Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Inteligencia de Amenazas Cibernéticas

DETECCIÓN, RESPUESTA Y BUENAS PRÁCTICAS ANTE ATAQUES CIBERNÉTICOS AVANZADOS

Autor: Lic. Gladys MARTINEZ

Tutora del Trabajo Final: Mg. Patricia Prandini

Fecha de Presentación: Diciembre de 2020

Cohorte 2013

Resumen

Desde el punto de vista del aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) tanto los Organismos Públicos como los Privados se encuentran actualmente en pleno funcionamiento e inmersos en una etapa de continuo cambio y evolución debido a la interacción de fuerzas que se producen entre el surgimiento de nuevas tecnologías, su necesidad de actualización y las adecuaciones normativas que se van generando en todo el ámbito de su accionar.

Estas tecnologías emergentes y la rápida expansión del USO DEL ciberespacio, representan un nuevo contexto importante en la política mundial.

Esto se debe a que el ciberespacio representa el ámbito virtual en el que se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y visualización de datos e información digital, a través de redes, software, hardware y firmware de dispositivos electrónicos, cuyo carácter distintivo está dado por el empleo excluyente de las tecnologías de información y comunicaciones.

Sin embargo, junto con el auge de las tecnologías y el avance en las comunicaciones e informática, han crecido también las amenazas. Pues toda información mediante la interconexión propiciada por el ciberespacio, puede ser accedida, percibida, interceptada, reunida, registrada, explotada, generada, construida, organizada, procesada, gestionada, afectada, transferida, comunicada, enrutada, multiplexada, asegurada, procesada, controlada, y también desvirtuada o peor aún, vulnerada y/o utilizada para fines distintos a los que fueron concebidas.

Es en este contexto que se hace imperativa la necesidad de establecer mecanismos que ayuden a evitar que cualquier evento adverso, real o potencial, comprometa la seguridad de los sistemas de información y las redes de computadoras, permitan la violación de las políticas de seguridad y/o afecten el normal desenvolvimiento del quehacer de la organización. Esto se

acentúa cuando estos incidentes, pueden trascender los límites organizacionales y nacionales.

El presente trabajo, plantea los requisitos necesarios para la implementación de medidas proactivas a fin de poder anticiparse a dichos incidentes. Se propone esclarecer los conceptos y metodología de la ciberinteligencia de amenazas cibernéticas, incluyendo un análisis de normas aplicables, estándares, software, especificaciones y recomendaciones técnicas necesarias para los procesos de detección, recopilación, procesamiento, análisis, difusión y retroalimentación (revisión) que permitan anticipar amenazas, vulnerabilidades y ataques a los sistemas de información.

Palabras Claves

Ciberinteligencia de amenazas (CTI por sus siglas en inglés de Cyber Threats Intelligence), Indicadores de Compromiso (IOC), Indicadores de ataque, Inteligencia artificial.

Declaración jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO
Gladys B. MARTINEZ
DNI 20.443179

Índice de contenido

Índice de figuras

1. Introducción.

Cada año las amenazas van evolucionando, los criminales se adaptan y se diversifican, y surgen nuevas amenazas aprovechando el avance vertiginoso de la tecnología. Las brechas de seguridad y los ciberataques de todo tipo se están volviendo más profesionales, sigilosos, automatizados y complejos. Estas formas avanzadas de ciberataques acompañados por la aparición de nuevos actores de amenazas superan muchas veces la defensa tradicional, incluyendo sus métodos y técnicas.

En este contexto, los equipos de operaciones de seguridad que se enfrentan a ese abrumador volumen de alertas, pueden perder información relevante.

La inteligencia de amenazas o Ciber Threat Intelligence, facilita la gestión de incidentes porque proporciona información en tiempo real, para contener, identificar y si es posible erradicar esas amenazas.

En ciberseguridad, la capacidad de predecir futuros ataques dirigidos incluso antes de que lleguen a las redes puede ayudar a las organizaciones a priorizar sus respuestas, acelerando el proceso de toma de decisiones y el tiempo de respuesta, proporcionando una mejor seguridad al elevar los niveles de preparación y alerta.

El presente trabajo, plantea los requisitos necesarios para la implementación de medidas proactivas a fin de poder anticiparse a dichos incidentes, logrando de ese modo una ciberdefensa más efectiva.

2. Conceptos Generales

2.1 Definiciones previas.

La Inteligencia de Amenazas Cibernéticas, en adelante **CTI** por sus siglas en inglés, *Cyber Threats Intelligence*, puede describirse como evidencia basada en conocimiento. Pero para tener una idea clara de su funcionamiento y características, debemos entender que ese concepto va más allá de obtener

una lista de direcciones IPs, hashes de archivos sospechosos, lista de malwares, etc. Involucra conceptos tales como:

- Indicadores de ataque: señales de alerta temprana que indican que un ataque es inminente o ya está en marcha, como ejecución de códigos, persistencia, secreto, control de mando y movimiento lateral dentro de una red.
- Vectores de ataque: término adoptado de la terminología militar, se refiere en ese ámbito a una falla presente en la defensa establecida[1]. En ciberseguridad, se refieren a medios (malwares, keyloggers, Ingeniería social, spoofing, DDoS, Sniffing, etc.[2]) utilizados por los atacantes para explotar las vulnerabilidades y obtener acceso a una computadora o red de computadoras para obtener algún beneficio. En suma, son los pasos que sigue un atacante para materializar una amenaza.
- Indicadores de compromiso (IOC): son los indicios de que un sistema u organización han sido atacados, es decir que su seguridad ha sido comprometida. La presencia de malware, firmas, exploits, vulnerabilidades y direcciones IP caracteriza el tipo de evidencia que se dejan cuando se realiza un ataque.

[1] ¿A qué se le conoce como vectores de ataque en ciberseguridad y cómo puedes eliminarlos de tus ambientes digitales? – [En línea] disponible en: https://www.gb-advisors.com/es/vectores-de-ataque-en-ciberseguridad/#:~:text=Vectores%20de%20ataque%20en%20ciberseguridad%3A%20Ataques%20activos

[2] Definiciones en Sección Glosario de Términos

Figura 1[1]: Diferencia entre IOC e IOA

– La comprensión no sólo de la importancia de detener el ataque sino también, mayor certeza de quién podría ser el atacante y las diferentes tácticas, técnicas y procedimientos (TTPs) empleados.

¿Qué actividad estamos viendo?	Observable	¿Qué amenazas debo buscar en mis redes y sistemas, y por qué?	Indicadores
¿Dónde se ha detectado esta amenaza?	Incidente	¿Qué es lo que hace?	Procedimientos
¿Qué debilidad explota esta amenaza?	Exploit Target	¿Por qué hace esto?	Campaign
¿Quién es el responsable de esta amenaza?	Threat Actor	¿Qué puedo hacer al respecto?	Curso de acción

Figura 2[3]: Comprendiendo el contexto de los eventos cibernéticos

– Todo otro concepto que permita entender los nuevos conceptos de defensa como la defensa activa y la inteligencia, para poder realizar una mejor implementación e impulsar acciones ante una amenaza o una amenaza posible o una ya identificada. Acciones que podemos apreciar en la siguiente figura:

[3] Threat intelligence sharing challenges: Understand the context of cyber events– [En línea] disponible en: https://www.helpnetsecurity.com/2017/04/07/threat-intelligence-sharing-challenges/

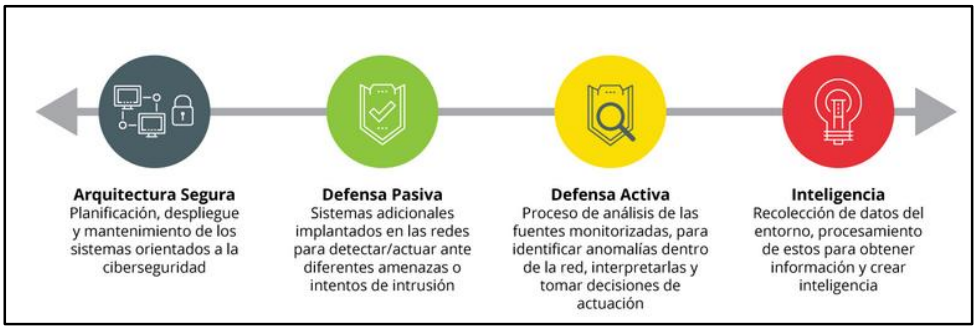

Figura 3[4]: Concepto de defensa y sus acciones.

2.2 Antecedentes.

2.2.1 Panorama de Amenazas

Cada año las amenazas van evolucionando, los criminales se adaptan y se diversifican, y surgen nuevas amenazas aprovechando el avance vertiginoso de la tecnología. Las brechas de seguridad y los ciberataques de todo tipo se están volviendo más profesionales, sigilosos, automatizados y complejos. Estas formas avanzadas de ciberataques acompañados por la aparición de nuevos actores de amenazas superan muchas veces la defensa tradicional, incluyendo sus métodos y técnicas.

En este contexto, los equipos de operaciones de seguridad que se enfrentan a ese abrumador volumen de alertas, pueden perder información relevante.

En síntesis, nos enfrentamos a las siguientes dificultades: Los equipos de operaciones de seguridad se enfrentan a un abrumador volumen de alertas.

– El arduo trabajo que supone para los equipos de respuesta a incidentes el contener y remediar completamente las intrusiones.

– Se observa una efectividad reducida en el uso de herramientas que mayormente se basan en lo conocido en la lucha contra lo desconocido.

[4] Defensa activa e inteligencia [En línea] Disponible en: https://www.incibe-cert.es/blog/defensa-activa-e-inteligencia-teoria-practica

– Se necesita un contexto externo para verificar el riesgo relacionado con problemas conocidos y proporcionar advertencias sobre amenazas emergentes e imprevistas.

Las herramientas que actualmente utilizamos, IDS/IPS/ SIEM son útiles para aquellas amenazas conocidas. Nos enfrentamos a un panorama en el que nuestra información interna no es suficiente. Los datos de tráfico, los registros de logs y las alertas, nos aportan valor en la gestión de riesgos pero no proporcionan ese contexto suficiente para construir el perfil de riesgo integral, y ciertamente no lo suficiente para definir una estrategia completa. El personal que se aboca a esta tarea debe ser proactivo en descubrir estos riesgos, porque al final es el contexto el que ayuda a determinar las amenazas potenciales que tienen mayor probabilidad de convertirse en reales para una empresa.

La Inteligencia de Amenazas Cibernéticas (CTI) permite analizar la información sobre las capacidades, oportunidades e intenciones de ciberataques a organizaciones, Estados, empresas y sus cadenas de suministros, y en particular a los ciudadanos. De este modo se brinda información específica para ayudar a defenderse de esas amenazas.

Figura 4[5]: Comprendiendo el contexto del análisis de eventos cibernéticos

Según los datos del informe anual “Panorama de Amenazas y Tendencias 2020” del Equipo de Respuesta a Incidentes del Centro

[5] Not all threat intelligence is created equal – [En línea] disponible en: https://www.helpnetsecurity.com/2017/02/27/focus-threat-intelligence/

Criptológico Nacional de España (CCN-CERT), el elemento disruptivo del año 2020 fue la pandemia de COVID-19 sufrida en todo el mundo. Su incidencia en el panorama de la ciberseguridad global al potenciar el teletrabajo, fue aprovechado por actores hostiles para robar información, incrementar el uso de Botnets, el resurgimiento de los mineros de criptomonedas o criptojacking y el uso de las campañas de ransomware, en el sector estatal, privado, bancario y con un alto impacto en el sector sanitario.

Algunos de los ataques ransomware sufridos en Argentina:

- En el sector privado, la compañía Telecom, sufrió un ataque de ransomware en el mes de julio. Los ciberdelincuentes solicitaron el pago de 7.5 millones de dólares en monero para recuperar los archivos cifrados. El ataque fue controlado.
- En el sector comercial, fue afectada la multinacional Cencosud. El ataque en nuestro país afectó a sus sucursales de Jumbo, Easy, Disco, Vea y Blainstein. Los cibercriminales amenazaron con publicar detalles personales de sus clientes, incluidas las credenciales de tarjetas de crédito.
- En el sector gubernamental, fueron secuestrados datos de la Dirección Nacional de Migraciones. Los ciberdelincuentes al no recibir el pago de unos 4 millones de dólares estadounidenses que reclamaban, liberaron la clave para descomprimir el archivo RAR que contenía 1,8 gigas. Este archivo contenía información crítica del Organismo. De similares características fue el ataque que sufrió la Agencia Nacional de Seguridad Vial, dependiente del Ministerio de Transporte (y no la Dirección de Vialidad Nacional como erróneamente se difundió en los medios de comunicación).
- Respecto al uso de Botnets, las más utilizadas por los actores de amenazas este año fueron Emotet, Dridex, Trickbot. Con relación a las campañas de ransonware, en el último trimestre del año 2020 se estaba investigado un caso como homicidio después de la muerte de un paciente en un hospital europeo que fue atacado por un ransomware.

– Cabe destacar además un incremento en el denominado fraude del CEO o BEC, Business E-mail Compromise, cuyo ciclo de ataque se puede apreciar en la siguiente imagen:

Figura 5[6]: Ciclo de Fraude al CEO, Europol

Por otro lado se incrementaron acciones ligadas a actores estatales en áreas como propaganda, desinformación y operaciones de influencia. Las redes sociales han sido usadas como vectores de ataque contra el ciudadano, para orquestar campañas de manipulación. A medida que persisten las tensiones geopolíticas, los actores de amenazas cibernéticas utilizan eventos globales de alto perfil para influir en la opinión de las masas aprovechando las nuevas tecnologías.

Un informe de la Universidad de Oxford[7], señala que encontraron evidencias de campañas organizadas de manipulación de los medios sociales

[6] INFOGRAFIA – [En línea] Disponible en: http://www.europol.europa.eu/sites/default/files/documents/es_1.pdf

[7] https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

en 70 países, frente a 48 países en 2018 y 28 países en 2017, registrándose un incremento del 150%. Parte de este crecimiento proviene de los nuevos participantes que están experimentando con las herramientas y técnicas de propaganda computacional durante las elecciones o como una nueva herramienta de control de la información.

Un análisis de la empresa de servicios de seguridad Positive Technologies[8] índica que:

- El número de ciberincidentes está creciendo rápidamente. En el primer trimestre de 2020, se detectó un 22,5% más de ataques que en el cuarto trimestre de 2019.
- El porcentaje de ataques dirigidos permanece sin cambios desde el 4º trimestre de 2019 (67%).
- En el primer trimestre 2020, hubo 23 grupos de APT muy activos. Sus ataques se dirigieron principalmente a agencias gubernamentales, industria, finanzas e instituciones médicas.
- Alrededor del 13% de todos los correos electrónicos de phishing del primer trimestre de 2020 estaban relacionados con COVID-19. De ellos, cerca de la mitad (44%) tenían como objetivo a individuos.
- Uno de cada cinco correos se envió a agencias gubernamentales.
- Más de un tercio (34%) de todos los ataques a organizaciones que usaban malware eran ataques con ransomware. Sodinokibi, Maze y DoppelPaymer fueron los más activos. Los operadores de estos y otros programas maliciosos crearon sus propios sitios web donde publican los datos robados si las víctimas se negaban a pagar el rescate.
- La proporción de ataques contra individuos fue del 14%. Los nombres de usuario y las contraseñas constituyeron la mitad de los datos

[8] https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2020-q1/#id2

robados. Esto se debe a que las campañas de malware contra individuos contenían un gran porcentaje de spyware (56%).

