1041	Exfiltration Over C2 Channel	may-transfer	Certificate File	Deceive	Decoy File	spoofs	File
		may-transfer	Certificate File	Detect	Certificate Analysis	analyzes	Certificate File
		produces	Internet Network Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		produces	Internet Network Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		produces	Internet Network Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		produces	Internet Network Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		produces	Internet Network Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		produces	Internet Network Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		produces	Internet Network Traffic	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		may-transfer	Certificate File	Evict	File Removal	deletes	File
		may-transfer	Certificate File	Harden	Local File Permissions	restricts	File
		may-transfer	Certificate File	Harden	File Encryption	encrypts	File
		may-transfer	Certificate File	Detect	File Integrity Monitoring	analyzes	File
		produces	Internet Network Traffic	Isolate	Network Traffic Filtering	filters	Network Traffic
		may-transfer	Certificate File	Restore	Restore File	restores	File
		may-transfer	Certificate File	Detect	File Analysis	analyzes	File
T1531	Account Access Removal	modifies	User Account	Evict	Account Locking	disables	User Account
		modifies	User Account	Restore	Unlock Account	restores	User Account
		modifies	User Account	Harden	Strong Password Policy	strengthens	User Account
		modifies	User Account	Harden	User Account Permissions	restricts	User Account
		modifies	User Account	Harden	One-time Password	authenticates	User Account
		modifies	User Account	Harden	Biometric Authentication	authenticates	User Account
		modifies	User Account	Harden	Multi-factor Authentication	authenticates	User Account
		modifies	User Account	Model	Access Modeling	maps	User Account

		modifies	User Account	Restore	Restore User Account Access	restores	User Account
T1485	Data Destruction	no defensive relations yet					
T1486	Data Encrypted for Impact	no defensive relations yet					
T1565	Data Manipulation	may-modify	Network Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		may-modify	Network Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		may-modify	Network Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		may-modify	Network Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		may-modify	Executable File	Detect	Emulated File Analysis	analyzes	Executable File
		may-modify	Executable File	Detect	Dynamic Analysis	analyzes	Executable File
		may-modify	Executable File	Deceive	Decoy File	spoofs	File
		may-modify	Network Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		may-modify	Network Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		modifies	File	Detect	File Integrity Monitoring	analyzes	File
		may-modify	Network Traffic	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		may-modify	Executable File	Evict	File Removal	deletes	File
		modifies	File	Harden	File Encryption	encrypts	File
		modifies	File	Harden	Local File Permissions	restricts	File
		may-modify	Executable File	Isolate	Executable Allowlisting	blocks	Executable File
		may-modify	Executable File	Isolate	Executable Denylisting	blocks	Executable File
		may-modify	Network Traffic	Isolate	Network Traffic Filtering	filters	Network Traffic
		modifies	File	Restore	Restore File	restores	File
		modifies	File	Detect	File Analysis	analyzes	File
T1565.001	Stored Data Manipulation	modifies	File	Deceive	Decoy File	spoofs	File
		modifies	File	Detect	File Integrity Monitoring	analyzes	File
		modifies	File	Evict	File Removal	deletes	File
		modifies	File	Harden	File Encryption	encrypts	File
		modifies	File	Harden	Local File Permissions	restricts	File
		modifies	File	Restore	Restore File	restores	File
		modifies	File	Detect	File Analysis	analyzes	File
T1491	Defacement	modifies	Network Resource	Deceive	Decoy Network Resource	spoofs	Network Resource
T1491.002	External Defacement	modifies	Network Resource	Deceive	Decoy Network Resource	spoofs	Network Resource
T1561	Disk Wipe	no defensive relations yet					
T1499	Endpoint Denial of Service						
T1498	Network Denial of Service	creates	Inbound Internet Network Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		creates	Inbound Internet Network Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		creates	Inbound Internet Network Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		creates	Inbound Internet Network Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		creates	Inbound Internet Network Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		creates	Inbound Internet Network Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic

		creates	Inbound Internet Network Traffic	Detect	Inbound Session Volume Analysis	analyzes	Inbound Internet Network Traffic
		creates	Inbound Internet Network Traffic	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		creates	Inbound Internet Network Traffic	Isolate	Network Traffic Filtering	filters	Network Traffic
		creates	Inbound Internet Network Traffic	Isolate	Inbound Traffic Filtering	filters	Inbound Network Traffic
T1498.002	Reflection Amplification	produces	Inbound Internet Network Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic
		produces	Inbound Internet Network Traffic	Detect	Inbound Session Volume Analysis	analyzes	Inbound Internet Network Traffic
		produces	Inbound Internet Network Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		produces	Inbound Internet Network Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		produces	Inbound Internet Network Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		produces	Inbound Internet Network Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		produces	Inbound Internet Network Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		produces	Inbound Internet Network Traffic	Detect	User Geolocation Logon Pattern Analysis	analyzes	Network Traffic
		produces	Inbound Internet Network Traffic	Isolate	Network Traffic Filtering	filters	Network Traffic
		produces	Inbound Internet Network Traffic	Isolate	Inbound Traffic Filtering	filters	Inbound Network Traffic
T1496	Resource Hijacking	no defensive relations yet					
T1489	Service Stop						
T1529	System Shutdown/Reboot						
T1657	Financial Theft						

10 Trabajos citados

[1] NIST, «COMPUTER SECURITY RESOURCE CENTER,» NIST, [En línea]. Available: https://csrc.nist.gov/glossary/term/cyber_risk. [Último acceso: 19 May 2020].

