AMENAZAS AVANZADAS PERSISTENTES: IMPACTO EN LAS PYMES COLOMBIANAS Y BUENAS PRÁCTICAS PARA SU PREVENCIÓN Y MANEJO

ADRIAN RODRIGO BARRERO ROMERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2023

AMENAZAS AVANZADAS PERSISTENTES: IMPACTO EN LAS PYMES COLOMBIANAS Y BUENAS PRÁCTICAS PARA SU PREVENCIÓN Y MANEJO

ADRIAN RODRIGO BARRERO ROMERO

TRABAJO DE GRADO

LUIS FERNANDO ZAMBRANO HERNANDEZ
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2023

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Bogotá (24, 2, 2023)

Dedicatoria

Dedico este trabajo a todos los empleados y empresarios de industrias en crecimiento que, como yo, han crecido y aportado a la industria nacional en su labor diaria.

Agradecimientos

Debo agradecer en primer lugar a mi familia, especialmente a mi madre y mi esposa, que han sido las mujeres tenaces y comprensivas, que apoyan cada paso de mi carrera profesional y están a mi lado dando aliento en cada embate y celebrando cada éxito por pequeño que sea.

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

ACTIVOS DE INFORMACIÓN: elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos, procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de la entidad, órgano u organismo. Este tipo de activo representa los datos de la organización, información que tiene valor para los procesos de negocio, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil para la ANH.[1]

AMENAZA: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la organización.[2]

BACKUP: en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperación en caso de su pérdida.[3]

CIBERSEGURIDAD: la ciberseguridad se define como una capa de protección para los archivos de información, a partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo.[4]

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.[5]

CONTRASEÑAS ROBUSTAS: tipo de contraseña que se caracteriza por ser suficientemente larga, que se crea al azar o mediante la combinación de caracteres alfanuméricos (letras mayúsculas y minúsculas, números y caracteres especiales) que dificultan de forma clara su revelación, ya que se requiere un tiempo elevado de cálculo para lograrlo.[6]

---

[1] J, Glosario - ISO27000.ES. [Sitio WEB]. August 2020. ISO27000.ES. [Disponible en 8 de August, 2020]. Recuperado de: https://www.iso27000.es/glosario.html
[2] Ibid.
[3] Ibid
[4] Ibid.
[5] Ibid.
[6] INCIBE, Glosario de términos de ciberseguridad. [Sitio WEB]. 2020. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

CONTROL: es toda actividad o procesos encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal.[7]

CONTROL DE ACCESO: sistema de verificación que permite el acceso a un determinado recurso si la persona o entidad tiene los derechos necesarios para solicitarlo. Este acceso puede ser a recursos de tipo físico (por ejemplo, a un edificio o un departamento) o lógicos (por ejemplo, a un sistema o una aplicación software específica).[8]

CONTROL DE ACCESO POR ROLES: sistema de verificación que permite o deniega el acceso a un recurso tecnológico según los derechos concedidos a cada usuario dependiendo de la clase o grupo a la que esté adscrito. Se pueden establecer roles, por ejemplo, por áreas de la empresa (ventas, operaciones...) o por la posición jerárquica dentro de la estructura; cada rol con los permisos necesarios para realizar su trabajo. Al dar de alta a un usuario en el sistema, el administrador le asignará un rol dependiendo de las tareas que deba realizar y que tendrá asociados los permisos de acceso necesarios.[9]

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI): instancia del nivel superior, que deben validar la Política de Información, así como los procesos, procedimientos y metodologías específicas de seguridad y privacidad de la información para el adecuado uso y administración de los recursos informáticos y físicos, asignados a los servidores públicos de cada ente público.[10]

CORREO ELECTRÓNICO: es un método de comunicación que utiliza dispositivos electrónicos para entregar mensajes a través de redes informáticas. Se refiere tanto al sistema de entrega como a los mensajes individuales que se envían y reciben.[11]

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [12]

---

[7] INCIBE, Glosario de términos de ciberseguridad. [Sitio WEB]. 2020. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf.
[8] Ibid.
[9] Ibid.
[10] Ibid.
[11] CLOUDFLARE, ¿Qué es el correo electrónico? | Definición de correo electrónico | Cloudflare. [Sitio WEB]. 2021. Learning. [Disponible en 31 de July, 2022]. Recuperado de: https://www.cloudflare.com/es-es/learning/email-security/what-is-email/
[12] J, Glosario - ISO27000.ES. [Sitio WEB]. August 2020. ISO27000.ES. [Disponible en 8 de August, 2020]. Recuperado de: https://www.iso27000.es/glosario.html

ENCARGADO DE SEGURIDAD: persona delegada cuyas funciones principales son asesorar en materia de seguridad de la información en la entidad y supervisar el cumplimiento de la presente Política.[13]

ESCRITORIO LIMPIO: es la protección que se deriva del control frente al uso y ubicación de papeles y medios removibles de almacenamiento de información que son manipulados en las estaciones de trabajo. Consiste en evitar la pérdida, daño o acceso no autorizado a la información durante y fuera de las horas laborales.[14]

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad. [15]

FIREWALL: Es un dispositivo que brinda seguridad a la red mediante el control de flujo de datos, dado por características como el origen, destino, tipo de tráfico o aplicación utilizada [16]. El Firewall inspecciona los paquetes de datos para obtener la información que permite determinar la decisión de permiso de paso del flujo de datos. Existen distintos tipos de este dispositivo dependiendo del nivel de inspección de paquetes que realiza, se pueden listar los siguientes:

- Proxy: Permite controlar el tráfico y proteger la navegación mediante el uso de caché.
- Firewall de inspección activa: Trabaja sobre por tipo y el origen o destino del tráfico, por lo cual se considera un Firewall tradicional. Monitorea y registra la actividad relacionada con las conexiones permitidas o restringidas.
- Firewall de administración unificada de amenazas (UTM). United thread management, UTM por las siglas en inglés, embebe funciones adicionales al anterior, como la inspección activa y la detección o prevención de intrusos (IDS/IPS) [17]. Puede incluir otros servicios como la gestión desde la nube o la inspección por antivirus.
- Firewall de próxima generación (NGFW). Incluyendo los 3 tipos anteriores, involucra controles a nivel de aplicación y análisis de malware avanzado. Puede

---

[13] J, Glosario - ISO27000.ES. [Sitio WEB]. August 2020. ISO27000.ES. [Disponible en 8 de August, 2020]. Recuperado de: https://www.iso27000.es/glosario.html

[14] UNIVERSIDAD TECNOLÓGICA DE PEREIRA, *SISTEMA INTEGRAL DE GESTIÓN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MANUAL GENERAL DE DIRECTRICES Versión: 4 Fecha: 28/11/2018 Código: 1313-MGD-01 Página: 1 de 61*

[15] J, Glosario - ISO27000.ES. [Sitio WEB]. August 2020. ISO27000.ES. [Disponible en 8 de August, 2020]. Recuperado de: https://www.iso27000.es/glosario.html

[16] CISCO, ¿Qué es un firewall? - Cisco. [Sitio WEB]. 2019. [Disponible en 17 de October, 2021]. Recuperado de: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

[17] GONZALEZ, *Sistemas de Detección de Intrusiones*, Diego González Gómez

incluir como mínimo: Funciones de firewall estándar; IDS / IPS integrado; inspección de capa 7, esto es, reconocimiento de aplicaciones; actualización dinámica de rutas; inteligencia de amenazas o inspección por firmas basadas en la nube.

- NGFW centrado en amenazas [18]. Este tipo de Firewall complementa el esquema de seguridad con el análisis de malware avanzado; agrega funciones que pueden incluir: Inventario de activos y valoración de riesgo; Automatización de seguridad inteligente que establece políticas y fortalece las defensas de forma dinámica para anticiparse y responder a los incidentes de seguridad; Correlación de eventos de dispositivos para la identificación de comportamientos sospechosos; Agilidad en la respuesta y eliminación de incidentes por memoria de comportamientos sospechosos; Políticas unificadas para simplicidad y agilidad en la detección y protección en todas las fases del ataque.
- Otros tipos de Firewall: Han aparecido en el mercado como DATABASE Firewall (DBF) y Firewall de Acceso WEB (WAF) con características y desempeño dedicado a cierto tipo de aplicación.

GESTIÓN DE INCIDENTES: listado de procedimientos previamente documentados sobre los pasos a seguir en caso de detectar una amenaza de ciberseguridad en la empresa. La gestión de incidentes está orientada a mitigar en el menor tiempo posible un incidente de seguridad identificándolo y asignando el personal que dará respuesta al mismo dentro de unos parámetros predefinidos.[19]

IDS: por sus siglas en inglés, Intrusion Detection System. Mediante diversos métodos de identificación de comportamientos sospechosos, se han diseñado aplicaciones y sistemas encargados de monitorear, identificar e incluso reportar, los orígenes y tipos de ataques que puedan estar ocurriendo en una red de computadoras, se han denominado IDS por sus siglas en inglés, Intrusion Detection System. En la actualidad estos dispositivos han evolucionado al punto de ofrecer distintos tipos de acuerdo con el punto de monitorización dónde se encuentre: monitoreo basado en la red, monitoreo basado en la aplicación, monitoreo en el objetivo, monitoreo en la maquina (HIDS o Host IDS) o máquinas y monitoreo híbrido [20].

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: un incidente de seguridad de la información se define como un acceso, uso, divulgación, modificación o destrucción no autorizada de la información de la ANH y de sus usuarios; un impedimento en la

[18] FIREWALLS.COM, Sophos Next Generation XG Firewalls - Information, Pricing, & Reviews. [Sitio WEB]. 2021. [Disponible en 17 de October, 2021]. Recuperado de: https://www.firewalls.com/brands/sophos/firewalls/xg.html
[19] INCIBE, Glosario de términos de ciberseguridad. [Sitio WEB]. 2020. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
[20] GONZALEZ, *Sistemas de Detección de Intrusiones*, Diego González Gómez

operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Información.[21]

INGENIERÍA SOCIAL: conjunto de técnicas que los delincuentes usan para engañar a los usuarios de sistemas/servicios TIC para que les faciliten datos que les aporten valor, ya sean credenciales, información sobre los sistemas, servicios instalados etc.[22]

INTEGRIDAD: propiedad de salvaguardar la exactitud y estado completo de los activos.[23]

INVENTARIO DE ACTIVOS: se define como una lista de todos aquellos recursos (físicos, software, documentos, servicios, personas, instalaciones, etc.) que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.[24]

IPS: por sus siglas en inglés, Intrusion Prevention System. Así como el IDS puede alertar un posible ataque, el IPS, por sus siglas en inglés, Intrusion Prevention System, tiene como objetivo adicional el poder detener el ataque, o evitar que continúe afectando el sistema mediante mecanismos como la activación de una regla en el Firewall, o el rechazo del tipo de tráfico identificado para el origen del ataque [25].

NO REPUDIO: capacidad de garantizar que una parte de un contrato o una comunicación no pueda negar la autenticidad de su firma en un documento o el envío de un mensaje enviado por un origen determinado.[26]

MALWARE: el malware es un tipo de software diseñado para obtener acceso no autorizado o causar daños en una computadora.[27]

---

[21] ICONTEC, NTC-ISO-IEC 27000:2017, ICONTEC, 2017
[22] INCIBE, Glosario de términos de ciberseguridad. [Sitio WEB]. 2020. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
[23] Ibid.
[24] INCIBE, Inventario de activos y gestión de la seguridad en SCI | INCIBE-CERT. [Sitio WEB]. December 29, 2016. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci
[25] CHAVEZ *ET AL.*, *Identificación de amenazas informáticas aplicando arquitecturas de Big Data*, INNOVA Research Journal. 6: 141–167
[26] Ibid
[27] CISCO, ¿Qué es la ciberseguridad? - Cisco. [Sitio WEB]. July 21, 2022. [Disponible en 31 de July, 2022]. Recuperado de: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

MEDIOS EXTRAÍBLES: son dispositivos de almacenamiento extraíbles que permiten realizar transferencias de información de manera rápida y directa, entre ellos se encuentran memorias USB, discos duros portátiles y tarjetas de memoria.[28]

METODOLOGÍA: Se trata de procesos ordenados que en secuencia orientan el trabajo a un objetivo establecido. Para el caso de la investigación científica se han definido diversas líneas de investigación, por ello, con el fin que los proceso puedan ser replicables se someten a la rigurosidad de la evaluación de la comunidad en el cumplimiento del objetivo o la resolución de la situación problema para la que se propone [29].

PHISHING (SUPLANTACIÓN DE IDENTIDAD): la suplantación de identidad (phishing) es la práctica de enviar correos electrónicos fraudulentos que se asemejan a correos electrónicos de fuentes de buena reputación. El objetivo es robar datos sensibles, como números de tarjetas de crédito e información de inicio de sesión. Es el tipo más común de ciberataque. Puede protegerse mediante la educación o una solución tecnológica que filtre los correos electrónicos maliciosos.[30]

POLÍTICA DE SEGURIDAD: son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos. Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información.[31]

PROPIETARIO/RESPONSABLE DE ACTIVO DE INFORMACIÓN: individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.[32]

RANSOMWARE: el ransomware es un tipo de software malicioso. Está diseñado para exigir dinero mediante el bloqueo del acceso a los archivos o el sistema informático hasta

---

[28] INCIBE, Protege tu información con los dispositivos de almacenamiento extraíbles. | INCIBE. [Sitio WEB]. September 13, 2018. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/protege-tu-informacion-los-dispositivos-almacenamiento-extraibles

[29] FERREYRO AND LONGHI, Metodología de la investigación, Encuentro Grupo Editor, Córdoba, Argentina, 2014

[30] CISCO, ¿Qué es la ciberseguridad? - Cisco. [Sitio WEB]. July 21, 2022. [Disponible en 31 de July, 2022]. Recuperado de: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

[31] INCIBE, Glosario de términos de ciberseguridad. [Sitio WEB]. 2020. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

[32] INCIBE, Glosario de términos de ciberseguridad. [Sitio WEB]. 2020. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

que se pague un rescate. El pago del rescate no garantiza que se recuperen los archivos o se restaure el sistema.[33]

REDES SOCIALES: son estructuras formadas en Internet por personas u organizaciones que se conectan a partir de intereses o valores comunes. A través de ellas, se crean relaciones entre individuos o empresas de forma rápida, sin jerarquía o límites físicos.[34]

RIESGO: es la definición de un escenario bajo el cual una amenaza puede explotar una vulnerabilidad, generando un impacto negativo al negocio (por ejemplo, pérdida de la continuidad, incumplimiento, pérdida de ingresos, entre otros). [35]

RIESGOS INFORMÁTICOS: Situaciones problema en potencia, capaces de afectar activos informáticos o sistemas. La identificación de riesgos informáticos permite vigilar y proponer controles adecuados para prevenir la materialización de eventos que afecten la disponibilidad, integridad o confidencialidad de la información, por ello, se pueden clasificar en: Riesgos de integridad, Riesgo de infraestructura, Riesgos de acceso, Riesgos de relación, Riesgos de utilidad [36].

SEGURIDAD DE LA INFORMACIÓN: protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar la materialización de los riesgos.[37]

SEGURIDAD EN INTERNET: es un término que describe la seguridad para actividades y transacciones realizadas en Internet. Es un componente particular de las principales ideas de ciberseguridad y seguridad informática, la cual involucra temas como la seguridad de los navegadores, las conductas en línea y la seguridad de redes.[38]

SEGURIDAD INFORMÁTICA: se encarga del aseguramiento de la infraestructura tecnológica mediante herramientas o elementos físicos, para evitar que se materialización las amenazas que se propagan por la red. [39]

---

[33] CISCO, ¿Qué es la ciberseguridad? - Cisco. [Sitio WEB]. July 21, 2022. [Disponible en 31 de July, 2022]. Recuperado de: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

[34] RDSTATION, ¿Qué son las Redes Sociales?【Guía completa + ejemplos】. [Sitio WEB]. 2022. [Disponible en 31 de July, 2022]. Recuperado de: https://www.rdstation.com/es/redes-sociales/

[35] J, Glosario - ISO27000.ES. [Sitio WEB]. August 2020. ISO27000.ES. [Disponible en 8 de August, 2020]. Recuperado de: https://www.iso27000.es/glosario.html

[36] SÁNCHEZ *ET AL.*, *MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES*

[37] SÁNCHEZ *ET AL.*, *MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES*

[38] KASPERSKY, ¿Qué es la seguridad en Internet? [Sitio WEB]. 2022. [Disponible en 31 de July, 2022]. Recuperado de: https://latam.kaspersky.com/resource-center/definitions/what-is-internet-security

[39] J, Glosario - ISO27000.ES. [Sitio WEB]. August 2020. ISO27000.ES. [Disponible en 8 de August, 2020]. Recuperado de: https://www.iso27000.es/glosario.html

SERVICIO: es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.[40]

SERVICIO EN LA NUBE: servicio que permite acceder desde cualquier dispositivo y lugar, tener directorios compartidos o trabajar de forma colaborativa.[41]

SIEM: Por sus siglas en inglés, Security Information and Event Management. Es un dispositivo que se encarga de brindar soluciones de seguridad de la información, como la protección de activos, la identificación de comportamientos sospechosos y el monitoreo de tráfico y eventos de sistemas, mediante la recolección y análisis integral de los eventos de sistemas y redes, identificando relaciones entre estos, en un proceso llamado correlación de eventos [42].

SHOULDER SURFING (Seguridad móvil): técnica de ingeniería social empleada por los atacantes con el objetivo de conseguir información de un usuario en concreto, por ejemplo, mirando por encima del hombro en un autobús.[43]

SOFTWARE: Definimos software del inglés como un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en un dispositivo. El software conforma todas aquellas acciones que se pueden realizar gracias a las instrucciones previamente contempladas y programadas e incluidas dentro de un programa que permite al usuario interactuar con el sistema de forma fácil e intuitiva.[44]

TELETRABAJO: actividad laboral que se desarrolla desde otros lugares que no sean las propias instalaciones de la organización.[45]

TERCERO(S): cualquier persona natural o jurídica en calidad de proveedor, outsourcing o consultor. [46]

---

[40] J, Glosario - ISO27000.ES. [Sitio WEB]. August 2020. ISO27000.ES. [Disponible en 8 de August, 2020]. Recuperado de: https://www.iso27000.es/glosario.html.

[41] INCIBE, TemáTICas Cloud | INCIBE. [Sitio WEB]. 2022. [Disponible en 2 de June, 2022]. Recuperado de: https://www.incibe.es/protege-tu-empresa/tematicas/cloud

[42] PODZINS AND ROMANOVS, Why SIEM is Irreplaceable in a Secure IT Environment? 2019. Pp. 1–5, in 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream)

[43] INCIBE, ¿Qué es el shoulder surfing? | INCIBE. [Sitio WEB]. September 11, 2020. [Disponible en 30 de April, 2022]. Recuperado de: https://www.incibe.es/sala-prensa/notas-prensa/el-shoulder-surfing

[44] INCIBE, Glosario de términos de ciberseguridad. [Sitio WEB]. 2020. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

[45] INCIBE, Ciberseguridad en el teletrabajo. [Sitio WEB]. 2020. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf

[46] J, Glosario - ISO27000.ES. [Sitio WEB]. August 2020. ISO27000.ES. [Disponible en 8 de August, 2020]. Recuperado de: https://www.iso27000.es/glosario.html

USUARIO: es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor del Directorio Activo, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado una contraseña para poder acceder a su cuenta.[47]

VULNERABILIDAD: Debilidad que puede ser explotada por las amenazas que afectan un activo o control [48]. Sin embargo, las vulnerabilidades de un activo pueden ser informáticas como un uso inapropiado de usuarios y contraseñas o físicas como la exposición del activo a personal no autorizado. Un activo puede ser vulnerable a eventos que afecten sus datos, la información que contiene o si el activo en sí mismo es un activo informático [49].

[47] J, Glosario - ISO27000.ES. [Sitio WEB]. August 2020. ISO27000.ES. [Disponible en 8 de August, 2020]. Recuperado de: https://www.iso27000.es/glosario.html
[48] ICONTEC, NTC-ISO-IEC 27000:2017, ICONTEC, 2017
[49] SOLARTE SOLARTE *ET AL.*, *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001*, Tecnológica ESPOL –RTE. 28

INTRODUCCIÓN

El problema de la ciber seguridad y la seguridad informática ha creado nuevos retos en el marco de las contingencias dadas por la respuesta a la pandemia de Coronavirus[5051]. El mundo interconectado y globalizado garantiza una rápida difusión de información, así como de noticias falsas, infecciones digitales y biológicas; vulnerabilidades de día cero (0 days) que son ampliamente explotadas en cuestión de horas; ataques coordinados por agrupaciones delincuenciales con estructuras sofisticadas y hacktivismo, son algunos de los retos de los equipos de ciber defensa de hoy en día.

Este documento contribuye en dar respuesta a interrogantes sobre el lugar del especialista de seguridad informática en este mundo caótico y amenazante para los activos de las empresas, sus clientes y partes interesadas por medio de un análisis documental a la que puede ser la amenaza de mayor impacto para organizaciones en el futuro cercano, estableciendo cómo las mejores prácticas del negocio pueden ayudar a estos profesionales a prepararse y responder a estas amenazas.

[50] MARIANO DÍAZ, La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad | Publicación | Comisión Económica para América Latina y el Caribe. [Sitio WEB]. 2020. [Disponible en 2 de April, 2022]. Recuperado de: https://www.cepal.org/es/publicaciones/46275-la-ciberseguridad-tiempos-covid-19-transito-ciberinmunidad

[51] NIETO, Cibercriminales a la caza de la vacuna para la COVID-19 - Una al Día. [Sitio WEB]. November 18, 2020. [Disponible en 2 de April, 2022]. Recuperado de: https://unaaldia.hispasec.com/2020/11/cibercriminales-a-la-caza-de-la-vacuna-para-la-covid-19.html

1. RESUMEN

En este trabajo se presenta un análisis sobre las amenazas que pueden ser de impacto fatal para las pequeñas y medianas empresas colombianas (PYMES), específicamente para informar sobre el impacto actual en las organizaciones de los ataques e incidentes por Amenazas Persistentes Avanzadas[52], proponer una serie de recomendaciones y mejores prácticas para la prevención y contención de este tipo de amenazas.

Se presenta un resumen de las fases de ataque cibernéticos definidas por distintos expertos que pueden ser aplicados en la identificación APT; el lector encontrará las metodologías que se encuentran actualmente en el mercado para la identificación de APT y los atacantes identificados como grupos APT. Posteriormente se presentan las técnicas documentadas que son utilizadas por estos grupos para lograr sus objetivos y se tabulan los resultados de las más comunes para allí establecer las de mayor impacto y frecuencia; y finalmente proponer controles adecuados para que las PYME puedan preparar su capital humano e infraestructura y contener eficazmente incidentes ocasionados por estas amenazas.

Con este proyecto se plantea la necesidad de que todas las empresas de todos los sectores productivos y tamaños se preocupen y preparen adecuadamente su equipo humano y tecnológico para atender adecuadamente eventos e incidentes informáticos, esto entendiendo que el factor humano es el mayor factor de vulnerabilidad de los sistemas.

Palabras clave: Tecnología de la información, Pequeña empresa, Colombia, información, comunicación.

[52] ROLDÁN *ET AL.*, *THE ADVANCED PERSISTENT THREATS (APT) AND ITS METHOD OF DELINQUENCY.*, LA AMENAZA PERSISTENTE AVANZADA (APA) Y SU MÉTODO DE DELINCUENCIA. 10: 127–143

SUMMARY

This paper presents an analysis of threats that can have a fatal impact on small and medium-sized Colombian companies (SMEs), specifically to report on the current impact on organizations of attacks and incidents by Advanced Persistent Threats, proposing a series of recommendations and best practices for the prevention and containment of this type of threat.