El último informe de Accenture Security "2020 Cyber Threatscape" revela cinco factores que influyen en el panorama de las ciberamenazas:

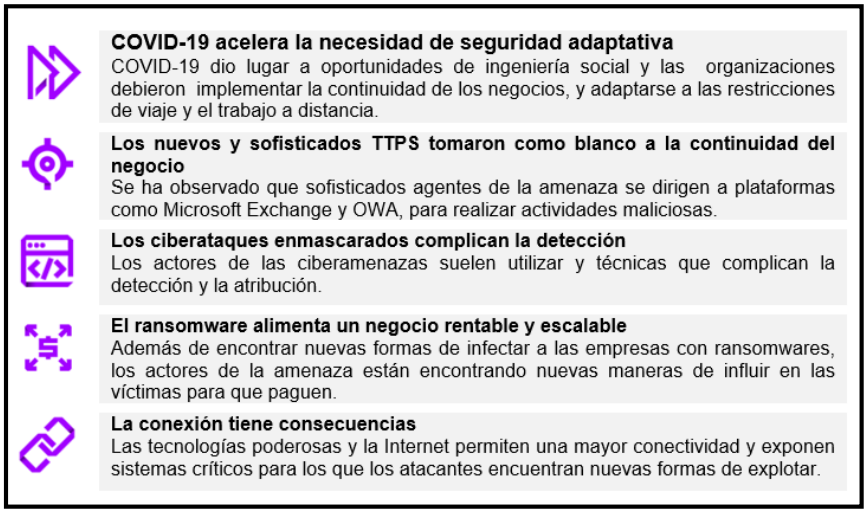

Figura 6[9]: Factores que influyen en el panorama de ciberamenazas

Un reporte de la Agencia de la Unión Europea para la Ciberseguridad indica cuáles fueron las 15 principales amenazas en los últimos doce meses del año 2020. Como podemos apreciar en la siguiente figura:

[9] 2020 Cyber Threatscape Report Executive Summary – [En línea] Disponible en: https://www.accenture.com/mu-en/insights/security/cyber-threatscape-report

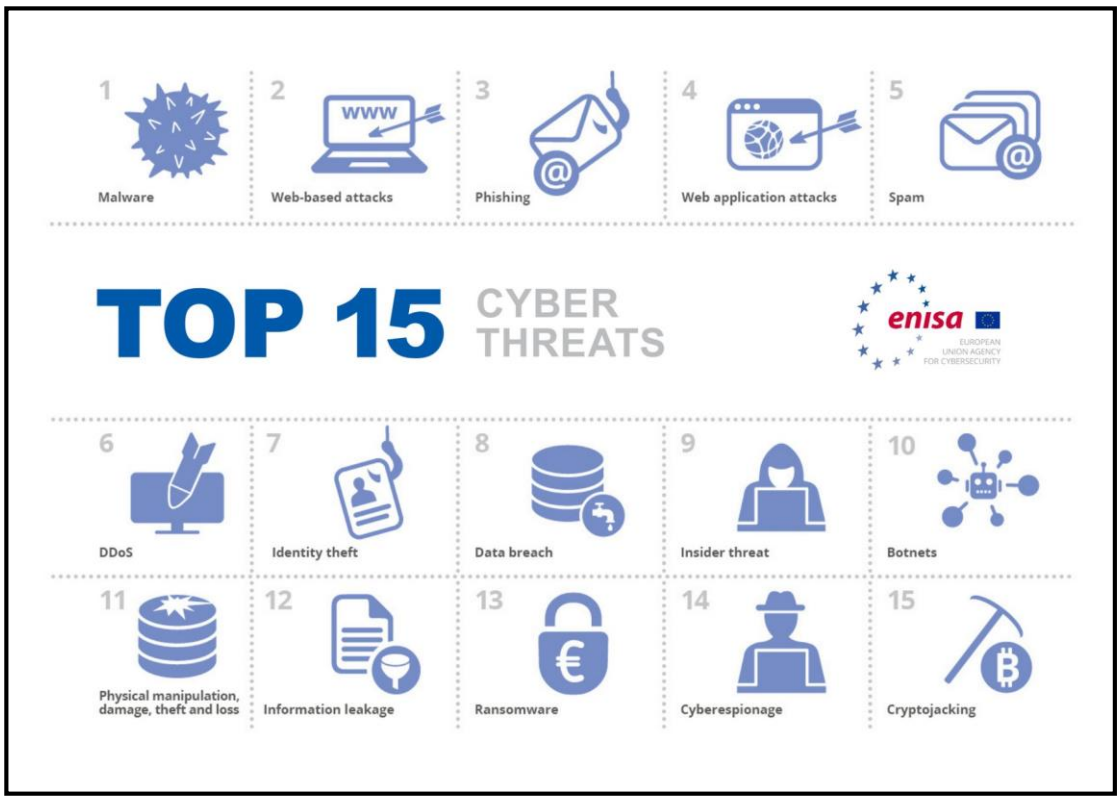

Figura 7 : Factores que influyen en el panorama de ciberamenazas [15]

En Argentina el último informe oficial sobre "el panorama de la ciberseguridad en números[10]" data del año 2016, por lo que sus conclusiones carecen de actualidad.

Una presentación de la empresa estatal ARSAT consignaba en la H4ck3d: Security Conference 2020 un "Análisis de la dinámica de ciberataques durante el COVID19". En su informe presentaron la evolución y el incremento de las amenazas en Argentina, tomando como modelos comparativos los meses de julio y agosto de 2019 y 2020. Y que el incidente más recurrente fue la Denegación de Servicio Distribuido (DDoS). Como podemos apreciar en la siguiente imagen.

[10] EL PANORAMA DE LA CIBERSEGURIDAD EN NÚMEROS-'[En línea] Disponible en: https://www.argentina.gob.ar/sites/default/files/cofemod_comisionciberseguridad_el_panorama_de_la_ciberseguridad_en_numeros_12-08-16.pdf

Figura 8: Análisis comparativo de ciberamenazas entre el año 2019 y 2020

En la siguiente figura se puede observar los incidentes en el SOC de ARSAT pre-COVID y post-COVID. La línea roja permite apreciar el incremento de incidentes el fin de semana.

En el 2020 los ataques DDoS se incrementaron en un 20%, los ramsonwares un 110%, los incidentes en capa 7, como por ejemplo SQL Injection se incrementaron en un 35% y los de fuerza bruta crecieron un 30% más con respecto al año 2019.

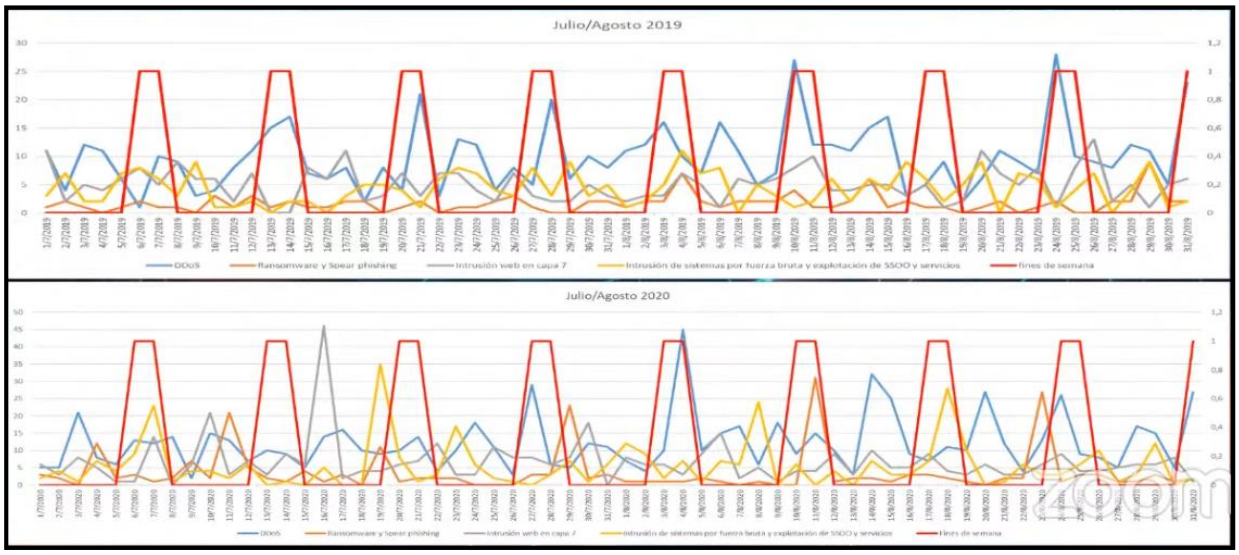

Figura 9: Incremento de ciberamenazas entre el año 2019 y 2020 __ DDoS __Ransomware y Spear Phishing __Intrusión web en capa7 __ Intrusión de sistemas por fuerza bruta y explotación de SSOO y servicios

El resultado de una encuesta de ESET Security[11] revela el panorama de amenazas en Argentina y su porcentaje de incremento en los últimos doce meses como podemos apreciar en la siguiente imagen:

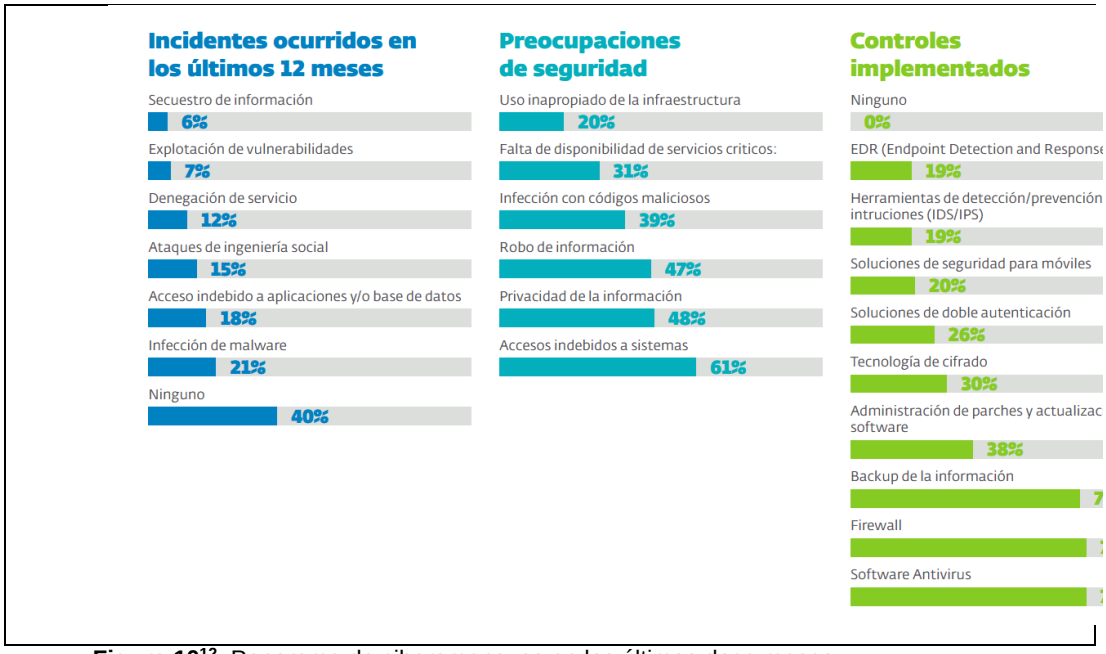

Figura 10[12]: Panorama de ciberamenazas en los últimos doce meses

Un informe del Observatorio de la Ciberseguridad en América Latina y el Caribe[13], nos permite apreciar los niveles de madurez (y su evolución entre el año 2016 y 2020) en el que se encuentra la República Argentina para hacer frente a las ciberamenazas, con los siguientes indicadores o dimensiones:

- D1-Política y Estrategia de Seguridad Cibernética
- D2-Cultura Cibernética y Sociedad.

[11] Seguridad en Latinoamérica: ¿Qué destacan los últimos informes? [En línea] Disponible en: https://security-report.eset-la.com/?utm_campaign=eset-la&utm_source=twitter&utm_medium=social&s=08

[12] Seguridad en Latinoamérica: ¿Qué destacan los últimos informes? Estado de la Seguridad en Argentina[En línea] Disponible en: https://security-report.eset-la.com/?utm_campaign=eset-la&utm_source=twitter&utm_medium=social&s=08

[13]CIBERSEGURIDAD RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE. [En línea] Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

– D3-Formación, Capacitación y Habilidades de Seguridad Cibernética.

– D4-Marcos Legales y Regulatorios.

– D5-Estándares, organizaciones y tecnologías.

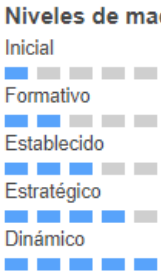

Figura 11: Niveles de Madurez en Argentina

2.2.2 Tendencias 2020

La crisis sanitaria y humanitaria provocada por la pandemia y el COVID-19, dio paso a un innovador cibercrimen. La rapidez con que las organizaciones tuvieron que adaptarse por el confinamiento, a la continuidad del negocio con un despliegue de entorno tecnológico de teletrabajo, no estuvo acompañados por un adecuado análisis de los riesgos asociados. Con ello se incorporaron deficiencias en la implementación de herramientas que

habilitaban el trabajo a distancia, que los ciberdelincuentes no dudaron en explotar.

Las formas de comunicación más utilizadas en esos entornos de trabajo, tales como las plataformas de comunicación, tecnologías VPN, etc. mostraron en el primer semestre del año 2020 vulnerabilidades que previsiblemente se pueden consolidar e incrementar durante todo el año. Según un informe de ESET los ataques al protocolo de escritorio remoto (RDP) crecieron en un 37%, y se espera que haya un aumento en el número de intentos de piratear las credenciales corporativas o explotar las vulnerabilidades en los sistemas de acceso remoto. Estas amenazas son especialmente relevantes para las empresas que no tienen una política estricta de contraseñas y que no realizan actualizaciones regulares de software.

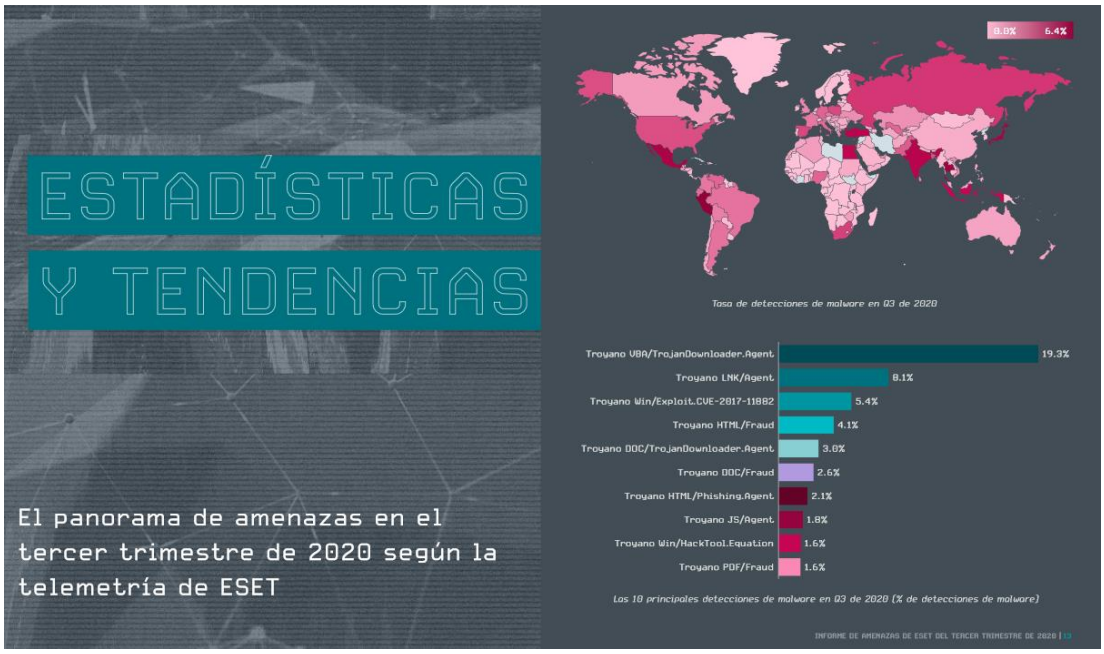

Figura 12:[14] Panorama de amenazas en el tercer trimestre de 2020

[14] Informe de amenazas de ESET para el tercer trimestre de 2020. [En línea] Disponible en: https://www.welivesecurity.com/wp-content/uploads/2020/11/Q3-2020_Threat_Report-ESP.pdf

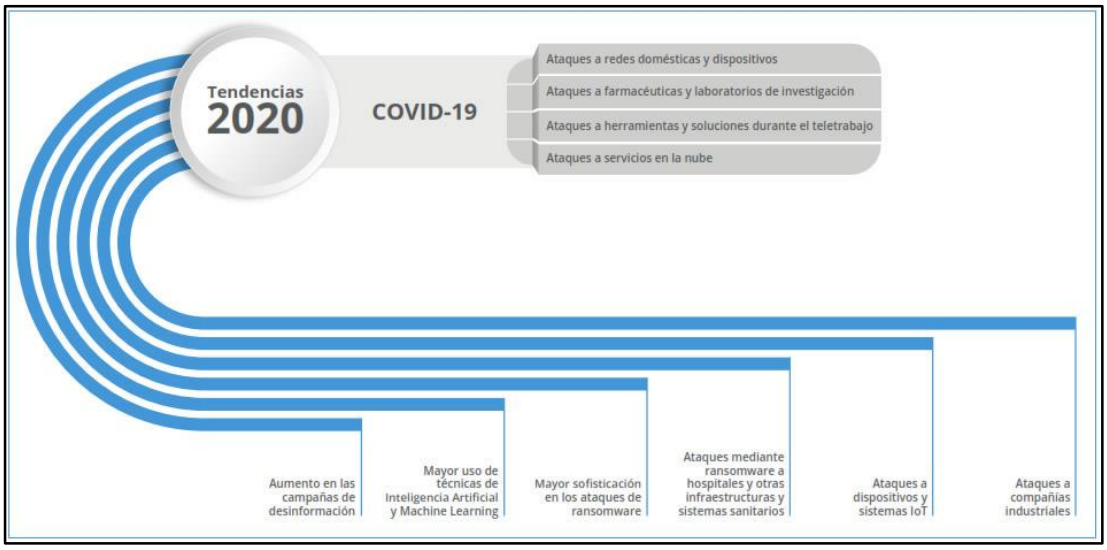

Figura 13:[5] Tendencias de Ciberamenazas a raíz de COVID-19– CCN-CERT Edición 2020

Una mención especial sobre la tendencia de amenazas es la creciente utilización y abuso de la Inteligencia Artificial (IA) por los actores de amenazas. La Organización de las Naciones Unidas y la Oficina Europea de Policía en su reporte "Malicious Uses and Abuses of Artificial Intelligence" compilado con TrendMicro (ONU, EUROPOL, TrendMicro, 2020)[15] predice que la IA será utilizada en el futuro como vector y como superficie de ataque.