[2] C. S. F. B. J. T. &. M. D. K. Kruse, «Cybersecurity in healthcare: A systematic review of modern threats and trend,» *Technology and Health Care,* 2017.

[3] D. R. A. Z. W. F. F. L. P. F. X. &. T. J. Wu, «Cybersecurity for digital manufacturing,» *Journal of Manufacturing Systems,* 2018.

[4] A. B. A. Ö. &. R. D. Niaz Kammoun, «Financial market reaction to cyberattacks,» *Cogent Economics & Finance,* 2019.

[5] S. Morgan, «cybersecurity ventures,» 07 Diciembre 2018. [En línea]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[6] W. E. Forum, «World Economic Forum Global Risks Perception Survey 2019–2020,» 2020. [En línea]. Available: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

[7] I. (. D. Corporation)., «The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast,» 2019. [En línea]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[8] Gartner, «Leading the IoT: Gartner Insights on How to Lead in a Connected World.,» 2017. [En línea]. Available: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf.

[9] Z. Doffman, «Cyberattacks on IoT Devices Surge 300% in 2019, 'Measured in Billions', Report Claims",» Forbes, 2019. [En línea]. Available: https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#43ec06af5892.

[10] F-Secure, «ATTACK LANDSCAPE H1 2019,» 2019. [En línea]. Available: https://blog-assets.f-secure.com/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf.

[11] A. Venkat, «Wikipedia Investigates DDoS Attack,» Bankinfosecurity.com, Information Security Media Group (ISMG), 2019 September. [En línea]. Available: https://www.bankinfosecurity.com/wikipedia-investigates-ddos-attack-a-13049.

[12] M. K. S. S. a. P. O. A. O. Almashhadani, «A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware,» *IEEE Access,* vol. 7, 2019.

[13] R. E. T. Landscape, «ENISA Threat Landscape 2020 - Ransomware,» April 2020. [En línea]. Available: https://www.enisa.europa.eu/publications/ransomware. [Último acceso: 27 10 2020].

[14] Gartner, «How Gartner Defines Threat Intelligence,» Gartner, 23 02 2016. [En línea]. Available: https://www.gartner.com/en/documents/3222217/how-gartner-defines-threat-intelligence. [Último acceso: 27 10 2020].

[15] J. Arreola, «Padrón electoral en la nube: ¿ciberproblemas a la mexicana?,» Forbes Mexico, 26 April 2016. [En línea]. Available: https://www.forbes.com.mx/padron-electoral-la-nube-ciberproblemas-la-mexicana/. [Último acceso: 13 May 2020].

[16] A. México, «Comunicado Oficial: Sin afectaciones a datos o recursos de asegurados: AXA,» 23 Octubre 2018. [En línea]. Available: https://axa.mx/web/blog/postura-de-axa-mexico. [Último acceso: 19 May 2020].

[17] R. C. Y. CIBERSEGURIDAD, «gobierno de Mexico,» 2019. [En línea]. Available: https://www.gob.mx/cms/uploads/attachment/file/478193/181.-_Riesgo_Cibern_tico_y_Ciberseguridad_2019.pdf. [Último acceso: 19 May 2020].

[18] P. d. c. e. México, «Comexi,» Junio 2018. [En línea]. Available: https://consejomexicano.org/multimedia/1528987628-817.pdf. [Último acceso: 08 May 2020].

[19] N. Rial, «Mexican hackers attack official sites,» New Europe, 17 September 2012. [En línea]. Available: https://www.neweurope.eu/article/mexican-hackers-attack-official-sites/. [Último acceso: 15 May 2020].

[20] CONDUSEF, «FRAUDES CIBERNÉTICOS TRADICIONALES,» 2020. [En línea]. Available: https://www.condusef.gob.mx/?p=estadisticas. [Último acceso: 18 May 2020].

[21] E. n. d. Ciberseguridad, «Gobierno de Mexico,» 2017. [En línea]. Available: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf. [Último acceso: 23 May 2020].

[22] SEGOB, «ACUERDO por el que se expide la Estrategia Digital Nacional 2021-2024.,» [En línea]. Available: https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gsc.tab=0.

[23] Fortinet, «Fortinet Threat Intelligence,» Fortinet, [En línea]. Available: https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html. [Último acceso: 03 May 2020].

[24] Cisco, «Cisco Cybersecurity Report Series,» Cisco, [En línea]. Available: https://www.cisco.com/c/en/us/products/security/security-reports.html#~more-reports. [Último acceso: 03 May 2020].

[25] Fireeye, «M-Trends 2020,» Fireeye, [En línea]. Available: https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html. [Último acceso: 03 May 2020].

