AMENAZAS PERSISTENTES AVANZADAS Y SU IMPACTO EN LATINOAMÉRICA ¿CÓMO ESTAR PREPARADOS?

Jorge A. Parra

***Abstract*— The evolution of the internet, globalization and the dynamism of information management is advancing very quickly. The rapid development of information technologies that converge on the Internet, the importance of privacy and security is also becoming a key concern around the world. This concern for development security is not only limited to multinational organizations and high-value government data, but also to mass users, as technologies evolve threats as well, this has brought with it a new generation of known threats as APT Advanced Persistent Threat, which have brought reputational, economic and governmental damages to different nations around the world, this article will focus on describing these threats, what their impact has been in Latin America and suggests the best practices to defend against these lethal threats.**

***Index Terms*—Advances Persistent Threats, Ataques de día cero, ciberseguridad, tácticas, técnicas, procedimientos, herramientas de ataque, adversarios, cibercrimen, hacktivismo, espionaje, ciberguerra.**

I. INTRODUCCION

El presente artículo describe los nuevo paradigmas de los ciberataques a nivel mundial, haciendo énfasis en el impacto que se ha registrado en Latinoamerica, y en cómo estas sofisticadas amenazas se han sintetizado en técnicas avanzadas de hacking, generando pérdidas millonarias en compañías alrededor del mundo, incluyendo todos los sectores de la economía [1]. La globalización, el constante cambio y evolución en las tecnologías de la información también han ido de la mano con un emergente y sofisticado nacimiento de ciberdelincuentes, los cuales hacen uso de tácticas y técnicas cada vez más sofisticadas para abusar de un sistema informático con diferentes fines. En la actualidad ya no se habla de adversarios o hackers sombrero negro intentando indisponer un sistema informático por alguna motivación personal, sino que también se habla de estucturas delincuenciales organizadas en busca de varios objetivos como lo son monetarios, activistas, daño de reputación, gubernamentales y guerreristas (ciberguerra). En algunos casos estas estructuras son financiadas por el crimen y en otros también por los gobiernos de algunos países que consideran relevante armarse de arsenales cibernéticos con el suficiente poder para generar daños económicos, sociales e industriales a países adversarios, sin el uso de armas bélicas ya conocidas [2]. A estas amenazas sofisticadas se les conoce como APT Advanced Persistent Threats o en español Amenazas Persistentes Avanzadas. Este artículo describirá el objetivo de este tipo de amenazas y cómo hacer frente a ellas de manera eficiente, mediante el desarrollo de mejores prácticas que permitan detectarlas y contenerlas.

II. APT (ADVANCED PERSISTENT THREATS)

Una Amenaza Avanzada Persistente es un conjunto de tácticas, técnicas y procedimientos que hacen compleja la detección de una intrusión cibernética en uno o varios sistemas informáticos, las siglas se adoptaron en el 2006 por la Fuerza Aérea de los estados unidos (USAF), para facilitar la discusión de las actividades de intrusión con sus homólogos civiles no autorizados a conocer detalles de los grupos y/o campañas que originaban las Amenazas Avanzadas Persistentes [2], los componentes de la terminología son los siguientes:

Amenaza: Significa que el adversario está organizado, financiado y motivado aumentando de manera significativa el riesgo y el impacto de que esta se materialice.
Avanzada: Significa que el adversario está familiarizado con las herramientas y técnicas de intrusión de sistemas informáticos, y es capaz de desarrollar ataques personalizados.
Persistente: Significa que el adversario tiene la intención de cumplir una misión. Reciben directivas y trabajan hacia objetivos específicos.

Una APT a menudo posee la habilidad de ocultarse dentro del tráfico de la red empresarial, interactuando solo lo suficiente para obtener lo que necesita para lograr sus objetivos. Logra Mimetizarse u ocultarse dentro de un conjunto de sistemas informáticos de una organización, sin ser detectado por los controles de seguridad tradicionales. Esta es una de las características principales de este tipo de amenazas, las cuales se convierten en un reto para los profesionales de seguridad de la información en las compañías de todo el mundo.

Ataque de día cero: Un ataque de día cero es una explotación a una vulnerabilidad no conocida sobre un sistema de información.
USAF: United States Air Force.
ISACA: *Information Systems Audit and Control Association, una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información.*

En un estudio realizado por ISACA a mas de 100.000 profesionales de la seguridad de información en 180 paises y con credenciales activas emitidas por esta entidad, parecen estar practicando una buena gestión de la seguridad al utilizar un enfoque basado en el riesgo para contrarrestar las APT dentro de sus empresas, sin embargo, las APT son amnezas relativamente nuevasy por esta razón deben ser gestionadas de forma diferente a como se gestiona una amenaza tradicional o conocida. Uno de los malentendidos más comunes entre la mayoría de los usuarios y profesionales de seguridad de la información, es pensar que las herramientas tradicionales de seguridad y los métodos de defensa son suficientes para enfrentar un ataque APT. Todavía hay una brecha considerable en la comprensión de lo que son las APT y cómo defenderse contra ellas. Este estudio demuestra que un 67.6% de los encuestados se sienten familiarizados con el término APT en comparación con un 53.4% que consideran que las APT son similares a las amenazas tradicionales [3].