"Los ciberdelincuentes están buscando formas de utilizar las herramientas de la IA en los ataques, pero también métodos a través de los cuales comprometer o sabotear los sistemas de IA existentes, como los que se utilizan en el reconocimiento de imágenes y voz y en la detección de malware." [8]

Las organizaciones pueden tomar medidas para un futuro más flexible y seguro si implementan soluciones de seguridad, políticas de actualización de parches considerando las amenazas más apremiantes, software antivirus

[15] https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence

con capacidad de detectar no sólo el correo malicioso sino signos de malware oculto u ofuscado, así como de bloquear la actividad maliciosa en diversos flujos de datos: correo electrónico, tráfico web, tráfico de red, almacenamiento de archivos y portales web, o asegurar a todos los usuarios, dispositivos y tráfico de red de forma consistente y con efectividad. También debe considerarse mejorar la conciencia de seguridad entre los clientes, recordarles regularmente cómo mantenerse a salvo en línea de los ataques más comunes, instar a que no introduzcan sus credenciales en sitios web sospechosos y a que no den esa información por correo electrónico o por teléfono, o informarlos qué deben hacer si sospechan de un fraude, y sobre eventos relacionados con la seguridad que contribuyan a su protección.

Pero, sobre todo, deben implementar un sistema de inteligencia de amenazas para anticiparse a los ciberataques, de modo de mantener una reacción proactiva frente a las tendencias detalladas precedentemente.

2.3 Qué es el Cyber Threats Intelligence – CTI

La inteligencia de amenazas puede definirse como inteligencia basada en conocimiento, Gartner [9] lo define como información basada en evidencias, incluido el contexto, los mecanismos, indicadores, implicancias y acciones recomendadas sobre una amenaza existente o potencial sobre los diferentes activos, que pueden ser usados para la toma de decisiones, acerca de la posible respuesta a esa amenaza o peligro.

El CTI permite detectar indicadores en las relaciones con amenazas, encontrar información referente a métodos de ataques, identificar amenazas de seguridad y tomar decisiones con antelación con el fin de responder a un ataque de manera precisa y efectiva.

Los datos de amenazas no dejan de ser datos. Un dato aislado tiene poca utilidad, si no se lo analiza a través de un contexto, que nos permite entender cuál es el objetivo y tipo de esa amenaza, y si detrás hay un agente de amenaza, comúnmente denominado *Threat Actor*.

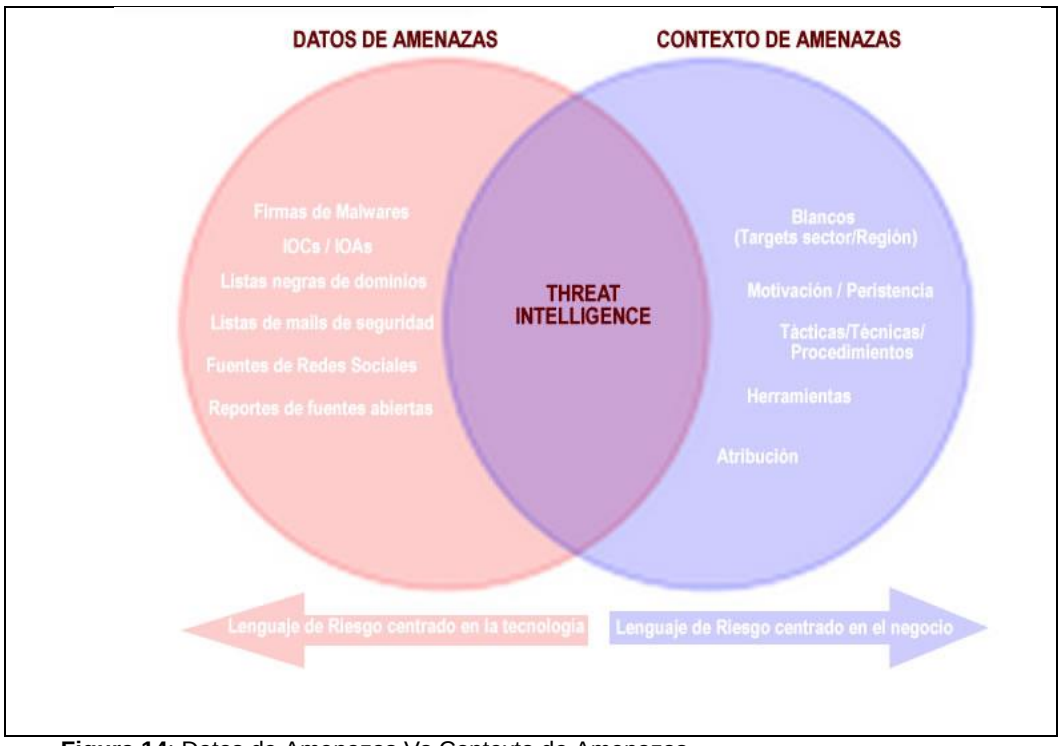

Figura 14: Datos de Amenazas Vs Contexto de Amenazas

El CTI visto como herramienta, nos permite enfrentarnos a esos riesgos (vulnerabilidad * impacto * amenaza). También nos facilita el proceso de conocimiento, cuyo propósito es entender al adversario, ayudarnos a anticiparnos a sus acciones y planificar una respuesta en consecuencia.

Al CTI lo podemos ver como en cuatro cuadrantes cuando nos enfrentamos a lo desconocido:

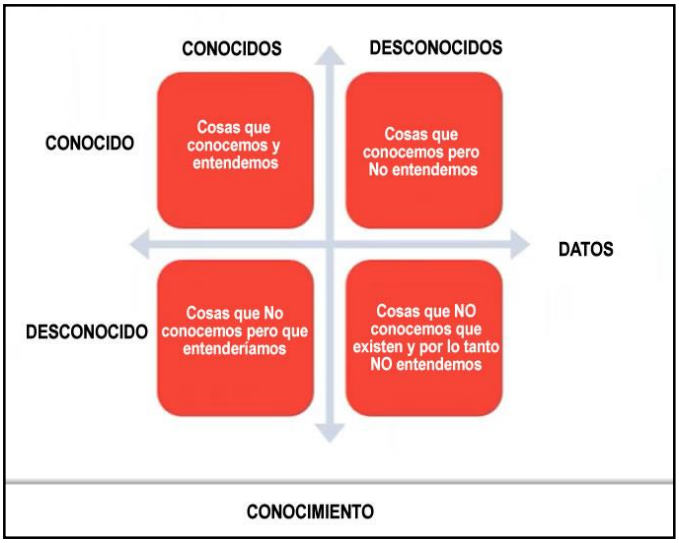

Figura 15: Los 4 cuadrantes del CTI

El cuadrante nos permite inferir las etapas para lograr una CTI. En la etapa Desconocido-Conocido, detectamos por una regla conocida que algo desconocido está sucediendo. En la etapa Desconocido-Desconocido, no se tiene idea acerca de las amenazas y se intenta localizarlas buscando información sobre las mismas. Una vez reunida la información, etapa Conocido-Desconocido, se realiza su análisis, para entender la naturaleza de las amenazas. Con el resultado de esta etapa nos encontramos en la etapa Conocido-Conocido, aquí se realiza el proceso de transformación de datos e información en conocimiento y es donde se mitigan las amenazas.

2.3.1 Características de CTI [11]

Entre los principales aspectos que caracterizan la CTI, se encuentran:

- Posibilita la recolección de datos, utilizando varias fuentes de códigos abiertos y comerciales, de fuentes internas y externas.
- Habilita la creación de alertas, así como su adaptación y priorización.
- Ayuda a identificar los Indicadores de Compromiso (IOCs) para prevenir de un posible ataque.
- Brinda habilidad para implementar nuevas estrategias de protección.
- Permite entender las perspectivas del Quién, Qué, Cuándo, Dónde, Porqué y Cómo, en relación a las amenazas emergentes.
- Posibilita la estimación de la probabilidad de riesgo y su impacto.
- Permite obtener varias soluciones de mitigación del riesgo.

2.3.2 Cualidades del Threat Intelligence [13]

Las cualidades del Threat Intelligence, se conocen generalmente como CART (por sus siglas en inglés de **C**ompleteness, **A**ccuracy, **R**elevance, **T**imeliness). En otras palabras, la calidad de la inteligencia sobre amenazas

debe medirse a través de cuatro dimensiones primarias: completitud, precisión, relevancia y oportunidad.

- Completitud, la inteligencia de la amenaza debe proporcionar suficientes detalles para permitir una respuesta adecuada
- Precisión, las fuentes de inteligencia de amenazas deben ser de una elevada fidelidad, con el menor ruido y falsos positivos posibles.
- Relevancia, la inteligencia de amenazas debe abordar solo las amenazas relevantes para la organización, con un método que permita una acción eficaz. El contenido debe tener valor para el área responsable de utilizarla.
- Oportunidad, la inteligencia de amenazas debe llegar en el momento adecuado para ser útil. Tiene una vida útil limitada.

Podemos si el *Threat Intelligence* cumple con esas cualidades haciendo las preguntas que siguen:

C Completa	• ¿cubre todos los dominios forenses digitales críticos? • ¿Incorpora análisis de vulnerabilidad? • ¿Existe una correlación en todo el espectro de amenazas e incorpora inteligencia y eventos que no son necesariamente ciberinteligencia para producir un perfil más completo de la amenaza?
A Completa	• ¿Qué fuentes de datos corroboran la inteligencia de amenazas para garantizar la precisión? • ¿Existen actualizaciones cuando se conoce o identifica nueva información? • ¿La inteligencia de amenazas está sujeta al tiempo para garantizar de tal manera que se entienda la naturaleza limitada de la información?
R Relevante	• ¿Qué fuentes de datos y visibilidad se utilizan e identifican las amenazas en una organización? • ¿Los analistas tienen experiencia en el negocio y operaciones para garantizar un contexto adecuado y recomendaciones viables? • ¿Existe un feedback que respalde una inteligencia más relevante?
T Oportuna	• ¿Cómo se entrega la inteligencia de amenazas para garantizar el consumo rápido? • ¿Cuánto tiempo transcurre entre el descubrimiento de una amenaza y la notificación? • ¿La información se divulga a medida que se aprende o se retiene para obtener más datos antes de informar?

Figura 16: Cualidades de CTI [13]

2.3.3 Tipos de inteligencia [12]

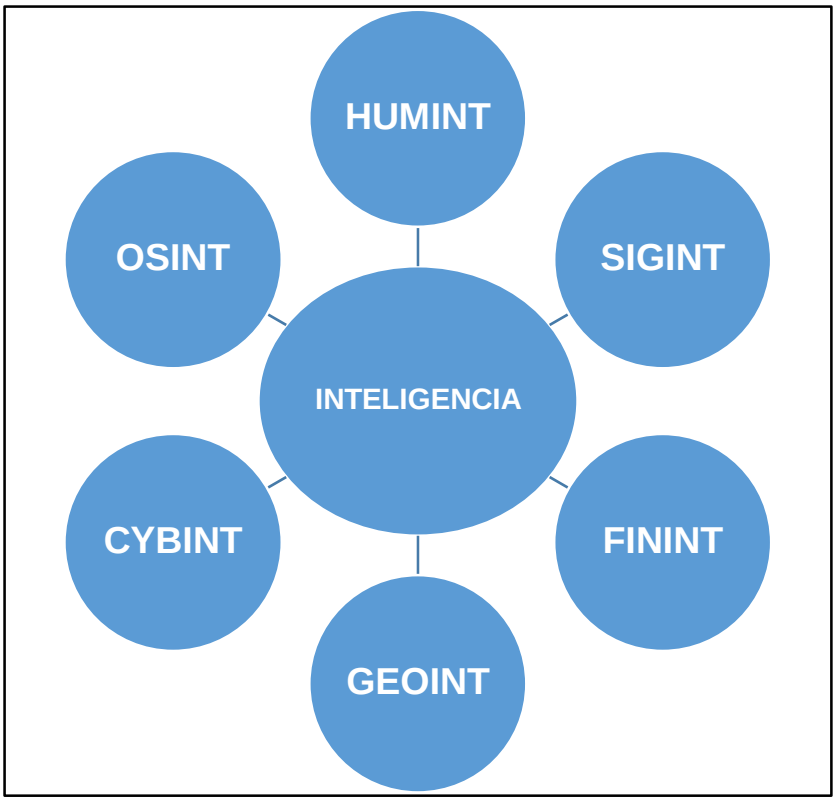

Figura 17: Tipos de inteligencia (Fuente: Elaboración propia)

2.3.3.1 OSINT

Son las siglas de Open Source INTelligence, y es la denominación más difundida para la inteligencia en fuentes abiertas. Agrupa a la información que puede obtenerse de los medios de comunicación (redes sociales, radio, diario, televisión, etc.), registros académicos y profesionales (publicaciones académicas, conferencias, etc.) y, datos públicos (reportes emitidos por organismos gubernamentales, censos, datos demográficos, discursos, etc.).

2.3.3.2 HUMINT

Son las siglas de HUMan INTelligence. Se define así a la recopilación de información proveniente de fuentes humanas. Puede ser realizada de forma abierta, utilizando cuestionarios, entrevistas, foros de debate, etc. O

puede realizarse en forma clandestina, como es el caso del espionaje, aunque para ello en Argentina se requiere de orden judicial.

2.3.3.3 SIGINT

Son las siglas de SIGnal INTelligence. Se refiere a las transmisiones electrónicas que pueden ser recogidas por barcos, aviones, sitios en tierra o satélites. La Inteligencia de las Comunicaciones (COMINT) es un tipo de SIGINT y se refiere a la interceptación de las comunicaciones entre dos partes.

2.3.3.4 FININT

Son las siglas de FINantial INTelligence. Es la recopilación de información sobre los asuntos financieros de las entidades de interés, para comprender su naturaleza y capacidades, y predecir sus intenciones.

2.3.3.5 GEOINT

Son las siglas de GEOspatial INTelligence, es inteligencia sobre la actividad humana en la tierra derivada de la explotación y el análisis de imágenes e información geoespacial que describe, evalúa y representa visualmente características físicas y actividades geográficamente referenciada en la Tierra.

2.3.3.6 CYBINT

Son las siglas de Cyber Intelligence. En general, se usa CYBINT para transmitir la idea de un conocimiento amplio y mejor calificado eventos reales o potenciales relacionados con el ciberespacio, que pueden poner en peligro una organización.