[26] ISO27000, « ISO/IEC 27032:2012 — Information technology — Security techniques — Guidelines for cybersecurity,» ISO/IEC, [En línea]. Available: https://www.iso27001security.com/html/27032.html. [Último acceso: 19 may 2020].

[27] F. C. y. C. Teconologico. [En línea]. Available: http://foroconsultivo.org.mx/. [Último acceso: 08 May 2020].

[28] I. a. d. i. y. t. d. México, «Foro Consultivo Cientifico y Tenologico,» 2018. [En línea]. Available: https://foroconsultivo.org.mx/proyectos_estrategicos/img/8/17.pdf. [Último acceso: 07 May 2020].

[29] F. Staff, «Cibercrimen afecta a uno de cada cuatro mexicanos, según aseguradoras,» forbes Mexico, 05 May 2019. [En línea]. Available: https://www.forbes.com.mx/cibercrimen-afecta-a-uno-de-cada-cuatro-mexicanos-segun-aseguradoras/. [Último acceso: 08 May 2020].

[30] M. A. Mares, «Cibercrimen, la amenaza,» El Economista, 02 Nov 2018. [En línea]. Available: https://www.eleconomista.com.mx/opinion/Cibercrimen-la-amenaza-20181102-0005.html. [Último acceso: 08 May 2020].

[31] G. Chávez, «Conectividad y ransomware agudizan costo del cibercrimen en México,» Expansion mx, 2017. [En línea]. Available: https://expansion.mx/tecnologia/2018/02/09/conectividad-y-ransomware-agudizan-costo-del-cibercrimen-en-mexico. [Último acceso: 08 May 2020].

[32] E. s. C. E. e. M. 2. D. t. entrega, «Asociacion de Internet MX,» Diciembre 2019. [En línea]. Available: https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/Estudio%20de%20Comercio%20Electro%CC%81nico%20en%20Me%CC%81xico%202019.pdf. [Último acceso: 08 May 2020].

[3 3] M. e. e. U. d. I. Mexicano, «15° Estudio sobre los Hábitos de los Usuarios de Internet en México 2018,» 31 Julio 2019. [En línea]. Available: https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/15%2BEstudio%2Bsobre%2Blos%2BHa_bitos%2Bde%2Blos%2BUsuarios%2Bde%2BInternet%2Ben%2BMe_xico%2B2019%2Bversio_n%2Bpu_blica.pdf. [Último acceso: 08 May 2020].

[3 4] G. d. Mexico, «Secretaria de Comunicaciones y Transportes,» [En línea]. Available: https://www.gob.mx/sct. [Último acceso: 12 May 2020].

[3 5] OEA. [En línea]. Available: http://www.oas.org/es/. [Último acceso: 12 May 2020].

[3 6] H. d. l. u. e. c. e. M. 2019, «Gobierno de Mexico,» 2019. [En línea]. Available: https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf. [Último acceso: 12 May 2020].

[3 7] P. Federal, «¿Conoces qué es el Phishing?,» Gobierno de Mexico, 08 Enero 2019. [En línea]. Available: https://www.gob.mx/policiafederal/es/articulos/conoces-que-es-el-phishing?idiom=es. [Último acceso: 12 May 2020].

[3 8] NIST, «NIST Information Technology Laboratory,» NIST, [En línea]. Available: https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary. [Último acceso: 19 May 2020].

[3 9] T. G. R. R. 2020, «The Global Risks Report 2020,» 16 January 2020. [En línea]. Available: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. [Último acceso: 12 May 2020].

[4 0] R. C. M. 2018, «Willis Towers Watson,» 04 December 2018. [En línea]. Available: https://www.willistowerswatson.com/es-MX/Insights/2018/12/riesgo-cibernetico-mexico-2018. [Último acceso: 13 May 2020].

[4 1] Fortinet, «Threat Intelligence Insider Latin America,» Fortinet, 10 april 2020. [En línea]. Available: https://www.fortinetthreatinsiderlat.com/. [Último acceso: 20 May 2020].

[4 2] L. F. D. P. D. D. P. E. P. D. L. PARTICULARES, «http://www.diputados.gob.mx/,» 2010. [En línea]. Available: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. [Último acceso: 23 may 2020].

[4 3] L. G. D. P. D. D. P. E. P. D. S. OBLIGADOS, «http://www.diputados.gob.mx/,» 2017. [En línea]. Available: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf. [Último acceso: 23 May 2020].

[4 4] G. d. Mexico, «¿Has sufrido acoso cibernético? ¡Identifica sus modalidades y protégete!,» [En línea]. Available: https://www.gob.mx/conavim/articulos/has-sufrido-acoso-cibernetico-te-decimos-a-donde-acudir. [Último acceso: 20 May 2020].

[4 5] Excelsior, «Cómo denunciar delitos cibernéticos en México,» Excelsior, 05 May 2019. [En línea]. Available: https://www.excelsior.com.mx/hacker/como-denunciar-delitos-ciberneticos-en-mexico/1311256. [Último acceso: 20 May 2020].

[4 6] S. d. Seguridad, «Unidad de Prevención e Investigación Cibernética,» Gobierno del Estado de México, [En línea]. Available: https://sseguridad.edomex.gob.mx/seguridad-publica-transito/policia-cibernetica. [Último acceso: 21 May 2020].