A summary of the cyber-attack phases defined by different experts that can be applied in APT identification is presented; the reader will find the methodologies that are currently on the market for the identification of APT and the attackers identified as APT groups. Subsequently, the documented techniques used by these groups to achieve their objectives are presented, and the results of the most common ones are tabulated to establish those with the greatest impact and frequency; and finally, propose adequate controls so that SMEs can prepare their human capital and infrastructure and effectively contain incidents caused by these threats.

With this project, the need arises for all companies of all productive sectors and sizes to worry about and adequately prepare their human and technological team to adequately attend to computer events and incidents, understanding that the human factor is the greatest vulnerability factor in the systems.

Keywords: Information technology, Small business, Colombia, information, communication.

2. PLANTEAMIENTO DEL PROBLEMA

En una sociedad que cada vez más se involucra en la conectividad, el 62.7% de las empresas en Colombia se ha involucrado en tecnologías de vanguardia, según la ANDI[53], todas estas empresas ya cuentan con una estrategia de transformación digital e invierten parte de sus recursos, hasta 15% de sus ingresos, en tecnologías de conectividad. De allí que los ciberdelitos hayan presentado un incremento de 21% entre 2020 y 2021, según cifras de la policía[54].

Se ha visto con preocupación que la información en temas relacionados con ciberdefensa, en la red, a pesar de ser muy fluida, es también abrumadora y es difícil para los equipos de respuesta filtrar adecuadamente en qué aspectos centrarse primero. Por ejemplo, vulnerabilidades de día cero, Amenazas Avanzadas Persistentes APT[55] y RAMSOMWARE. El último año se ha identificado la existencia de la oferta de servicios criminales por módulos, por ejemplo, RANSOMWARE AS A SERVICE (RAAS), como lo indica CISA [56], que hace más complejo identificar el origen, los métodos y las estrategias de defensa aún para las organizaciones que ya tienen una infraestructura y procesos maduros de seguridad de la información y cibernética.

Desde la academia podrían ofrecerse servicios de información gratuitos en línea que adelanten los filtros adecuados de la criticidad y foco de las amenazas nuevas. Estas herramientas podrían denominarse Inteligencia de amenazas desde la academia, documentos de soporte para el estudio de los profesionales de la ciberseguridad en las organizaciones, metodologías aplicadas en el sector industrial colombiano y análisis profundo de las amenazas más recurrentes o peligrosas.

Algunos de los obstáculos que se encuentran las compañías pequeñas y medianas en el problema de afrontar nuevas amenazas cibernéticas son:

---

[53] NATHALIA MORALES, Andi insiste en una apuesta por la transformación digital para ganar competitividad. [Sitio WEB]. October 2021. LR - Empres. [Disponible en 7 de May, 2022]. Recuperado de: https://www.larepublica.co/empresas/andi-insiste-en-una-apuesta-por-la-transformacion-digital-para-ganar-competitividad-3243005

[54] YOHAI, Informe SAFE - Tendencias Del Cibercrimen 2021 - 2022, 2021

[55] WELIVESECURITY, Guía definitiva para entender y protegerte de las APT | WeLiveSecurity. [Sitio WEB]. 2014. [Disponible en 2 de May, 2022]. Recuperado de: https://www.welivesecurity.com/la-es/2014/08/29/guia-definitiva-entender-protegerte-apt/

[56] CISA, *The CISA on DarkSide Ransomware and Best Practices for Preventing Business Disruption from Ransomware Attacks.*, Seybold Report: Analyzing Publishing Technologies. 21: 4–7

Programas de concienciación a los colaboradores: Es un factor fundamental para resolver la mayoría de los vectores de ataque exitosos, sin embargo, es un reto aún poco explorado por las organizaciones.

Servicios de ciber defensa costosos: El aspecto económico ha afectado a todos los sectores en tiempos de pandemia[57][58], especialmente para invertir en lo que aparentemente es solo un gasto en servicios que no retornan a la organización.

Las amenazas persistentes avanzadas APT, de sus siglas en inglés, Advanced Persistent Threat[59], es un ataque por el cual el delincuente permanecerá silenciosamente dentro de la infraestructura de la organización víctima, usando códigos maliciosos a medida o completamente nuevos para este propósito, lo que hace especialmente difícil de identificar para un equipo de respuesta. Este nuevo paradigma resulta en que las herramientas disponibles para la respuesta de las organizaciones son costosas y difíciles de implementar.

Poca visibilidad de las entidades gubernamentales de ciberdefensa: Entidades como el CCIT, COLCERT y la policía cibernética[60] son poco conocidas y pocas denuncias se realizan, lo que hace difícil trazar a los delincuentes y detener sus actividades.

Añadido a esto, la legislación colombiana[61] aún tiene un trecho por recorrer en cuanto a investigación y castigo a los delincuentes informáticos. La Cámara de Colombiana de Informática y Telecomunicaciones CCIT reportó que el ciberdelito por actores APT en Colombia ya se ha reportado desde 2021[62], siendo el más predominante el APT-C-36[63] especializado en espionaje de entidades financieras, petroleras, grandes manufacturas y gobierno de Colombia. APT-C-36 suplanta la URL de la entidad de aduanas e impuestos DIAN, cuyo URL original es “muisca.dian.gov.co” usando una URL maliciosa “diangovcomuiscia.com”, la organización envía órdenes de embargo suplantando la DIAN

---

[57] NIETO, Cibercriminales a la caza de la vacuna para la COVID-19 - Una al Día. [Sitio WEB]. November 18, 2020. [Disponible en 2 de April, 2022]. Recuperado de: https://unaaldia.hispasec.com/2020/11/cibercriminales-a-la-caza-de-la-vacuna-para-la-covid-19.html

[58] CCIT, Ciberdelitos en el sector empresarial aumentaron en 2021 - CCIT - Cámara Colombiana de Informática y Telecomunicaciones. [Sitio WEB]. July 26, 2021. [Disponible en 18 de October, 2021]. Recuperado de: https://www.ccit.org.co/en_los_medios/ciberdelitos-en-el-sector-empresarial-aumentaron-en-2021/

[59] RED SEGURIDAD, Amenaza Persistente Avanzada (APT): ¿cómo funciona este ciberataque? [Sitio WEB]. 2021. Redaccion. [Disponible en 2 de May, 2022]. Recuperado de: https://www.redseguridad.com/actualidad/cibercrimen/amenaza-persistente-avanzada-apt-como-funciona-este-ciberataque_20210420.html

[60] CCIT, TENDENCIAS CIBERCRIMEN COLOMBIA. [Sitio WEB]. 2019. CCIT. [Disponible en 18 de October, 2021]. Recuperado de: http://www.ccit.org.co

[61] SENADO, LEY 1273 2009. [Sitio WEB]. January 5, 2009. [Disponible en 12 de October, 2021]. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[62] YOHAI, Informe SAFE - Tendencias Del Cibercrimen 2021 - 2022, 2021

[63] MITRE ATT&CK, APT-C-36, Blind Eagle, Group G0099 | MITRE ATT&CK®. [Sitio WEB]. 2022. [Disponible en 18 de October, 2022]. Recuperado de: https://attack.mitre.org/groups/G0099/

indicando que adjunto se encuentra el documento oficial del embargo y debe responderse inmediatamente, proporcionan un archivo cifrado y la clave el cual al intentar abrirse infecta el dispositivo.

Las entidades afectadas actualmente por estos atacantes son de gran tamaño, gubernamentales, petroleras, o relacionadas con el sector bancario, por ello cuentan con equipos de respuesta, centros de operaciones de seguridad, procedimientos documentados y probados de atención a incidentes y en su mayoría están obligadas a reportarlos a entidades de vigilancia como la Superintendencia Financiera. Por ello se puede suponer que se sabe de estos ataques porque las víctimas han sido capaces de identificarlos y se han visto obligados a reportarlos, sin embargo, entidades de menor tamaño pueden ser vulnerables a dichos incidentes y no detectarlos, o de hacerlo posiblemente prefieran mantenerlo en privado para no afectar su imagen con clientes y proveedores.

Por ello, como respuesta la academia puede ofrecer productos como artículos, documentos, investigaciones y soluciones metodológicas que ofrezcan a las organizaciones instrumentos para fortalecer los procesos, equipos, metodologías y herramientas de defensa cibernética.

Por las razones descritas en los párrafos anteriores, en este trabajo se presenta un registro documental de las amenazas persistentes avanzadas APT, su impacto actual en las organizaciones enfocando en aquellas en crecimiento que no cuentan aún con infraestructura dedicada y especializada en defensa cibernética. Con el desarrollo del documento se busca responder a la cuestión:

¿Cómo el uso de buenas prácticas en las PYMES en Colombia puede aportar en la prevención y gestión Amenazas Persistentes Avanzadas, APT?

3. JUSTIFICACION

El incremento de las organizaciones que se han involucrado en medios digitales y su incursión en soluciones de conectividad para fines comerciales, operativos y de apoyo[64], ha resultado en el correspondiente aumento de ataques y evolución de los métodos de ataque cada vez más sofisticados[65]. Por ello las organizaciones deben tomar medidas en distintos focos[66], formación de su personal, herramientas de seguridad, evaluación de riesgos de seguridad de sus sistemas, proveedores y demás actividades que se listan en distintas guías de buenas prácticas y estándares que distintas organizaciones han emitido para orientarlas en la protección de sus activos[67]. Sin embargo, la implementación y mantenimiento de sistemas y equipos de seguridad informática son un costo alto para las organizaciones, especialmente las que no cuentan con flujos económicos grandes; por ejemplo, Microsoft ha incrementado su inversión en ciberseguridad en USD $1 Billón por año desde 2015[68], Google duplicaría esa cifra en los siguientes 5 años, números lejanos a lo que podría invertir una organización en Colombia.

En un estudio realizado a las Pymes de manufactura en Bogotá[69], se encontró que hasta un 65% de estas industrias usaban medios electrónicos, ya sea para fines comerciales o comunicación con clientes, sin embargo, más de la mitad de estas (36.3 % de la muestra) no usa ninguna herramienta o método de ciberseguridad. Estos resultados, tomados en la capital del país, dónde la brecha digital es casi nula y entidades como la Cámara Colombiana de Tecnologías de la Información CCIT, la Cámara de Comercio de Bogotá CCB, las principales universidades del país, y el mayor número de clientes posibles,

---

[64] ARIANA MENDOZA, Las tendencias de 2021 sobre la inmersión digital en las empresas. [Sitio WEB]. February 1, 2021. Covid-19 teletrabajo. [Disponible en 20 de February, 2022]. Recuperado de: https://appsimplantadores.com/tendencias-inmersion-digital-2021/

[65] CEPAL, *Digital technologies for a new future*, ECALC ONU. 43

[66] CESI, *RESEARCH IN THE FRAMEWORK OF CESI'S PROJECT "DIWORK-DIGITALISING PUBLIC SERVICES: MAKING IT WORK FOR CITIZENS, BUSINESS AND WORKERS" FINAL REPORT*, Visionary Analytics

[67] ESPINOZA AND ANTONIO, *Importancia de los modelos para el gobierno de la seguridad de la información en las empresas: una revisión sistemática de la literatura.*, Importance of Models for Government of Information Security in Companies: A Systematic Review of the Literature. 40: 1–14

[68] BRAUE, Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025. [Sitio WEB]. September 10, 2021. Cybercrime Mag. [Disponible en 22 de July, 2022]. Recuperado de: https://cybersecurityventures.com/cybersecurity-spending-2021-2025/

[69] LADINO FERNÁNDEZ *ET AL.*, *Industria 4.0: el reto para las pymes manufactureras de Bogotá, Colombia.*, Industry 4.0: The Challenge for Manufacturing SMEs in Bogotá, Colombia. 12: 110–127

entonces, es de esperarse que la situación no mejore en otras ciudades o empresas en las regiones.

Por las características de los ataques de los grupos que realizan el despliegue de Amenazas Persistentes Avanzadas APT, normalmente orientados a grandes industrias, las empresas en crecimiento son presas fáciles, si estos atacantes decidieran que son sus objetivos. Esto último, es exactamente lo que ha venido pasando a nivel internacional[70], en 2017 un reconocido casino de estados unidos fue hackeado a través de su tanque de peces, el exótico ataque, se llevó a cabo por medio del sistema de sensoria del tanque que reportaba los datos a la red del casino para el ajuste de temperatura, salinidad y alimentación; 10 GB de datos fueron filtrados a una IP en Finlandia[71]. Lo que estos ataques demuestran es que las cadenas de suministro son una brecha que debe tomarse en cuenta por las compañías, y que estos proveedores comiencen a preocuparse por la seguridad de sus activos, servicios y procesos.

Un grupo como APT-C-36[72], puede orientar sus ataques a las cadenas de suministro y de esta manera poner en riesgo a las PYMES para así llegar a sus clientes. Como ya se expuso en párrafos anteriores, las APT buscarán mantener silenciosamente la exfiltración[73] y dado el bajo grado de inversión en ciberseguridad de estas empresas, seguramente serán exitosos.

La academia tiene un papel fundamental en el seguimiento y propuesta de nuevas formas de delitos informáticos y las APT son una amenaza para los datos de todos, no solo para las PYMES, las grandes organizaciones, sino para todos los que contratan con entidades bancarias o de crédito, proveedores de internet, proveedores de telefonía móvil, y todos los servicios a los que voluntariamente se le debe entregar información.

Por lo anterior, en este documento se presentan los métodos actualmente utilizados para detectar, prevenir y enfrentar Amenazas Persistentes Avanzadas APT, recomendando la aplicación de las mejores prácticas que permitan la protección de los activos frente a APT para las pequeñas y medianas empresas colombianas (PYMES), para informar sobre el impacto actual en las organizaciones de los ataques e incidentes por Amenazas

---

[70] DESAI AND MAKRIDIS, *IDENTIFYING CRITICAL INFRASTRUCTURE IN A WORLD WITH SUPPLY CHAIN AND CROSS-SECTORAL CYBERSECURITY RISK.*, Jurimetrics: The Journal of Law, Science & Technology. 62: 173–195

[71] SEE LEE MATHEWS, Criminals Hacked A Fish Tank To Steal Data From A Casino. [Sitio WEB]. July 17, 2017. [Disponible en 22 de March, 2022]. Recuperado de: https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/?sh=5b24215432b9

[72] MITRE ATT&CK, APT-C-36, Blind Eagle, Group G0099 | MITRE ATT&CK®. [Sitio WEB]. 2022. [Disponible en 18 de October, 2022]. Recuperado de: https://attack.mitre.org/groups/G0099/

[73] RED SEGURIDAD, Amenaza Persistente Avanzada (APT): ¿cómo funciona este ciberataque? [Sitio WEB]. 2021. Redaccion. [Disponible en 2 de May, 2022]. Recuperado de: https://www.redseguridad.com/actualidad/cibercrimen/amenaza-persistente-avanzada-apt-como-funciona-este-ciberataque_20210420.html

Persistentes Avanzadas APT y proponer una metodología aplicable para este tipo de organizaciones.

4. OBJETIVOS

4.1 OBJETIVOS GENERAL

Proponer mecanismos y recomendaciones como buenas prácticas del negocio para la prevención de ataques del tipo Amenazas Persistentes Avanzadas APT orientado a Pequeñas y medianas Empresas – Pymes Colombianas.

4.2 OBJETIVOS ESPECÍFICOS

- Estructurar el estado del arte referente a las Amenaza Persistente Avanzada - APT que impactan a las PYMES colombianas, con el fin reconocer los vectores de ataque más comunes en este sector de la economía.

- Determinar las metodologías actuales de prevención de ataques APT, con el fin de ser propuesta como estrategia para la reducción de la superficie de riesgo de una PYMES.

- Construir informe técnico que plantee Técnicas, Tácticas y Procedimientos - TTP comunes en ataques APT, el cual sirva como apoyo en la toma de decisiones en el momento de presentarse un evento de ciberseguridad.

5. MARCO REFERENCIAL

5.1 MARCO CONCEPTUAL

5.1.1 Amenaza: Según la definición dada en la ISO 27000:2017[74].

Una amenaza es una causa probable de la ocurrencia de un incidente, este puede causar daño o pérdida de las condiciones de seguridad de un sistema u organización.

5.1.2 Persistente. Se trata de una situación que perdura en el tiempo o que insistentemente actúa por cumplir con su objetivo.

Para el caso de amenazas informáticas, se trata de programas maliciosos que están diseñados para mantener un ataque durante prolongados lapsos de tiempo [75], bien sea para permanecer sin ser detectado en un sistema o para sabotear una infraestructura.

5.1.3 Avanzada. El término se emplea en tecnología para señalar que se encuentra en el nivel más alto de sofisticación.

Por ejemplo, super computadoras o tecnología espacial. Par el caso particular de los sistemas informáticos, se trata del uso de últimas tecnologías de automatización como son herramientas de inteligencia artificial, técnicas heurísticas, software de código dinámico [76].

5.1.4 Amenazas Persistentes Avanzadas, APT. Son programas elaborados para evitar sistemas de control establecidos en la infraestructura de la víctima [77].

Sus víctimas pueden ser personas u organizaciones para espionaje, suplantación de identidad o daño reputacional. Se denominan persistentes debido a que cuentan con infraestructura que se distribuye en múltiples orígenes y tienen la capacidad de mantener un ataque de manera constante por largos lapsos de tiempo, incluso años evitando ser detectados mientras extraen información clave para afinar el ataque.

---

[74] ICONTEC, NTC-ISO-IEC 27000:2017, ICONTEC, 2017

[75] MÁRQUEZ DÍAZ, *Armas cibernéticas. Malware inteligente para ataques dirigidos : Cyber Weapons. Intelligent Malware for Targeted Attacks*, Revista Ingenierías USBMed. 8: 48–57

[76] BALBÁS GUTIÉRREZ, ATAQUES AL CRIPTOSISTEMA RSA (ATTACKS ON RSA) Trabajo de fin de Grado para acceder al GRADO EN MATEMÁTICAS., Universidad de Cantabria, Santander Cantabria, July 2019, pp.

[77] ROLDÁN *ET AL.*, *THE ADVANCED PERSISTENT THREATS (APT) AND ITS METHOD OF DELINQUENCY.*, LA AMENAZA PERSISTENTE AVANZADA (APA) Y SU MÉTODO DE DELINCUENCIA. 10: 127–143

Estos ataques son realizados por individuos u organizaciones criminales [78] que cuentan con amplios conocimientos en ciberseguridad, por lo cual se les facilita identificar vulnerabilidades de día 0 y explotarlas antes que las víctimas puedan corregirlas, comprometiendo varios equipos de la infraestructura rápidamente, elevando privilegios en estos y alojando puertas traseras para silenciosamente seguir extrayendo datos [79].

Estos ataques se llevan a cabo siguiendo un proceso lógico que puede incluir el uso de ingeniería social, aprovechamiento de bases de datos filtradas, monitoreo constante de los puntos expuestos y otros mecanismos de captura de información de la víctima. Los pasos pueden darse de la siguiente manera [80]:

Determinación de la víctima y su superficie de ataque (infraestructura y personas), seguido de monitoreo y campañas de ingeniería social hasta lograr acceso.

- Introducción de software malicioso, puertas traseras y ampliación de la superficie de ataque.
- Escalamiento de privilegios.
- Recopilar información y Movimiento lateral iterando los puntos 2 y 3.
- Extracción de la información.

5.1.5 IOC Los indicadores de compromiso.

Los indicadores de compromiso, o IOC, por sus siglas en inglés, son características que los investigadores forenses han detectado para una amenaza, de esta forma otro investigador pueda observarla e identificarla ágilmente. Actualmente existen bases de datos de IOC que son utilizadas por investigadores a nivel mundial y son alimentadas ya sea públicamente o por fabricante de herramientas de seguridad. Al instalar un antivirus este descarga una réplica de las bases de datos de IOC o firmas. Cuando se usa un HIDS la base de datos se encuentra en el servidor o SIEM.

[78] INCIBE, CSIRT-CV e INTECO-CERT publican el informe: “Detección de APTs” | INCIBE. [Sitio WEB]. 2015. [Disponible en 2 de May, 2022]. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/deteccion-apts

[79] WELIVESECURITY, Guía definitiva para entender y protegerte de las APT | WeLiveSecurity. [Sitio WEB]. 2014. [Disponible en 2 de May, 2022]. Recuperado de: https://www.welivesecurity.com/la-es/2014/08/29/guia-definitiva-entender-protegerte-apt/

[80] S21SEC, *Segundo semestre 2021*, Threat Landscape Report. 1: 1–38

5.2 MARCO HISTÓRICO

Las Amenazas Persistentes Avanzadas APT, podrían relacionarse con las secuelas de lo que fue la guerra fría, un enfrentamiento entre estados que desde 1945 hasta 1960 aproximadamente, que no se desarrolló en un campo de batalla y no requirió inversión a gran escala en armamentos por los estados en conflicto. Esto debido a que la confrontación se hizo sin enfrentamientos abiertos entre soldados, sino en el marco del espionaje e inteligencia de sus militares. La relación entre APT y guerra fría radica en el gran esfuerzo e inversión de organizaciones por especializar la infiltración de sus recursos en el terreno enemigo y obtener información sobre estos, ya no en el marco de la lucha entre Democracia y Socialismo, sino en la obtención de datos estratégicos sobre economía, recursos militares, disuasión atómica[81].

La guerra fría motivó grandes inversiones en inteligencia militar y ciber inteligencia, esto desencadenó una amplia especialización de equipos y tecnologías de la información para estos objetivos. La denominada "Guerra fría cibernética" [82] fue introducida en 2013 por el conflicto entre Estados Unidos y China.

Los actores especializados para ataques cibernéticos pueden haber surgido en el mismo momento de la guerra fría, pero solo fueron catalogados recientemente (el grupo con actividad más antigua fue en 2005, APT30[83]); actualmente existen especialistas de seguridad encargados de hacerles seguimiento. Mandiant ha publicado una lista de los actores APT que contempla un registro de las organizaciones por su cantidad de campañas con el esquema APTXX, donde XX es el número de campañas del actor[84].

Estos especialistas de seguridad cuentan con equipos de inteligencia para descubrir las Tácticas, Técnicas y Procedimientos (TTPs)[85] para la identificación de las agrupaciones, así por ejemplo el grupo APT28, conocido como TSAR TEAM[86] fue identificado por su preferencia por objetivos en países europeos, entre ellos la mayoría miembros de la

---

[81] ECONOMIA3.COM, APT - Economia3. [Sitio WEB]. December 21, 2013. [Disponible en 26 de June, 2022]. Recuperado de: https://economia3.com/2013/12/21/16316-apt/

[82] LATERCERA.COM, La "Guerra Fría cibernética" entre Estados Unidos y China - La Tercera. [Sitio WEB]. February 2, 2013. [Disponible en 26 de June, 2022]. Recuperado de: https://www.latercera.com/noticia/la-guerra-fria-cibernetica-entre-estados-unidos-y-china/

[83] BROADBAND4EUROPE, Cyber security: APT30 and lessons for ASEAN - Broadband 4 Europe. [Sitio WEB]. April 15, 2015. Cyber Secur. [Disponible en 26 de June, 2022]. Recuperado de: https://www.broadband4europe.com/cyber-security-apt30-lessons-asean/

[84] MANDIANT, Advanced Persistent Threats (APTs) | Threat Actors & Groups. [Sitio WEB]. 2022. [Disponible en 26 de June, 2022]. Recuperado de: https://www.mandiant.com/resources/apt-groups

[85] Tácticas, Técnicas y Procedimientos (TTPs). | El Blog de Tiro Táctico (EBdT2). [Sitio WEB]. June 4, 2022. [Disponible en 26 de June, 2022]. Recuperado de: https://tirotactico.net/2011/06/04/68/

[86] MINISERIO DE DEFENSA ESPAÑOL AND INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS, *SECRETARÍA GENERAL TÉCNICA*, Boletín IEEE. 83

OTAN[87] y otras organizaciones de defensa y seguridad. El software utilizado por APT28 tiene comentarios en ruso y sus operaciones se identificaron en horarios laborales del huso horario cercano a Moscú, por ello se especula que tiene inversión del gobierno ruso.