Este estudio motiva y requiere la necesidad de generar campañas de concienciación para este tipo de amenazas, con el fin de reducir al máximo la brecha de entendimiento que se tiene con respecto a las APT y el impacto que puede generar este tipo de intrusiones en una compañía, independiente del sector de la economía en el que opere.

III. HISTORIA

Con el pasar de la historia se han descubierto múltiples ciberamenazas que han provocado diferentes tipos de daños y perjucios tanto a empresas en todos los sectores de la economía, como a gobiernos e instituciones, además, de los millones de usuarios que tienen o han tenido acceso a las tecnologías de la información. Estas amenazas desde los orígenes de la informática han ido evolucionando y creciendo a medida que las tecnologías de la información y la era del Internet han evolucionado, tanto en número como en tipo y variedad.

Seguramente en este momento se está planeando o materializando un incidente que involucre un APT en cualquier lugar del mundo, sin importar el sector económico o institución. Se desconocen los fines exactos para los cuales se puede estar usando la APT, y el objetivo al que quieren llegar los adversarios. En este capítulo se escribirá acerca de los 3 incidentes de seguridad más representativos catalogados como una Amenaza Persistente Avanzada, los cuales fueron descubiertos en los primeros años de este siglo y aún se desconoce desde cuando estaban operando; los incidentes mas representativos son:

1) Operación Aurora: APT descubierta a finales de 2009 pero se cree que esta se ha estado desarrollando y evolucionando desde el año 2006, afectó empresas como Google, Adobe, Yahoo, Symantec, Juniper Systems, Rackspace, entre otros, todas referencias de investigación coinciden con que su origen es chino. Con respecto a sus objetivos existen varias hipótesis. Sin embargo, hay dos de ellas que coiciden en las referencias consultadas, por un lado, que el ataque fue motivado con el ánimo de robar propiedad intelectual a grandes compañías; y por el otro, que su objetivo principal fue la intención de robar cuentas de Gmail de activistas de derechos humanos en China. Para este ataque se utilizó principalmente un ataque de día cero para Internet Explorer en su version 6.0 mediante Java Scripts que redirigían a un sitio web con software malicioso que se descargaba automáticamente, y una vez puesto en memoria extraía información sensible de las máquinas infectadas. Las contramedidas tomadas para esta APT fue instalar los parches lanzados pocos días después de la detección, además de implementar controles como agentes de antivirus basados en firmas, filtros de correos y IDS/IPS, no obstante, esta APT logró generar gran controversia en muchas de las empresas involucradas, así como impactos en su imagen, dentro de las empresas afectadas por esta APT se encontraban Google, Symantec, Yahoo, Adobe, Juniper y RackSpace [4][5][6].

2) Stuxnet: Esta ha sido una de las APT mas mencionada en los últimos años, debido a la sofisticación e impacto de haberse materializado, considerada una de las primeras armas de la ciberguerra [7], Stuxnet es un gusano informático que aprovechando una vulnerabilidad de los sistemas operativos Windows, lograba llegar a explotar otras cuatro vulnerabilidades de día cero que emplean los programas de monitorización y control industrial (SCADA), se cree que este gusano se creó para sabotear el programa nuclear iraní por los gobiernos de Estados Unidos e Isrrael, con el fin de generar un daño en la planta nuclear cambiando la velocidad de las centrifugadoras que enrriquecian el uráneo, acelerándolas y realentizándolas de manera paulatina hasta que esta colapsaran [8].

3) GhostNet: Esta es una APT que tuvo como objetivo espiar los colaboradores de Dalai Lama en medio del conflicto entre China y el Tibet, específicamente un ataque generado desde la República Popular de China hacia los sistemas informáticos pertenecientes a embajadas, ministerios de asuntos exteriores y otras oficinas gubernamentales, y los centros de exiliados tibetanos del Dalai Lama en India, Londres y la ciudad de Nueva York se vieron comprometidos esto asociado al conflicto entre China y el Tibet [9]. Esta APT se logró mediante técnicas de phishing dirigido conocido como spear phishing y muy usada en la actualidad, los correos electrónicos se envían a organizaciones específicas que contienen información relevante al contexto que manejaban estas organizaciones. Estos correos electrónicos contenían archivos adjuntos maliciosos, que cuando se abrían, insertan un troyano en el sistema. Este troyano se conectaba de nuevo a un servidor de comando y control, generalmente ubicado en China, para recibir comandos. El computador infectado ejecutaba comandos especificados por el servidor de comando y control. En ocasiones, el comando especificado por el servidor de control hacia que el computador infectado descarga e instala un troyano conocido como Gh0st Rat que permitia a los atacantes obtener un control completo y en tiempo real de los computadores con Microsoft Windows [10]. Los investigadores declararon que no podían concluir que el gobierno chino era responsable de la red de espionaje. [10] Sin embargo, un informe de investigadores de la Universidad de Cambridge

menciona que el gobierno chino puede estar detrás de las intrusiones que analizaron en la Oficina del Dalai Lama.