[4 7] J. L. Covarrubias, «El estatus de México y el Convenio sobre la Ciberdelincuencia de Budapest,» forojuridico, 2020. [En línea]. Available: https://forojuridico.mx/el-estatus-de-mexico-y-el-convenio-sobre-la-ciberdelincuencia-de-budapest/.

[4 8] Senado de la República, 2020.

[4 9] CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, «CÓDIGO PENAL FEDERAL,» Secretaría de Gobernación, Última Reforma DOF 18-10-2023. [En línea]. Available: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf. [Último acceso: 2023].

[5 0] CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, «LEY FEDERAL DE PROTECCIÓN DE DATOS PERSON,» [En línea]. Available: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. [Último acceso: 2023].

[5 1] CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, «LEY GENERAL DE PROTECCIÓN DE DATOS PERSO,» [En línea]. Available: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf.

[5 2] CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, «LEY FEDERAL DE PROTECCIÓN A LA PROPIEDAD INDUSTRIAL,» [En línea]. Available: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPPI.pdf.

[5 3] CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, «LEY DE INSTITUCIONES DE CRÉDITO,» [En línea]. Available: https://www.diputados.gob.mx/LeyesBiblio/pdf/LIC.pdf.

[5 4] Banco de Mexico, «REGLAS DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIO,» [En línea]. Available: https://www.banxico.org.mx/marco-normativo/normativa-emitida-por-el-banco-de-mexico/circular-14-2017/%7BA06FBFEE-06BB-F249-32FC-25B334B2A744%7D.pdf.

[5 5] Comision Nacional Bancaria de Valores, «DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INSTITUCIONES DE CRÉDITO,» Gobierno de Mexico, [En línea]. Available: https://www.cnbv.gob.mx/Normatividad/Disposiciones%20de%20carácter%20general%20aplicables%20a%20las%20instituciones%20de%20crédito.pdf.

[5 6] Secretaria de Goberncion, «DECLARATORIA de vigencia de la Norma Mexicana NMX-COE-001-SCFI-2018.,» 2019. [En línea]. Available: https://www.dof.gob.mx/nota_detalle.php?codigo=5559015&fecha=30/04/2019#gsc.tab=0.

[5 7] Secretaria de Gobernacion, «NOM-151-SCFI-2016,» [En línea]. Available: https://dof.gob.mx/nota_detalle.php?codigo=5478024&fecha=30/03/2017#gsc.tab=0.

[5 8] Secretaria de Gobernacion, «NMX-I-25021-NYCE-2015,» [En línea]. Available: https://www.dof.gob.mx/nota_detalle.php?codigo=5388688&fecha=14/04/2015#gsc.tab=0.

[5 9] R. N. d. I. Financiera, «cnvb.gob.mx,» 2019. [En línea]. Available: https://www.cnbv.gob.mx/Inclusi%C3%B3n/Documents/Reportes%20de%20IF/Reporte%20de%20Inclusion%20Financiera%209.pdf. [Último acceso: 25 May 2020].

[6 0] C. N. B. y. d. Valores, «La CNBV en el Foro sobre Ciberseguridad: “Fortaleciendo la ciberseguridad para la estabilidad del sistema financiero mexicano,» 23 oct 2017. [En línea]. Available: https://www.gob.mx/cnbv/prensa/la-cnbv-en-el-foro-sobre-ciberseguridad-fortaleciendo-la-ciberseguridad-para-la-estabilidad-del-sistema-financiero-mexicano. [Último acceso: 25 May 2020].

[6 1] C. N. B. y. d. Valores, «Foro de Ciberseguridad,» 2017, 2020 23 Oct. [En línea]. Available: https://www.gob.mx/cnbv/articulos/foro-de-ciberseguridad. [Último acceso: 25 May].

[6 2] T. S. O. I. T. C. M. F. SYSTEM, «http://www.oas.org/,» 2019. [En línea]. Available: http://www.oas.org/en/sms/cicte/Documents/reports/The-State-of-Cybersecurity-in-the-Mexican-Financial-system.pdf. [Último acceso: 26 May 2020].

[6 3] Banco de Mexico, «Reporte de Estabilidad Financiera,» 2023.

[6 4] R. McMillan, «Definition: Threat Intelligence,» Gartner Research, 2016 May 2013. [En línea]. Available: https://www.gartner.com/en/documents/2487216/definition-threat-intelligence.

[6 5] 2. S. C. T. I. (. Survey, «https://www.sans.org/,» 2020. [En línea]. Available: https://www.sans.org/reading-room/whitepapers/analyst/2020-cyber-threat-intelligence-cti-survey-39395. [Último acceso: 27 May 2020].

[6 6] D. C. Ahlberg, The Threat Intelligence Handbook, CyberEdge Group, 2019.

[67] D. O. A. C. T. I. FRAMEWORK, «International Journal of Innovative Research in Technology & Science,» Nov 2017. [En línea]. Available: http://ijirts.org/volume5issue6/IJIRTSV5I6013.pdf. [Último acceso: 29 May 2020].