En 2017, se hizo público uno de los primeros ciberataques a nivel mundial conocido como WannaCry[88]. En el cual, este RANSOMWARE, un software malicioso cifra el contenido del disco y se propaga por la red realizando para afectar de la misma manera otros dispositivos. Luego, pide una cantidad de dinero en criptomonedas a cambio de la clave de cifrado. WannaCry sigue siendo una de las mayores amenazas en el ciberespacio. WannaCry se aprovechó de una vulnerabilidad Zero Day, vulnerabilidades sin identificar que aún no tienen un mecanismo de defensa.

Con WannaCry se dio a conocer el grupo conocido como THE SHADOW BROKERS, quienes anunciaron haber accedido a la NSA (National Security Agency) de Estados Unidos. En la declaración afirmaron haber extraído el 10% del software malicioso utilizado por la NSA, lo que denota que los estados cuentan con un equipo de ciber ataque, adicional a las entidades públicas de ciber defensa, además de la peligrosidad de estos grupos, pues uno solo, con una sola pieza de código, lograron afectar gran cantidad de organizaciones y usuarios a nivel mundial.

Aunque la identificación de grupos APT, es relativamente reciente, ya es tan ampliamente conocido en el mundo de la ciber inteligencia que algunos grupos han mutado para convertirse en AVT, ADVANCED VOLATILE THREAT, amenaza avanzada volátil, que a diferencia de las tradicionales APT, son organizaciones que no buscan permanecer y persistir en sus objetivos sin ser detectadas, adicionalmente esperan desvanecerse una vez obtienen su objetivo sin dejar rastro en los sistemas afectados[89].

Ambos, APT y AVT, representan riesgos para las organizaciones, pero especialmente para las PYMES, debido a que pueden, en ambos casos, resultar en compromiso de datos de sus clientes corporativos y afectar operaciones y clientes finales masivamente. En los capítulos siguientes el lector encontrará información sobre las amenazas más recientes y un análisis de su impacto a las Pymes para poder resaltar la importancia de la preparación de estas organizaciones y algunos métodos para realizarlo.

---

[87] OTAN, ¿Qué es la OTAN? [Sitio WEB]. 2022. [Disponible en 26 de June, 2022]. Recuperado de: https://www.nato.int/nato-welcome/index_es.html

[88] KASPERSKY, Todo sobre el ransomware WannaCry. [Sitio WEB]. June 1, 2022. [Disponible en 26 de June, 2022]. Recuperado de: https://www.kaspersky.es/resource-center/threats/ransomware-wannacry

[89] PIERLUIGI PAGANINI, CyberCriminals and their APT and AVT TechniquesSecurity Affairs. [Sitio WEB]. February 23, 2015. [Disponible en 26 de June, 2022]. Recuperado de: https://securityaffairs.co/wordpress/33999/cyber-crime/apt-and-avt-techniques.html

5.3 MARCO LEGAL

El congreso de la república de Colombia ajustó el código penal para la tipificación delitos informáticos en el año 2009.

Los atentados a la confidencialidad, integridad y disponibilidad de la información se consideran delitos de acuerdo con las disposiciones legales por el articulado denominado "de la protección de la información y de los datos" con el objetivo de proteger y conservar los sistemas basados en el uso de las tecnologías de información y de las comunicaciones.

La ley establece sanciones económicas y penas privativas de la libertad para quienes sean hallados culpables de afectar un sistema informático por:

- Sabotear,
- Dañar,
- Obstaculizar o
- Acceder ilegalmente.

Además, contempla algunos agravantes que podrían aumentar la pena principal.

Según la Ley 1273 2009[90], Algunos de los delitos relacionados en la ejecución de Amenazas Persistentes Avanzadas APT son:

Artículo 269A: Acceso abusivo a un sistema informático: De hecho, es el objetivo de un atacante, acceder o afectar un sistema de forma abusiva.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación: La posible suplantación o afectación a un sistema.

Artículo 269D: Daño Informático: La destrucción o alteración de datos de los sistemas.

Artículo 269E: Uso de software malicioso: El uso de herramientas que alteren el normal funcionamiento de un sistema. En este aspecto se verá el uso de códigos de comando y control.

[90] SENADO, LEY 1273 2009. [Sitio WEB]. January 5, 2009. [Disponible en 12 de October, 2021]. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Artículo 269G: Suplantación de sitios web para capturar datos personales: Específicamente utilizado en campañas de Phishing para engañar a los usuarios.

Artículo 269H: Circunstancias de agravación punitiva: "Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales."[91]

[91] SENADO, LEY 1273 2009. [Sitio WEB]. January 5, 2009. [Disponible en 12 de October, 2021]. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

5.4 MARCO TEÓRICO

A partir de fuentes libres y públicas, como la policía nacional de Colombia, el Ministerio de las Tecnologías de la información y las Comunicaciones, y organizaciones de expertos en ciberseguridad, se presentan a continuación los incidentes reportados que se adjudican a actores APT.

5.4.1 Delitos informáticos denunciados durante el periodo 2020 - 2023.

La policía colombiana registra los reportes de delitos informáticos denunciados a través del CAI Virtual[92], allí se pueden verificar los análisis de datos realizados por esta entidad colombiana, evidenciando los incrementos de delitos cibernéticos entre el 2019 y 2020 de la manera presentada en la Tabla 1. Balance de variación de delitos informáticos 2019-2020.

Tabla 1. Balance de variación de delitos informáticos 2019-2020.

Ley 1273 2009	2019	2020	Variación %
Suplantación de sitios web	733	3499	377
Interceptación de datos informáticos	291	975	235
Violación de datos personales	2032	5794	185
Obstaculización ilegítima de sistema informático o red de telecomunicación	73	204	179
Transferencia no consentida de activos	1018	2064	103
Acceso abusivo a un sistema informático	2303	4417	94
Hurto por Medios Informáticos y Semejantes	7383	10208	38
Uso de software malicioso	293	399	36
Daño informático	1174	403	-132

Fuente: CAI Virtual, Policía Nacional de Colombia[93].

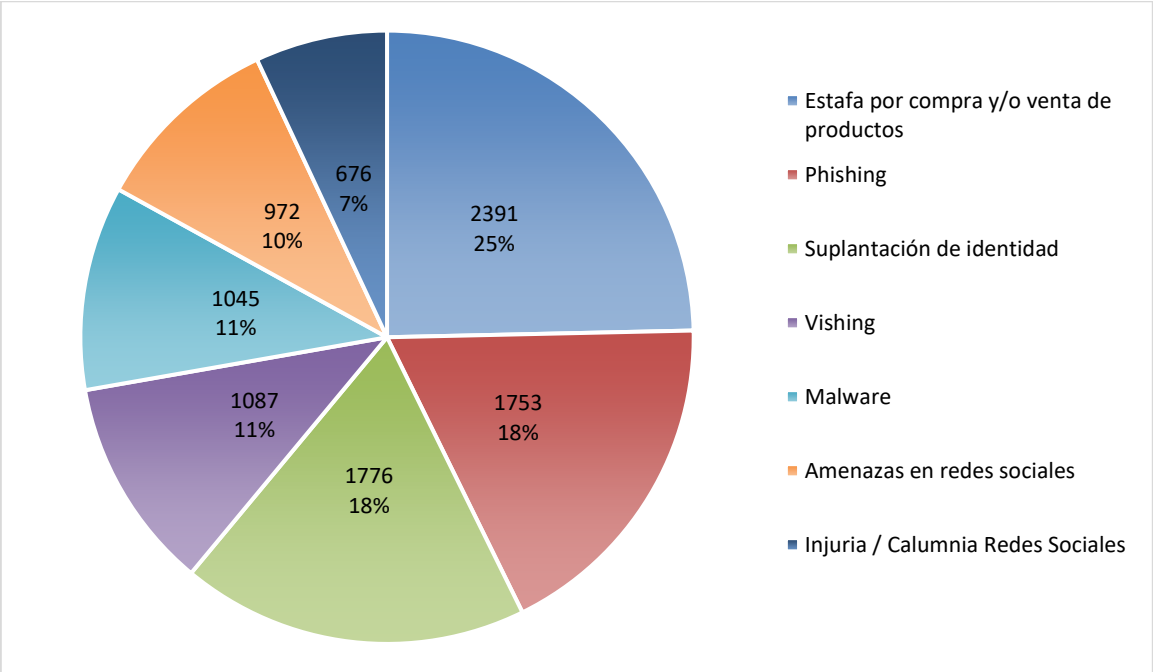
Como se puede observar el top 5 de delitos reportados en 2020 son:

1. Hurto por Medios Informáticos y Semejantes
2. Violación de datos personales
3. Acceso abusivo a un sistema informático
4. Suplantación de sitios web
5. Transferencia no consentida de activos

De éstos se resalta en cuanto a su incremento en ocurrencia reportada, los ubicados en la posición 4 y 2, sin embargo, 3 y 5 duplicaron sus números. Estos datos muestran una tendencia a la sofisticación técnica de los ataques y al aumento significativo en todos los frentes registrados por la policía.

[92] POLICIA, *BALANCE CIBERCRIMEN 2020*, BALANCE CIBERCRIMEN
[93] Ibid.

Figura 1. Modalidad de ataques, cifras de reporte a CAI Virtual.



Fuente: CAI Virtual, Policía Nacional de Colombia[94].

En 2020 el CAI Virtual atendió aproximadamente 12000 incidentes y 8000 correos, entre los cuales la modalidad de ataque utilizada en el 75% de los casos se encuentra entre:

- Estafa por compra y/o venta de productos
- Phishing
- Suplantación de identidad
- Vishing

Otra fuente de datos es la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), que presenta un informe nada alentador de 7 billones de ataques cibernéticos recibidos en Colombia, solo durante el 2021[95]. Allí por primera vez una entidad colombiana acepta la afectación ocurrida por la actividad grupos como Blind Eagle o APT-C36[96]; el informe presenta la cifra de 193 sitios web del estado que han sido

[94] POLICIA, *BALANCE CIBERCRIMEN 2020*, BALANCE CIBERCRIMEN
[95] CCIT, Estudio trimestral de ciberseguridad: Ataques a entidades de gobierno - CCIT - Cámara Colombiana de Informática y Telecomunicaciones. [Sitio WEB]. April 2022. Estudios. [Disponible en 19 de November, 2022]. Recuperado de: https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/
[96] MITRE ATT&CK, APT-C-36, Blind Eagle, Group G0099 | MITRE ATT&CK®. [Sitio WEB]. 2022. [Disponible en 18 de October, 2022]. Recuperado de: https://attack.mitre.org/groups/G0099/

comprometidas de alguna manera. El vector de ataque identificado es la *captura de credenciales guardadas en el navegador* mediante el uso de software malicioso.

El reporte de CCIT incluye información sobre la afectación ocurrida en el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima) que afectó el 80 % de su infraestructura tecnológica y que se debió a un Ransomware conocido como BlackByte.

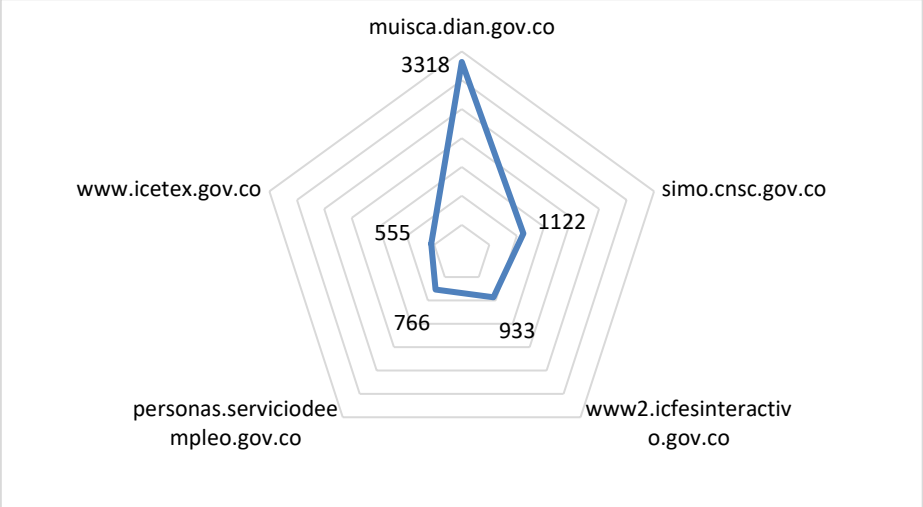
Otras entidades afectadas fueron: Dirección de Impuestos y Aduanas Nacionales (DIAN), la Comisión Nacional del Servicio Civil (CNSC), el Instituto Colombiano para la Evaluación de la Educación (ICFES), la Unidad del Servicio de Empleo, la Agencia Nacional de Contratación Pública, el ICETEX, COLPENSIONES, la Secretaría de Hacienda del Distrito de Bogotá, Migración Colombia, el Fondo Nacional del Ahorro y la Alcaldía de Medellín.

Tabla 2. Balance de variación de delitos informáticos 2021-2022 Q1.

Ley 1273 2009	2021	2022
Hurto por Medios Informáticos y Semejantes	3981	3574
Violación de datos personales	3204	1947
Suplantación de sitios web	1545	914

Fuente: CCIT, Informe trimestral 2022[97].

Figura 2. Exposición de credenciales de sitios web gubernamentales.



[97] CCIT, Estudio trimestral de ciberseguridad: Ataques a entidades de gobierno - CCIT - Cámara Colombiana de Informática y Telecomunicaciones. [Sitio WEB]. April 2022. Estudios. [Disponible en 19 de November, 2022]. Recuperado de: https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/

Fuente: CCIT, Informe trimestral 2022[98].

Aunque estos números presentan una aproximación al estado de ciberseguridad de la nación, no pueden ser relacionados con actores APT, puesto que no existen datos que los relacionen; es por ello que, ahora, se deben analizar los actores identificados al momento en la región.

Los dos delitos más reportados a cierre de 2022 fueron el Hurto por medios informáticos (25413) y Acceso abusivo por medio informático (13318)[99], tuvieron un crecimiento de 34% y 62% respectivamente. Acceso abusivo por medio informático presentó un incremento que lo llevó a subir una posición en el ranking desde 2020. Así el nuevo TOP 5 en 2022 es:

1. Hurto por Medios Informáticos y Semejantes
2. Acceso abusivo a un sistema informático
3. Violación de datos personales
4. Suplantación de sitios web
5. Transferencia no consentida de activos

5.4.2 Actores APT en Colombia y la región latinoamericana. No es posible identificar un actor APT que se enfoque en una nación únicamente, sin embargo, existen focalizaciones regionales.

Para realizar una aproximación hacia la situación real de las PYMES en cuanto al riesgo de ser atacadas por un actor APT, se presentan los actores más representativos en la región y sus casos de éxito.

Tabla 3. APT identificadas con actividad en Latinoamérica.

Nombre	Grupo	Objetivos
APT-C-36 **Blind Eagle**[100]	G0099	INCI (Instituto Nacional de Ciegos de Colombia) Ecopetrol (Compañía Colombiana de Petróleos) Hocol (Filial de Ecopetrol) Fabricante de llantas en Colombia (IMSA) Empresa de logística en Colombia (Almaviva) Banco en Colombia (Banco de Occidente) ATH División de Colombia Sucursal de Sun Chemical en Colombia

[98] CCIT, Estudio trimestral de ciberseguridad: Ataques a entidades de gobierno - CCIT - Cámara Colombiana de Informática y Telecomunicaciones. [Sitio WEB]. April 2022. Estudios. [Disponible en 19 de November, 2022]. Recuperado de: https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/

[99] CCIT, Estudio Anual de Ciberseguridad. [Sitio WEB]. Bogota, 2023. [Disponible en 20 de March, 2023]. Recuperado de: https://www.ccit.org.co/wp-content/uploads/estudio-anual-de-ciberseguridad.pdf

[100] MITRE ATT&CK, APT-C-36, Blind Eagle, Group G0099 | MITRE ATT&CK®. [Sitio WEB]. 2022. [Disponible en 18 de October, 2022]. Recuperado de: https://attack.mitre.org/groups/G0099/

Poseidon[101]	G0033	Se han identificado al menos 35 empresas víctimas con objetivos principales, incluidas instituciones financieras y gubernamentales, empresas de servicios públicos de telecomunicaciones, manufactura, energía y otros servicios, así como empresas de medios y relaciones públicas, todas ubicadas o con actividades en Brasil.
Sowbug[102]	G0054	Miembros del gobierno o personajes estratégicos en Sudamérica y suroriente de Asia.
APT-C-43 Machete[103]	G0095	La mayor parte de las víctimas procedían predominantemente de Ecuador, Venezuela, Perú, Argentina y Colombia; sin embargo, se identificaron otras víctimas en Corea, Estados Unidos, República Dominicana, Cuba, Bolivia, Guatemala, Nicaragua, México, Inglaterra, Canadá, Alemania, Rusia y Ucrania. Los objetivos incluían una amplia gama de entidades de alto perfil, incluidos servicios de inteligencia, militares, proveedores de servicios públicos (telecomunicaciones y energía), embajadas e instituciones gubernamentales.
APT-38 BeagleBoyz	G0082	Entidades financieras en: Argentina, Brasil, Bangladesh, Bosnia y Herzegovina, Bulgaria, Chile, Costa Rica, Ecuador, Ghana, India, Indonesia, Japón, Jordania, Kenia, Kuwait, Malasia, Malta, México, Mozambique, Nepal, Nicaragua, Nigeria, Pakistán, Panamá , Perú, Filipinas, Singapur, Sudáfrica, Corea del Sur, España, Taiwán, Tanzania, Togo, Turquía, Uganda, Uruguay, Vietnam, Zambia
APT-15 Ke3chang Vlxen Panda[104]	G0004	Entidades de petróleo, gobierno, diplomático, militar y ONG en América Central y del Sur, el Caribe, Europa y América del Norte desde al menos 2010

Fuente: Propia.

Durante el año 2022 se presentaron ataques reportados por entidades de gran tamaño en Colombia, estas fueron entre otras, Salud Total EPS, Colsanitas por su empresa multinacional Keralty, EPM y Afinia[105]; para otras entidades como La fiscalía general de la Nación se reportó como vulnerada por los activistas cibernéticos Guacamaya[106] quienes indican haber extraído 11 TB de datos entre correos confidenciales y documentos de más de 38000 carpetas de la red privada de la entidad. Aunque estos

[101] SECURELIST, Poseidon Group: a Targeted Attack Boutique specializing in global cyber-espionage | Securelist. [Sitio WEB]. February 9, 2016. APT REPORTS. [Disponible en 11 de October, 2022]. Recuperado de: https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/

[102] BROADCOM, Sowbug: Cyber espionage group targets South American and Southeast Asian governments . [Sitio WEB]. November 17, 2017. Endpoint Prot. [Disponible en 11 de December, 2022]. Recuperado de: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=d544bd14-1dd2-4ab6-a5a0-181788b7d73b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[103] BLACKBERRY, El Machete's Malware Attacks Cut Through LATAM. [Sitio WEB]. March 22, 2017. Res. Intell. [Disponible en 11 de October, 2022]. Recuperado de: https://blogs.blackberry.com/en/2017/03/el-machete-malware-attacks-cut-through-latam

[104] Ke3chang, APT15, Mirage, Vixen Panda, GREF, Playful Dragon, RoyalAPT, NICKEL, Group G0004 | MITRE ATT&CK®. [Sitio WEB]. [Disponible en 24 de January, 2023]. Recuperado de: https://attack.mitre.org/groups/G0004/

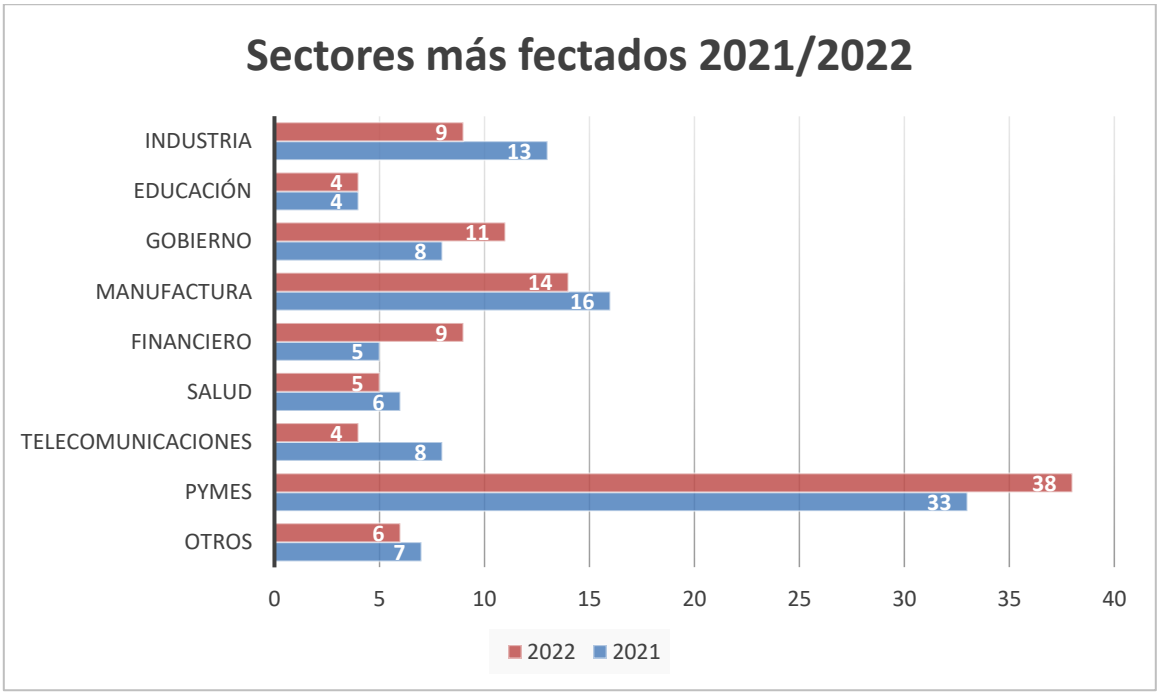
[105] LA REPUBLICA, El problema de los hackers hay que priorizarlo. [Sitio WEB]. December 22, 2022. EDITORIAL. [Disponible en 22 de December, 2022]. Recuperado de: https://www.larepublica.co/opinion/editorial/el-problema-de-los-hackers-hay-que-priorizarlo-3513522?utm_medium=Social&utm_source=Twitter#Echobox=1671709093

[106] EL ESPECTADOR, Guacamaya leaks: Últimas noticias, fotos, videos, artículos de opinión de Guacamaya leaks | EL ESPECTADOR. [Sitio WEB]. December 29, 2022. [Disponible en 22 de December, 2022]. Recuperado de: https://www.elespectador.com/tags/guacamaya-leaks/

eventos no pueden vincularse con grupos APT, es claro que hay un interés global de los ciber delincuentes por los activos informáticos de Colombia.