2.3.3.7 MASINT

Son las siglas de Measurement And Signature INTelligence. Se trata de la inteligencia de medición y firma. Es una rama técnica de la recopilación de inteligencia, que sirve para detectar, rastrear, identificar o describir las características distintivas de las fuentes de destino fijas o dinámicas. Es utilizada casi exclusivamente en los ambientes militares, ya que analiza las señales que emiten los equipamientos como armas y dispositivos de rastreo.

Generalmente los datos son obtenidos a través de técnicas de SIGINT.

2.3.4 Fuentes de inteligencia

2.3.4.1 Indicadores de Compromiso (IOCs) [12]

Están asociados con actividad maliciosa. Los hashes de muestras de malware, o de archivos MD5 y SHA1, los movimientos laterales dentro de la red, los scans, las direcciones IP y los nombres de dominios pueden ser usados para actualizar los firewalls y sistemas de detección, así como contribuir a entender las tácticas, técnicas y procedimientos de los *Threat Actors .* Un IoC es un esquema, normalmente escrito en XML, en el que se especifican ciertos detalles técnicos replicables enlazados mediante operadores lógicos (AND, OR, etc), para evidenciar o indicar si un sistema ha sido o no comprometido.

Un IOC puede escribirse en varios formatos bajo diferentes esquemas XML (STIX, OTX, CIF, OpenIOC). Es un documento de intercambio de información, fácilmente adaptable y en constante actualización, flexible, con evidencias específicas de un sistema en particular y generales de todos los sistemas afectados.

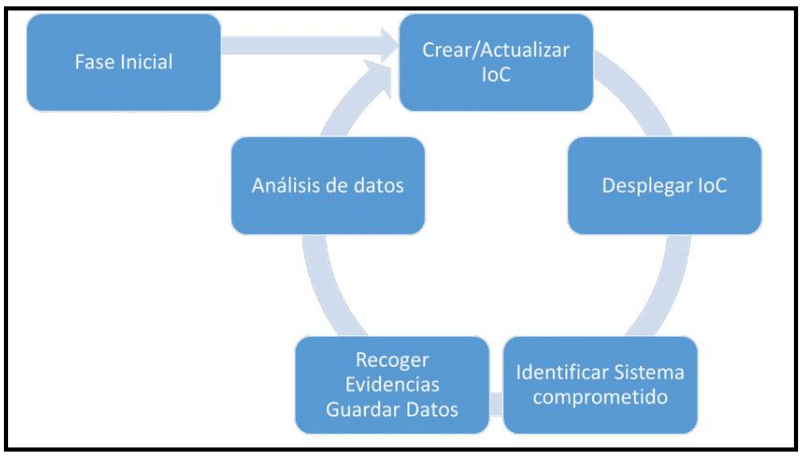

Figura 18: Ciclo de aplicación de un IoC durante un incidente, documento en continuo cambio de forma recursiva [11]

2.3.4.2 Tácticas, Técnicas y Procedimientos (TTPs)

Se trata del intercambio de inteligencia sobre actores conocidos. Cada actor tiene una huella digital característica, por ejemplo los movimientos laterales que utilizan normalmente dentro de la red, o la forma que emplean dichos actores para elevar privilegios en un sistema, etc. Es lo que constituye su táctica, técnica y procedimientos (TTP). Conocerlos permitirá crear medidas de detección específicas, mejorando la defensa frente a estos posibles escenarios.

2.3.4.3 Información automática de herramientas.

Muchas organizaciones tienen automatizadas las funciones de recolección de datos, las cuales permiten a su equipo de CTI, la visualización y el análisis del perímetro de su infraestructura de tecnología de información.

2.3.4.4 Alertas de seguridad.

Son las notificaciones que le indican al equipo CTI de que un proceso anómalo está sucediendo.

2.3.4.5 Reporte o Informe de Inteligencia de Amenazas.

Es el reporte sobre el análisis de las amenazas. La información contenida en el reporte debe ser oportuna, precisa, procesable, relevante, y adecuada a los distintos perfiles profesionales a los que va dirigida y que son los que toman las decisiones.

2.4 Niveles de CTI

La inteligencia de amenazas tiene tres niveles, denominados estratégico, táctico y operacional, como podemos apreciar en la siguiente figura:

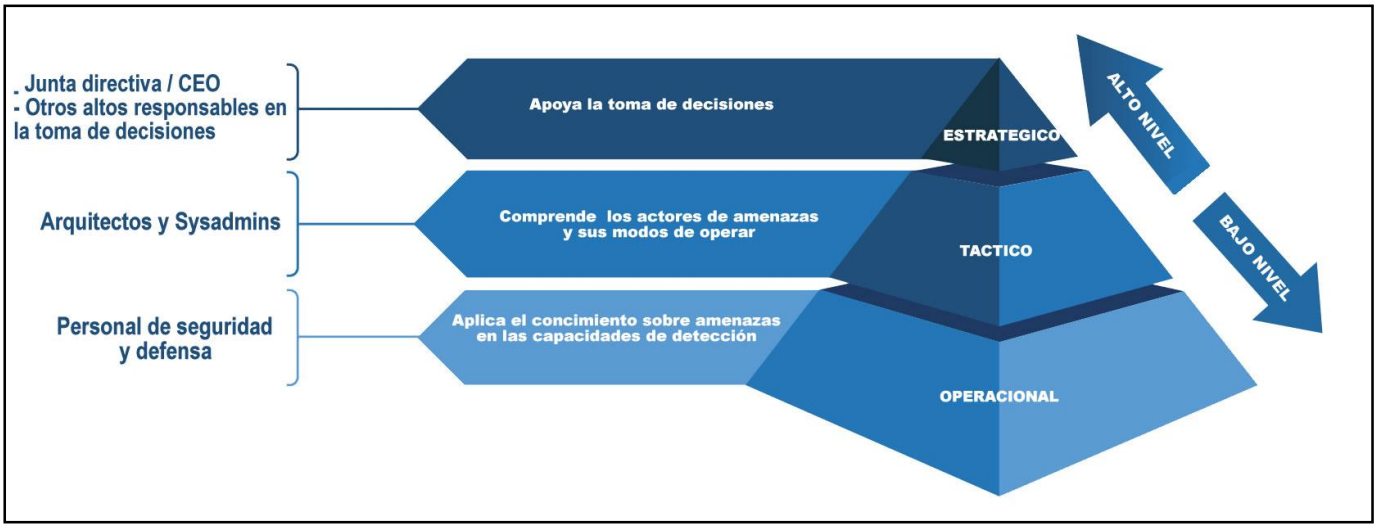

Figura 19: Niveles del *Threat Intelligence* [13]

La inteligencia táctica se construye en base a recomendaciones sobre los procedimientos de respuesta a incidentes, la estratégica se construye en base a conocimientos que la inteligencia táctica ha reunido. El análisis de los datos puede utilizarse para la ayuda en la toma de decisiones e incrementar el nivel de seguridad de la organización. La inteligencia operacional tiene el componente activo de detectar de forma ágil, rápida y oportuna cualquier indicio de actividad sospechosa.

En este marco, es posible realizar el siguiente detalle:

– Inteligencia estratégica sobre amenazas: existe para informar a los altos funcionarios y juntas ejecutivas de las decisiones sobre los cambios

más amplios en el panorama de las amenazas. Debido a esta audiencia, los productos de inteligencia estratégica se expresan en un lenguaje carente de tecnicismos y se centran en cuestiones de riesgo comercial más que en los aspectos técnicos específicos.

El formato de presentación de informes de los productos estratégicos de inteligencia sobre amenazas cibernéticas reflejará esta visión a largo plazo y a menudo se difundirá mensual o trimestralmente para ayudar a la formulación de una estrategia a largo plazo.

- Inteligencia táctica sobre amenazas: tiene un componente más técnico. Se centra en las tácticas, técnicas y procedimientos de los atacantes. Está relacionado con los vectores de ataque específicos usados por los actores de amenazas en una industria o una ubicación geográfica y con su modo de operar. Es utilizado por el personal operativo (personal de respuesta a incidentes, profesionales de ciberseguridad, gerentes de servicios de TI, gerentes de operaciones de ciberseguridad, administradores y arquitectos de redes) para garantizar que los controles y procesos técnicos sean adecuados para la prevención de riesgos.

Los indicadores de compromiso (IOC) son el principal producto de los proveedores de inteligencia de amenazas tácticas. Son especialmente útiles para actualizar los sistemas de defensa basados en firmas para defenderse de los tipos de ataque conocidos y también para tomar medidas más proactivas. El formato de presentación de informes de los productos tácticos de inteligencia sobre amenazas cibernéticas es del tipo forense e incluye información altamente técnica, informes de campañas de spam, malwares, datos e informes sobre incidentes, reportes de grupos de ataque, y de inteligencia humana en general.

- Inteligencia operacional sobre amenazas: La inteligencia de amenazas operacionales a menudo se relaciona con detalles de posibles operaciones inminentes contra una organización. Ayuda al personal de seguridad a anticipar cuándo y de dónde vendrán los ataques. Esta información está destinada a gerentes, jefes, al departamento de sistemas,

forenses de seguridad y al equipo de detección de fraudes, por ejemplo. Se recopila de fuentes humanas, como HUMINT, de fuentes OSINT, de redes chat, de foros, etc. Como puede apreciarse, las fuentes de recopilación son bastante variadas.

Ayuda a la organización a comprender los posibles actores de la amenaza junto con su intención, capacidad y oportunidad de atacar, los activos de TI vulnerables y el impacto del ataque, si tiene éxito. Asiste también a los equipos de respuesta a incidentes y forenses a implementar medidas de seguridad con el objeto de identificar y detener los próximos ataques, mejorar la capacidad de detectar ataques en una etapa temprana y reducir su daño en los activos de TI.

El formato de presentación de informes de los productos operacionales de inteligencia sobre amenazas cibernéticas contiene actividades maliciosas identificadas, cursos de acción recomendados y advertencias de ataques emergentes. Presenta además información accionable para ayudar a mejorar la capacidad de detección.

El siguiente gráfico explica los tipos de inteligencia, quién la utiliza, por qué es valiosa, qué preguntas responden y el valor que proporciona a las organizaciones:

Figura 20: Detalles de los Niveles del Threat Intelligence [15]

2.5 Ciclo de Vida del CTI

El Ciclo de Inteligencia sobre Amenazas Cibernéticas prepara a las organizaciones para afrontar las amenazas, posibilita la predicción y detección de brechas, y responder a los incidentes o recuperarse de ellos.

El ciclo tiene cinco fases principales, conformadas en un proceso de naturaleza cíclica. Esto implica que cada fase debe incorporar un proceso de revisión para asegurar que el material requerido se procese y se transmita correctamente, y que las necesidades del consumidor de inteligencia están constantemente en el centro del proceso.

Las fases del ciclo de inteligencia se describen en la siguiente figura:

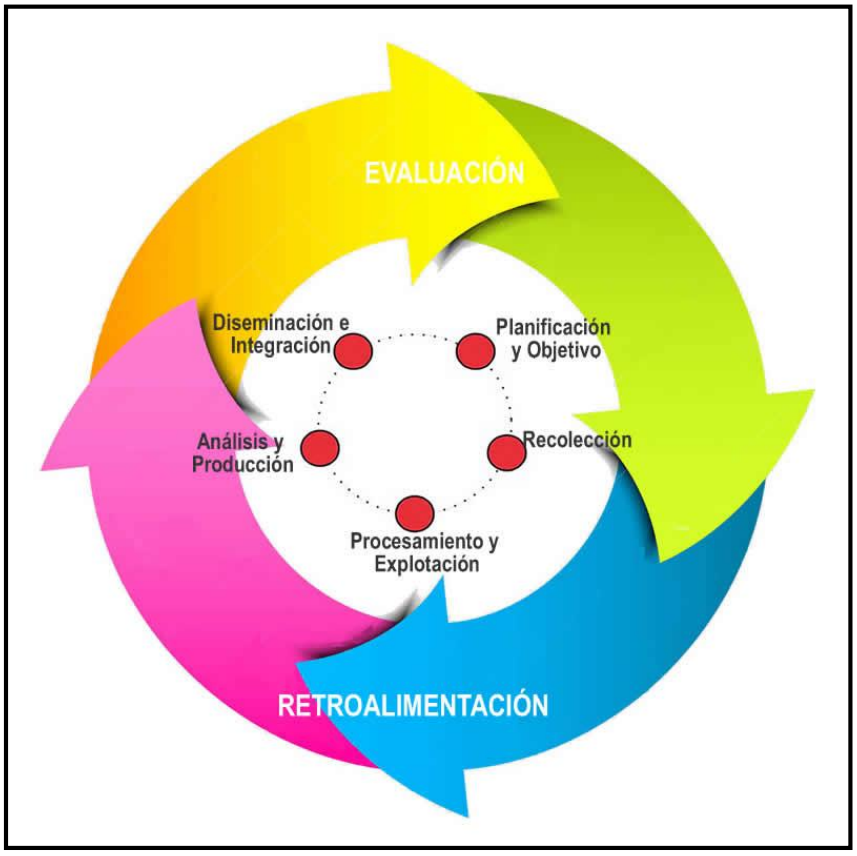

Figura 21: Ciclo de Vida del *Threat Intelligence* [16]

2.5.1 Planificación y Objetivo

Es en la fase de inicio, que se define el objetivo, se determinan las necesidades y de acuerdo a ellas, se planifica el tipo de inteligencia y los procedimientos necesarios para obtenerla. El proceso consiste en identificar, priorizar y validar las necesidades de inteligencia, traducirlas de modo que sean observables, preparar planes de recopilación, emitir solicitudes de reunión, producción y difusión de información y vigilar continuamente la disponibilidad de los datos reunidos.

2.5.2 Recolección

Durante esta fase se adquiere la información de las distintas fuentes posibles, tanto técnicas como humanas e incluye tanto la adquisición de información como el suministro de esa información a las áreas de elaboración y producción. Esta fase incluye la elaboración de guías de recolección para garantizar la óptima utilización de los recursos de inteligencia disponibles.

La recopilación se puede realizar a través de una variedad de medios como extracción de metadatos y registros de las redes internas, registros de los dispositivos de seguridad, recolección de datos sobre noticias, blogs de código abierto, de sitios web o foros, extracción de datos provenientes de la web profunda, datos de proveedores de seguridad, informes de malwares, entre otros. En esta fase será necesaria la cooperación con otras organizaciones para compartir datos privados e incluso tener una presencia activa en la web oscura, para obtener conjuntos de datos más complejos.

Las operaciones de recolección dependen de comunicaciones seguras, rápidas, redundantes y fiables para permitir el intercambio de datos y ofrecer oportunidades para el seguimiento cruzado de los activos y los intercambios de información entre ellos. Una vez reunida, la información se correlaciona y se envía para su procesamiento y producción.

2.5.3 Procesamiento y explotación

Esta fase implica la conversión de la información recolectada en un formato adecuado para la producción de inteligencia, es decir, en un formato comprensible que pueda ser fácilmente utilizado por los analistas de inteligencia, o como entrada de una herramienta automatizada.

El procesamiento puede incluir actividades como la traducción y la reducción de los mensajes interceptados a formato escrito para permitir un análisis y una comparación detallados con otra información, de manera de proporcionarles un contexto y descartar posibles ambigüedades. Otros tipos de procesamiento incluyen la producción de video, el procesamiento fotográfico y la correlación de la información recogida por las plataformas técnicas de inteligencia.

La información recolectada a menudo puede necesitar de correlación, clasificación y verificación para evaluar su utilidad.

2.5.4 Análisis y producción

Se trata del proceso de analizar, evaluar, interpretar e integrar los datos y la información procesada, transformándola en productos de inteligencia terminados. Implica un proceso más humano, que convierte la información procesada en inteligencia, que pueda ayudar a las decisiones. Estas decisiones pueden involucrar la investigación de una amenaza específica potencial, o si se está produciendo un ataque, se extrae conocimientos sobre su metodología y se determinan las acciones a tomar así como los procesos y herramientas a utilizar para bloquearlo.

Se analiza la coherencia de los datos procesados y se los ordena de manera efectiva, se evalúa su relevancia para extraer conclusiones, qué información es útil y cuál será descartada por redundante, errónea o inaplicable al requisito de inteligencia.

El producto final de esta fase, debe permitirle al analista extraer conclusiones analíticas respaldadas por los datos disponibles. La forma en la que se presenta la información es especialmente importante. El informe debe

ser conciso, y evitar términos o jerga confusa y excesivamente técnica. Debe incluir también un curso de acción recomendado.