[68] Fortinet, «FortiGuard Labs,» Fortinet, [En línea]. Available: https://fortiguard.com/. [Último acceso: 01 06 2020].

[69] C. systems, «Talos,» Cisco systems, [En línea]. Available: https://talosintelligence.com/. [Último acceso: 01 06 2020].

[70] Fireeye, «Mandiant Threat Intelligence,» Fireeye, [En línea]. Available: https://www.fireeye.com/solutions/cyber-threat-intelligence.html. [Último acceso: 01 06 2020].

[71] Facebook, «ThreatExchange Documentation,» Facebook, [En línea]. Available: https://developers.facebook.com/docs/threat-exchange/v2.12. [Último acceso: 06 01 2020].

[72] P. K. D. ,. V. M. ,. A. J. ,. T. F. Sudip Mittal*, «CyberTwitter: Using Twitter to generate alerts for Cybersecurity Threats and Vulnerabilities,» *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM),* 2016.

[73] G. C. T. I. f. T. U. N. Classification, «Gathering Cyber Threat Intelligence from Twitter Using Novelty Classification,» 2019. [En línea]. Available: https://www.researchgate.net/publication/334223932_Gathering_Cyber_Threat_Intelligence_from_Twitter_Using_Novelty_Classification. [Último acceso: 01 06 2020].

[74] Recorded Future, The Security Intelligence Handbook Third Edition, Annapolis, MD: CyberEdge Group, LLC.

[75] W. Tounsi, «What is Cyber Threat Intelligence and How is it Evolving?,» de *What is Cyber Threat Intelligence and How is it Evolving?*, 2019, p. 49.

[76] A. Ramsdale , S. Shiaeles y N. Kolokotronis, «A Comparative Analysis of Cyber-Threat Intelligence,» MDPI, 2020.

[77] C. Johnson, L. Badger, D. Waltermire, J. Snyder y C. Skorupka, «Guide to Cyber Threat Information Sharing,» NIST, 2016.

[78] M. E. Korstanje, Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities, IGI Global, 2016.

[79] D. Spike E. , A. Tweed, L. Rouse, B. Chu, D. Qi, Y. Hu, J. Yang y E. Al-Shaer, «Strategic Cyber Threat Intelligence Sharing: A Case Study of IDS Logs,» IEEE, Waikoloa, HI, USA, 2016.

[80] D. Chismon y M. Ruks, «Threat Intelligence: Collecting, Analysing, Evaluating,» MWR Infosecurity, 2015.

[81] F. o. I. R. a. S. Teams, «PRIMERA Historia,» [En línea]. Available: https://www.first.org/about/history. [Último acceso: 25 08 2020].

[82] F. o. I. R. a. S. Teams, «Métodos y metodología,» [En línea]. Available: https://www.first.org/global/sigs/cti/curriculum/methods-methodology#:~:text=The%20analysis%20phase%20of%20the,impact%20of%20the%20collected%20data.. [Último acceso: 26 08 2020].

[83] Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Lockheed Martin Corporation, «LM-White-Paper-Intel-Driven-Defense,» [En línea]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf. [Último acceso: 28 08 2020].

[84] SANS, «Leveraging the Human to Break the Cyber Kill Chain,» SANS, 2016. [En línea]. Available: https://www.sans.org/security-awareness-training/blog/leveraging-human-break-cyber-kill-chain. [Último acceso: 02 09 2020].

[85] T. &. R. A. Yadav, «Technical Aspects of Cyber Kill Chain,» *Third International Symposium on Security in Computing and Communications,* 2015.

[86] T. D. A. B. Dargahi, «A Cyber-Kill-Chain based taxonomy of crypto-ransomware features,» *J Comput Virol Hack Tech,* pp. 277-309, 2019.

[87] B. I. A. A. M. S. T. Sahalu B. Junaidu, «Proposed Framework for Effective Detection and Prediction of Advanced Persistent Threats Based on the Cyber Kill Chain,» *Scientific and Practical Cyber Security Journal,* vol. 3, nº 3, 2019.

[88] Shodan, «Shodan,» [En línea]. Available: https://www.shodan.io/search?query=country%3A%22MX%22. [Último acceso: 05 06 2020].

[89] lockheedmartin, «Applying Cyber Kill Chain® Methodology to Network Defense,» lockheedmartin, 2015. [En línea]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf. [Último acceso: 02 09 2020].

[90] A. P. C. B. Sergio Caltagirone, «The Diamond Model of Intrusion Analysis,» 2013. [En línea]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf. [Último acceso: 03 09 2020].

[91] Q. M. A. N. I. A. A. C. a. J. D. Hamad AL-Mohannadi, «Cyber-Attack Modeling Analysis Techniques: An Overview,» de *4th International Conference on Future Internet of Things and Cloud Workshops*, United Kingdom, Warwickshire, 2016 .

[92] Q. M. A. N. I. A. A. C. a. J. D. H. Al-Mohannadi, «Cyber-Attack Modeling Analysis Techniques: An Overview,» *IEEE 4th International Conference on Future Internet of Things and Cloud Workshops,* 2016.