La cámara colombiana de tecnología y telecomunicaciones reporta que el sector más afectado por ciberdelincuentes es el sector PYMES[107] y lo más preocupante es que solo 7% de estas empresas superan el siguiente año al ataque, estas cifras pueden verse en la Figura 3. Sectores más afectados 2021-2022 en Colombia.

Figura 3. Sectores más afectados 2021-2022 en Colombia.



Fuente: CCIT, Estudio Anual de Ciberseguridad. [Sitio WEB]. Bogotá, 2023.[108].

Lo anterior indica que este año habrá un 14% Pymes menos que en 2021 en el mercado debido a ataques cibernéticos.

[107] CCIT, Estudio Anual de Ciberseguridad. [Sitio WEB]. Bogota, 2023. [Disponible en 20 de March, 2023]. Recuperado de: https://www.ccit.org.co/wp-content/uploads/estudio-anual-de-ciberseguridad.pdf
[108] Ibid.

6. DESARROLLO DE LOS OBJETIVOS

6.1 DESARROLLO OBJETIVO 1: ESTRUCTURAR EL ESTADO DEL ARTE REFERENTE A LAS AMENAZA PERSISTENTE AVANZADA

En este capítulo el lector encontrará modelos de ataque utilizados para determinar distintas etapas de ataque que ayudan a identificar estructuras comunes en ataques sofisticados de grupos APT.

6.1.1 Cadena de la Muerte, Kill-Chain Apt. Permiten conocer los pasos utilizados por los atacantes para lograr con éxito.

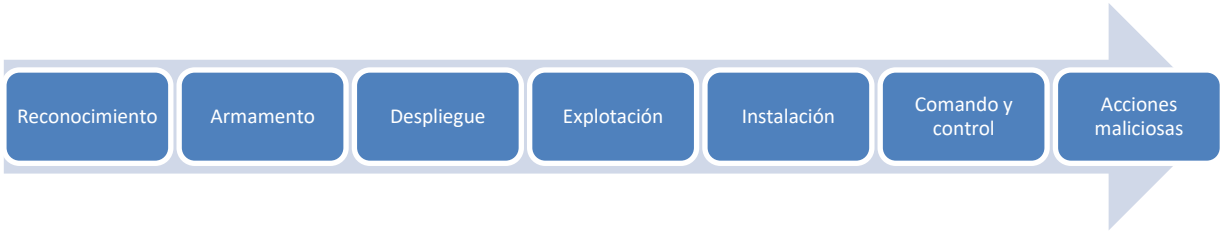
Para poder identificar los mecanismos de defensa contra APT, se deben conocer los pasos utilizados por los atacantes para lograr con éxito un ataque a una organización. Para identificar causa raíz de las alarmas o incidentes de seguridad apropiadamente se han propuesto métodos de cadena de la muerte o Kill-Chain para segregar la lógica y prácticas utilizadas por los atacantes, esto resulta en alarmas más detalladas y efectivas.

Existen 3 modelos de kill-chain, Lockheed Martin Kill-Chain, Ciclo de vida de Mandiant Attack y Bryant Kill-Chain.[109]

6.1.2 Fases según LOCKHEED MARTIN KILL-CHAIN.

Consiste en siete pasos ordenados que describen los objetivos de los atacantes en cada uno y que deben completarse para que la red sea comprometida exitosamente y poder llevar a cabo las actividades maliciosas como el hurto de datos, denegación de servicios, suplantación de actores cibernéticos o destrucción de información.

Figura 4. Fases de ataque modelo: Lockheed Martin Kill-Chain.



Fuente: XUAN, C. Do, and M. H. DAO. A Novel Approach for APT Attack Detection Based on Combined Deep Learning m...: EBSCOhost. April 11, 2021. Neural Computing and Applications. 2021[110].

[109] BRYANT AND SAIEDIAN, *A novel kill-chain framework for remote security log analysis with SIEM software*, Computers & Security. 67: 198–210

[110] XUAN AND DAO, *A novel approach for APT attack detection based on combined deep learning m...: EBSCOhost*, Neural Computing and Applications. 2021

Las fases son dispuestas de forma lineal que no identifica posibles pasos que debn depender de decisiones, como se observa en la Figura 4. Fases de ataque modelo: Lockheed Martin Kill-Chain. Estas fases son:

6.1.2.1 Reconocimiento de Información. Recoger información de distintas fuentes públicos como motores de búsqueda y registros DNS para detectar fugas de información, analizar los servicios publicados en el servidor objetivo, analizar los archivos en busca de información en los metadatos, identificar métodos de entrada al servidor.

6.1.2.2 Armamento. La construcción de aplicaciones personalizadas para la carga, envío y enmascaramiento de payloads y exploits.

6.1.2.3 Despliegue. Identificados los puntos de acceso y víctimas, los atacantes se disponen a hacer llegar los códigos y engaños para obtener acceso a los activos objetivo.

6.1.2.4 Explotación. Una vez obtenido acceso a credenciales o canales de acceso a los datos sigue la identificación y explotación de vulnerabilidades para obtener los privilegios necesarios para permanecer silenciosamente en el sistema objetivo.

6.1.2.5 Instalación. Obteniendo los privilegios necesarios se procese a crear los ambientes y puertas traseras que permitan el constante acceso y control del sistema de la víctima.

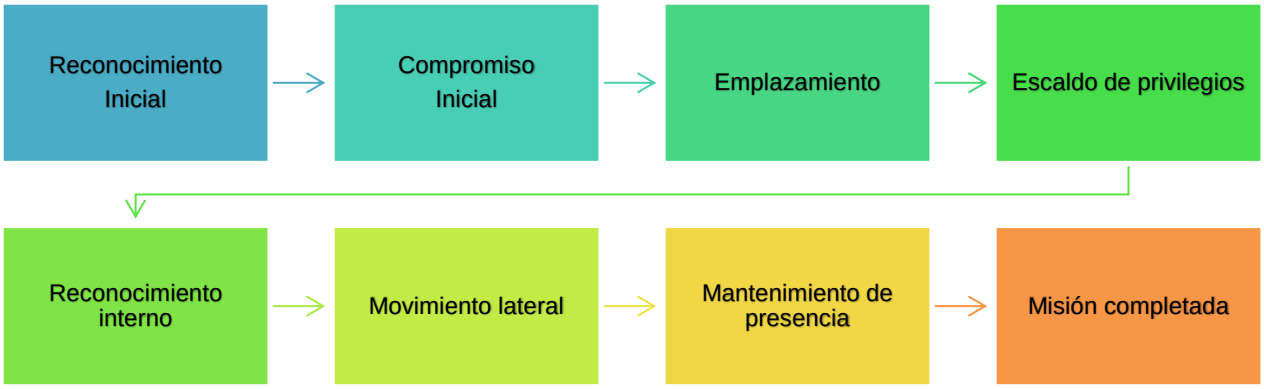
6.1.2.6 Comando y control. Es exactamente eso, tomar control y lanzar las órdenes que permitan mantener el acceso silencioso a los sistemas y ejecutar las acciones maliciosas.

6.1.2.7 Acciones maliciosas. Obtener el lucro de la información obtenida, la extorsión al objetivo y la venta de datos que será utilizada para nuevas campañas.

6.1.3 Ciclo De Vida De MANDIANT ATTACK

Publicado en el 2012, el modelo de Mandiant de ciclo de vida del ataque se diferencia del modelo de Lockheed Martin porque se enfoca mayormente en las actividades dentro de la organización objetivo o en sus activos afectados. Así pues, el reconocimiento inicial hace parte de las fases que son directamente en activos, al contrario de la fase de reconocimiento de Lockheed Martin que puede no involucrar ningún activo de la víctima. Otra característica diferencial es el ciclo recursivo de reconocimiento interno y movimiento lateral, esto se puede apreciar en la Figura 5. Fases de ataque modelo: Mandiant Attack Lifecycle.

Figura 5. Fases de ataque modelo: Mandiant Attack Lifecycle.



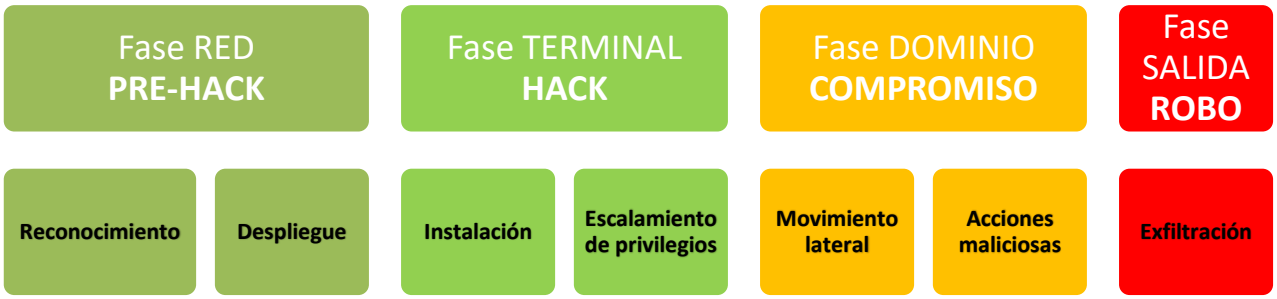
Fuente: XUAN, C. Do, and M. H. DAO. A Novel Approach for APT Attack Detection Based on Combined Deep Learning m...: EBSCOhost. April 11, 2021. Neural Computing and Applications. 2021[111].

Para esta aproximación el autor establece que hay un ciclo entre las fases Escalado de privilegios, Reconocimiento interno, Movimiento lateral y Mantenimiento de presencia antes de finalizar el compromiso de los datos.

6.1.4 Fases según BRYANT KILL-CHAIN

Un modelo lineal que se distribuye en 4 dominios de ataque o fases y 7 pasos se presenta en Figura 6. Fases de ataque modelo: Bryant Kill-Chain.

Figura 6. Fases de ataque modelo: Bryant Kill-Chain.



Fuente: XUAN, C. Do, and M. H. DAO. A Novel Approach for APT Attack Detection Based on Combined Deep Learning m...: EBSCOhost. April 11, 2021. Neural Computing and Applications. 2021[112].

Cuenta también con siete pasos, al igual que el modelo Lockheed Martin, pero, desde el punto de vista de los activos de la víctima, algunas actividades no pueden ser observadas, como la construcción del armamento del atacante. Adicionalmente se

---

[111] XUAN AND DAO, *A novel approach for APT attack detection based on combined deep learning m...: EBSCOhost*, Neural Computing and Applications. 2021

[112] XUAN AND DAO, *A novel approach for APT attack detection based on combined deep learning m...: EBSCOhost*, Neural Computing and Applications. 2021

agregan nuevas fases como lo son el movimiento lateral y la exfiltración. Otro cambio es el resumen en fases macro o que simbolizan el estado de compromiso de los activos: Pre-hack, hack, compromiso y robo; estas fases también simbolizan el estado de los datos accedidos por el atacante: RED, TERMINAL, DOMINIO y SALIDA.

6.1.5 Definiciones de ataques Amenazas Persistentes Avanzadas, APT

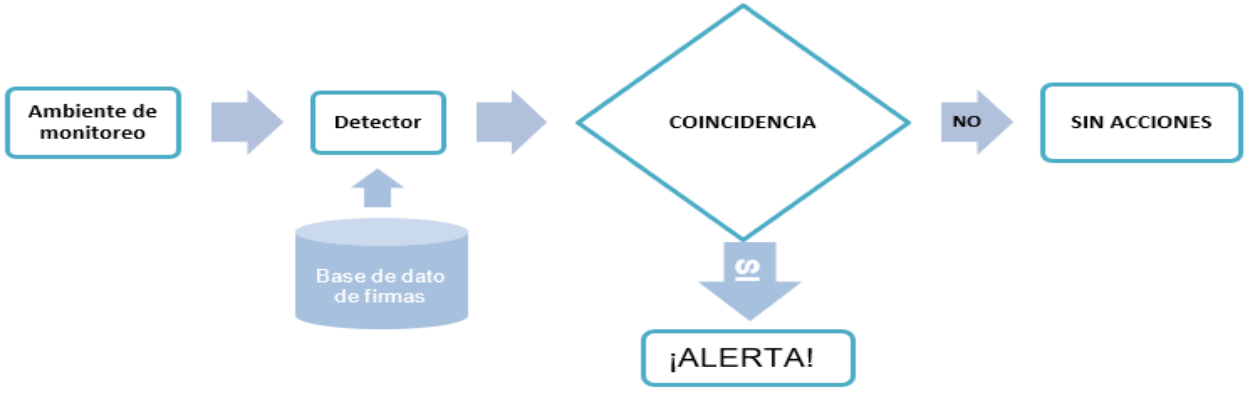
Se puede decir que los actores de ataques de tipo APT se categorizan en dos grupos: Con objetivo definido, Sin objetivo o de difusión[113]. En la primera el atacante ha definido claramente su víctima, por el contrario, en el segundo grupo están estos ataques en el que el cibercriminal busca la mayor cantidad de objetivos posibles para luego enfocarse en los que han logrado mayor grado de avance.

Hay dos mecanismos de detección de amenazas, que según como los sistemas de defensa de una organización estén diseñados para detectarlos, estos son: Basados en firmas o basados en anomalías.

6.1.5.1 Detección basada en firmas. Se presentan los métodos de intrusión en Figura 7. Detección basada en firmas.

En cuatro pasos se obtiene una alerta al identificarse una actividad coincidente con la base de datos de firmas como se presenta en Figura 7. Detección basada en firmas.

Figura 7. Detección basada en firmas.



Fuente: MUDZINGWA, D., and R. AGRAWAL. A Study of Methodologies Used in Intrusion Detection and Prevention Systems (IDPS). 2012. Conference Proceedings - IEEE SOUTHEASTCON[114].

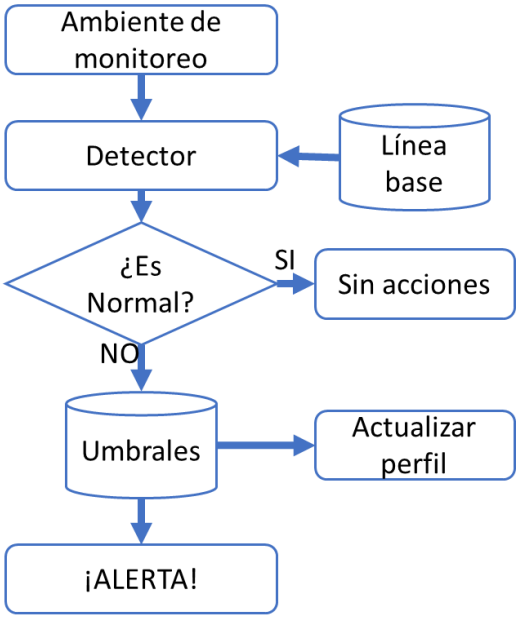
[113] ADAM KHALID *ET AL.*, *Advanced Persistent Threat Detection: A Survey*, 3rd International Cyber Resilience Conference
[114] MUDZINGWA AND AGRAWAL, *A study of methodologies used in intrusion detection and prevention systems (IDPS)*, Conference Proceedings - IEEE SOUTHEASTCON

En la metodología de detección basada en firmas, se aplica la comparación de las firmas de los objetos monitoreados con la base de datos de firmas obtenidas de la inteligencia de amenazas o las fuentes privadas de cada fabricante de dispositivos que ofrecen estas funcionalidades; una vez el sistema detecta una coincidencia alerta o toma las medidas predefinidas para que el equipo de respuesta implemente las acciones correspondientes.

6.1.5.2 Detección basada en anomalías. La organización ha definido una línea de base de comportamiento de los usuarios, la red, las aplicaciones o todo lo que este sujeto de monitoreo por parte de la misma y el sistema detectará si hay desviaciones de este comportamiento para alertar al equipo de respuesta; es común también definir umbrales de alerta para las desviaciones, por ejemplo si un usuario realiza múltiples intentos errados de inicio de sesión con contraseña errada, puede ser normal que le tome unos segundos intentar nuevamente, es una alerta que realice 60 intentos por minuto.

El diagrama de flujo del proceso descrito es presentado en la Figura 8. Detección basada en anomalías.

Figura 8. Detección basada en anomalías.



Fuente: MUDZINGWA, D., and R. AGRAWAL. A Study of Methodologies Used in Intrusion Detection and Prevention Systems (IDPS). 2012. Conference Proceedings - IEEE SOUTHEASTCON[115].

[115] MUDZINGWA AND AGRAWAL, *A study of methodologies used in intrusion detection and prevention systems (IDPS)*, Conference Proceedings - IEEE SOUTHEASTCON

6.1.5.3 Modelos de Kill-Chain y detección de APT. Los modelos de detección de APT se han caracterizado por tratar de encajar en los modelos de Kill-Chain establecidos y los modelos de detección descritos arriba, sin embargo, algunos autores han identificado que los actores se prestan de realizar gran aporte de sus actividades fuera de la vista observable de los equipos de defensa de las organizaciones, involucrando la cadena de suministro y los estudios previos al ataque[116]. Por lo anterior, el enfoque de Kill-Chain por el ciclo de vida de Mandiant deja por fuera este aspecto y se centra en las actividades de defensa de un incidente inminente sin tener en cuenta las actividades preventivas.

6.1.6 Características y ciclo de vida de las APT.

En los apartados anteriores se presentaron los modelos de estudio de las fases de ataque de grupos APT bajo la premisa que: los objetivos de ataque de estos grupos, al ser de gran envergadura y abundante financiación, son instituciones gubernamentales o entidades de gran tamaño con infraestructura y equipo humano de alto desempeño que cuenta con sofisticadas herramientas de seguridad y un músculo financiero para mejorar continuamente estas soluciones. En resumen, ataques sofisticados para organizaciones sofisticadas.

Se puede observar que los modelos de ataque de los grupos APT son sofisticados, pueden involucrar la participación de múltiples actores, personas y computadoras zombis, y además están preparados para pasar sin ser detectados por herramientas de seguridad un largo periodo de tiempo.

Lo anterior significa que, si dentro de su objetivo principal, los actores identifican un elemento vulnerable en la cadena de suministro, dadas por empresas más pequeñas con poca inversión en seguridad y posiblemente de menor inversión y esfuerzo para ser comprometidas, serán un objetivo paralelo dentro del ataque principal e incluso pueden favorecer este.

Por ello es necesario que las grandes empresas evalúen la seguridad de sus proveedores, y que de igual manera todas las pequeñas y medianas empresas que deseen hacer parte de la cadena de suministro de grandes empresas se preocupen por el desarrollo e implementación de controles de seguridad adecuados.

---

[116] AIMAD BERADY *ET AL.*, *Modeling the Operational Phases of APT Campaigns*, 2019 International Conference on Computational Science and Computational Intelligence (CSCI)

6.2 DESARROLLO OBJETIVO 2: DETERMINAR LAS METODOLOGÍAS ACTUALES DE PREVENCIÓN DE ATAQUES APT

A continuación, se presentan al lector las metodologías de prevención de APT, entendidas como procesos ordenados para lograr un objetivo claro, la preparación, defensa y respuesta a ataques de grupos APT, así como un análisis de sus ventajas y desventajas.

6.2.1 Metodologías y Modelos De Seguridad En Prevención De APT

Los profesionales y especialistas en seguridad informática junto con la academia han abordado el tema con múltiples investigaciones y de allí han surgido algunas metodologías que ofrecen tasas de detección y prevención aceptables. A continuación, se detallan algunas de las más recientes y efectivas:

6.2.1.1 Machine Learning Methodology

Utilizando bases de datos de ataques identificados sobre el vector de ataque Spear Phishing; Jadala, Pasupuleti, Baba, Raju y Ravinder propusieron una metodología de identificación y defensa basado en Machine Learning[117]. Este, utiliza modelo de datos por atributos en el entrenamiento del algoritmo y puesta a prueba por complemento de navegador que lo soporte.

Otros autores han abordado este modelo en distintos puntos de contacto con el atacante, por ejemplo, directamente en el tráfico de red, Xuan y Dao propusieron el análisis de datos de la capa de red del modelo OSI[118] inspeccionando las características como IP de origen y destino en una propuesta híbrida[119].

Otro ejemplo es el modelo propuesto por Li, Li, Xuan y Guo[120], en el cual el aprendizaje se soporta en datos de peticiones de resolución DNS que identifica el 96.2 % de los dispositivos infectados.

---

[117] JADALA, VIJAYA CHANDRA;PASUPULETI, SAI KIRAN;SAI BABA, *Analyzing and Detecting Advanced Persistent Threat Using Machine Learning Methodology*, Lecture Notes on Data Engineering and Communications Technologies. 93: 497–506

[118] ORACLE, Modelo de referencia OSI (Guía de administración del sistema: servicios IP). [Sitio WEB]. 2010. [Disponible en 10 de July, 2022]. Recuperado de: https://docs.oracle.com/cd/E19957-01/820-2981/ipov-8/index.html

[119] XUAN AND DAO, *A novel approach for APT attack detection based on combined deep learning m...: EBSCOhost*, Neural Computing and Applications. 2021

[120] LI *ET AL.*, *Identifying compromised hosts under APT using DNS request sequences*, Journal of Parallel and Distributed Computing. 152: 67–78

La mayoría de los modelos propuestos hasta el momento se enfocan en la predicción de actividades sospechosas para distintos tipos de dispositivos, IoT[121][122], o aislando algún factor diferencial del tipo o grupo atacante como las API de llamadas al servidor [123].

Los anteriores están clasificados dentro de los sistemas de detección de intrusiones distribuidas (DIDS) o en las terminales (HIDS) [124]; como alternativa, Panahnejad y Meghdad presentan una propuesta basada en el modelo Cyber Kill-Chain[125], el cual define 7 fases en las cuales puede ser detenido un ataque cibernético: 1- Reconocimiento, 2- Weaponization o diseño de armamento, 3- Envío, 4- Explotación, 5- Instalación, 6- Comando y control y 7- Acciones en los objetivos. La propuesta usa el método de aprendizaje por clasificación Bayesiana y toma de decisiones por el proceso de jerarquía analítica (AHP Analityc Hierarchy process). Sus resultados fueron de 99% y la tasa de falsos positivos y negativos de 1,9 % y 3,6% menos que los modelos existentes, sin embargo, el costo computacional es elevado.

6.2.1.2 Block Chain IA

Mediante la combinación de Tecnologias de BLOCKCHAIN, Inteligencia Artificial IA, y conceptos de 0 confianza o redes Zero Trust, se han propuesto la combinación de réplica y cifrado que ofrece BlockChain con la prevención a ataques que puedan detectarse mediante IA[126].

6.2.1.3 Detección Por Anomalía

En Future Generation Computer Systems Volumen 108[127], el equipo de Ghita Berrada propone una alternativa para resolver el problema del costo computacional de los algoritmos de IA y Machine Learning. Utilizando métodos estadísticos sobre datos obtenidos de 4 sistemas operativos distintos para tratar de identificar dónde se encuentran los ataques, resultando un éxito de al menos 87% y hasta 99,6% para SO

---

[121] CHENG *ET AL.*, Predicting the APT for Cyber Situation Comprehension in 5G-Enabled IoT. [Sitio WEB]. April 2021. [Disponible en 10 de July, 2022]. Recuperado de: https://web-p-ebscohost-com.bibliotecavirtual.unad.edu.co/ehost/pdfviewer/pdfviewer?vid=0&sid=9acb599c-ba80-4309-a29c-453f40ec03f8%40redis

[122] SHUDONG LI *ET AL.*, Attribution Classification Method of APT Malware in IoT Using Machine Learn...: EBSCOhost. [Sitio WEB]. September 2021. [Disponible en 10 de July, 2022]. Recuperado de: https://web-p-ebscohost-com.bibliotecavirtual.unad.edu.co/ehost/pdfviewer/pdfviewer?vid=0&sid=8f9c765c-5836-4043-bb55-33a1f6655ea7%40redis

[123] CHAOXIAN WEI *ET AL.*, *Toward Identifying APT Malware through API System Calls.: EBSCOhost*, Security and Communication Networks. 2021

[124] GONZALEZ, *Sistemas de Detección de Intrusiones*, Diego González Gómez

[125] PANAHNEJAD AND MEGHDAD, *APT-Dt-KC: advanced persistent threat detection based on kill-chain model*, The Journal of Supercomputing. 78: 8644–8677

[126] RAHMAN *ET AL.*, *Blockchain based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat*, 1

[127] BERRADA *ET AL.*, *A baseline for unsupervised advanced persistent threat detection in system-level provenance*, Future Generation Computer Systems. 108: 401–413

Andorid y Windows respectivamente. Esto es un avance en la detección rápida de bajo costo, pero se debe suponer que el atacante es capaz de alterar sus acciones para intentar evadir la detección de comportamiento.