2.5.5 Diseminación e integración

Durante esta fase se distribuye la información en un lenguaje y formato claro y conciso y en un medio asequible. Puede incluir informes verbales, escritos y productos de imágenes, resúmenes ejecutivos y presentaciones destinadas a los tomadores de decisiones.

El tipo de informe dependerá de los perfiles profesionales a los que está dirigido, dependiendo del nivel de la estructura del *Cyber Threat Intelligence* ocupen. Si el informe está dirigido a personal del nivel estratégico debe incluir información sobre impacto económico, el histórico de ataques y las tendencias y toda otra información que pueda afectar a las decisiones de la junta directiva.

Si está dirigido a personal del nivel táctico, responsable de sistemas o infraestructura, el informe contendrá información sobre metodologías de los atacantes, así como sus tácticas, técnicas y procedimientos. Si está dirigido al nivel operacional, es decir aquellos responsables de seguridad operativa el informe contendrá formas de mitigación de posibles ataques y recomendaciones de medidas y acciones necesarias antes un posible ataque.

Durante el proceso de integración, el producto terminado vuelve a la cima, iniciándose el ciclo nuevamente.

2.5.6 Evaluación y retroalimentación

Constituyen un marco común a todas las fases. En todo momento se evalúan si los resultados que se van obteniendo son útiles y se contemplan las oportunidades de mejora en cualquiera de las fases.

2.6 Defensa y ataque

La defensa en el mundo digital está constituida por una serie de acciones que se realizan en respuesta ante una amenaza identificada. Para poder implementar una defensa efectiva, es imprescindible considerar a su

contrario, el ataque. Además entender a los actores que están detrás y la metodología utilizada. Tener un profundo y amplio entendimiento de los actores de amenazas, grupos de amenazas, actores del estado nación, grupos *hacktivistas*, y cómo evolucionan con el tiempo, es clave para desarrollar una inteligencia aplicable a la defensa.

Los componentes de una defensa efectiva pueden ser apreciados en la siguiente figura:

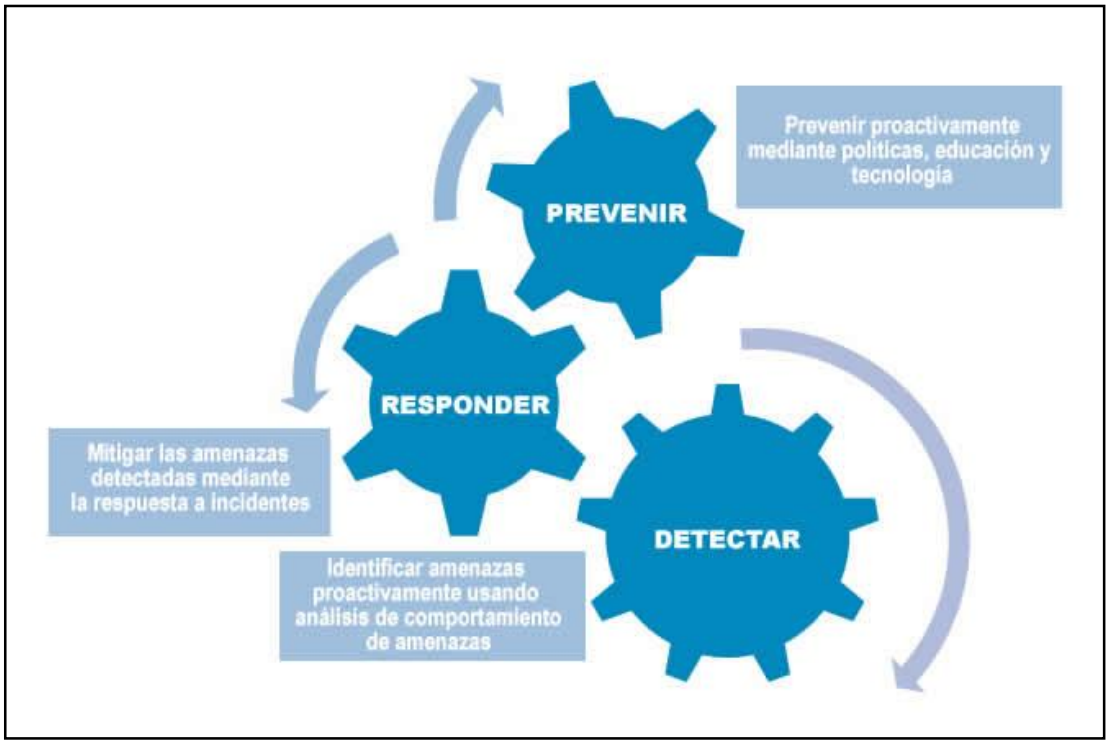

Figura 22: Componentes de una defensa efectiva que se beneficia del *Threat Intelligence* [17]

- Detectar: la inteligencia de amenazas permite detectar un ataque antes de que ocurra, a través de análisis de comportamientos sospechosos que pueden estar ocurriendo en la red. Se necesita contar con tecnologías de detección capaces de acceder a los datos de inteligencia de amenazas en tiempo real.
- Responder: la respuesta a los incidentes basado en información obtenida de la inteligencia de amenazas, permite la recuperación más rápida

ante a un ataque y la reducción del tiempo de permanencia del atacante, es decir que la actividad puede volver a la normalidad más rápidamente con un menor impacto. Asimismo, permite contar con información inteligente de la acción a llevar a cabo después del proceso de investigación de incidentes y planificar acciones que impidan que el ataque vuelva a repetirse.

– Prevenir: la acción de prevención basada en la inteligencia de amenazas permite implementar medidas proactivas para identificar potenciales atacantes así como sus intenciones y métodos.

2.6.1 Amenaza

Se entiende por amenaza la intersección de tres conceptos: oportunidad, capacidad e intención.

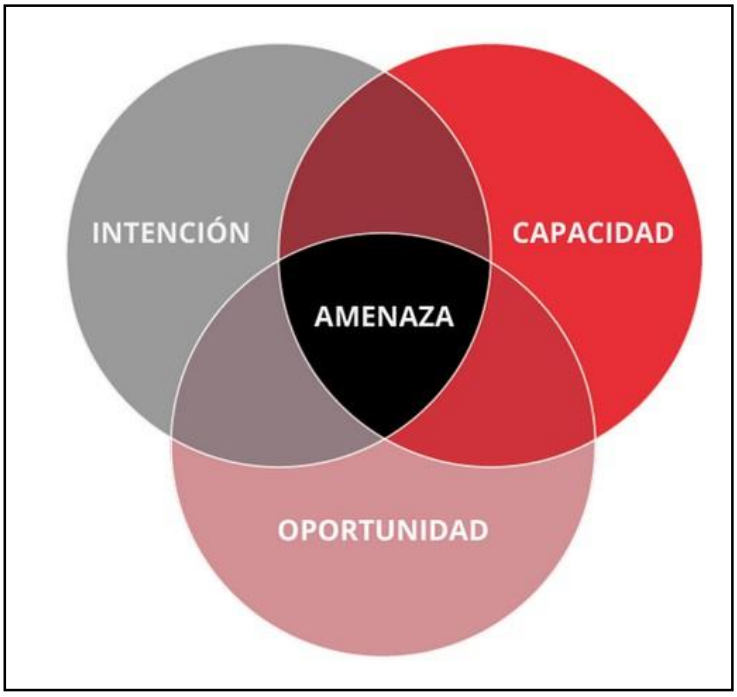

Figura 23: Amenaza: oportunidad, capacitación e intención [17]

La capacidad, incluye los recursos técnicos para generar una amenaza, La oportunidad es el momento propicio para explotar una vulnerabilidad y la intención es la voluntad de llevar a cabo la materialización de la amenaza.

Para llevar a cabo la inteligencia de amenazas en una organización, es crucial contar con un equipo de especialistas con capacidad para identificar los actores de amenazas y clasificarlos por el nivel de impacto en la organización.

2.6.2 Actores de amenazas

La siguiente tabla tipifica los actores de amenazas y muestra el objetivo que persiguen y los métodos que utilizan:

QUIEN	Estados	Criminales organizados	Ciberterroristas	Hacktivistas	Amenazas persistentes avanzadas	Insiders
PORQUE	Disrupción de infraestructuras críticas. Robo de secretos comerciales, industriales y/o militares	Beneficio económico a través del fraude, extorsión.	Inculcar el miedo para que los objetivos de los atacantes cumplan las demandas	Disrupción, humillación política	Robo de propiedad intelectual, beneficio económico a través de espionaje	Emocional, o necesidades financieras
QUE COMO	Espionaje diplomático, cibersabotaje.	Malware, troyanos, ransomware	usando la cibernética para desarrollar sus programas (reclutar, incitar, entrenar, planear y financiar)	Denegación de servicio, brechas de seguridad	Malware dirigido, espionaje corporativo	Uso de conocimiento interno para robar datos. Realizar fraudes

Figura 24:[16] Actores de amenazas

2.6.3 Métodos

– Ingeniería social: una táctica común, a veces incluso no técnica, que se basa en la interacción humana para engañar a otras personas a fin de que rompan los procedimientos de seguridad normales, permitiéndoles obtener información que puede ser útil para explotar vulnerabilidades.

– *Phishing – Spear Phishing:* mensajes de correo electrónico generales o dirigidos, publicaciones en línea, u otras comunicaciones electrónicas que se hacen pasar por una parte confiable en un intento de

[16] Cybercamp 17 Threat Intelligence – Desde qué es hasta cómo lo hago. [En línea] Disponible en https://es.slideshare.net/WiktorNykielLION/cybercamp17-threat-intelligence-desde-qu-es-hasta-cmo-lo-hago - Slide 28 de 78

engañar al objetivo para que divulgue información o descargue software malicioso.

- Malware destructivo: es una categoría de código malicioso que incluye virus, gusanos y troyanos. El malware destructivo utilizará herramientas de comunicación populares para propagarse, incluyendo gusanos enviados por correo electrónico y archivos infectados por virus descargados de conexiones *peer-to-peer*.
- *Exploits kits:* Paquetes que contienen programas maliciosos que se utilizan principalmente para llevar a cabo ataques automatizados desde dispositivos de almacenamiento con el fin de propagar el malware. Estos kits se venden en el mercado negro, donde se pagan precios que van desde varios cientos a mil dólares estadounidenses. Estos kits buscarán explotar las vulnerabilidades existentes en los sistemas afectándolos silenciosa y fácilmente.
- Descargas de almacenamientos: Un programa que se instala automáticamente en la computadora de un objetivo con sólo visitar un sitio web. Las víctimas no tienen que hacer clic explícitamente en un enlace dentro de la página.
- Denegación de servicio distribuido: A través de programas informáticos y/o un mayor número de participantes, los hackers inundan el sitio web del objetivo del ataque con más tráfico del que el servidor puede manejar. A medida que el sitio intenta procesar el gran volumen de tráfico malicioso, deniega el acceso de los usuarios legítimos. El gran volumen de tráfico puede causar el colapso de los servidores.
- Amenaza avanzada persistente (APT): [19] La definición ampliamente aceptada de amenaza persistente avanzada es que se trata de un ataque selectivo de ciberespionaje o cibersabotaje llevado a cabo bajo el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política. No todos los ataques de este tipo son muy avanzados y sofisticados, del mismo modo que no todos los ataques selectivos complejos y bien estructurados son una amenaza

persistente avanzada. La motivación del adversario y no tanto el nivel de sofisticación o el impacto, es el principal diferenciador de un ataque APT de otro llevado a cabo por ciberdelincuentes o hacktivistas.

Puede apreciarse el ciclo de vida de la APT en la siguiente figura:

Figura 25: Ciclo de vida de la Amenaza Persistente Avanzada

– Recolección/Preparación: durante esta etapa el atacante identifica y selecciona el objetivo y a continuación inicia el proceso de investigación y recolección de información estratégica sobre la víctima. Este proceso puede ser pasivo, porque intenta evitar la detección por parte de la organización y sólo recolecta información de dominios utilizados, direcciones de correo electrónico, mediante búsquedas en redes sociales sobre los

empleados, realiza búsquedas de publicaciones en conferencias, noticias, visitas a sitios web, artículos académicos, etc.

Por otro lado, la recolección activa de información, puede dejar rastros pasibles de ser detectados por la organización o víctima objetivo, como por ejemplo escaneos de red, discusiones en redes sociales, foros, análisis de activos expuestos en internet, etc.

El paso siguiente es crear, reunir o adquirir las ciberarmas que se utilizarán en el ataque. Algunas de ellas pueden ser herramientas de acceso remoto que permiten al atacante acceder y obtener el control del equipo comprometido. Estos elementos son también conocidos como *RAT* por sus siglas en inglés de *Remote Acces Trojans*. También pueden utilizarse herramientas de explotación de vulnerabilidades, denominadas *exploits,* y *malware* o código malicioso que se envía a la víctima con un *payload*, es decir la carga que será luego activada para obtener control del equipo de la víctima u objetivo del ataque.

La fase de preparación finaliza cuando el atacante comprueba que puede evadir los controles de seguridad de la víctima objetivo, a través de una serie de pruebas para asegurar puede lograr la intrusión sin ser detectado.

- Intrusión: en esta fase el atacante luego de prepararse, intenta lograr el acceso al equipo de la víctima objetivo o a la red en la que este se encuentra, con la intención de tomar el control de su dispositivo o recopilar información confidencial. Lo hace desplegando las ciberarmas elegidas durante la fase de la preparación, siendo los medios más utilizados el correo electrónico usando la metodología *Spear Phishing, (*detallada en el punto anterior), dispositivos de almacenamiento USB o sitios web infectados.

Una vez activado el código malicioso que le permite el acceso al atacante, se crean accesos remotos ocultos denominados puertas traseras o *Backdoors.* Seguidamente se establece una conexión, normalmente cifrada, entre la infraestructura del atacante y el equipo comprometido, permitiéndole al intruso tomar el comando y control (C&C).

- Propagación: en esta fase, dado que existe la posibilidad de que el equipo vulnerado no contenga información sensible, el atacante necesitará buscar otros objetivos dentro de la red, como servidores de bases de datos, de archivos, etc. e ir propagándose dentro de la red colindante (LAN, o *Local Area Network*) o a través de internet. Con la propagación, el atacante asume un mayor riesgo de ser detectado.
- Persistencia: en esta fase, el atacante escala privilegios, logrando inclusive convertirse en administrador y obtiene un acceso elevado a recursos de una aplicación o un usuario que normalmente están protegidos, para mantener el acceso prolongado al sistema objetivo. De este modo, evade los dispositivos de seguridad mutando dinámicamente el malware utilizado.
- Extracción de Datos: en esta fase el atacante, gracias al escalamiento de privilegios, obtiene acceso a información sensible de la víctima objetivo y de su infraestructura que le permite analizar cómo moverse por dentro del dispositivo o de la red para lograr la recopilación y extracción de los datos recogidos que a su vez dirige a los servidores externos.
- Borrado de Huellas: en esta fase, el intruso después de haber logrado su objetivo, procede a eliminar los rastros que pudieran evidenciar su presencia y toda aquella información que pudieran revelar sus acciones, tácticas, técnicas y procedimientos.
- Indicadores de un ataque persistente avanzado: Pueden constituir indicadores, entre otros, hallar código malicioso en los datos adjuntos de uno o varios mensajes de correo electrónico o en la descarga de una página web, notar un incremento alto de inicios de sesión con privilegios elevados durante el periodo nocturno, descubrir conexiones salientes a servidores C&C conocidos, hallar troyanos en endpoint o recursos de red de archivos compartidos, encontrar alto volumen de almacenamiento en sitios en los que no debiera haberlos, detectar comunicaciones anómalas cifradas en SSL o, detectar entradas de registro con comandos de activación y desactivación del firewall o del antivirus.

2.6.4 La pirámide del dolor [21]

La denominada “pirámide del dolor” permite apreciar la relación existente entre distintos tipos de indicadores de compromiso que se pueden utilizar para detectar las actividades de un atacante y cuánto dolor o impacto le causará al adversario cuando se puedan bloquear esos indicadores.

Fue creada por David Bianco en el año 2013, a raíz de un informe publicado por Mandiant sobre APT1 que perfilaba a un grupo conocido como Comment Crew, en el cual sugerían su vínculo con la Unidad 61398 del Ejército Popular de Liberación chino, al notar que la forma de aplicación de los indicadores no estaba siendo utilizados de manera efectiva.