[93] MITRE, «Corporate Overview,» [En línea]. Available: https://www.mitre.org/about/corporate-overview. [Último acceso: 04 11 2020].

[94] MITRE, «Groups,» MITRE, [En línea]. Available: https://attack.mitre.org/groups/. [Último acceso: 04 11 2020].

[95] T. A. J. C. P. M. a. S. N. G. G. R. Kwon, «Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping,» de *Resilience Week (RWS)*, Salt Lake City, 2020.

[96] MITRE ATT&CKÒ: Design and Philosophy, «MITRE,» [En línea]. Available: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf. [Último acceso: 04 11 2020].

[97] MITRE, «Enterprise Matrix,» [En línea]. Available: https://attack.mitre.org/matrices/enterprise/. [Último acceso: 04 11 2020].

[98] MITRE, «About Shield's structure and terminology,» [En línea]. Available: https://shield.mitre.org/resources/getting-started. [Último acceso: 04 11 2020].

[99] MITRE, «Active Defense Matrix,» [En línea]. Available: https://shield.mitre.org/matrix/. [Último acceso: 04 11 2020].

[100] A. de Melo e Silva, J. J. Costa Gondim, R. de Oliveira Albuquerque y L. J. GarcÃa Villalba, «A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence,» *Future Internet,* 2020.

[1 C. S. ,. A. M. ,. a. R. B. Clemens Sauerwein, «Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives,» de *Internationalen Tagung Wirtschaftsinformatik*, St. Gallen, Switzerland, 2017.
]
[1 10.1145/2994539.2994542, «MISP - The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform,» *Workshop on Information Sharing and Collaborative Security ,* 2016.
]
[1 MISP, «MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing,» [En línea]. Available: https://www.misp-project.org/features.html. [Último acceso: 08 11 2020].
]
[1 C. &. D. A. &. W. G. &. I. A. Wagner, «MISP -The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform,» *3rd ACM Workshop on Information Sharing and Collaborative Security,* 2016.
]
[1 Virus total, 09 2021. [En línea]. Available: https://support.virustotal.com/hc/en-us/categories/360000160117-About-us.
]
[1 Virus Total, 09 2021. [En línea]. Available: https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works.
]
[1 Y. L. L. S. y. G. W. Peng, «Opening the Blackbox of VirusTotal: Analyzing Online Phishing Scan Engines,» *Internet Measurement Conference,* 2019.
]
[1 W. S. S. K. S. L. Y. G. K. y. Y. H. H. H. Shin, «Twiti: Social Listening for Threat Intelligence,» *Association for Computing Machinery.*
]
[1 M. N. y. A. B. B. D. L. G. Wang, «Gathering Cyber Threat Intelligence from Twitter Using Novelty Classification,» *researchgate,* 2019.
]
[1 GitHub, «Twint Project,» [En línea]. Available: https://github.com/twintproject/twint.
]
[1 Y. N. Imamverdiyev, «SOCIAL MEDIA AND SECURITY CONCERNS,» *Problems of information society,* 2016.
]
[1 TrapX, «TrapX,» [En línea]. Available: https://trapx.com. [Último acceso: 07 11 2020].
]
[1 Attivo Networks, «ThreatDefend® Detection & Response Platform,» [En línea]. Available: https://attivonetworks.com/product/deception-technology/. [Último acceso: 07 11 2020].
]
[1 Fortinet, «FortiDeceptor,» [En línea]. Available: https://www.fortinet.com/products/fortideceptor. [Último acceso: 07 11 2020].
]
[1 2. D. B. I. Report, «Enterprise Verizon,» [En línea]. Available: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf. [Último acceso: 07 11 2020].
]
[1 B. J. R. E. Sanjeev Kumar, «Multi Platform Honeypot for Generation of Cyber Threat Intelligence,» de *9th International Conference on Advanced Computing (IACC)*, 2017.
]
[1 Telekom Security, «Introduction into T-Pot: A Multi-Honeypot Platform,» 2015. [En línea]. Available: http://github.security.telekom.com/2015/03/honeypot-tpot-concept.html. [Último acceso: 07 11 2020].
]
[1 elastic, «¿Qué es el ELK Stack?,» [En línea]. Available: https://www.elastic.co/es/what-is/elk-stack. [Último acceso: 07 11 2020].
]
[1 spiderfoot, «Spiderfoot,» [En línea]. Available: https://www.spiderfoot.net. [Último acceso: 07 11 2020].
]
[1 Crown Copyright 2016, «Cyberchef,» [En línea]. Available: https://gchq.github.io/CyberChef/. [Último acceso: 07 11 2020].
]
[1 Suricata, «Suricata,» [En línea]. Available: https://suricata-ids.org. [Último acceso: 07 11 2020].
]
[1 McAfee Labs, «Informe de McAfee Labs sobre amenazas,» McAfee, 2021.
]
[1 SophosLabs, «INFORME DE AMENAZAS 2021 DE SOPHOS,» Sophos, 2020.
]
[1 M. Sikorski y A. Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, San Fransico: No Starch Press, 2012, p. xxviii.
]
[1 S. Talukder, «Tools and Techniques for Malware Detection and Analysis,» de *arXiv.org*, 2020.
]