6.2.1.4 Honey Pot

Una herramienta de defensa es el uso de HONEY POT[128] o trampa de miel que permite recuperar datos del atacante mientras éste distrae su atención tratando de obtener información de un señuelo. La propuesta de Wen Tian[129] es el uso de dispositivos industriales de internet de las cosas (IIoT) para ser introducido a una red definida por software (SDN[130]), esta propuesta requiere una constante interacción entre atacante y defensa, por ello no se considera un sistema de detección automática, adicionalmente el autor evaluó su desempeño y concluye que es más eficiente a mayor número de servidores señuelo.

6.2.2 Comparativo de metodologías.

Dadas las 4 estrategias presentadas en el apartado anterior, podemos concluir que, son sofisticadas en su diseño e implementación y esto significa un esfuerzo económico en recursos computacionales y humanos como se muestra en la Tabla 4. Ventajas y desventajas de metodologías de detección APT para PYMES.

Tabla 4. Ventajas y desventajas de metodologías de detección APT para PYMES.

	VENTAJAS	DESVENTAS	APLICA PYME	REQUISITOS
Machine Learning	Entrenado a las amenazas existentes Reentrenado para nuevas amenazas Detecta 99% de las amenazas con 1,9% de falsos positivos.	Requiere gran cantidad de datos y atributos de amenazas conocidas, poco probable en las más recientes. Cada entrenamiento requiere tiempo y esfuerzo, dando ventana sin protección.	NO	Altas capacidades de procesamiento Altas capacidades de talento humano

[128] KASPERSKY, ¿Qué es un honeypot? Cómo colaboran los honeypots con la seguridad. [Sitio WEB]. 2022. [Disponible en 10 de July, 2022]. Recuperado de: https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot

[129] WEN TIAN *ET AL.*, *Honeypot Detection Strategy Against Advanced Persistent Threats in Industrial Internet of Things: A Prospect Theoretic Game*, IEEE INTERNET OF THINGS JOURNAL

[130] KARMAKAR *ET AL.*, SDN enabled secure IoT architecture. 2019. Pp. 581–585, in 2019 IFIP/IEEE Symposium on Integrated Network and Service Management, IM 2019. vol. 1109.

Block Chain	Bajo consumo de procesamiento en comparación con Machine learning. Orientado a organizaciones que no han implementado mecanismos de defensa por su costo de procesamiento.	Requiere entrenamiento con las mismas consideraciones de Machine Learning. Su eficacia es de 90%. Cada elemento de la red debe convertirse en un nodo Block Chain.	NO	Medianas capacidades de procesamiento Muy Altas capacidades de talento humano
Anomalía	Tasa de éxito de 99.6% Menor costo computacional. No requiere entrenamiento. Multiplataforma.	Declarado ineficiente contra un atacante que se adapte. Ajuste de falsos positivos demasiado complejo.	NO	Bajas capacidades de procesamiento Medianas capacidades de talento humano
Honey Pot	Efectivo contra Bots. No altera los dispositivos actuales de la red.	Requiere dispositivos dedicados Requiere personal dedicado Mas eficiente a mayor cantidad de dispositivos y personas del lado del defensor	SI	Bajas capacidades de procesamiento Muy Altas capacidades del talento humano

Fuente: Propia.

Teniendo en cuenta que no es costo-eficiente para las PYMES emplear expertos de ciberseguridad de planta en su organización ni dedicar recursos computacionales exclusivamente a esta tarea, difícilmente tendrán la preocupación de implementar sofisticados mecanismos de protección, está demostrada su des preocupación y desconocimiento en el tema[131].

6.2.3 Modelos y mejores prácticas.

Dentro de los modelos y las mejores prácticas de ciberseguridad existentes, se encuentran las propuestas por entidades sin ánimo de lucro, gobiernos y entidades privadas, por ello es difícil elegir una alternativa adecuada para cada organización. A continuación, se presentan 4 de los modelos de mejores prácticas más conocidos y aplicados a nivel mundial, sus ventajas y desventajas para poder establecer si pueden ser aplicables a PYMES en Colombia.

[131] MORA FRANCO, *El desconocimiento de las pymes colombianas frente a las amenazas persistentes avanzadas*, Instname:Universidad Piloto de Colombia

6.2.3.1 Modelo NIST: El Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. ha desarrollado un marco de ciberseguridad ampliamente utilizado que se enfoca en cinco funciones principales: identificar, proteger, detectar, responder y recuperar. Cada función se divide en categorías de seguridad y subcategorías de controles de seguridad que se utilizan para ayudar a las organizaciones a desarrollar y mejorar sus programas de ciberseguridad. Este modelo fue actualizado recientemente de su versión 1.1[132] a la versión 2.0[133].

6.2.3.1.1 Ventajas:

- El modelo NIST es ampliamente utilizado y reconocido como un marco de ciberseguridad sólido.
- Proporciona una estructura clara y concisa para el desarrollo y mejora de los programas de ciberseguridad.
- Se adapta a diferentes tipos y tamaños de organizaciones.

6.2.3.1.2 Desventajas:

- Puede resultar demasiado detallado y complicado para algunas organizaciones más pequeñas o menos complejas (PYMES).
- La implementación completa del modelo NIST puede ser costosa y requerir mucho tiempo.

6.2.3.2 Modelo CIS Controls: El Centro de Seguridad Cibernética (CIS)[134] ha desarrollado un conjunto de 20 controles de seguridad que se consideran esenciales para la protección de sistemas y datos. Los controles están diseñados para ayudar a las organizaciones a prevenir, detectar y responder a los ciberataques.

6.2.3.2.1 Ventajas:

- Los controles de CIS son fáciles de entender y aplicar.
- Se han adaptado a diferentes entornos y situaciones de seguridad cibernética.
- El modelo CIS Controls es reconocido por muchas organizaciones como una guía de ciberseguridad eficaz.

---

[132] INSTITUTE OF STANDARDS AND TECHNOLOGY, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*
[133] *Updating the NIST Cybersecurity Framework – Journey To CSF 2.0 | NIST*
[134] CENETER OF INTERNET SECURITY, CIS Critical Security Controls. [Sitio WEB]. 2023. [Disponible en 13 de March, 2023]. Recuperado de: https://www.cisecurity.org/controls_pre

6.2.3.2.2 Desventajas:

- El enfoque en los controles de seguridad puede resultar demasiado limitado para algunas organizaciones.
- Puede ser difícil de aplicar a organizaciones que tienen requisitos de seguridad cibernética más específicos o complejos.

6.2.3.3 Modelo de seguridad de ciclo de vida: Este modelo se enfoca en la seguridad cibernética a lo largo del ciclo de vida del desarrollo de sistemas, desde la planificación hasta el desmantelamiento[135]. Se basa en el principio de que la seguridad cibernética debe ser una consideración integral en cada etapa del ciclo de vida del sistema.

6.2.3.3.1 Ventajas:

- El modelo de seguridad de ciclo de vida ayuda a garantizar que la seguridad cibernética se integre de manera efectiva en el desarrollo de sistemas y procesos de negocio.
- Permite a las organizaciones identificar y abordar problemas de seguridad cibernética en cada etapa del ciclo de vida.

6.2.3.3.2 Desventajas:

- Puede ser difícil de implementar en organizaciones que no tienen una cultura de seguridad cibernética sólida.
- Requiere una planificación y coordinación cuidadosas para garantizar que la seguridad cibernética se aborde en todas las etapas del ciclo de vida del sistema.

[135] MICROSOFT, Microsoft Security Development Lifecycle. [Sitio WEB]. 2023. [Disponible en 13 de May, 2023]. Recuperado de: https://www.microsoft.com/en-us/securityengineering/sdl?SilentAuth=1

6.2.3.4 Modelo de madurez de ciberseguridad: Este modelo evalúa el nivel de madurez de la seguridad cibernética de una organización y proporciona un marco para la mejora continua[136]. El modelo se basa en niveles de madurez que se centran en áreas clave de seguridad cibernética, como la gestión de riesgos, la planificación y la implementación de controles de seguridad.

6.2.3.4.1 Ventajas:

- El modelo de madurez de ciberseguridad permite a las organizaciones evaluar su postura de seguridad cibernética y desarrollar un plan de mejora específico.
- Es un enfoque holístico que aborda la seguridad cibernética en múltiples áreas.
- Puede adaptarse a diferentes tamaños y tipos de organizaciones.

6.2.3.4.2 Desventajas:

- Puede ser costoso y requiere mucho tiempo para realizar una evaluación completa.
- Requiere una comprensión profunda de la seguridad cibernética y los controles para llevar a cabo la evaluación con precisión.

6.2.4 Herramientas para la detección de APTS.

Las herramientas de detección de APT (amenazas persistentes avanzadas) son soluciones de seguridad diseñadas específicamente para identificar y responder a amenazas sofisticadas y persistentes que pueden pasar desapercibidas por soluciones de seguridad convencionales.

Estas herramientas utilizan técnicas avanzadas de detección y análisis, como la inteligencia artificial, el análisis de comportamiento y el análisis de anomalías, para identificar y detener amenazas avanzadas. También pueden incluir capacidades de respuesta y remediación, como la eliminación de malware y la restauración de sistemas comprometidos.

Algunas herramientas populares de detección de APT a continuación:

[136] U.S. DEPARTMENT OF DEFENSE, Chief Information Officer: CMMC. [Sitio WEB]. 2021. [Disponible en 13 de March, 2023]. Recuperado de: https://dodcio.defense.gov/CMMC/

6.2.4.1 El Security Information and Event Management (SIEM)[137] es una solución de seguridad de tecnología de la información que proporciona una visión unificada de la seguridad de la red. Una solución SIEM recopila y analiza datos de múltiples fuentes en tiempo real para detectar, identificar y responder a amenazas de seguridad.

El SIEM funciona mediante la recopilación de registros de eventos y alertas de seguridad de dispositivos de red, aplicaciones y sistemas de seguridad, y la correlación de esta información para identificar patrones de actividad sospechosa y posibles amenazas. Las soluciones SIEM también pueden incluir la capacidad de monitorear y analizar el tráfico de red, identificar vulnerabilidades en la seguridad de la red y crear informes y alertas personalizados.

Algunos ejemplos de soluciones SIEM comerciales son:

- IBM QRadar[138]
- Splunk Enterprise Security[139]
- LogRhythm NextGen SIEM[140]
- SkyHigh Security[141]
- AlienVault AT&T Cybersecurity[142]

Las soluciones SIEM pueden ser muy efectivas para detectar y responder a amenazas de seguridad avanzadas y persistentes, pero pueden requerir una configuración y administración cuidadosas para obtener el máximo beneficio. Además, las soluciones SIEM pueden ser costosas y requieren una inversión significativa en tiempo y recursos para implementar y mantener.

---

[137] BRYANT AND SAIEDIAN, *A novel kill-chain framework for remote security log analysis with SIEM software*, Computers & Security. 67: 198–210

[138] IBM, Security QRadar | IBM. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.ibm.com/qradar

[139] SPLUNK, Splunk Enterprise Security | Splunk. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.splunk.com/en_us/products/enterprise-security.html?301=/en_us/software/enterprise-security.html

[140] LOGRHYTHM, Page not found | LogRhythm. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://logrhythm.com/products/nextgen-siem/

[141] SKYHIGH SECURITY, Enterprise Cloud Data Protection - Skyhigh Security. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.skyhighsecurity.com/en-us/

[142] AT&T, AlienVault is now AT&T Cybersecurity. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://cybersecurity.att.com/

6.2.4.2 EDR significa Endpoint Detection and Response (Detección y Respuesta en el Punto Final)[143] y es una solución de seguridad diseñada específicamente para la detección y respuesta a amenazas en los puntos finales (por ejemplo, computadoras, servidores, dispositivos móviles).

Una solución EDR puede monitorear continuamente los puntos finales en busca de comportamientos sospechosos y actividad maliciosa, y responder automáticamente a las amenazas detectadas. Además, la solución EDR puede proporcionar una mayor visibilidad en la actividad de los puntos finales y recopilar y analizar datos para mejorar la postura de seguridad general de la organización.

Algunas soluciones EDR comerciales incluyen:

- CrowdStrike Falcon Endpoint Protection[144]
- VMware Security[145]
- Symantec Endpoint Detection and Response (Broadcom)[146]
- McAfee MVISION EDR, Trellix[147]
- SentinelOne Endpoint Protection Platform[148]

Las soluciones EDR son una capa crítica de seguridad para cualquier organización, ya que pueden detectar y responder rápidamente a amenazas en los puntos finales, donde los datos y sistemas críticos están en riesgo. Sin embargo, como con cualquier solución de seguridad, es importante evaluar cuidadosamente las características y capacidades de la solución EDR antes de implementarla para asegurarse de que se ajuste a las necesidades específicas de la organización.

[143] TECNOZERO, ¿Qué es un EDR? ¿Por qué es diferente de un antivirus? | tecnozero. [Sitio WEB]. 2022. Antivirus y ramsomware. [Disponible en 23 de March, 2022]. Recuperado de: https://www.tecnozero.com/antivirus-y-anti-ransomware/que-es-un-edr/

[144] CROWDSTRIKE, The CrowdStrike Falcon® Platform: One Platform, Complete Protection. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.crowdstrike.com/falcon-platform/

[145] VMWARE, VMware Security Solutions. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.vmware.com/security.html

[146] BROADCOM, Endpoint Security Complete. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.broadcom.com/products/cybersecurity/endpoint/end-user/complete

[147] TRELLIX, XDR Ecosystem | Trellix. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.trellix.com/en-us/products.html

[148] SENTINELONE, XDR Ingestion - SentinelOne. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.sentinelone.com/platform/xdr-ingestion/

6.2.4.3 Un Sistema de Prevención de Intrusos (IPS) es una solución de seguridad que se encarga de la detección y prevención de intrusiones en la red[149]. El IPS monitorea el tráfico de red en busca de comportamientos maliciosos y puede tomar medidas activas para bloquear y prevenir dichos comportamientos.

Existen dos tipos de IPS: el IPS basado en host y el IPS basado en red. El IPS basado en host se instala en un dispositivo de red específico y monitorea el tráfico de red entrante y saliente. El IPS basado en red, por otro lado, monitorea todo el tráfico de red que pasa a través de un punto específico de la red.

Algunas soluciones IPS comerciales incluyen:

- Cisco Firepower Next-Generation Intrusion Prevention System[150]
- Palo Alto Networks Intrusion Prevention System[151]
- Check Point Intrusion Prevention System[152]
- Fortinet Intrusion Prevention System[153]

El IPS es una herramienta crítica para la protección de la red y puede ayudar a prevenir intrusiones y ataques maliciosos. Sin embargo, es importante tener en cuenta que un IPS puede generar falsos positivos y que la configuración inadecuada puede llevar a bloqueos innecesarios del tráfico legítimo. Como con cualquier solución de seguridad, es importante evaluar cuidadosamente las características y capacidades de un IPS antes de implementarlo.

6.2.4.4 Análisis de comportamiento de la red (NBA, por sus siglas en inglés) es una técnica de seguridad que se utiliza para monitorear y analizar el tráfico de red en busca de patrones y comportamientos anómalos que puedan indicar actividades maliciosas o intrusiones en la red.

El NBA se basa en la idea de que las actividades de red normales siguen ciertos patrones y comportamientos predecibles. Cuando se detectan desviaciones significativas de estos patrones, se pueden identificar posibles amenazas o actividades sospechosas. Algunas

---

[149] VERSA NETWORKS, IDS frente a IPS: diferencias entre IDS e IPS | Versa Networks. [Sitio WEB]. 2023. [Disponible en 13 de March, 2023]. Recuperado de: https://versa-networks.com/es/sd-wan/ids-ips/

[150] CISCO, Cisco Secure IPS - Cisco. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.cisco.com/c/en/us/products/security/ngips/index.html?dtid=osscdc000283

[151] PALOALTO, Advanced Threat Prevention - Palo Alto Networks. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.paloaltonetworks.com/network-security/advanced-threat-prevention

[152] CHECKPOINT, Quantum Intrusion Prevention System (IPS) - Check Point Software. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.checkpoint.com/quantum/intrusion-prevention-system-ips/

[153] FORTINET, FortiGuard Intrusion Prevention Service | Fortinet. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/intrusion-prevention

de las actividades que pueden detectarse mediante el análisis de comportamiento de la red incluyen el tráfico de datos inusuales, la comunicación con dominios sospechosos, cambios en los patrones de comunicación y la identificación de ataques conocidos.

El análisis de comportamiento de la red generalmente se lleva a cabo utilizando herramientas y soluciones especializadas, como sistemas de detección de intrusiones basados en comportamiento (BIDS, por sus siglas en inglés) y plataformas de seguridad de red que integran funcionalidades de NBA.

Algunas soluciones populares de análisis de comportamiento de la red incluyen:

- Cisco Stealthwatch[154]
- Darktrace Enterprise Immune System[155]
- ExtraHop Reveal(x)[156]
- Vectra Cognito[157]

El análisis de comportamiento de la red puede ayudar a detectar amenazas desconocidas y ataques avanzados que no pueden ser identificados por herramientas de seguridad tradicionales. Sin embargo, es importante tener en cuenta que el NBA también puede generar falsos positivos y que su implementación efectiva requiere una comprensión profunda de los patrones normales de comportamiento de la red y un monitoreo continuo.

6.2.4.5 Análisis de vulnerabilidades El análisis de vulnerabilidades es una actividad fundamental en la gestión de la seguridad de la información. Consiste en identificar y evaluar las debilidades y fallos de seguridad en los sistemas, aplicaciones y redes de una organización con el fin de determinar su nivel de riesgo y tomar medidas para mitigarlos.

El análisis de vulnerabilidades generalmente se realiza utilizando herramientas automatizadas conocidas como escáneres de vulnerabilidades. Estas herramientas examinan los sistemas en busca de vulnerabilidades conocidas, como configuraciones incorrectas, versiones de software obsoletas, falta de parches de seguridad y errores de programación. Algunas de las áreas clave que se pueden evaluar durante el análisis de vulnerabilidades son:

---

[154] CISCO, Cisco Secure Network Analytics - Cisco. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.cisco.com/site/us/en/products/security/security-analytics/secure-network-analytics/index.html

[155] DARKTRACE, Productos | Darktrace. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://es.darktrace.com/products

[156] EXTRAHOP, EXTRAHOP REVEAL(X) 360. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.extrahop.com/products/cloud/

[157] VECTRA, Prevent Cyberattacks with Vectra AI. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.vectra.ai/

- Sistemas operativos: Se analizan los sistemas operativos en busca de configuraciones inseguras, puertos abiertos y servicios innecesarios que puedan ser explotados por atacantes.
- Aplicaciones web: Se identifican vulnerabilidades comunes en las aplicaciones web, como inyecciones SQL, cross-site scripting (XSS) y fallos de autenticación.
- Redes: Se escanean los dispositivos de red en busca de vulnerabilidades, como configuraciones inseguras de firewalls, enrutadores y switches.
- Configuraciones de seguridad: Se evalúan las configuraciones de seguridad de los sistemas y aplicaciones para identificar posibles brechas.

Algunas herramientas populares de análisis de vulnerabilidades son:

- Nessus[158]
- OpenVAS[159]
- Qualys Vulnerability Management Response[160]
- Rapid7 Nexpose[161]

Es importante destacar que el análisis de vulnerabilidades debe ser un proceso continuo, ya que nuevas vulnerabilidades y amenazas surgen constantemente. Además, es crucial que las organizaciones tomen medidas rápidas para remediar las vulnerabilidades detectadas y establecer un programa de gestión de vulnerabilidades sólido.

[158] TENABLE, NESSUS by TENABLE. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.tenable.com/products/nessus

[159] OPENVAS, Background — Greenbone Documentation documentation. [Sitio WEB]. 2021. Hist. OPENVAS. [Disponible en 7 de November, 2021]. Recuperado de: https://greenbone.github.io/docs/background.html#history-of-the-openvas-project

[160] QUALYS, Qualys VMDR - Vulnerability Management Tool | Qualys. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.qualys.com/apps/vulnerability-management-detection-response/

[161] RAPID7, Nexpose On-Premise Vulnerability Scanner - Rapid7. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.rapid7.com/products/nexpose/

6.2.4.6 Los sistemas de prevención de pérdida de datos (DLP, por sus siglas en inglés)[162] son soluciones de seguridad diseñadas para proteger la información sensible y confidencial de una organización, evitando su filtración, pérdida o uso no autorizado. Estos sistemas se centran en monitorear, controlar y proteger los datos en reposo, en tránsito y en uso en diferentes puntos, como terminales o estaciones de trabajo, redes y servidores.

Los sistemas de DLP utilizan una combinación de tecnologías y políticas para identificar y controlar la transferencia o acceso no autorizado de datos confidenciales. Algunas de las características y capacidades comunes de los sistemas de DLP incluyen:

- Identificación y clasificación de datos: Los sistemas de DLP pueden identificar y clasificar automáticamente los datos confidenciales, como información personal, datos financieros o secretos comerciales.
- Monitoreo de tráfico de red: Los sistemas de DLP supervisan el tráfico de red en busca de patrones y comportamientos sospechosos que puedan indicar una posible fuga de datos.
- Control de políticas: Los sistemas de DLP aplican políticas predefinidas o personalizadas para controlar cómo se manejan y comparten los datos confidenciales, como bloquear la transferencia de archivos o aplicar cifrado.
- Prevención de filtraciones: Los sistemas de DLP pueden detectar y prevenir la transferencia no autorizada de datos confidenciales a través de medios como correo electrónico, mensajería instantánea, servicios en la nube, dispositivos extraíbles, entre otros.
- Auditoría y generación de informes: Los sistemas de DLP registran y auditan todas las actividades relacionadas con los datos confidenciales, y generan informes detallados para fines de cumplimiento y monitoreo.

Algunas soluciones populares de DLP:

- Symantec Data Loss Prevention (Broadcom)[163]
- McAfee Total Protection for DLP (TRELLIX)[164]
- Forcepoint DLP[165]

---

[162] REYES ROIG, Guia de implementacion de la seguridad en redes de Nucleo Mpls., D - Instituto Superior Politecnico Jose Antonio Echeverria. CUJAE, 2010, 145 p., 145, pp.

[163] BROADCOM, Symantec DLP | Sensitive data protection and compliance. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.broadcom.com/products/cybersecurity/information-protection/data-loss-prevention

[164] TRELLIX, XDR Ecosystem | Trellix. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.trellix.com/en-us/products.html

[165] FORCEPOINT, Forcepoint ONE DLP – DLP Software-as-a-Service | Forcepoint. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.forcepoint.com/product/forcepoint-one-dlp

- Digital Guardian Data Loss Prevention[166]

Es importante destacar que la implementación exitosa de un sistema de DLP requiere una comprensión clara de los datos confidenciales de la organización, así como una configuración adecuada y una colaboración estrecha con las políticas de seguridad internas. Además, el DLP debe formar parte de un enfoque integral de seguridad de la información que incluya medidas de protección en diferentes capas de la infraestructura de TI.