El objetivo de detectar indicadores es darles una respuesta, y una vez que esto ocurra lo suficientemente rápido, se busca bloquear el uso de esos indicadores por parte del adversario. Sin embargo, es importante considerar que no todos los indicadores son iguales y algunos de ellos son mucho más valiosos que otros.

En la siguiente figura pueden apreciarse en detalle estos indicadores:

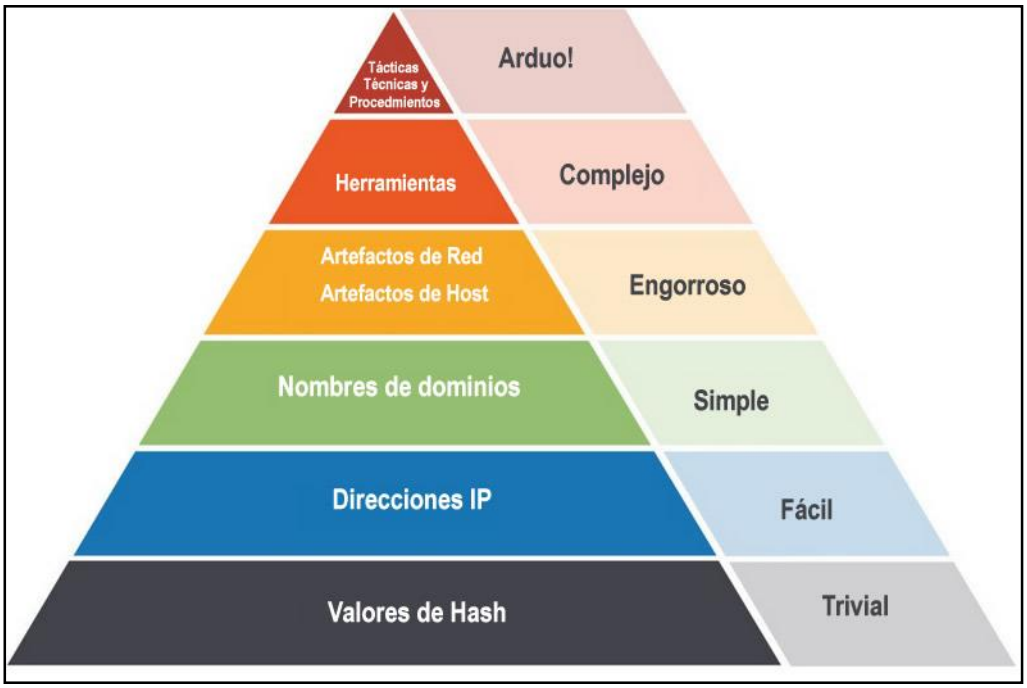

Figura 26: La pirámide del dolor [21]

2.6.4.1 Tipos de Indicadores

Constituyen ejemplos de indicadores:

- Valores de hash: hashes que corresponden a archivos sospechosos o maliciosos específicos, como por ejemplo SHA1, MD5 u otros. Se usan para referenciar unívocamente muestras de malware o archivos involucrados en una intrusión.
- Direcciones IP: dirección IP o un bloque de IPs de una porción de red.
- Nombres de dominio: podría ser un nombre de dominio en sí mismo (por ejemplo, "evil.net") o tal vez incluso un subdominio comprometido (por ejemplo, "this.is.sooooo.evil.net")
- Artefactos de red: aquellas partes de la actividad que pueden tender a distinguir la actividad maliciosa de la de los usuarios legítimos. Los ejemplos típicos pueden ser patrones URI, información C2 integrada en protocolos de red, valores distintivos de HTTP User-Agent o SMTP Mailer, etc.
- Artefactos de host: elementos que puede ayudar a distinguir las actividades maliciosas de las legítimas en uno o más hosts. Pueden ser claves de registro o valores que se sabe que fueron creados por piezas específicas de malware, archivos o directorios que se colocaron en ciertos lugares o que usan ciertos nombres, servicios maliciosos o casi cualquier otra cosa que sea distintiva.
- Herramientas: software utilizado por el atacante, como códigos diseñados para crear documentos maliciosos para *spearphishing*, puertas traseras utilizadas para establecer C&C o descifradores de contraseñas u otras utilidades basadas en host que quieran usar después del compromiso.
- Tácticas, técnicas y procedimientos(TTPs): metodología que utiliza el atacante, como por ejemplo *spearphishing* con un archivo PDF troyanizado o con un enlace a un archivo .SCR malicioso disfrazado como ZIP, etc.

2.6.4.2 La pirámide explicada

El ancho y los colores de la pirámide son muy importantes para comprender el valor de este tipo de indicadores.

- Valores hash: los indicadores hash son muy precisos, son más resistentes al cambio y la manipulación, cualquier cambio en un archivo aunque sea uno intrascendente, da como resultado un valor de hash completamente diferente. Como la probabilidad de que dos archivos distintos coincidan en su valor de hash es baja, se puede descartar casi por completo.
- Dirección IP: Las direcciones IP son el indicador más fundamental. El atacante necesita tener una conexión de red de algún tipo para llevar a cabo un ataque y una conexión significa necesariamente una dirección IP. Está en la parte más ancha de la pirámide porque hay muchos de ellos. Cualquier adversario razonablemente avanzado puede cambiar las direcciones IP cuando le convenga, con muy poco esfuerzo. En algunos casos, si están utilizando un servicio de proxy anónimo como Tor o algo similar, pueden cambiar las IP con bastante frecuencia. Es por eso que las direcciones IP son verdes en la pirámide: si se bloquea al adversario el uso de una de sus IPs, generalmente puede recuperarse sin esfuerzo.
- Nombres de dominio: los nombres son un poco más difíciles de cambiar, porque necesitan estar registrados y alojados en algún lugar. Si bien existe una gran cantidad de proveedores DNS poco estrictos y hasta gratuitos, y es sencillo cambiar los dominios, los nuevos dominios pueden tardar un tiempo en ser visibles y estar accesibles, por lo que es un poco más difícil de cambiar que las direcciones IP.
- Artefactos de red y host: en este nivel de la pirámide se aprecia el impacto negativo del atacante. Cuando se puede detectar y responder a los indicadores de este nivel, se puede lograr que el atacante regrese a su laboratorio y reconfigure y/o recompile sus herramientas. Un ejemplo sería cuando se descubre que la herramienta de reconocimiento HTTP del atacante usa una cadena distintiva de *User-Agent* o que simplemente utilizó su nombre.

Si se bloquea cualquier solicitud que presente este User-Agent particular, lo obliga a regresar y pasar algún tiempo para: i) averiguar cómo detectó su herramienta de reconocimiento; y ii) solucionarlo. La solución puede ser trivial, pero al menos lo obligó a hacer un esfuerzo para identificar y superar ese obstáculo.

– Herramientas: esta parte de la pirámide implica investigar, encontrar una herramienta que permita detectar variaciones en los archivos, incluso si son mínimos o moderados, desarrollarla, y aprender a utilizarla. Con ella se puede detectar las herramientas utilizadas por el atacante para bloquearlo. Algunos ejemplos de indicadores de herramientas podrían incluir firmas AV o Yara, si son capaces de encontrar variaciones de los mismos archivos incluso con cambios moderados. Las herramientas de conocimiento de redes con un protocolo de comunicación distintivo también pueden encajar en este nivel, en el que cambiar el protocolo requeriría reescribir sustancialmente la herramienta original. Además, como se ha mencionado anteriormente, los hashes borrosos probablemente entrarían en este nivel.

Siempre que reciba nueva información sobre un adversario (de cualquier APT), se debe revisar cuidadosamente contra la Pirámide del Dolor. Para cada párrafo, se puede preguntar "¿Hay algo que pueda usar para detectar la actividad del adversario?.¿Dónde en la pirámide y cuánto dolor le puede causar al adversario?

Una conclusión clave de la Pirámide del Dolor de Bianco es que los TTP son los indicadores más valiosos ya que reflejan el comportamiento del atacante, y éste requiere un tiempo significativo y una inversión monetaria. Sin embargo, los TTP también son difíciles de modelar y detectar utilizando herramientas tradicionales. A diferencia de muchos otros indicadores, los TTP son solo reconocibles una vez que alguien ha sido capaz de reconstruir la narrativa de un ataque.

2.7 Marcos analíticos para CTI

Los marcos analíticos proporcionan una estructura para analizar ataques y adversarios, permiten una comprensión amplia para entender cómo piensan los atacantes, su metodología, dónde ocurren los eventos específicos y el ciclo de vida de un ataque. Este conocimiento resultante permitirá tomar rápidas medidas para detener cuanto antes a los atacantes.

Existen tres tipos:

- Cyber Kill Chain
- Modelo diamante
- MITRE ATT&CK

2.7.1 Cyber Kill chain

Proporciona un marco para describir y abordar las fases de un ataque. Se lo trata como una cadena porque se compone de una serie de pasos necesarios, donde una mitigación en cualquiera de ellos supone la ruptura de la cadena, lo cual refleja el ataque frustrado.

Kill chain o cadena de la muerte, es un modelo desarrollado en los años 90 por la Fuerza Aérea de los Estados Unidos, que consta de seis pasos para llevar a cabo una operación militar:

1) Encontrar (Find)
2) Asegurar (Fix)
3) Rastrear (Track)
4) Elegir blanco (Target)
5) Abordar (Engange)
6) Evaluar (Assess)

Basado en esta secuencia de pasos, se modeló el marco Cyber Kill Chain, como forma de descripción de los pasos que se llevan a cabo durante un ataque y cómo protegerse.

La siguiente figura describe el marco mencionado:

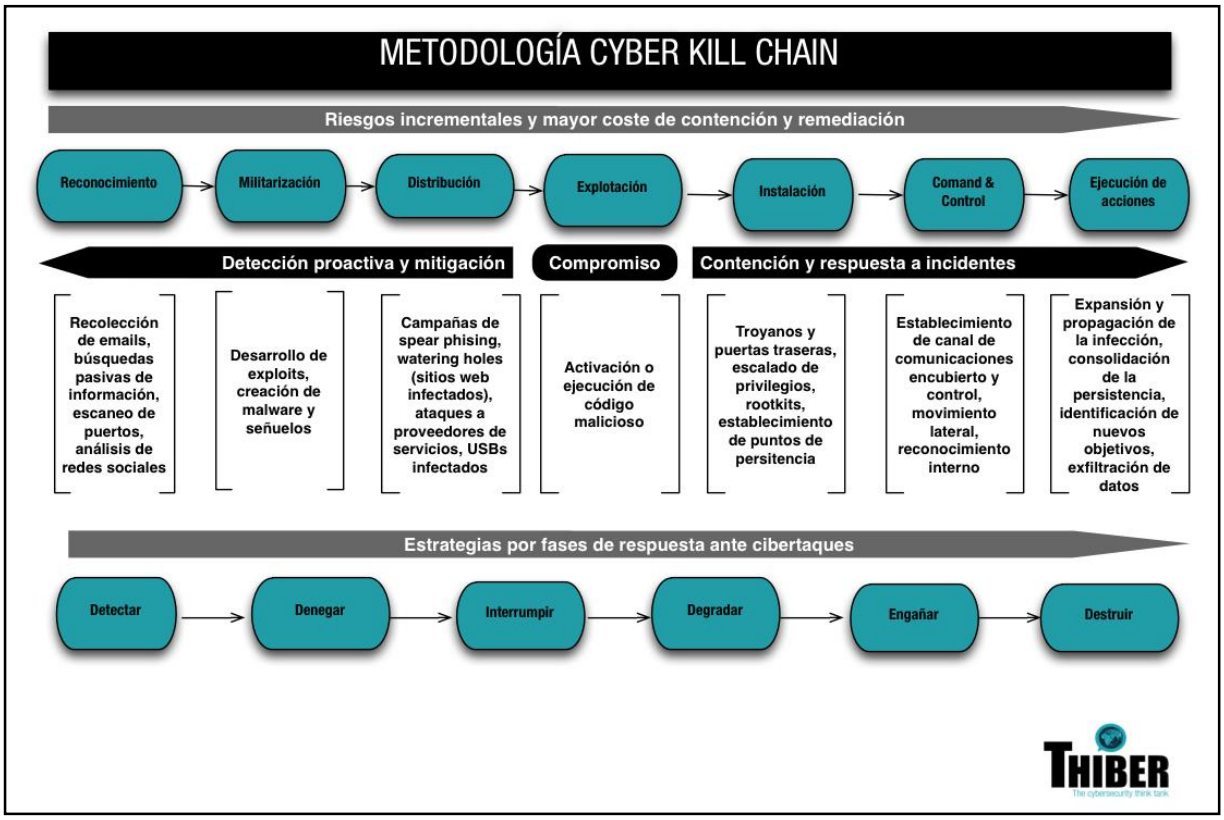

Figura 27: Fases de Cyber Kill Chain [22]

Descripción de los eslabones de la cadena:

- Reconocimiento (*Reconnaissance*): los atacantes realizan la investigación, identificación y selección de la víctima objetivo. Es la etapa de recolección de información a partir de fuentes abiertas, como por ejemplo listas de correo electrónico, redes sociales, sitios web, etc.
- Militarización *(Weaponization):* el atacante analiza los datos recopilados sobre la víctima objetivo para determinar qué métodos de ataque va a utilizar para explotar y obtener el acceso no autorizado. El objetivo de este eslabón es la preparación de la vía de intrusión.
- Entrega *(Delivery):* una vez seleccionado el método a utilizar, se determina el mecanismo más conveniente de distribución de la amenaza, que puede ser un *phishing*, la entrega de un dispositivo de almacenamiento (USB) infectado o el montaje de un sitio vulnerable, entre otros. Es una etapa clave porque mide la efectividad de las estrategias de defensa implementadas por la organización objetivo.

- Explotación *(Exploitation)*: si la propagación fue exitosa, el atacante espera que el código malicioso sea ejecutado para obtener acceso remoto al sistema de la víctima, explotar la vulnerabilidad elegida y propagar la infección a otros sistemas. En esta etapa la organización objetivo tendrá la tarea de evitar la explotación de las vulnerabilidades, utilizando estrategias de mitigación.
- Instalación *(Installation)*: en esta etapa la explotación de la vulnerabilidad es utilizada para acceder al sistema de la víctima y tratar de asegurarse el acceso de forma permanente, es decir lograr la persistencia por ejemplo creando un *backdoor,* o puerta trasera.

El atacante intentará ocultar su presencia y actividades maliciosas de los controles de seguridad de la víctima como firewalls utilizando por ejemplo técnicas de cifrado.

- Mando y control *(Command and Control):* en esta etapa de la cadena, se realiza la gestión del acceso conseguido. El atacante establece los canales de comunicación que le van a permitir controlar a distancia el sistema vulnerado con sistemas de mando y control. Se aplican técnicas de escalada de privilegios y se continúa ocultando la evidencia de compromiso.
- Ejecución de acciones sobre Objetivos *(Actions on Objectives)*: esta es la etapa en la que el atacante ejecuta acciones para obtener información, moverse dentro de la red buscando otros objetivos o lograr accesos a aplicaciones específicas.

Las fases descriptas pueden ocurrir en paralelo y no necesariamente de manera secuencial.

El *Kill Chain* tiene ciertas limitaciones, siendo una de las grandes críticas a este marco que no tiene en cuenta la forma en que funcionan muchos ataques modernos, por ejemplo, en muchos casos de *Phishing* se omite la etapa de explotación por completo y en cambio confían en que la víctima abra un archivo con macros incrustados al hacer clic en él. Sin embargo, aún con esta limitación este marco provee una buena línea de base para detectar ataques y saber dónde bloquearlos.

2.7.2 El modelo diamante

Constituye un modelo matemático que permite la aplicación de la teoría de juegos y, la teoría de clasificación *clustering* con la finalidad de mejorar el proceso de análisis y toma de decisiones.

El modelo establece un método formal que aplica principios científicos al análisis de intrusión, medición, comprobación y repetición, proporcionando un lineamiento integral para la documentación, síntesis y correlación de la actividad.

Este enfoque científico y su simplicidad producen mejoras en la eficacia, eficiencia y precisión analítica. El modelo proporciona oportunidades para integrar la inteligencia en tiempo real para la defensa de la red, automatizando la correlación entre los eventos, clasificándolos con cierto grado de confianza sobre las campañas de los adversarios y prediciendo las operaciones de los atacantes mientras se planifican y ponen en práctica estrategias de mitigación.