[1 M. Conti, T. Dargahi y A. Dehghantanha, Cyber Threat Intelligence: Challenges and Opportunities, Springer International Publishing, 2018.
26
]
[1 Forcepoint, «Cyber Edu: Sandbox Security,» Forcepoint, [En línea]. Available: https://www.forcepoint.com/cyber-edu/sandbox-security. [Último acceso: 10 September 2021].
27
]
[1 CrowdStrike, «CROWDSTRIKE FALCON SANDBOX MALWARE ANALYSIS,» 2021. [En línea]. Available: https://www.crowdstrike.com/wp-
28 content/uploads/2020/03/FalconXSandboxDatasheet.pdf. [Último acceso: 14 September 2021].
]
[1 Fortinet, «FortiSandbox Datasheet,» 2021. [En línea]. Available: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf. [Último acceso: 14
29 September 2021].
]
[1 CrowdStrike, «Falcon Sandbox,» [En línea]. Available: https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/. [Último acceso: 14
30 September 2021].
]
[1 Cuckoo, «Cuckoo Sandbox,» Cuckoo, [En línea]. Available: https://cuckoosandbox.org/. [Último acceso: 14 September 2021].
31
]
[1 Gartner, «Security Orchestration, Automation and Response (SOAR),» [En línea]. Available: https://www.gartner.com/en/information-technology/glossary/security-
32 orchestration-automation-response-soar. [Último acceso: 31 08 2021].
]
[1 S. Shea, «SOAR (security orchestration, automation and response),» techtarget, [En línea]. Available: https://searchsecurity.techtarget.com/definition/SOAR. [Último acceso:
33 31 08 2021].
]
[1 M. &. R. S. &. A. (. D. A. &. R. Y. Abu, «Cyber threat intelligence – Issue and challenges,» *Indonesian Journal of Electrical Engineering and Computer Science.,* 2018.
34
]
[1 Fortinet, «Threat Intelligence at Machine Speed,» [En línea]. Available: https://www.fortinet.com/fortiguard/labs. [Último acceso: 06 11 2020].
35
]
[1 K. O. &. C. Doerr, «Cyber Threat Intelligence: A Product Without a Process?,» *International Journal of Intelligence and CounterIntelligence,* 2020.
36
]
[1 Fortinet, «Fortinet Threat Intelligence Insider Latin America,» Fortinet, 27 11 2019. [En línea]. Available: https://www.fortinetthreatinsiderlat.com/es/Q1-
37 2020/MX/html/trends#trends_position. [Último acceso: 01 06 2020].
]
[1 Shodan, «What is Shodan?,» [En línea]. Available: https://help.shodan.io/the-basics/what-is-shodan. [Último acceso: 05 06 2020].
38
]
[1 A. A. a. I. Alsmadi, «IoT and the Risk of Internet Exposure: Risk Assessment Using Shodan Queries,» *2019 IEEE 20th International Symposium on A World of Wireless,*
39 *Mobile and Multimedia Networks,* 2019.
]
[1 Shodan, «Mexico Internet Exposure Dashboard,» [En línea]. Available: https://exposure.shodan.io/#/MX. [Último acceso: 05 06 2020].
40
]
[1 B. Packets®, «Bad Packets® Cyber Threat Intelligence,» [En línea]. Available: https://badpackets.net/threat-intelligence/. [Último acceso: 05 06 2020].
41
]
[1 B. Packets®, «Mirai-like Botnet Hosts,» Bad Packets®, [En línea]. Available: https://mirai.badpackets.net/accounts/login/?next=/%3Fpage%3D27651%26sort%3Dcountry.
42 [Último acceso: 05 06 2020].
]
[1 A. K. M. V. G. a. T. M. O. P. Dwyer, «Profiling IoT-Based Botnet Traffic Using DNS,» *019 IEEE Global Communications Conference (GLOBECOM),* 2019.
43
]
[1 V. G. a. T. M. Angelos K. Marnerides, «Identifying infected energy systems in the wild,» de *e-Energy '19: Proceedings of the Tenth ACM International Conference on Future*
44 *Energy Systems*, Phoenix AZ, 2019.
]
[1 APWG, «APWG,» [En línea]. Available: https://apwg.org/. [Último acceso: 06 06 2020].
45
]
[1 P. Feeds, «openphish,» [En línea]. Available: https://openphish.com/phishing_feeds.html. [Último acceso: 06 06 2020].
46
]
[1 openphish, «https://openphish.com/feed.txt,» [En línea]. Available: https://openphish.com/feed.txt. [Último acceso: 06 06 2020].
47
]
[1 Urlhaus, [En línea]. Available: https://urlhaus.abuse.ch/feeds/country/MX/. [Último acceso: 07 06 2020].
48
]
[1 N. Young, «github.com,» [En línea]. Available: https://github.com/twintproject/twint. [Último acceso: 07 06 2020].
49
]
[1 Facebook, [En línea]. Available: https://developers.facebook.com/programs/threatexchange/. [Último acceso: 07 06 2020].
50
]

[151] IBM, [En línea]. Available: https://www.ibm.com/mx-es/security/xforce. [Último acceso: 07 06 2020].