6.2.4.7 Herramientas de análisis de tráfico de red: son utilizadas para monitorear, capturar y analizar el tráfico de red con el fin de obtener información sobre el rendimiento de la red, identificar problemas, detectar actividades maliciosas y realizar investigaciones forenses. Estas herramientas proporcionan una visibilidad profunda del tráfico de red y permiten analizar datos en tiempo real o retrospectivamente.

Algunas herramientas populares de análisis de tráfico de red:

- Wireshark: Es una herramienta de análisis de protocolos de red de código abierto. Permite capturar y examinar el tráfico de red en detalle, decodificar protocolos y filtrar información específica. Wireshark es ampliamente utilizado debido a su amplia gama de funcionalidades y su comunidad activa de usuarios.[167]
- SolarWinds Network Performance Monitor: Es una solución completa de monitoreo de redes que también incluye capacidades de análisis de tráfico. Proporciona visualizaciones y análisis detallados del tráfico de red, así como alertas de rendimiento y capacidad.[168]
- PRTG Network Monitor: Es una herramienta de monitoreo de red que también ofrece funcionalidades de análisis de tráfico. Permite capturar y analizar el tráfico de red en tiempo real, y proporciona informes y gráficas detalladas para ayudar en la identificación de problemas y en la optimización del rendimiento de la red.[169]
- tcpdump: Es una herramienta de línea de comandos utilizada para capturar y analizar el tráfico de red en sistemas basados en UNIX y Linux. Permite filtrar y

[166] FORTRA, Data Loss Prevention Solutions from Fortra. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.digitalguardian.com/solutions/data-loss-prevention
[167] WIRESHARK, Wireshark · Go Deep. [Sitio WEB]. 2022. [Disponible en 29 de October, 2022]. Recuperado de: https://www.wireshark.org/
[168] SOLARWINDS, Network Performance Monitor - Onsite & Remote Monitoring | SolarWinds. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.solarwinds.com/network-performance-monitor
[169] PAESSLER, Discover the 3 Paessler PRTG monitoring solutions. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.paessler.com/prtg

examinar paquetes de red en tiempo real o desde archivos de captura previos. Es una herramienta poderosa y flexible para analizar el tráfico de red.[170]

Estas son solo algunas de las herramientas disponibles para el análisis de tráfico de red. Cada una tiene sus propias características y funcionalidades, por lo que es importante evaluar las necesidades específicas de cada entorno antes de elegir una herramienta en particular.

6.2.4.8 El análisis de programas maliciosos[171], también conocido como análisis de malware, es el proceso de examinar y comprender el comportamiento, la estructura y las funcionalidades de software malicioso con el fin de identificar sus características, detectar amenazas y desarrollar contramedidas.

Existen diferentes enfoques y técnicas utilizadas en el análisis de malware, entre las cuales se incluyen:

- Análisis estático: Consiste en examinar el código y la estructura del programa malicioso sin ejecutarlo. Se analizan los archivos binarios, scripts o documentos maliciosos en busca de patrones, firmas o características específicas que puedan indicar su naturaleza maliciosa. Esto se puede realizar utilizando herramientas de análisis estático, como desensambladores, depuradores o emuladores.
- Análisis dinámico: Implica ejecutar el malware en un entorno controlado, como un sandbox, una máquina virtual o un entorno aislado, para observar su comportamiento en tiempo real. Se monitorean las acciones del malware, como la creación de archivos, la comunicación de red o la modificación del sistema, para entender sus efectos y funcionalidades. Herramientas de análisis dinámico, como Cuckoo Sandbox o FireEye, se utilizan para este propósito.
- Análisis de red: Se enfoca en examinar el tráfico de red generado por el malware. Se capturan y analizan los paquetes de red para identificar las comunicaciones maliciosas, los servidores de comando y control (C&C) y otros indicadores de compromiso (IOC). Herramientas como Wireshark, Bro o Suricata se utilizan para analizar el tráfico de red.
- Análisis de código: En este enfoque, se examina el código fuente del malware para comprender su lógica y funcionalidades. Esto puede ayudar a identificar técnicas de evasión, vulnerabilidades explotadas o métodos de propagación utilizados por el malware.

[170] TCPDUMP, Home | TCPDUMP & LIBPCAP. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.tcpdump.org/

[171] KUMAR AND SUBBIAH, *Zero-Day Malware Detection and Effective Malware Analysis Using Shapley Ensemble Boosting and Bagging Approach.*, Sensors (14248220). 22: 2798

Algunas herramientas comunes utilizadas en el análisis de malware incluyen:

- IDA Pro: Un potente desensamblador y depurador utilizado para el análisis estático y dinámico de malware[172].
- OllyDbg: Un depurador de código de nivel de ensamblador para análisis de malware.[173]
- YARA: Una herramienta de reconocimiento y reglas de análisis utilizada para identificar patrones específicos en archivos o procesos.[174]
- VirusTotal: Un servicio en línea que permite subir archivos sospechosos y analizarlos utilizando múltiples motores antivirus.[175]

Es importante tener en cuenta que el análisis de malware es un campo complejo y en constante evolución. Se requiere un buen entendimiento de las técnicas de malware, conocimiento en programación y habilidades de reversión de ingeniería para realizar un análisis efectivo.

6.2.4.9 Las herramientas de inteligencia de amenazas[176] (TI, por sus siglas en inglés) son soluciones que recopilan, analizan y generan información sobre amenazas de seguridad en tiempo real, con el objetivo de proporcionar a las organizaciones conocimientos y alertas tempranas sobre posibles ataques cibernéticos. Estas herramientas ayudan a las organizaciones a tomar decisiones informadas y a fortalecer sus defensas contra amenazas conocidas y emergentes.

Algunas herramientas populares de inteligencia de amenazas:

- Recorded Future: Es una plataforma de TI que recopila y analiza datos de amenazas de fuentes abiertas y cerradas en tiempo real. Proporciona inteligencia accionable para identificar, comprender y mitigar amenazas cibernéticas.[177]
- ThreatConnect: Es una plataforma de inteligencia de amenazas que permite recopilar, analizar y compartir información sobre amenazas. Facilita la

[172] HEX-RAYS, Hex Rays - State-of-the-art binary code analysis solutions. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://hex-rays.com/ida-pro/
[173] OLLYDBG, OllyDbg v1.10. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.ollydbg.de/viewer.htm
[174] READTHEDOCS, Welcome to YARA's documentation! — yara 4.2.0 documentation. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://yara.readthedocs.io/en/v4.2.2/index.html
[175] VIRUSTOTAL, VirusTotal - Home. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.virustotal.com/gui/home/upload
[176] MOHSIN AND ANWAR, Where to Kill the Cyber Kill-Chain: An Ontology-Driven Framework for IoT Security Analytics. (1)National University of Sciences and Technology, 2017. Pp. 23–28, in Proceedings - 14th International Conference on Frontiers of Information Technology, FIT 2016
[177] RECORDEDFUTURE, Recorded Future: Securing Our World With Intelligence. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.recordedfuture.com/

colaboración entre equipos de seguridad y ayuda a priorizar y responder a las amenazas de manera efectiva.[178]

- Anomali ThreatStream: Es una plataforma de gestión de inteligencia de amenazas que centraliza y normaliza datos de múltiples fuentes de amenazas. Permite analizar, correlacionar y tomar acciones basadas en inteligencia en tiempo real.[179]
- TRELLIX Intelligence: Es una solución de inteligencia de amenazas que combina datos de inteligencia con análisis de seguridad para ofrecer información detallada sobre amenazas y ataques en curso.[180]

Estas herramientas proporcionan inteligencia contextualizada sobre amenazas cibernéticas, como indicadores de compromiso (IOC), tácticas, técnicas y procedimientos (TTP), y otros datos relevantes para ayudar a las organizaciones a comprender y mitigar los riesgos de seguridad. Cada herramienta tiene sus propias características y enfoques, por lo que es importante evaluar las necesidades específicas de cada organización antes de seleccionar una herramienta de inteligencia de amenazas.

6.2.4.10 Herramientas de simulación de ataques, también conocidas como herramientas de pruebas de penetración o herramientas de evaluación de vulnerabilidades, se utilizan para simular y evaluar posibles escenarios de ataque en los sistemas y redes de una organización. Estas herramientas ayudan a identificar y corregir vulnerabilidades antes de que sean explotadas por atacantes reales. A continuación, se presentan algunas herramientas populares de simulación de ataques:

- Metasploit: Es una plataforma de pruebas de penetración ampliamente utilizada que proporciona una amplia gama de exploits, payloads y herramientas para realizar pruebas de seguridad en sistemas y redes.[181]
- Burp Suite: Es una suite de herramientas de pruebas de seguridad diseñada para realizar pruebas de aplicaciones web. Permite descubrir vulnerabilidades, como inyecciones SQL, cross-site scripting (XSS) y secuencias de comandos entre sitios (XSS).[182]
- Nessus: Es una herramienta de evaluación de vulnerabilidades que escanea sistemas y redes en busca de posibles debilidades y agujeros de seguridad.

[178] THREATCONECT, Cyber Threat Intelligence Company | ThreatConnect. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://threatconnect.com/
[179] ANOMALI, Anomali ThreatStream Threat Intelligence Management. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.anomali.com/products/threatstream
[180] TRELLIX, XDR Ecosystem | Trellix. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.trellix.com/en-us/products.html
[181] ORCERO, Kali Linux, RA-MA Editorial, Madrid, 2018
[182] PORTSWIGGER, Burp Suite - Application Security Testing Software - PortSwigger. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://portswigger.net/burp

Proporciona informes detallados y recomendaciones para solucionar las vulnerabilidades encontradas.[183]

- Cobalt Strike: Es una herramienta de simulación de ataques que permite realizar pruebas de intrusión, escenarios de ataque y simulaciones de adversarios. Ofrece una amplia gama de funcionalidades, incluyendo la generación de malware, el control de sistemas comprometidos y la simulación de ataques de red.[184]

Estas son solo algunas de las herramientas disponibles para la simulación de ataques. Es importante tener en cuenta que el uso de estas herramientas debe llevarse a cabo de manera ética y legal, obteniendo el permiso adecuado para probar los sistemas y redes de una organización. Además, se recomienda contar con profesionales de seguridad con experiencia en el uso de estas herramientas para garantizar pruebas efectivas y precisas.

6.2.4.11 10 herramientas, ¿son útiles para PYMES en Colombia?

Las herramientas mencionadas anteriormente, como SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), IPS (Intrusion Prevention System), NBA (Network Behavior Analysis), análisis de vulnerabilidades y DLP (Data Loss Prevention), juegan un papel importante en la reducción de la superficie de riesgo para las PYMES. Sin embargo, es importante tener en cuenta los siguientes puntos al considerar su viabilidad para aplicar a pymes en Colombia:

- Recursos y presupuesto: Estas herramientas a menudo requieren una inversión financiera significativa, tanto para la adquisición como para el mantenimiento y la gestión continua. Las PYMES deben evaluar si tienen los recursos y el presupuesto necesarios para implementar y utilizar estas herramientas de manera efectiva.
- Personal y habilidades técnicas: Estas herramientas a menudo requieren personal capacitado y con conocimientos técnicos para su configuración, gestión y análisis de resultados. Las PYMES deben considerar si tienen el personal adecuado con las habilidades necesarias o si necesitan contratar a profesionales externos.
- Escala y complejidad de la infraestructura: Estas herramientas son más adecuadas para PYMES con infraestructuras de TI más grandes y complejas. Si una pyme tiene una infraestructura más pequeña y menos compleja, es posible que algunas de estas herramientas sean demasiado robustas o no sean necesarias en ese nivel de escala.
- Cumplimiento normativo: Algunas PYMES pueden estar sujetas a regulaciones específicas en cuanto a la seguridad de la información, y estas herramientas

[183] TENABLE, NESSUS by TENABLE. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.tenable.com/products/nessus

[184] FORTRA, Data Loss Prevention Solutions from Fortra. [Sitio WEB]. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.digitalguardian.com/solutions/data-loss-prevention

pueden ayudar a cumplir con los requisitos normativos. Es importante evaluar si las herramientas seleccionadas cumplen con los estándares y regulaciones aplicables en Colombia.

En resumen, si una PYME cuenta con los recursos financieros, personal capacitado y una infraestructura de TI adecuada, estas herramientas pueden ser viables y ayudar a reducir la superficie de riesgo. Sin embargo, es fundamental evaluar cuidadosamente las necesidades y capacidades específicas de la PYME antes de implementar estas soluciones. Es también necesario recordar que gran cantidad de PYMES no conocen sobre APT y posiblemente esta no sea una motivación para su implementación.[185]

[185] MORA FRANCO, *El desconocimiento de las pymes colombianas frente a las amenazas persistentes avanzadas*, Instname:Universidad Piloto de Colombia

6.3 DESARROLLO OBJETIVO 3: TÁCTICAS TÉCNICAS Y PROCEDIMIENTOS TTP COMUNES EN ATAQUES APT

Las tácticas, técnicas y procedimientos (TTP) utilizadas por grupos de amenazas persistentes avanzadas (APT) representan una serie de acciones utilizadas para llevar a cabo ataques cibernéticos de manera sigilosa y persistente. Estas TTP son estudiadas y documentadas por organizaciones de seguridad, como MITRE Corporation[186], que ha creado el marco de conocimiento ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) para categorizar y analizar estas tácticas.

El marco ATT&CK proporciona una visión detallada de las TTP utilizadas por APT en diferentes etapas del ciclo de vida del ataque. Cubre una amplia gama de tácticas, desde el reconocimiento inicial y la entrega del malware hasta el control y la persistencia en los sistemas comprometidos. Cada táctica se divide en técnicas específicas, que describen cómo se implementan las tácticas. Por ejemplo, las técnicas pueden incluir la explotación de vulnerabilidades conocidas o el uso de ingeniería social para obtener acceso no autorizado.

Otra referencia importante en el campo de la seguridad cibernética es el Top 20 Critical Security Controls del Consorcio de Sistemas de Automatización de Seguridad Nacional (SANS)[187]. Estos controles críticos están diseñados para ayudar a las organizaciones a prevenir, detectar y responder a los ataques cibernéticos más comunes y efectivos. Los controles abarcan áreas clave como la administración de inventarios de hardware y software, la seguridad de la configuración, la autenticación y el acceso seguro, y la supervisión y respuesta a incidentes.

El MITRE Shield[188] es otro marco de seguridad que se centra en las defensas contra los ataques cibernéticos. A diferencia de ATT&CK, que se enfoca en las tácticas utilizadas por los atacantes, Shield se centra en las acciones defensivas que las organizaciones pueden tomar para protegerse. Shield proporciona una lista de técnicas defensivas que las organizaciones pueden implementar para frustrar las tácticas y técnicas utilizadas por los atacantes.

Por último, la cadena de ataque cibernético, o Cyber Kill Chain, es un modelo que describe las diferentes etapas que suelen seguir los atacantes para llevar a cabo un ataque exitoso. Estas etapas incluyen el reconocimiento, la entrega, la explotación, el

---

[186] MITRE ATT&CK, Techniques - Enterprise | MITRE ATT&CK®. [Sitio WEB]. 2023. Tech. . [Disponible en 25 de February, 2023]. Recuperado de: https://attack.mitre.org/techniques/enterprise/

[187] SANS, 20 Critical Security Controls | SANS Institute. [Sitio WEB]. March 30, 2023. [Disponible en 30 de March, 2023]. Recuperado de: https://www.sans.org/webcasts/20-critical-security-controls-96685/

[188] FOWLER *ET AL.*, *An Introduction to MITRE Shield*

control, la persistencia y el objetivo final. El modelo de Cyber Kill Chain[189] ayuda a las organizaciones a comprender cómo los atacantes avanzan en cada etapa y proporciona un marco para la detección y la respuesta temprana a los ataques.

Soportados en la metodología de análisis de ataques de cadena de la muerte presentada en 6.1.2, se puede obtener información de las tácticas, técnicas y procedimientos utilizados por los atacantes al desplegar campañas APT[190].

Mohsin y Anwar hacen un estudio de las TTPs que se han identificado en múltiples trabajos[191] para definir su ontología de detección y protección contra APT de acuerdo con la fase de la Cadena de la Muerte donde se frustre el ataque. En dicho trabajo se plantean las preguntas que son fundamentales para el presente análisis:

- ¿Qué control se adapta a mi entorno?,
- ¿Qué partes de mi red?,
- ¿aplicarlo en qué etapa de ataque producirá los beneficios deseados?
- ¿incurre en cuanto costo? e
- ¿induce qué tipo de gastos generales operativos?

Teniendo en cuenta que el atacante deberá emplear distintas tácticas, técnicas y procedimientos en cada fase de la campaña, explotando vulnerabilidades de la tecnología, que pueden ser detectadas y/o detenidas con distintos controles en cada uno.

6.3.1 Tácticas Técnicas y Procedimientos, Top 7. Del consolidado de las TTPs se tabulan por tipo y frecuencia, para analizar únicamente las más comunes.

Se seleccionan las TTP más comunes, teniendo en cuenta su tipo de técnica se puede ubicar en la fase de ataque de Lockheed Martin Kill-Chain (LM KC) para poder identificar los controles más adecuados que deberían implementarse para la reducción de riesgo de las organizaciones. Se realizó la selección de la lista de Tácticas más recurrentes en los últimos ataques asociados a APT que afectaron la región y se tabularon por cantidad de veces que aparecieron como se muestra en Figura 9. TTPs, Top 7 frecuencia de uso por APTs en Colombia y la región.

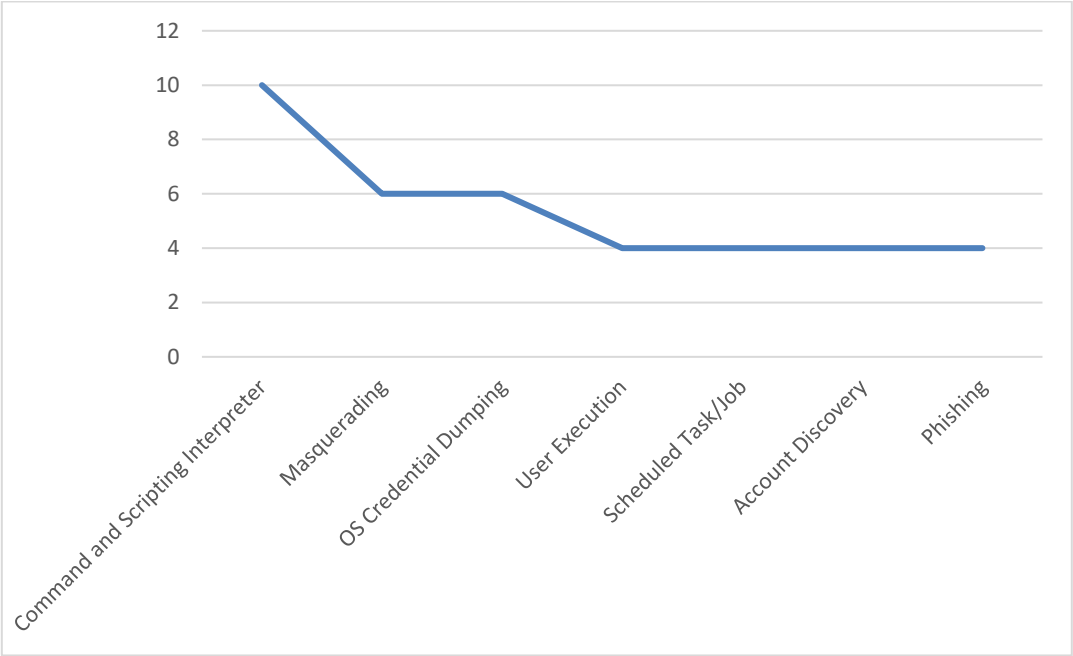
---

[189] MOHSIN AND ANWAR, Where to Kill the Cyber Kill-Chain: An Ontology-Driven Framework for IoT Security Analytics. (1)National University of Sciences and Technology, 2017. Pp. 23–28, in Proceedings - 14th International Conference on Frontiers of Information Technology, FIT 2016

[190] PANAHNEJAD AND MEGHDAD, *APT-Dt-KC: advanced persistent threat detection based on kill-chain model*, The Journal of Supercomputing. 78: 8644–8677

[191] MOHSIN AND ANWAR, Where to Kill the Cyber Kill-Chain: An Ontology-Driven Framework for IoT Security Analytics. (1)National University of Sciences and Technology, 2017. Pp. 23–28, in Proceedings - 14th International Conference on Frontiers of Information Technology, FIT 2016

Figura 9. TTPs, Top 7 frecuencia de uso por APTs en Colombia y la región.



Fuente: Propia.

Para prevenir los ataques enumerados, se pueden proponer algunas buenas prácticas, los cuales se listan a continuación según el orden de mayor a menor aparición en las técnicas identificadas que usan los grupos activos en la región:

6.3.1.1 Intérprete de secuencias de comandos y comandos (Command and Scripting Interpreter): deshabilitar o restringir el acceso a lenguajes de secuencias de comandos innecesarios y aplicar parches a los motores de secuencias de comandos.

6.3.1.2 Enmascaramiento (Masquerading): implementar controles de acceso sólidos, además revisar y controlar periódicamente los registros del sistema para detectar actividades inusuales.

6.3.1.3 Volcado de credenciales del sistema operativo (OS Credential Dumping): usar contraseñas seguras, autenticación de múltiples factores y exigir cambio de contraseñas regularmente. Guardar las contraseñas de forma segura, usando una función de resumen robusta o controles alternativos de cifrado, además establecer controles de acceso sólidos.

6.3.1.4 Ejecución del usuario (User Execution): bloquear los archivos adjuntos ejecutables en los correos electrónicos y utilizar software de protección de puntos finales, antimalware, para detectar y prevenir la ejecución de código malicioso.

6.3.1.5 Tareas/trabajos programados (Scheduled Task/Job): restringir los privilegios para crear y modificar tareas/trabajos programados y revisar regularmente los registros del sistema en busca de actividades sospechosas.

6.3.1.6 Descubrimiento de cuentas (Account Discovery): Supervisar regularmente los registros del sistema e implementar políticas de contraseña seguras.

6.3.1.7 Phishing: Proporcionar capacitación para la concientización de los usuarios e implementar la autenticación de múltiples factores. Bloquear los correos electrónicos y las URL sospechosas e implementar el filtrado y el análisis de correos electrónicos.

Es importante recordar que ningún control individual puede prevenir todos los ataques, y la implementación de una combinación de controles es el mejor enfoque para mitigar el riesgo.

6.4 MEJORES PRÁCTICAS PARA LA PREVENCIÓN Y ATENCIÓN A INCIDENTES POR APT

Se puede identificar que algunos controles son más adecuados para prevenir determinado tipo de riesgo de afectación a las organizaciones. A continuación, se presentan algunos controles que pueden prevenir o responder a determinadas técnicas o fases de ataque, esto, basado en juicio de experto.

Se han podido identificar tipos de ataque muy específicos para los APT que han tenido actividad en Colombia por lo cual se pueden determinar algunos controles que pueden ser más efectivos para cada uno como se muestra en la Tabla 5. TTP y controles por fase de ataque.

Tabla 5. TTP y controles por fase de ataque.