Consta de cuatro fases o aristas relacionadas con los atacantes como puede apreciarse en la siguiente figura:

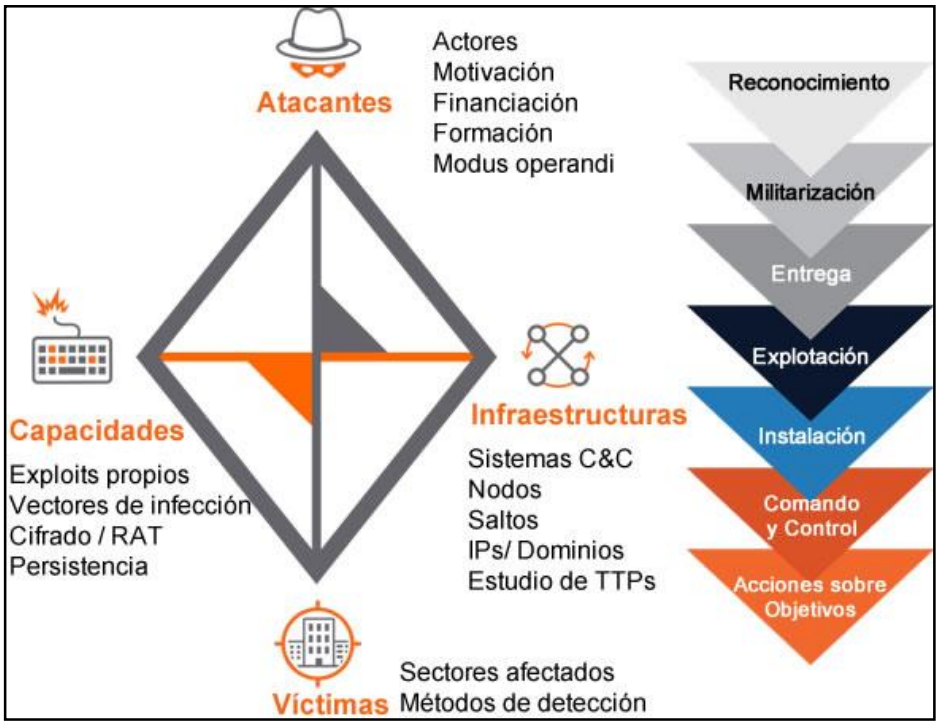

Figura 28: El modelo diamante [23]

Descripción de los cuadrantes del modelo:

- Actores de amenazas o *threat actors*, su motivación, financiación, su formación y el modus operandi.
- Las capacidades, los exploits propios, los vectores de infección, metodología, la capacidad que tiene ese adversario para atacar a la víctima.
- Víctima objetivo, si el ataque es hacia un sector o a una organización y si el objetivo cuenta con métodos de detección.
- Infraestructura, cuál va a ser la infraestructura que va a utilizar el atacante para actuar sobre ese objetivo y si va a utilizar sistemas de comando y control, nodos, IPs, dominios. En este cuadrante se realiza el estudio de las tácticas, técnicas y procedimientos.

2.7.3 MITRE ATT&CK

Mitre es un centro de investigación y desarrollo no comercial, que tiene sus orígenes en el Instituto Tecnológico de Massachusetts (MIT, por sus siglas en inglés), cuando un grupo de científicos desarrolló sistemas de defensa aérea y computadoras durante la Segunda Guerra Mundial. Ha tenido un gran impacto en la industria de la seguridad, incluido el desarrollo y mantenimiento de las bases de datos de vulnerabilidades y exposiciones comunes, conocidas con el código CVE.

Ha desarrollado un marco de trabajo o *framework* conocido como MITRE ATT&CK, (por sus siglas en *inglés Adversarial Tactics, Techniques, and Common Knowledge*), es decir Tácticas, Técnicas y Conocimiento Común del Adversario.

Este modelo es una evolución de la *cyber killchain* y puede ser utilizado para caracterizar y describir mejor el comportamiento del adversario, una vez que logra la intrusión inicial y comienza a buscar su verdadero objetivo. Posibilita la organización y categorización de los distintos tipos de ataques, amenazas y procedimientos realizados por los atacantes como así también identificar las vulnerabilidades en los sistemas informáticos.

Esta categorización contiene una lista de técnicas que un adversario podría utilizar para realizar esa táctica. Las técnicas se descomponen para proporcionar una descripción de los indicadores, el análisis de detección y la determinación de estrategias de mitigación posibles.

MITRE separó a ATT&CK en diferentes matrices: la matriz pre-ATT&CK contiene tácticas y técnicas relacionadas con las acciones que los atacantes realizan antes de intentar la explotación de un sistema, una red o un objetivo en particular y la matriz ATT&CK para empresas, que contiene diferentes categorías de tácticas para describir el comportamiento del adversario. Podemos apreciar ambas en la siguiente figura:

Tácticas PRE-ATT&CK	Tácticas de ATT&CK para empresas
• Definición de prioridades • Selección de objetivos • Recopilación de información • Identificación de debilidades • Operaciones de seguridad adversas • Establecer y mantener la infraestructura • Desarrollo del personaje • Creación de funciones • Implementación de funciones	• Acceso inicial • Ejecución • Persistencia • Escalado de privilegios • Evasión de defensas • Acceso a credenciales • Identificación • Movimiento lateral • Recolección • Comando y control • Exfiltración • Impacto

Figura 29: Matrices ATT&CK

ATT&CK es útil en una amplia gama de funciones de seguridad, desde las operaciones y el análisis de amenazas hasta la respuesta a incidentes. Posibilita el rastreo y comportamiento del atacante en una manera estructurada y de forma repetitiva, permite a los equipos priorizar la respuesta a incidentes, obtener un mapa de indicadores de los atacantes e identificar las brechas de seguridad de la organización.

En la siguiente figura podemos apreciar una vista parcial de la matriz de MITRE ATT&CK:

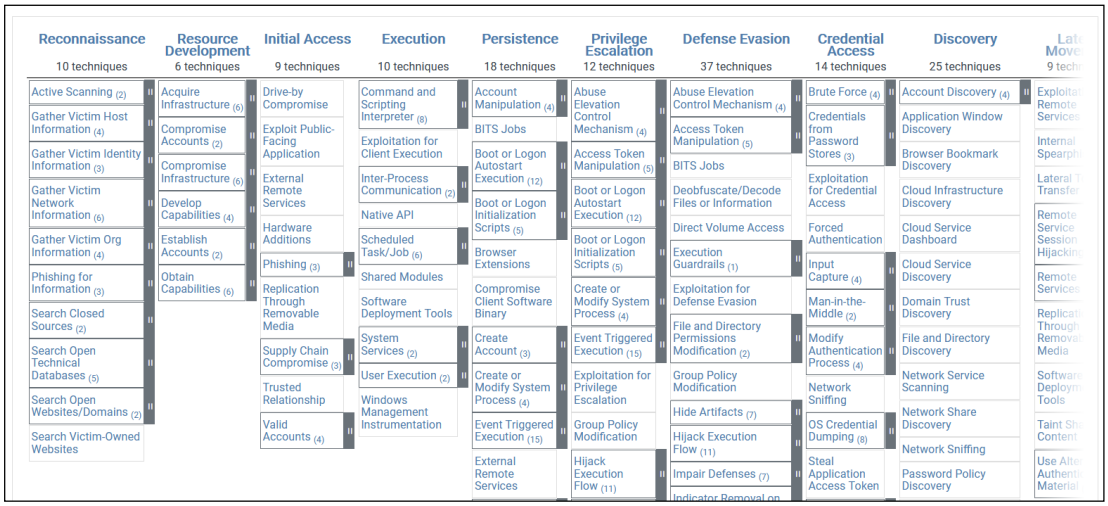

Figura 30: Matriz ATT&CK [24]

Los marcos de inteligencia pueden utilizarse para normalizar la forma en que sus equipos de seguridad monitorean las amenazas, los indicadores, las vulnerabilidades y los actores. De este modo los encargados de seguridad pueden planificar teniendo en cuenta los escenarios posibles y capacitar a todo el personal involucrado en el caso que sea necesario.

2.8 Herramientas y recursos de CTI

Entre las herramientas y recursos de CTI disponibles se encuentran:

– Investigación colaborativa de amenazas (CRITS - COLLABORATIVE RESEARCH INTO THREATS. Es de MITRE. Se trata de un repositorio colaborativo de malware y amenazas, basado en código abierto, para crear una herramienta unificada para analistas y expertos en seguridad dedicados a la defensa de amenazas. En este caso los CRITS utilizan una jerarquía simple pero muy útil para estructurar la información de amenazas cibernéticas que les da a los analistas el poder de pivotar en los metadatos para descubrir contenido relacionado, previamente desconocido.

- Marco de inteligencia colectiva (CIF - COLLECTIVE INTELLIGENCE FRAMEWORK). Se trata de un sistema de gestión de inteligencia de amenazas de código abierto. Los tipos más comunes de información sobre amenazas almacenados en este sistema son IPs, dominios, URLs. CIF permite combinar información conocida sobre amenazas maliciosas de muchas fuentes y usarlas para identificación, detección y mitigación.
- Marco de código abierto para la reunión y el procesamiento de información sobre amenazas (GOSINT - OPEN SOURCE THREAT INTELLIGENCE GATHERING AND PROCESSING FRAMEWORK). Es un marco de código abierto utilizado para emplear, procesar y exportar indicadores de compromiso.
- Marco de gestión de la inteligencia sobre las amenazas cibernéticas (MANTIS – MANAGEMENT THREAT INTELLIGENCE). Constituye una implementación de código abierto, un marco para gestionar la inteligencia de amenazas expresadas en estándares como Stits, cybots, como biotdef. Brinda una información sobre amenazas y repositorios que también tiene capacidades de navegación, filtrado y búsqueda.
- Plataforma de intercambio de información sobre malware (MISP - MALWARE INFORMATION SHARING PLATFORM). Es la plataforma de intercambio de amenazas, una solución de software libre y código abierto para recopilar, almacenar, distribuir y compartir indicadores de compromiso. Brinda también información sobre amenazas relacionadas con análisis de incidentes de seguridad. Es una plataforma bastante usada por los CERTs europeos.
- MINEL, de Palo Alto. Es un marco de procesamiento de indicadores de código abierto. Tiene una arquitectura modular y simplifica la agregación, la aplicación y el intercambio de indicadores de amenazas.
- Tu inteligencia de amenaza diaria (YETI – YOUR EVERY DAY THREAT INTELLIGENCE). Se trata de una plataforma de código abierto destinada a organizar observables, indicadores de compromiso, TTPs y conocimientos sobre amenazas en un único repositorio unificado.

- Estándares para el intercambio de información que valoran o integran todos los marcos mencionados. Se trata de STIX y TAXII, una iniciativa para la prevennción y mitigación de los ataques. STIX establece el QUÉ de la inteligencia de amenazas, mientras que TAXII define CÓMO se transmite esa información. Son estándares para mejorar y posibilitar el intercambio de información en un lenguaje que se entienda o que pueda ser interpretado por la máquina.

Se encuentra disponible en línea un compendio de *framerworks*, plataformas, herramientas, formatos estandarizados de información para compartir (IOCs), investigaciones, estándares utilizados y libros, en el enlace:

https://github.com/hslatman/awesome-threat-intelligence#sources (09-12-2020)

3 Propuesta Institucional / Organizacional

3.1 Recomendaciones para aplicar técnicas de ciberinteligencia de amenazas [1]

Para diseñar un programa de inteligencia de amenazas efectivo, será necesario inicialmente establecer las prioridades que reflejen con precisión las necesidades generales de la organización y sus objetivos. Esto implica el desarrollo de un conjunto preciso de objetivos y la determinación de requerimientos de seguridad de cada uno de ellos, así como los beneficios que el uso de herramientas de inteligencia de amenazas les proporcionará. En este contexto, se deberán considerar los siguientes aspectos:

- Identificar los riesgos de CTI
  - ¿Cuáles son los mayores riesgos que acompaña el uso de estas técnicas?
  - ¿De qué forma abordará la inteligencia de amenazas cada uno de esos riesgos?
  - ¿Cuál es el posible impacto de cada Riesgo?

- Considerar la relevancia de la información, la tecnología y las personas
  - ¿Qué espacios deben ser ocupados por la información, la tecnología y las personas para hacer efectiva la inteligencia de seguridad en esas áreas?
- Determinar proactivamente las mejores fuentes externas
  - ¿Es posible construir una infraestructura de recolección y métodos de intercambio flexibles?
  - ¿Cómo asegurar que las nuevas fuentes de datos puedan ser manejadas por la infraestructura de recolección y almacenamiento?
  - ¿Se puede maximizar la automatización de la recopilación de datos?
- Considerar las siguientes preguntas en cuanto a la recolección de fuentes:
  - ¿Cuáles son las fuentes de información más importantes o más utilizadas en su organización?
  - ¿Qué tan valiosa es cada una de ellas?
  - ¿Son principalmente internas o externas?
  - ¿Se recogen automáticamente o hay algún tipo de esfuerzo manual involucrado?
  - ¿Conoce el origen de la información recibida?
  - ¿Planea añadir nuevas fuentes en un futuro próximo?
  - ¿Qué tipo de información proporcionarán?
- Maximizar las actividades proactivas
  - ¿Se mantiene familiarizado con las amenazas y tendencias actuales?
  - ¿Se encuentra en condiciones de predecir los retos futuros
- Acortar el tiempo necesario para investigar los incidentes
  - ¿Se pueden acortar los tiempos asignados a la investigación de los incidentes sin comprometer los resultados?

- Examinar todas las fuentes y datos pertinentes
  - ¿Se puede asegurar que se revisará cada uno de los conjuntos de datos relacionados en su repositorio de datos?
  - ¿Se pueden pensar otras formas de extraer información interesante?
  - ¿Es posible facilitar la recopilación e integración de datos adicionales?
  - ¿Cómo asegurar la calidad de las fuentes de datos?
- Aumentar la productividad
  - ¿Se han utilizado herramientas robustas, interactivas y automatizadas?
  - ¿Los procesos se encuentran bien documentados?
  - ¿Se aplican técnicas de visualización para comprender mejor los datos?

La inteligencia de amenazas es integral, relevante y fácil de consumir, tiene el potencial de revolucionar la forma en que operan los diferentes roles en la organización. Es importante identificar todos los usuarios potenciales de la organización y alinear la inteligencia a sus casos únicos de uso. También se deben describir los beneficios de la inteligencia de seguridad de cada grupo en términos de tiempos de respuesta, ahorro de costos, eficiencia del personal, decisiones de inversión, etc. Las necesidades y los beneficios no siempre son obvios.

Documentar estos detalles permitirá establecer prioridades, justificar inversiones, y encontrar nuevas áreas para aplicar la seguridad de inteligencia.

Cada informe y comunicación sobre inteligencia de amenazas que se realice debe posibilitar que las partes involucradas tomen decisiones y adopten las medidas y acciones apropiadas. Deben contener información básica como el probable actor o actores de la amenaza, las técnicas y herramientas utilizadas por estos, probables objetivos en la organización, si la amenaza representa para ella un peligro real, la probabilidad de que los

controles de seguridad existentes sean capaces de mitigar la amenaza y medidas recomendadas para responder ante estas.

También es recomendable automatizar todo lo posible ya que los programas de inteligencia de seguridad efectivos se centran típicamente en la automatización desde su etapa inicial. Esta automatización comienza por las tareas fundamentales como la agregación de datos, la comparación, el etiquetado, y la contextualización.

Cuando estas tareas son realizadas por máquinas, el personal es liberado para centrarse en realizar una efectiva toma de decisiones informadas (basadas en conocimiento).

La integración de la inteligencia de seguridad con los procesos e infraestructura existente en la organización es una forma efectiva de hacer accesible y utilizable la inteligencia, sin abrumar a los equipos con nuevas tecnologías.

El valor que se obtiene de la inteligencia de seguridad está directamente relacionado a su capacidad de hacerlo relevante para la organización y de aplicarlo tanto a los procesos de seguridad existentes como a los nuevos.