[152] checkpoint, «Live Cyber Threat Map,» [En línea]. Available: https://threatmap.checkpoint.com/. [Último acceso: 07 06 2020].

[153] A10, «DDOS WEAPONS INTELLIGENCE MAP,» [En línea]. Available: https://threats.a10networks.com/. [Último acceso: 07 06 2020].

[154] mrlooquer, [En línea]. Available: https://mrlooquer.com/. [Último acceso: 08 06 2020].

[155] Muñoz, M., Peralta, M., & Laporte, C. Y., «nálisis de las debilidades que presentan las Entidades Muy Pequeñas al implementar el estándar ISO/IEC 29110: Una comparativa entre estado del arte y el estado de la práctica,» *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação,,* pp. pp 85-96, 2019.

[156] Fortinet, «Next-Generation Firewall (NGFW),» [En línea]. Available: https://www.fortinet.com/products/next-generation-firewall.

[157] R. Chandel, «Threat Intelligence: MISP Lab Setup,» Hacking Articles, 08 18 2020. [En línea]. Available: https://www.hackingarticles.in/threat-intelligence-misp-lab-setup/. [Último acceso: 31 08 2021].

[158] A. E. T. Cavazos, «Generando un Laboratorio personal en casa usando VMWare ESXi - 2021,» 10 02 2021. [En línea]. Available: https://www.linkedin.com/pulse/generando-un-laboratorio-personal-en-casa-usando-vmware-torres/. [Último acceso: 31 08 2021].

[159] MITRE, «Reconnaissance,» [En línea]. Available: https://attack.mitre.org/tactics/TA0043/.

[160] MITRE, «Active Scanning: Scanning IP Blocks,» [En línea]. Available: https://attack.mitre.org/techniques/T1595/001/.

[161] MITRE, «Active Scanning: Vulnerability Scanning,» [En línea]. Available: https://attack.mitre.org/techniques/T1595/002/.

[162] MITRE, «Gather Victim Network Information: DNS,» [En línea]. Available: https://attack.mitre.org/techniques/T1590/002/.

[163] MITRE, «Initial Access,» [En línea]. Available: https://attack.mitre.org/tactics/TA0001/.

[164] MITRE, «Exploit Public-Facing Application,» [En línea]. Available: https://attack.mitre.org/techniques/T1190/.

[165] MITRE, «External Remote Services,» [En línea]. Available: https://attack.mitre.org/techniques/T1133/.

[166] MITRE, «Supply Chain Compromise: Compromise Software Supply Chain,» [En línea]. Available: https://attack.mitre.org/techniques/T1195/002/.

[167] MITRE, «Execution,» [En línea]. Available: https://attack.mitre.org/tactics/TA0002/.

[168] MITRE, «Command and Control,» [En línea]. Available: https://translate.google.com/?hl=es&sl=en&tl=es&text=The%20adversary%20is%20trying%20to%20communicate%20with%20compromised%20systems%20to%20control%20them.%0A%0ACommand%20and%20Control%20consists%20of%20techniques%20that%20adversaries%20may%20use%20to%20c.

[169] Recorded Future, «What Is Threat Intelligence?,» [En línea]. Available: https://www.recordedfuture.com/threat-intelligence/.

[170] J. M. Stecklein, J. Dabney, B. Dick, B. Haskins, R. Lovell y G. Moroney, «Error Cost EscalationThrough the Project Life Cycle,» Toulouse, 2004.

[171] J. Z. P. R. S. G. Y. X. a. L. Y. Z. Nan Sun, «Data-driven cybersecurity incident prediction: A survey,» *IEEE COMMUNICATIONS SURVEYS & TUTORIAL,* p. 29, 2018.

[172] Nestor Gilbert, «Number of Email Users Worldwide 2020: Demographics & Predictions,» Finances Online, [En línea]. Available: https://financesonline.com/number-of-email-users/. [Último acceso: 27 10 2020].

[173] I. L. Stats, «Internet Live Stats,» [En línea]. Available: https://www.internetlivestats.com/one-second/#email-band. [Último acceso: 27 10 2020].

[174] Interpol, «Business Email Compromise Fraud,» [En línea]. Available: https://www.interpol.int/en/Crimes/Financial-crime/Business-Email-Compromise-Fraud. [Último acceso: 27 10 2020].

[175] R. Leszczyna y M. R. Wróbel, «Threat intelligence platform for the energy sector,» *Software, practice & experience,* vol. 49, nº 8, pp. 1225 - 1254, 2019.

[176] Y. a. R. V. Creado, «Active cyber defence strategies and techniques for banks and financial institutions,» , *Journal of Financial Crime,* vol. 27, nº 3, 2020.

[177] E. A. B. T. a. J. H. N. Moustafa, «A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems,» *IEEE Access,* vol. 6, 2018.

[178] McAfee, «McAfee Advanced Threat Defense,» McAfee, [En línea]. Available: https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-advanced-threat-defense.pdf. [Último acceso: 14 September 2021].