Fase LM KC	TTP	Control
Reconocimiento	Captura de datos por Ingeniería Social (Phishing) Account Discovery	Control de información pública Concienciación
Armamento	Carga activa, Masquerading Web clonada	Antimalware Firewall
Despliegue	Phishing, Vishing, Smishing User Execution	Controles de correo Antimalware Concienciación
Explotación	CVEs, Vulnerabilidades de día cero Account Discovery	Parcheo Cifrado Antimalware Concienciación
Instalación	Elevación de privilegios Cambios en archivos del sistema	Firewall HIDS SIEM
Comando y Control	Command and Scripting Interpreter Cambios en los servicios Scheduled Task/Job	Antimalware Parches de seguridad Firewall HIDS SIEM
Acciones	Puerta trasera Fuerza bruta Otras cargas activas OS Credential Dumping	Firewall SIEM

Fuente: Propia.

De acuerdo con las publicaciones de Mitre[192] (https://attack.mitre.org/techniques), se determinan que para las 14 TTPs se pueden aplicar 9 Controles en total que pueden ser mitigatorios para más de una TTP.

[192] MITRE ATT&CK, Techniques - Enterprise | MITRE ATT&CK®. [Sitio WEB]. 2023. Tech. . [Disponible en 25 de February, 2023]. Recuperado de: https://attack.mitre.org/techniques/enterprise/

Se listan las TTP y se presentan estadísticas para ayudar a indicar cuáles son los controles de mayor importancia. Se puede identificar visualmente que el control que mitiga más TTP es la implementación de HIDS en los activos, como se aprecia en la Tabla 6. Controles para cada TTP.

Tabla 6. Controles para cada TTP.

TTP	Concienciación	Antimalware	Controles de correo	Control de información pública	Cifrado	Parcheo	HIDS	SIEM	Firewall
Phishing, Vishing, Smishing.	X	X	X	X					
CVEs, Vulnerabilidades de día cero	X	X		X	X	X			
Account Discovery	X				X		X		
Cambios en los servicios							X	X	X
Elevación de privilegios		X					X		X
OS Credential Dumping		X					X	X	
Puerta trasera		X					X	X	X
Carga activa		X					X		
Command and Scripting Interpreter		X							X
Masquerading	X						X		
Scheduled Task/Job		X					X		
User Execution	X							X	
Web clonada	X								X
Cambios en archivos del sistema							X		

Fuente: Propia.

De acuerdo con lo anterior se puede establecer que el 75% de los controles a mitigar TTP en cada fase de ataque se encuentran en tener un adecuado programa de concienciación en seguridad, implementar soluciones de seguridad como son HIDS, Antimalware y Firewall, conclusión obtenida del análisis de la Tabla 7. Controles y su impacto en las TTP. Pero, si un correo no controlado llegase a una estación de trabajo sin parches, todo este escenario de protección podría verse en un alto riesgo de compromiso, es por ello por lo que se debe observar la implementación de controles como una combinación de las mejores prácticas y no como elementos aislados.

Tabla 7. Controles y su impacto en las TTP.

CONTROL	TTPs	Impacto
HIDS	9	25%
Antimalware	7	19%
Concienciación	6	17%
Firewall	5	14%
SIEM	4	11%
Cifrado	2	6%
Controles de correo	1	3%
Control de información pública	1	3%
Parcheo	1	3%

Fuente: Propia.

Desde el punto de vista preventivo se ha abordado el enfoque en los controles que de ser implementados mitigan el riesgo de compromiso u ocurrencia de un evento relacionado con los ataques documentados que se originan en grupos APT, sin embargo, es necesario establecer también el escenario en que una organización ha sido afectada y debe tomar medidas de contención, respuesta y recuperación, de acuerdo con las mejores prácticas de la NIST[193].

[193] AWS, *MARCO NIST CIBERSEGURIDAD Un abordaje integral de la Ciberseguridad*, OAS.Org. 5: 1–19

7. CONSTRUIR INFORME TÉCNICO QUE PLANTEE TÉCNICAS, TÁCTICAS Y PROCEDIMIENTOS

A continuación, se presentan los aspectos más relevantes de los planteamientos de los numerales anteriores, ordenados a modo de informe técnico.

7.1 INTRODUCCIÓN

INFORME TÉCNICO DE CIBERSEGURIDAD SOBRE AMENAZAS PERSISTENTES AVANZADAS (APT)

En Colombia la definición oficial de una PYME se basa en el número de empleados y los ingresos generados por la empresa. Según la Ley 905 de 2004[194], se consideran pequeñas cuando tienen un máximo de 200 empleados y sus ingresos brutos totales o activos son iguales o inferiores a 100000 salarios mínimos mensuales legales vigentes.

Fecha: abril 23 de 2023

7.2 RESUMEN EJECUTIVO

Este informe presenta los hallazgos y recomendaciones obtenidos del análisis documental sobre Amenazas Persistentes Avanzadas (APT) que operan en Colombia y la región. El objetivo de este informe es identificar los riesgos asociados con las APT y presentar las mejores prácticas y recomendaciones para fortalecer la seguridad de las pequeñas y medianas empresas PYMES.

Las PYMES en Colombia están expuestas a riesgos asociados a actividades APT debido a su participación en la cadena de suministro de infraestructuras críticas y de grandes corporaciones, esto las ubica en el camino para que los atacantes logren comprometer grandes corporaciones o infraestructura necesaria para el funcionamiento de gobierno y cumplimiento de derechos.

Los ataques de APT son sofisticados y pueden soportar largos periodos de tiempo en actividad para eludir sistemas de seguridad conocidos, sin embargo, existen controles claves que pueden ser implementados por cualquier organización para preparar la organización para evitar, mitigar y responder adecuadamente estos incidentes.

[194] SENADO, LEY 905 DE 2004, CONGRESO DE COLOMBIA, Bogotá, August 2, 2004

Las PYME en general no se preocupan por fortalecer sus sistemas y preparar sus equipos en cuanto a seguridad informática, tampoco conocen el riesgo que las APT representan.

7.3 PERFIL DE LAS AMENAZAS

Se identificaron cuatro APT conocidas en el panorama de amenazas actuales: APT28, APT29, APT30 y APT-C-36. Estas APT se caracterizan por su sofisticación y su capacidad para eludir las medidas de seguridad tradicionales. Sus TTP incluyen el uso de malware personalizado, técnicas de phishing avanzadas y explotación de vulnerabilidades conocidas.

Para que los equipos técnicos de las compañías en crecimiento soporten su toma de decisiones en el momento de presentarse un evento de ciberseguridad de manera más eficaz contra cada tipo de ataque, se presenta a continuación un esquema de los puntos de interrupción posibles para la contención, respuesta y recuperación, de estos eventos con el menor impacto negativo a la organización.

Se establecerán las TTP en la capa de ataque o fases de ataque definidas en Figura 4. Fases de ataque modelo: Lockheed Martin Kill-Chain. A partir de allí se definirán las mejores prácticas de respuesta.

Tabla 8. Top 7 TTP vs Fase L-M Kill-Chain.

TTP	Reconocimiento	Armamento	Despliegue	Explotación	Instalación	Comando y control	Acciones maliciosas
Intérprete de secuencias de comandos y comandos (Command and Scripting Interpreter).		X	X	X	X	X	X
Enmascaramiento (Masquerading).		X	X	X	X		X
Volcado de credenciales del sistema operativo (OS Credential Dumping).				X			
Ejecución del usuario (User Execution).			X		X		
Tareas/trabajos programados (Scheduled Task/Job).			X	X	X		
Descubrimiento de cuentas (Account Discovery).		X	X				
Phishing (Ingeniería Social).	X	X	X				

Fuente: Propia.

Con este insumo se van a presentar apartados del “Play-Book” (PB) correspondiente propuesto por el Consorcio de Respuesta a Incidentes (IRC por sus siglas en inglés) al

tipo de incidente que puede identificarse dentro de la galería[195]; estos pueden ser de 9 tipos:

- Malware Outbreak.
- Phishing.
- Data Theft.
- Virus Outbreak.
- Denial of Service.
- Unauthorized Access.
- Elevation Of Privilege.
- Root Access.
- Improper Usage.

Estos PB cuentan con procedimientos paso a paso para implementar panes para preparar el equipo técnico y las partes interesadas en la eficaz preparación, detección, análisis, contención, erradicación, recuperación y manejo posterior a estos 9 tipos de incidente.

7.4 PLAY BOOKS (PB) DE MEJORES PRÁCTICAS

A continuación, se presentan los 9 planes de respuesta a cada tipo de incidente con una breve descripción.

7.4.1 Phishing (Ingeniería Social). Es tal vez la clave de los ataques exitosos, tanto así que IRC le dedica un PB completo; Sigue siendo una amenaza para Colombia, especialmente porque APT-C-36 se ha reconocido como activa en 2023[196].

Es por ello por lo que es crítico que los usuarios sean quienes lo detecten y de haber sido comprometidos informar inmediatamente al equipo técnico para el aislamiento e investigación de lo ocurrido.

[195] IRC - INCIDENT RESPONSE CONSORTIUM, Incident Response Consortium | The First & Only IR Community. [Sitio WEB]. 2023. [Disponible en 25 de February, 2023]. Recuperado de: https://www.incidentresponse.org/

[196] CHECKPOINT, BlindEagle Targeting Ecuador With Sharpened Tools - Check Point Research. [Sitio WEB]. January 5, 2023. Reearch. [Disponible en 25 de February, 2023]. Recuperado de: https://research.checkpoint.com/2023/blindeagle-targeting-ecuador-with-sharpened-tools/

7.4.2 Intérprete De Secuencias De Comandos Y Comandos (Command And Scripting Interpreter). Esta técnica se puede encontrar en las fases desde la preparación del ataque hasta el Comando y Control e incluso en las actividades maliciosas, por lo cual, puede ser un punto calve para lograr efectivamente contener un evento de infección de tipo APT.

Puede ser difícil para el equipo técnico de una compañía identificar que se han comprometido los intérpretes de comandos de los activos de la empresa, a menos que ésta se haya preparado con la implementación de un SIEM, HIDS o un antimalware avanzado. Por ello, es probable que gran cantidad de las compañías colombianas no cuenten con estas herramientas y no logren identificar la presencia del adversario hasta que haya un compromiso mayor de la red.

Esta TTP puede coincidir con 3 “Play-Book” (PB), Malware Outbreak, Virus Outbreak, y Improper Usage.

7.4.3 Enmascaramiento (Masquerading). Dentro de las fases L-M Kill-Chain, se ubica muy similar al TTP Interprete de comandos, esto es porque, al igual que se usa para proteger los datos de los adversarios, los atacantes pueden usar enmascaramiento para evadir los sistemas de detección de amenazas efectivamente, ocultando la carga activa o los enlaces a sitios web maliciosos, e incluso para ocultar el robo de datos.

Una vez se detectan transmisiones o archivos con cifrado desconocido, la recomendación es aislar el elemento y reportar a los investigadores usando SANDBOX[197] o con las autoridades (CAI Virtual de la policía[198], COLCERT[199]), quienes pueden determinar si se trata efectivamente de una amenaza.

[197] POLICIA NACIONAL DE COLOMBIA, Sandbox | Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL. [Sitio WEB]. 2023. [Disponible en 25 de February, 2023]. Recuperado de: https://cc-csirt.policia.gov.co/Sandbox

[198] POLICIA NACIONAL DE COLOMBIA, PONAL | CAI Virtual. [Sitio WEB]. 2023. [Disponible en 25 de February, 2023]. Recuperado de: https://caivirtual.policia.gov.co/

[199] MINTIC, ColCERT. [Sitio WEB]. 2023. Noticias. [Disponible en 25 de February, 2023]. Recuperado de: https://www.colcert.gov.co/800/w3-channel.html

7.4.4 Descubrimiento De Cuentas (Account DiscoverY). Esta TTP puede identificarse desde la preparación del ataque mediante técnicas como la Inteligencia de Fuentes Abiertas (OSINT), hasta el despliegue en la búsqueda de movimiento lateral o para escalamiento de privilegios.

Su detección puede dar mediante la correlación en SIEM o HIDS, por lo cual, gran cantidad de organizaciones se encontrarán expuestas al no tener estos elementos de seguridad.

Si se logra la identificación, la recomendación general es realizar un despliegue de renovación de credenciales y endurecimiento de sistemas[200] para la eliminación de cuentas de servicio no utilizadas o que representan un riesgo.

7.4.5 Ejecución Del Usuario (User Execution). Es parte complementaria de las técnicas de ingeniería social, el Phishing, Vishing, Smishing y otras técnicas que buscan que el usuario sea quien otorga acceso, información o ejecuta la tarea maliciosa.

Su identificación también se relaciona directamente con herramientas avanzadas, pero el factor clave es la experticia de los usuarios que han ganado con un plan de concienciación.

Si se identifica compromiso mediante esta TTP se debe informar inmediatamente al equipo técnico para el aislamiento e investigación de lo ocurrido.

7.4.6 Tareas/Trabajos Programados (Scheduled Task/Job). Para los grupos APT el tiempo juega a favor, no tienen problema para mantener un ataque por meses o años, esto para las organizaciones es un problema, puesto que el tiempo se traduce en costos para mantener sistemas y recursos técnicos, tecnológicos y humanos para atender los sistemas y procesos de seguridad.

Los adversarios pueden dejar tareas que garanticen su presencia en el sistema comprometido, por lo cual desde el punto de vista preventivo, esta opción debe ser controlada y restringida en los dispositivos; pero, desde el punto de vista reactivo, el aislamiento y análisis de los activos comprometidos puede tomar tiempo que puede representar aún más gastos para la organización, por lo cual en lo posible una respuesta rápida y determinante sería la mejor opción para las PYMES.

[200] CENETER OF INTERNET SECURITY, CIS WorkBench / Downloads. [Sitio WEB]. 2018. [Disponible en 3 de September, 2022]. Recuperado de: https://workbench.cisecurity.org/files/2235

7.4.7 Volcado De Credenciales Del Sistema Operativo (Os Credential Dumping). Esta TTP puede ser usada para el movimiento lateral por los adversarios, dado que el tiempo, como se menciona antes, juega a favor del atacante, una estrategia es que los usuarios y credenciales tengan una vida útil limitada y que se exija a los usuarios la renovación y uso de credenciales fuertes.

Sin embargo, en el evento de identificarse el compromiso de las credenciales, la recomendación general, es realizar un despliegue de renovación de credenciales y endurecimiento de sistemas[201] para la eliminación de cuentas de servicio no utilizadas o que representan un riesgo.

7.5 CONCLUSIONES DEL INFORME

Como se han presentado, parece casi imperceptible, pero se observa que para que los ataques de APT sean efectivamente identificados, contenidos y atendidos, el factor crítico, es el que para la mayoría de las organizaciones es el más débil, el factor humano. Fortaleciendo la pericia y preparación de los colaboradores se logra contener entre el 50 y el 75 % de las TTP. Lo anterior significa que cada colaborador esté vigilante de sus comunicaciones, credenciales, identificando comportamientos anómalos en ellas y reportándolos oportunamente.

Otra recomendación importante es que las organizaciones empiecen a preocuparse por implementar soluciones de seguridad como Firewall y Antimalware corporativos.

[201] CENETER OF INTERNET SECURITY, CIS WorkBench / Downloads. [Sitio WEB]. 2018. [Disponible en 3 de September, 2022]. Recuperado de: https://workbench.cisecurity.org/files/2235

8. CONCLUSIONES

Se identificó que las APT son un riesgo real para todas las organizaciones sin distinción de su tamaño, puesto que en el contexto histórico se evidencia que las cadenas de suministro se han convertido en su objetivo reciente, con el objeto de vulnerar empresas pequeñas y medianas, que cuentan con incipientes o nulos controles de seguridad, para llegar desde su infraestructura a organizaciones más grandes y con datos de mayor valor.

Se identifican tecnologías aún en desarrollo para la detección y protección contra APT, que en su mayoría son complejas y requieren una inversión considerable para su implementación, lo cual puede dejar por fuera a las empresas medianas y pequeñas.

Se identifica que existen controles comunes que pueden ser aplicados por cualquier organización para detección y control de APT. Teniendo en cuenta el problema de la inversión para las PYMES en estos aspectos, controles como un programa de concienciación, el uso de cortafuegos (Firewall) y Antimalware, puede impactar en el 50% de las TTP identificadas.

Para las pequeñas y medianas empresas puede ser un reto oneroso la implementación de herramientas sofisticadas con detección basada en inteligencia artificial, Block Chain, o comportamiento; sin embargo, la adecuada implementación de controles mitigatorios puede ser determinante en la respuesta y contención de ataques.

Se presentó un informe de planes de respuesta para cada una de las TTP del top 7 identificadas, encontrando que en 4 de ellas (Phishing, Descubrimiento de cuentas, Ejecución de usuario y Volcado de Credenciales del Sistema Operativo), es de vital importancia la preparación del usuario final mediante programas de concienciación y el uso de credenciales fuertes y de corta vida útil.

A partir de las propuestas dadas por Incident Response Cosortium, y del análisis realizado a los controles de mitigación de las principales TTP, se puede determinar que, un adecuado programa de concienciación en seguridad, implementar soluciones de seguridad como son HIDS, Antimalware y Firewall, responden al 75% de éstas y se encuentran entre las recomendaciones dadas por las mejores prácticas de la industria.

9. RECOMENDACIONES

La protección de los activos de información no es un tema que competa únicamente a las grandes empresas, las PYMES deben tomar conciencia en su participación en la cadena de suministro y las consecuencias que los incidentes pueden tener en cuanto a la continuidad de las organizaciones en el mercado.

Las organizaciones ciber criminales interactúan para mejorar sus resultados, entonces es imposible que las organizaciones legales puedan resistir los ataques sin una integración de esfuerzos.

Es imperativo que todas las organizaciones, sin importar su tamaño, implementen programas de concienciación en seguridad de la información y ciberseguridad para generar una cultura de cuidado de los activos de la organización, clientes, proveedores y personas.

En la misma línea las instituciones académicas deben reforzar los programas de tecnologías de la información con conciencia de seguridad de la información y ciberseguridad, para garantizar que, desde el proceso de formación de los futuros administradores y diseñadores de tecnología, este capital humano conozca las mejores prácticas y tenga conciencia de la importancia de su labor en la protección de la información.

Los directivos de todas las organizaciones deben otorgar la importancia e inversión a los controles y medidas de seguridad como la gestión de actualizaciones y parches, programas de concienciación y uso de herramientas de protección criptográficas y de identificación de amenazas, y donde sea posible la concentración y análisis de LOGS, en su infraestructura, para reducir la superficie de ataque de los atacantes.

BIBLIOGRAFÍA

ADAM KHALID, ANAZIDA ZAINAL, MOHD AIZAINI MAAROF, and FUAD A. GHALEB. Advanced Persistent Threat Detection: A Survey. 2021. 3rd International Cyber Resilience Conference.

AIMAD BERADY, VALERIE VIET TRIEM TONG, GILLES GUETTE, CHRISTOPHE BIDAN, and GUILLAUME CARAT. Modeling the Operational Phases of APT Campaigns. 2019. 2019 International Conference on Computational Science and Computational Intelligence (CSCI).

ANOMALI. Anomali ThreatStream Threat Intelligence Management. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.anomali.com/products/threatstream.

ARIANA MENDOZA. Las Tendencias de 2021 Sobre La Inmersión Digital En Las Empresas. February 1, 2021. Covid-19 teletrabajo. [Disponible en 20 de February, 2022]. Recuperado de: https://appsimplantadores.com/tendencias-inmersion-digital-2021/.

AT&T. AlienVault Is Now AT&T Cybersecurity. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://cybersecurity.att.com/.

AWS, O. MARCO NIST CIBERSEGURIDAD Un Abordaje Integral de La Ciberseguridad. 2019. OAS.Org. 5: 1–19.

BALBÁS GUTIÉRREZ, D. ATAQUES AL CRIPTOSISTEMA RSA (ATTACKS ON RSA) Trabajo de Fin de Grado Para Acceder Al GRADO EN MATEMÁTICAS. Universidad de Cantabria, Santander Cantabria, July 2019. 2019. pp.

BERRADA, G., J. CHENEY, S. BENABDERRAHMANE, W. MAXWELL, H. MOOKHERJEE, A. THERIAULT, and R. WRIGHT. A Baseline for Unsupervised Advanced Persistent Threat Detection in System-Level Provenance. North-Holland, July 1, 2020. Future Generation Computer Systems. 108: 401–413.

BLACKBERRY, C. T. R. T. El Machete’s Malware Attacks Cut Through LATAM. March 22, 2017. Res. Intell. [Disponible en 11 de October, 2022]. Recuperado de: https://blogs.blackberry.com/en/2017/03/el-machete-malware-attacks-cut-through-latam.

BRAUE, D. Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025. September 10, 2021. Cybercrime Mag. [Disponible en 22 de July, 2022]. Recuperado de: https://cybersecurityventures.com/cybersecurity-spending-2021-2025/.

BROADBAND4EUROPE. Cyber Security: APT30 and Lessons for ASEAN - Broadband 4 Europe. April 15, 2015. Cyber Secur. [Disponible en 26 de June, 2022]. Recuperado de: https://www.broadband4europe.com/cyber-security-apt30-lessons-asean/.

BROADCOM. Endpoint Security Complete. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.broadcom.com/products/cybersecurity/endpoint/end-user/complete.

BROADCOM. Symantec DLP | Sensitive Data Protection and Compliance. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.broadcom.com/products/cybersecurity/information-protection/data-loss-prevention.

BROADCOM, E. P. Sowbug: Cyber Espionage Group Targets South American and Southeast Asian Governments . November 17, 2017. Endpoint Prot. [Disponible en 11 de December, 2022]. Recuperado de: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=d544bd14-1dd2-4ab6-a5a0-181788b7d73b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

BRYANT, B. D., and H. SAIEDIAN. A Novel Kill-Chain Framework for Remote Security Log Analysis with SIEM Software. Elsevier Advanced Technology, June 1, 2017. Computers & Security. 67: 198–210.

CCIT. Estudio Trimestral de Ciberseguridad: Ataques a Entidades de Gobierno - CCIT - Cámara Colombiana de Informática y Telecomunicaciones. April 2022. Estudios. [Disponible en 19 de November, 2022]. Recuperado de: https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/.

CCIT. Estudio Anual de Ciberseguridad. Bogota, 2023. [Disponible en 20 de March, 2023]. Recuperado de: https://www.ccit.org.co/wp-content/uploads/estudio-anual-de-ciberseguridad.pdf.

CCIT, C. Ciberdelitos En El Sector Empresarial Aumentaron En 2021 - CCIT - Cámara Colombiana de Informática y Telecomunicaciones. July 26, 2021. [Disponible en 18 de October, 2021]. Recuperado de: https://www.ccit.org.co/en_los_medios/ciberdelitos-en-el-sector-empresarial-aumentaron-en-2021/.

CCIT, C. TENDENCIAS CIBERCRIMEN COLOMBIA. 2019. CCIT. [Disponible en 18 de October, 2021]. Recuperado de: http://www.ccit.org.co.

CENETER OF INTERNET SECURITY. CIS Critical Security Controls. 2023. [Disponible en 13 de March, 2023]. Recuperado de: https://www.cisecurity.org/controls_pre.

CENETER OF INTERNET SECURITY. CIS WorkBench / Downloads. 2018. [Disponible en 3 de September, 2022]. Recuperado de: https://workbench.cisecurity.org/files/2235.

CEPAL. Digital Technologies for a New Future. 2021. ECALC ONU. 43.

CESI. RESEARCH IN THE FRAMEWORK OF CESI'S PROJECT "DIWORK-DIGITALISING PUBLIC SERVICES: MAKING IT WORK FOR CITIZENS, BUSINESS AND WORKERS" FINAL REPORT. 2022. Visionary Analytics.