Se puede elegir empezar de forma sencilla con su personal actual con pocas fuentes de datos, en lugar de construir un equipo de inteligencia de seguridad dedicado, e integrar la CTI con las herramientas de seguridad existentes como su SIEM y su sistema de gestión de la vulnerabilidad, para ir escalando. De este modo se beneficiaría con la inclusión de personal dedicado, más fuentes de datos y una mayor integración de herramientas, más automatización y mejores flujos de trabajo.

Finalmente, a medida que el equipo de inteligencia de seguridad madure, se necesitará incorporar personal hábil en correlación de los datos externos con la telemetría interna, especialistas en ingeniería inversa de malware, en reconstrucción de ataques (forenses), una mejor conciencia de la situación de amenaza y recomendaciones para los controles de seguridad. También en la detección proactiva de amenazas internas, la educación de los

empleados y clientes sobre las amenazas cibernéticas y la identificación y gestión de las fuentes de información respectivas.

En la siguiente figura se puede apreciar el rol que cumple la inteligencia de amenazas en la defensa activa cibernética:

MODELO DE MADUREZ DE CAPACIDADES TECNICAS DE DEFENSA ACTIVA CIBERNETICA		
DIMENSION	CAPACIDAD	CONTROL
1. APRENDER DE LOS ENEMIGOS	1.1 ENTRENAMIENTO	1.1.1 Ingeniería Reversa
		1.1.2 Análisis de Malware
		1.1.3 Inteligencia Artificial / Machine Learning
		1.1.4 Capacitación en Tecnologías
		1.1.5 Certificaciones técnicas de seguridad
	1.2 TECNOLOGÍA	1.2.1 Sensores de detección
		1.2.2 Análisis de Malware
		1.2.3 Inteligencia de Amenazas
		1.2.4 Monitoreo
		1.2.5 Respuesta y Manipulación
2. INTELIGENCIA DE AMENAZAS	2.1 ENTRENAMIENTO	2.1.1 OSINT
		2.1.2 Compartir Información
		2.1.3 Forense
		2.1.4 Malware
		2.1.5 Machine Learning
	2.2 TECNOLOGÍA	2.2.1 OSINT
		2.2.2 Compartir Información
		2.2.3 Forense
		2.2.4 Malware
		2.2.5 Machine Learning
3. OFENSIVA	3.1 ENTRENAMIENTO	3.1.1 Denegación de Servicios
		3.1.2 Creación de Exploits
		3.1.3 Hacking
		3.1.4 Ingeniería Social
		3.1.5 Red Team
	3.2 TECNOLOGÍA	3.2.1 Hacking
		3.2.2 Exploits
		3.2.3 Infraestructura
		3.2.4 Red Team
		3.2.5 Equipamiento

Figura 31: Nivel de madurez de capacidades técnicas de defensa activa cibernética[17]

[17] Fuente: www.kravmagahacking.com

4 Conclusiones finales

La inteligencia de ciberamenazas provee una visión general y constituye una herramienta relevante para contrarrestar los efectos nocivos de los recientes avances de la ciberdelincuencia y los problemas emergentes relacionados con ella. En Argentina el último informe oficial sobre “el panorama de la ciberseguridad en números” data del año 2016, por lo que sus conclusiones carecen de actualidad, lo que implica que gubernamentalmente se está lejos de contribuir un equilibrio entre defensores y atacantes.

Sin embargo, los reportes de organismos europeos, de universidades extrajeras y empresas privadas del país y del exterior[18], a los que se ha tenido acceso durante el desarrollo de este trabajo, permiten inferir que los ataques en el ciberespacio continúan evolucionando en complejidad y sofisticación. Particularmente en el año 2020, sus acciones maliciosas fueron facilitadas por el elemento disruptivo a nivel mundial que trajo aparejada la pandemia del COVID-19. Esta situación que potenció el teletrabajo, dejó expuestos a altos niveles de ciberamenazas a muchas empresas/organizaciones, que no contaban con una planificación ordenada para la continuidad del negocio en esta modalidad. Esto se reflejó en récords de ciberataques de todo tipo, dejando en evidencia la falta de capacitación, concientización y preparación para hacer frente a las ciberamenazas.

La vertiginosa evolución de la tecnología y su temprana y de algún modo, impetuosa adopción por parte de las organizaciones ha facilitado el avance de los atacantes en la ocultación de sus rastros por anonimización y cifrado dificultando su detección. Se ha notado también un incremento en el secuestro de información por ciberdelincuentes, motivados por la rentabilidad

[18]Centro Criptológico Nacional de España-Universidad de Oxford - Empresa de servicios de seguridad Positive Technologies - Agencia de la Unión Europea para la Ciberseguridad - ESET Security - Accenture Security- Observatorio de la Ciberseguridad en América Latina y el Caribe - TrendMicro

económica y, aprovechando el uso de monedas virtuales, que permiten el ocultamiento de su identidad.

Por lo expuesto se puede concluir que la comprensión de las ciberamenazas y de la forma en que evolucionan, es un fundamento clave para asumir la necesidad de implementar un sistema de inteligencia de amenazas que permita anticiparse proactivamente a los ciberataques. De esta forma la aplicación apropiada de técnicas de CTI habilitará que las tendencias importantes sean comprendidas no sólo por los profesionales que se dedican a la protección de la tecnología y la información sino también por todos aquellos encargados de tomar decisiones en la organización.

Finalmente, un programa de inteligencia de amenazas contemplar su administración personalizada de acuerdo a los requerimientos específicos de cada organización, contar con acceso a fuentes de datos actualizadas y con acceso a las investigaciones más recientes sobre métodos de ataques e implementar soluciones reales. En otras palabras, se deberá llevar adelante un programa de inteligencia de amenazas integral que identifique posibles problemas y ofrezca soluciones.

A nivel gubernamental, se deberá tener en cuenta la necesidad de brindar acceso a información actualizada sobre el panorama de ciberamenazas, de manera que las organizaciones puedan desarrollar y definir sus estrategias de ciberdefensa.

A nivel empresarial, se deberá desarrollar el concepto de inteligencia estratégica y táctica e implementar modelos de madurez para hacer frente a las ciberamenazas.

También sería conveniente, desarrollar programas de investigación y planes de estudio con formación en ciberinteligencia, que incluyan técnicas de aprendizaje innovadoras que conduzcan al desarrollo de la inteligencia basada en conocimiento.

Glosario de términos [19]

- **Malware**: En español software malicioso. Es la conjugación de las primeras tres letras de las palabras Malicious Software.
- **Keylogger**: Es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.
- **Ingeniería social**: Mecanismo para obtener información o datos de naturaleza sensible. Las técnicas de ingeniería social son tácticas de persuasión que suelen valerse de la buena voluntad y falta de precaución de los usuarios, y cuya finalidad consiste en obtener cualquier clase de información, en muchas ocasiones claves o códigos.
- **Hash:** Conjunto de bits obtenidos como resultado de aplicar una función resumen a unos datos.
- **Spoofing:** Consiste en usurpar una identidad electrónica para ocultar la propia identidad y así cometer delitos en Internet. La suplantación de identidad en términos de seguridad de redes, hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.
- **DoS:** Acrónimo de Denial of Service, o Denegación de Servicio en español. En términos de seguridad informática, es el conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma no permitir que sus legítimos usuarios puedan utilizar los servicios por prestados por él. El ataque consiste en, saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

- **DDoS:** Acrónimo de Denial of Distributed Service o Denegación de Servicio Distribuida en español. Se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino.
- **Sniffing:** Es el rastreo o monitoreo en tiempo real de la información transmitida entre los nodos lógicos o físicos de una red. El atacante no tiene por qué impedir la recepción o cambiar el contenido, sino que simplemente observa y lee el tráfico. El atacante puede precipitar o influir indirectamente en el contenido de la transacción observada, pero nunca es el destinatario previsto de la información. En teoría, cualquier medio de transmisión puede ser rastreado si el atacante puede escuchar el contenido entre el remitente y el destinatario.
- **IDS:** Acrónimo de Intrusion Detection System o Sistema de detección de Intrusiones en español. Es el software o hardware utilizado para identificar o alertar acerca de intentos de intrusión en redes o sistemas. Está conformado por sensores que generan eventos de seguridad; una consola que supervisa eventos y alertas y controla los sensores; y un motor central que registra en una base de datos los eventos denotados por los sensores. Utiliza un sistema de reglas que generan alertas en respuesta a cualquier evento de seguridad detectado.
- **IPS:** Acrónimo de Intrusion Prevention System o Sistema de Prevención de Intrusiones de Seguridad, en español. Va un paso más allá que el IDS y bloquea el intento de intrusión.
- **SIEM:** Acrónimo de Security Information and Event Management o Sistema de Gestión de Eventos e Información de Seguridad, en español. Es un sistema que centraliza el almacenamiento y la interpretación de los datos relevante de seguridad.
- **Ransomware:** Es un código malicioso utilizado para secuestrar datos. Constituye, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

- **Botnet:** El término se refiere a una red de computadoras que han sido infectados por programas nocivos (virus informáticos). Esta red de computadoras afectadas (conocidas como “zombies”) puede ser activada para realizar determinadas acciones como ataques a los sistemas de información (ciberataques). Los zombies pueden ser controlados por otor computador, con frecuencia sin el conocimiento de los usuarios de los dispositivos afectados. El equipo «controlador» también se conoce como el «centro de dirección y control». Las personas que controlan este centro incurren en una infracción penal, ya que utilizan los ordenadores afectados para lanzar ataques contra los sistemas de información. Es muy difícil rastrear a los autores porque los dispositivos que conforman el botnet y realizan el ataque pueden encontrarse en un lugar diferente del propio infractor.
- **Phishing:** Es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc) de forma fraudulenta. El estafador o “phisher” suplanta la indetidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, sms o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador.
- **Spear Phishing:** Se trata de un Phishing dirigido de forma que se maximiza la probabilidad de que el sujeto objeto del ataque pique el anzuelo y brinde la información requerida por el estafador.
- **Backdoor:** O puerta trasera, en español. Se trata de cualquier punto débil de un programa o sistema mediante el cual, una persona no autorizada puede acceder a un sistema. Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito, por los propios autores pero al ser descubiertas por terceros, pueden ser utilizadas con fines ilícitos. Por otro lado, también se consideran puertas traseras a los programas que, una vez instalados en el

ordenador de la víctima, dan el control de éste de forma remota al ordenador del atacante. Por lo tanto, aunque no son específicamente virus, pueden llegar a ser un tipo de malware que funcionan como herramientas de control remoto. Cuentan con una codificación propia y usan cualquier servicio de Internet, como el correo electrónico, los sistemas de mensajería instantánea, los protocolos Http, FTP, Telnet o los canales de chat.

- **Trojan:** O caballo de Troya, en español. Es una clase de software malicioso que al instalarse permite al usuario ejecutar funciones normalmente, mientras ejecutan funciones maliciosas sin que éste lo sepa.
- **CVE**: Son las siglas de Common Vulnerabilities and Exposures o vulnerabilidades y exposiciones de uso común, en español. Es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, donde cada referencia tiene un número de identificación único. De esta forma provee una nomenclatura común para el conocimiento público de este tipo de problemas y así facilita la posibilidad de compartir datos sobre dichas vulnerabilidades. Fue definido y es mantenido por The MITRE Corporation (por eso a veces a la lista se la conoce por el nombre MITRE CVE List) con fondos de la National Cyber Security Division del gobierno federal de los Estados Unidos de América. Forma parte del llamado Security Content Automation Protocol.

Bibliografía

1. The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence by Recorded Future English | 2018 | ISBN: 0999035460 | 94 Pages | PDF | 11.2 MB – 23-11-2020

2. Collaborative Cyber Threat Intelligence - Detecting and Responding to Advanced Cyber Attacks at the National Level - © 2018 by Taylor & Francis Group, LLC CRC Press is an imprint of Taylor & Francis Group, an Informal business -International Standard Book Number-13: 978-1-138-03182-1 - 23-11-2020

3. Threat Intelligence y la importancia del intercambio de información sobre amenazas [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2019/10/04/threat-intelligence-importancia-intercambio-informacion-amenazas/ 23-11-2020

4. Indicadores de Ataque Vs. Indicadores de Compromiso [En línea]. Disponible en: https://www.crowdstrike.com.br/recursos/white-papers/indicadores-de-ataque-vs-indicadores-de-comprometimento/ 30-11-2020

5. Informe de Ciberamenazas y Tendencias – Edición 2020. [En línea]. Disponible en: https://cuadernosdeseguridad.com/wp-content/uploads/2020/10/Informe-Ciberamenazas-Tendencias-2020.pdf 30-11-2020

6. CYBER THREATSCAPE REPORT2020 - Accenture Security https://www.accenture.com/_acnmedia/PDF-137/Accenture-2020-Cyber-

Threatscape-Report.pdf#zoom=50 07-12-2020

7. Informe de amenazas – Tercer trimestre 2020 ESET [En Línea] Disponible en: https://www.welivesecurity.com/wp-content/uploads/2020/11/Q3-2020_Threat_Report-ESP.pdf 07-12-2020

8. MALICIOUS USES AND ABUSES OF ARTIFICIAL INTELLIGENCE [En línea] Disponible en: https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence 07-12-2020

9. La ONU y Europol advierten de la creciente ciberamenaza de la IA. [En línea] Disponible en: https://www.ciberseguridadlatam.com/2020/11/21/la-onu-y-europol-advierten-de-la-creciente-ciberamenaza-de-la-ia/ 30-11-2020

10. Executive Perspectives on Cyber Threat Intelligence – Understanding the options, the value and the Market [En línea] Disponible en: https://www.gartner.com/imagesrv/media-products/pdf/iSight/iSight-1-254H72D.pdf 03-12-2020

11. CyberThreat Intelligence: el área que toda empresa de seguridad necesita [En línea] Disponible en: https://empresas.blogthinkbig.com/cyber-threat-intelligence-empresas/

12. El valor de los indicadores de compromiso en la industria [En línea] Disponible en: https://www.incibe-cert.es/blog/el-valor-los-indicadores-compromiso-industria 30-11-2020

13. Intelligence Sources in the Process of Collection of Information by the U.S. Intelligence Community. [En línea] Disponible en: https://www.researchgate.net/publication/340647256_Intelligence_Sources_in_the_Process_of_Collection_of_Information_by_the_US_Intelligence_Community/link/5e96e6d1a6fdcca78918e8a5/download 08-12-2020

14. Industrial Control Threat Intelligence. [En línea] Disponible en: https://www.dragos.com/wp-content/uploads/Industrial-Control-Threat-Intelligence-Whitepaper.pdf 08-12-2020

15. Cyber threat intelligence: The cyber defender's most valuable weapon. [En línea] Disponible en: https://www.accenture.com/us-en/blogs/blogs-cyber-intelligence 08-12-2020

16. ENISA Threat Landscape 2020 – Top 15 Threats https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape-2020-top-15-threats/view 07-12-2020

17. Defensa Activa e Inteligencia: Threat Intelligence en los entornos industriales [En línea] Disponible en: https://www.incibe-cert.es/blog/defensa-activa-e-inteligencia-threat-intelligence-los-entornos-industriales 30-11-2020

18. Industrial Control Threat Intelligence [En línea] Disponible en: https://www.dragos.com/wp-content/uploads/Industrial-Control-Threat-Intelligence-Whitepaper.pdf

19. GUÍA DE SEGURIDAD (CCN-STIC-401) Glosario y Abreviaturas. [En línea] Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=47.html 09-12-2020

20. Lista de herramientas de inteligencia de amenazas cibernéticas más importantes para hackers y profesionales de la seguridad. [En línea] Disponible en: https://gbhackers.com/cyber-threat-intelligence-tools/ 09-12-2020

21. The Pyramid of Pain. [En línea] Disponible en: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html 24-11-2020

22. Básicos polext: Riesgos del ciberespacio. THIBER en política exterior. [En línea] Disponible en: https://www.thiber.org/2014/12/23/basicospolext-riesgos-del-ciberespacio-thiber-en-politica-exterior/ 24-11-2020

23. Ciclo de Inteligencia y Análisis de Intrusiones [En línea] Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1093-ccn-stic-425-ciclo-de-inteligencia-y-analisis-de-intrusiones/file.html 05-12-2020

24. Matriz para empresas [En línea] Disponible en: https://attack.mitre.org/matrices/enterprise/ 05-12-2020

25. Threat Hunting: El valor de la proactividad de las amenazas [En línea] Disponible en: https://www.tendencias.kpmg.es/2019/04/threat-hunting-proactividad-amenazas/ 06-12-2020