CHAOXIAN WEI, QIANG LI, DONG GUO, and XIANGYU MENG. Toward Identifying APT Malware through API System Calls.: EBSCOhost. December 9, 2021. Security and Communication Networks. 2021.

CHAVEZ, F., A. VARGAS, and M. MINA. Identificación de Amenazas Informáticas Aplicando Arquitecturas de Big Data. APA, 2021. INNOVA Research Journal. 6: 141–167.

CHECKPOINT. Quantum Intrusion Prevention System (IPS) - Check Point Software. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.checkpoint.com/quantum/intrusion-prevention-system-ips/.

CHECKPOINT. BlindEagle Targeting Ecuador With Sharpened Tools - Check Point Research. January 5, 2023. Reearch. [Disponible en 25 de February, 2023]. Recuperado de: https://research.checkpoint.com/2023/blindeagle-targeting-ecuador-with-sharpened-tools/.

CHENG, X., Q. LUO, Y. PAN, Z. LI, J. ZHANG, and B. CHEN. Predicting the APT for Cyber Situation Comprehension in 5G-Enabled IoT. April 2021. [Disponible en 10 de July, 2022]. Recuperado de: https://web-p-ebscohost-com.bibliotecavirtual.unad.edu.co/ehost/pdfviewer/pdfviewer?vid=0&sid=9acb599c-ba80-4309-a29c-453f40ec03f8%40redis.

CISA. The CISA on DarkSide Ransomware and Best Practices for Preventing Business Disruption from Ransomware Attacks. Joss Group, July 12, 2021. Seybold Report: Analyzing Publishing Technologies. 21: 4–7.

CISCO. ¿Qué Es Un Firewall? - Cisco. 2019. [Disponible en 17 de October, 2021]. Recuperado de: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html.

CISCO. ¿Qué Es La Ciberseguridad? - Cisco. July 21, 2022. [Disponible en 31 de July, 2022]. Recuperado de: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html.

CISCO. Cisco Secure IPS - Cisco. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.cisco.com/c/en/us/products/security/ngips/index.html?dtid=osscdc000283.

CISCO. Cisco Secure Network Analytics - Cisco. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.cisco.com/site/us/en/products/security/security-analytics/secure-network-analytics/index.html.

CLOUDFLARE. ¿Qué Es El Correo Electrónico? | Definición de Correo Electrónico | Cloudflare. 2021. Learning. [Disponible en 31 de July, 2022]. Recuperado de: https://www.cloudflare.com/es-es/learning/email-security/what-is-email/.

CROWDSTRIKE. The CrowdStrike Falcon® Platform: One Platform, Complete Protection. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.crowdstrike.com/falcon-platform/.

DARKTRACE. Productos | Darktrace. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://es.darktrace.com/products.

DESAI, D. R., and C. A. MAKRIDIS. IDENTIFYING CRITICAL INFRASTRUCTURE IN A WORLD WITH SUPPLY CHAIN AND CROSS-SECTORAL CYBERSECURITY RISK. American Bar Association, 2022. Jurimetrics: The Journal of Law, Science & Technology. 62: 173–195.

ECONOMIA3.COM. APT - Economia3. December 21, 2013. [Disponible en 26 de June, 2022]. Recuperado de: https://economia3.com/2013/12/21/16316-apt/.

EL ESPECTADOR. Guacamaya Leaks: Últimas Noticias, Fotos, Videos, Artículos de Opinión de Guacamaya Leaks | EL ESPECTADOR. December 29, 2022. [Disponible en 22 de December, 2022]. Recuperado de: https://www.elespectador.com/tags/guacamaya-leaks/.

ESPINOZA, M., and M. ANTONIO. Importancia de Los Modelos Para El Gobierno de La Seguridad de La Información En Las Empresas: Una Revisión Sistemática de La Literatura. Talleres de Impresos Oma, July 22, 2019. Importance of Models for Government of Information Security in Companies: A Systematic Review of the Literature. 40: 1–14.

EXTRAHOP. EXTRAHOP REVEAL(X) 360. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.extrahop.com/products/cloud/.

FERREYRO, A., and A. L. De LONGHI. Metodología de la investigación. Encuentro Grupo Editor, Córdoba, Argentina, 2014.

FIREWALLS.COM. Sophos Next Generation XG Firewalls - Information, Pricing, & Reviews. 2021. [Disponible en 17 de October, 2021]. Recuperado de: https://www.firewalls.com/brands/sophos/firewalls/xg.html.

FORCEPOINT. Forcepoint ONE DLP – DLP Software-as-a-Service | Forcepoint. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.forcepoint.com/product/forcepoint-one-dlp.

FORTINET. FortiGuard Intrusion Prevention Service | Fortinet. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/intrusion-prevention.

FORTRA. Data Loss Prevention Solutions from Fortra. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.digitalguardian.com/solutions/data-loss-prevention.

FOWLER, C., M. GOFFIN, B. HILL, R. LAMOURINE, and A. SOVERN. An Introduction to MITRE Shield. 2020.

GONZALEZ, D. Sistemas de Detección de Intrusiones. 2003. Diego González Gómez.

HEX-RAYS. Hex Rays - State-of-the-Art Binary Code Analysis Solutions. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://hex-rays.com/ida-pro/.

IBM. Security QRadar | IBM. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.ibm.com/qradar.

ICONTEC. NTC-ISO-IEC 27000:2017. ICONTEC, 2017.

INCIBE. Glosario de Términos de Ciberseguridad. 2020. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf.

INCIBE. Inventario de Activos y Gestión de La Seguridad En SCI | INCIBE-CERT. December 29, 2016. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci.

INCIBE. Protege Tu Información Con Los Dispositivos de Almacenamiento Extraíbles. | INCIBE. September 13, 2018. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/protege-tu-informacion-los-dispositivos-almacenamiento-extraibles.

INCIBE. TemáTICas Cloud | INCIBE. 2022. [Disponible en 2 de June, 2022]. Recuperado de: https://www.incibe.es/protege-tu-empresa/tematicas/cloud.

INCIBE. ¿Qué Es El Shoulder Surfing? | INCIBE. September 11, 2020. [Disponible en 30 de April, 2022]. Recuperado de: https://www.incibe.es/sala-prensa/notas-prensa/el-shoulder-surfing.

INCIBE. Ciberseguridad En El Teletrabajo. 2020. [Disponible en 31 de July, 2022]. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf.

INCIBE. CSIRT-CV e INTECO-CERT Publican El Informe: “Detección de APTs” | INCIBE. 2015. [Disponible en 2 de May, 2022]. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/deteccion-apts.

INSTITUTE OF STANDARDS AND TECHNOLOGY, N. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. 2014.

IRC - INCIDENT RESPONSE CONSORTIUM. Incident Response Consortium | The First & Only IR Community. 2023. [Disponible en 25 de February, 2023]. Recuperado de: https://www.incidentresponse.org/.

J, L. N. A. Y. R. S. Glosario - ISO27000.ES. August 2020. ISO27000.ES. [Disponible en 8 de August, 2020]. Recuperado de: https://www.iso27000.es/glosario.html.

JADALA, VIJAYA CHANDRA;PASUPULETI, SAI KIRAN;SAI BABA, C. M. H. ;Hrushikesav. R. S. ;Ravinde. N. Analyzing and Detecting Advanced Persistent Threat Using Machine Learning Methodology. 2022. Lecture Notes on Data Engineering and Communications Technologies. 93: 497–506.

KARMAKAR, K. K., V. VARADHARAJAN, S. NEPAL, and U. TUPAKULA. SDN Enabled Secure IoT Architecture. 2019. vol. 1109. Pp. 581–585, in 2019 IFIP/IEEE Symposium on Integrated Network and Service Management, IM 2019.

KASPERSKY. ¿Qué Es La Seguridad En Internet? 2022. [Disponible en 31 de July, 2022]. Recuperado de: https://latam.kaspersky.com/resource-center/definitions/what-is-internet-

security.

KASPERSKY. Todo Sobre El Ransomware WannaCry. June 1, 2022. [Disponible en 26 de June, 2022]. Recuperado de: https://www.kaspersky.es/resource-center/threats/ransomware-wannacry.

KASPERSKY. ¿Qué Es Un Honeypot? Cómo Colaboran Los Honeypots Con La Seguridad. 2022. [Disponible en 10 de July, 2022]. Recuperado de: https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot.

KUMAR, R., and G. SUBBIAH. Zero-Day Malware Detection and Effective Malware Analysis Using Shapley Ensemble Boosting and Bagging Approach. MDPI, April 2022. Sensors (14248220). 22: 2798.

LA REPUBLICA. El Problema de Los Hackers Hay Que Priorizarlo. December 22, 2022. EDITORIAL. [Disponible en 22 de December, 2022]. Recuperado de: https://www.larepublica.co/opinion/editorial/el-problema-de-los-hackers-hay-que-priorizarlo-3513522?utm_medium=Social&utm_source=Twitter#Echobox=1671709093.

LADINO FERNÁNDEZ, J. M., D. L. BRICEÑO BARRERO, and L. A. RODRÍGUEZ ROJAS. Industria 4.0: El Reto Para Las Pymes Manufactureras de Bogotá, Colombia. Revista Mutis, January 2022. Industry 4.0: The Challenge for Manufacturing SMEs in Bogotá, Colombia. 12: 110–127.

LATERCERA.COM. La “Guerra Fría Cibernética” Entre Estados Unidos y China - La Tercera. February 2, 2013. [Disponible en 26 de June, 2022]. Recuperado de: https://www.latercera.com/noticia/la-guerra-fria-cibernetica-entre-estados-unidos-y-china/.

LI, M., Q. LI, G. XUAN, and D. GUO. Identifying Compromised Hosts under APT Using DNS Request Sequences. Academic Press, June 1, 2021. Journal of Parallel and Distributed Computing. 152: 67–78.

LOGRHYTHM. Page Not Found | LogRhythm. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://logrhythm.com/products/nextgen-siem/.

MANDIANT. Advanced Persistent Threats (APTs) | Threat Actors & Groups. 2022. [Disponible en 26 de June, 2022]. Recuperado de: https://www.mandiant.com/resources/apt-groups.

MARIANO DÍAZ, R. La Ciberseguridad En Tiempos Del COVID-19 y El Tránsito Hacia Una Ciberinmunidad | Publicación | Comisión Económica Para América Latina y El

Caribe. 2020. [Disponible en 2 de April, 2022]. Recuperado de: https://www.cepal.org/es/publicaciones/46275-la-ciberseguridad-tiempos-covid-19-transito-ciberinmunidad.

MÁRQUEZ DÍAZ, J. E. Armas Cibernéticas. Malware Inteligente Para Ataques Dirigidos : Cyber Weapons. Intelligent Malware for Targeted Attacks. January 1, 2017. Revista Ingenierías USBMed. 8: 48–57.

MICROSOFT. Microsoft Security Development Lifecycle. 2023. [Disponible en 13 de May, 2023]. Recuperado de: https://www.microsoft.com/en-us/securityengineering/sdl?SilentAuth=1.

MINISERIO DE DEFENSA ESPAÑOL, and INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS. SECRETARÍA GENERAL TÉCNICA. July 2020. Boletín IEEE. 83.

MINTIC. ColCERT. 2023. Noticias. [Disponible en 25 de February, 2023]. Recuperado de: https://www.colcert.gov.co/800/w3-channel.html.

MITRE ATT&CK. APT-C-36, Blind Eagle, Group G0099 | MITRE ATT&CK®. 2022. [Disponible en 18 de October, 2022]. Recuperado de: https://attack.mitre.org/groups/G0099/.

MITRE ATT&CK. Techniques - Enterprise | MITRE ATT&CK®. 2023. Tech. . [Disponible en 25 de February, 2023]. Recuperado de: https://attack.mitre.org/techniques/enterprise/.

MOHSIN, M. (1), and Z. (2) ANWAR. Where to Kill the Cyber Kill-Chain: An Ontology-Driven Framework for IoT Security Analytics. (1)National University of Sciences and Technology, 2017. Pp. 23–28, in Proceedings - 14th International Conference on Frontiers of Information Technology, FIT 2016.

MORA FRANCO, C. F. El Desconocimiento de Las Pymes Colombianas Frente a Las Amenazas Persistentes Avanzadas. Universidad Piloto de Colombia, January 29, 2015. Instname:Universidad Piloto de Colombia.

MUDZINGWA, D., and R. AGRAWAL. A Study of Methodologies Used in Intrusion Detection and Prevention Systems (IDPS). 2012. Conference Proceedings - IEEE SOUTHEASTCON.

NATHALIA MORALES. Andi Insiste En Una Apuesta Por La Transformación Digital Para Ganar Competitividad. October 2021. LR - Empres. [Disponible en 7 de May, 2022]. Recuperado de: https://www.larepublica.co/empresas/andi-insiste-en-una-apuesta-por-la-transformacion-digital-para-ganar-competitividad-3243005.

NIETO, A. Cibercriminales a La Caza de La Vacuna Para La COVID-19 - Una Al Día. November 18, 2020. [Disponible en 2 de April, 2022]. Recuperado de: https://unaaldia.hispasec.com/2020/11/cibercriminales-a-la-caza-de-la-vacuna-para-la-covid-19.html.

OLLYDBG. OllyDbg v1.10. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.ollydbg.de/viewer.htm.

OPENVAS, G. N. Background — Greenbone Documentation Documentation. 2021. Hist. OPENVAS. [Disponible en 7 de November, 2021]. Recuperado de: https://greenbone.github.io/docs/background.html#history-of-the-openvas-project.

ORACLE. Modelo de Referencia OSI (Guía de Administración Del Sistema: Servicios IP). 2010. [Disponible en 10 de July, 2022]. Recuperado de: https://docs.oracle.com/cd/E19957-01/820-2981/ipov-8/index.html.

ORCERO, D. S. Kali Linux. RA-MA Editorial, Madrid, 2018.

OTAN. ¿Qué Es La OTAN? 2022. [Disponible en 26 de June, 2022]. Recuperado de: https://www.nato.int/nato-welcome/index_es.html.

PAESSLER. Discover the 3 Paessler PRTG Monitoring Solutions. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.paessler.com/prtg.

PALOALTO. Advanced Threat Prevention - Palo Alto Networks. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.paloaltonetworks.com/network-security/advanced-threat-prevention.

PANAHNEJAD, M., and M. MEGHDAD. APT-Dt-KC: Advanced Persistent Threat Detection Based on Kill-Chain Model. November 8, 1234. The Journal of Supercomputing. 78: 8644–8677.

PIERLUIGI PAGANINI. CyberCriminals and Their APT and AVT TechniquesSecurity Affairs. February 23, 2015. [Disponible en 26 de June, 2022]. Recuperado de: https://securityaffairs.co/wordpress/33999/cyber-crime/apt-and-avt-techniques.html.

PODZINS, O., and A. ROMANOVS. Why SIEM Is Irreplaceable in a Secure IT Environment? 2019. Pp. 1–5, in 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream).

POLICIA, C. V. BALANCE CIBERCRIMEN 2020. 2020. BALANCE CIBERCRIMEN.

POLICIA NACIONAL DE COLOMBIA. Sandbox | Equipo de Respuesta a Incidentes de Seguridad Informática de La Policía Nacional CSIRT-PONAL. 2023. [Disponible en 25 de February, 2023]. Recuperado de: https://cc-csirt.policia.gov.co/Sandbox.

POLICIA NACIONAL DE COLOMBIA. PONAL | CAI Virtual. 2023. [Disponible en 25 de February, 2023]. Recuperado de: https://caivirtual.policia.gov.co/.

PORTSWIGGER. Burp Suite - Application Security Testing Software - PortSwigger. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://portswigger.net/burp.

QUALYS. Qualys VMDR - Vulnerability Management Tool | Qualys. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.qualys.com/apps/vulnerability-management-detection-response/.

RAHMAN, Z., X. YI, and I. KHALIL. Blockchain Based AI-Enabled Industry 4.0 CPS Protection against Advanced Persistent Threat. February 2022. 1.

RAPID7. Nexpose On-Premise Vulnerability Scanner - Rapid7. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.rapid7.com/products/nexpose/.

RDSTATION. ¿Qué Son Las Redes Sociales?【Guía Completa + Ejemplos】. 2022. [Disponible en 31 de July, 2022]. Recuperado de: https://www.rdstation.com/es/redes-sociales/.

READTHEDOCS. Welcome to YARA's Documentation! — Yara 4.2.0 Documentation. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://yara.readthedocs.io/en/v4.2.2/index.html.

RECORDEDFUTURE. Recorded Future: Securing Our World With Intelligence. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.recordedfuture.com/.

RED SEGURIDAD. Amenaza Persistente Avanzada (APT): ¿cómo Funciona Este Ciberataque? 2021. Redaccion. [Disponible en 2 de May, 2022]. Recuperado de: https://www.redseguridad.com/actualidad/cibercrimen/amenaza-persistente-avanzada-apt-como-funciona-este-ciberataque_20210420.html.

REYES ROIG, D. Guia de implementacion de la seguridad en redes de Nucleo Mpls. D - Instituto Superior Politecnico Jose Antonio Echeverria. CUJAE, 2010, 145 p. 145. 2010. pp.

ROLDÁN, K. S. N., J. V. VERDUGO, and E. O. B. ROMERO. THE ADVANCED PERSISTENT THREATS (APT) AND ITS METHOD OF DELINQUENCY. July 2016. LA

AMENAZA PERSISTENTE AVANZADA (APA) Y SU MÉTODO DE DELINCUENCIA. 10: 127–143.

S21SEC. Segundo Semestre 2021. 2021. Threat Landscape Report. 1: 1–38.

SÁNCHEZ, L. E., D. VILLAFRANCA, E. FERNÁNDEZ-MEDINA, and M. PIATTINI. MGSM-PYME: Metodología Para La Gestión de La Seguridad y Su Madurez En Las PYMES. 2009.

SANS. 20 Critical Security Controls | SANS Institute. March 30, 2023. [Disponible en 30 de March, 2023]. Recuperado de: https://www.sans.org/webcasts/20-critical-security-controls-96685/.

SECURELIST. Poseidon Group: A Targeted Attack Boutique Specializing in Global Cyber-Espionage | Securelist. February 9, 2016. APT REPORTS. [Disponible en 11 de October, 2022]. Recuperado de: https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/.

SEE LEE MATHEWS. Criminals Hacked A Fish Tank To Steal Data From A Casino. July 17, 2017. [Disponible en 22 de March, 2022]. Recuperado de: https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/?sh=5b24215432b9.

SENADO, C. LEY 1273 2009. January 5, 2009. [Disponible en 12 de October, 2021]. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

SENADO, C. LEY 905 DE 2004. CONGRESO DE COLOMBIA, Bogotá, August 2, 2004.

SENTINELONE. XDR Ingestion - SentinelOne. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.sentinelone.com/platform/xdr-ingestion/.

SHUDONG LI, QIANQING ZHANG, XIAOBO WU, WEIHONG HAN, and ZHIHONG TI. Attribution Classification Method of APT Malware in IoT Using Machine Learn...: EBSCOhost. September 2021. [Disponible en 10 de July, 2022]. Recuperado de: https://web-p-ebscohost-com.bibliotecavirtual.unad.edu.co/ehost/pdfviewer/pdfviewer?vid=0&sid=8f9c765c-5836-4043-bb55-33a1f6655ea7%40redis.

SKYHIGH SECURITY. Enterprise Cloud Data Protection - Skyhigh Security. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.skyhighsecurity.com/en-us/.

SOLARTE SOLARTE, F. N., E. R. ENRIQUEZ ROSERO, and M. del C. BENAVIDES. Metodología de Análisis y Evaluación de Riesgos Aplicados a La Seguridad Informática y de Información Bajo La Norma ISO/IEC 27001. December 31, 2015. Tecnológica ESPOL –RTE. 28.

SOLARWINDS. Network Performance Monitor - Onsite & Remote Monitoring | SolarWinds. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.solarwinds.com/network-performance-monitor.

SPLUNK. Splunk Enterprise Security | Splunk. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.splunk.com/en_us/products/enterprise-security.html?301=/en_us/software/enterprise-security.html.

TCPDUMP. Home | TCPDUMP & LIBPCAP. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.tcpdump.org/.

TECNOZERO. ¿Qué Es Un EDR? ¿Por Qué Es Diferente de Un Antivirus? | Tecnozero. 2022. Antivirus y ramsomware. [Disponible en 23 de March, 2022]. Recuperado de: https://www.tecnozero.com/antivirus-y-anti-ransomware/que-es-un-edr/.

TENABLE. NESSUS by TENABLE. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.tenable.com/products/nessus.

THREATCONECT. Cyber Threat Intelligence Company | ThreatConnect. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://threatconnect.com/.

TRELLIX. XDR Ecosystem | Trellix. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.trellix.com/en-us/products.html.

U.S. DEPARTMENT OF DEFENSE. Chief Information Officer: CMMC. 2021. [Disponible en 13 de March, 2023]. Recuperado de: https://dodcio.defense.gov/CMMC/.

UNIVERSIDAD TECNOLÓGICA DE PEREIRA. SISTEMA INTEGRAL DE GESTIÓN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MANUAL GENERAL DE DIRECTRICES Versión: 4 Fecha: 28/11/2018 Código: 1313-MGD-01 Página: 1 de 61. November 28, 2018.

VECTRA. Prevent Cyberattacks with Vectra AI. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.vectra.ai/.

VERSA NETWORKS. IDS Frente a IPS: Diferencias Entre IDS e IPS | Versa Networks. 2023. [Disponible en 13 de March, 2023]. Recuperado de: https://versa-

networks.com/es/sd-wan/ids-ips/.

VIRUSTOTAL. VirusTotal - Home. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.virustotal.com/gui/home/upload.

VMWARE. VMware Security Solutions. 2023. [Disponible en 18 de March, 2023]. Recuperado de: https://www.vmware.com/security.html.

WELIVESECURITY. Guía Definitiva Para Entender y Protegerte de Las APT | WeLiveSecurity. 2014. [Disponible en 2 de May, 2022]. Recuperado de: https://www.welivesecurity.com/la-es/2014/08/29/guia-definitiva-entender-protegerte-apt/.

WEN TIAN, GUANGJIE LIU, and YUEWEI DAI. Honeypot Detection Strategy Against Advanced Persistent Threats in Industrial Internet of Things: A Prospect Theoretic Game. December 15, 2021. IEEE INTERNET OF THINGS JOURNAL.

WIRESHARK. Wireshark · Go Deep. 2022. [Disponible en 29 de October, 2022]. Recuperado de: https://www.wireshark.org/.

XUAN, C. Do, and M. H. DAO. A Novel Approach for APT Attack Detection Based on Combined Deep Learning m...: EBSCOhost. April 11, 2021. Neural Computing and Applications. 2021.

YOHAI, A. Informe SAFE - Tendencias Del Cibercrimen 2021 - 2022. 2021.

Tácticas, Técnicas y Procedimientos (TTPs). | El Blog de Tiro Táctico (EBdT2). June 4, 2022. [Disponible en 26 de June, 2022]. Recuperado de: https://tirotactico.net/2011/06/04/68/.

Ke3chang, APT15, Mirage, Vixen Panda, GREF, Playful Dragon, RoyalAPT, NICKEL, Group G0004 | MITRE ATT&CK®. [Disponible en 24 de January, 2023]. Recuperado de: https://attack.mitre.org/groups/G0004/.

Updating the NIST Cybersecurity Framework – Journey To CSF 2.0 | NIST. Gaithersburg, MD, April 16, 2018.