IV. CICLO DE VIDA DE UNA APT

Cada paso en una APT incluye un movimiento muy minucioso, planeado y estudiado por los atacantes. Esto incluye la creación de diagramas lógicos de la infraestructura de TI de la organización o el objetivo que se atacará, ingeniería de malware, ataques de ingeniería social y extracción de datos no detectados. Las APT por lo general se dividen en 4 grandes fases: incursión, descubrimiento, captura y exfiltración [11], En cada fase se puede usar una variedad de técnicas, herramientas y tácticas como se describe a continuación:

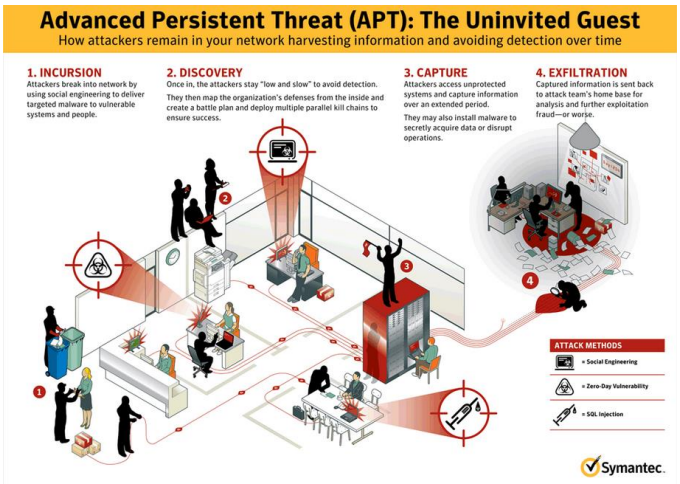

Ilustración 1. Fases de una APT [11].

Incursión: Los atacantes investigan e identifican a las personas a las que se dirigirán en los ataques, mediante la búsqueda pública u otros métodos, y obtienen sus direcciones de correo electrónico o algún dato que pueda transformarse en un vector de ataque mediante alguna técnica de ingeniería social. Por lo general, todo comienza con correos electrónicos de phishing, donde el atacante se dirige a usuarios específicos dentro de la compañía objetivo con correos electrónicos falsos que incluyen enlaces o archivos PDF maliciosos o documentos adjuntos de Microsoft Office. Estos archivos infectados en la máquina de la persona objetivo le dan al atacante una entrada en la puerta de la organización, y un pase directo para iniciar con la siguiente fase [11] [12] [13].

Descubrimiento: Esta fase es una de las mas críticas de las APT, dado que el atacante debe estudiar cuidadosamente todos los movimientos del objetivo sin ser descubierto, por lo general instrucciones operativas,funcionalidad de los sistemas de información del objetivo, rutas de recursos expuestos, contraseñas débiles, puntos de acceso adicionales en caso de perder el punto de acceso con el que ya cuentan, esto lo logra mediante movimientos laterales, y herramientas de reconocimiento pasivo sobre la red, a fin de estudiar en datalle el objetivo y saber el momento exacto de configurar las fases siguientes [11] [12] [13].

Captura: En esta fase los ciberdelincuentes ya tienen acceso a información confidencial expuesta, y usan todo tipo de malware para este fin, dentro de los mas conocidos están las herramientas de RAT (remote accces tools) las cuales permiten acceder de manera completa a las máquinas comprometidas de manera remota, con una previa y simple instrucción de comunicación a un servidor de comando y control, el cual se encarga de generar ordenes a las máquinas comprometidas de manera remota. En esta fase la infraestutura del objetivo ya está expuesta y a merced de los atacantes. Esto abriría la posibilidad de pasar a la siguiente fase [11] [12] [13].

Exfiltración: Esta es la fase en la que se obtiene la joya de la corona y en la que el atacante inicia la extracción de información manteniendo como premisa el sigilo, en ocasiones la información es extraída mediante peticiones DNS que a simple vista en un análisis de red parecen legítimos, en otras ocasiones los atacantes logran establecer VPN o redes privadas virtuales mediante protocolos de cifrado, para evitar que sean interceptados por algún dispositivo de control. Todo depende del tipo de exfiltración que el atacante esté realizando y del objetivo del ataque y/o objetivo seleccionado [11] [12] [13].

Una vez completadas todas las fases de una APT, el atacante logra su objetivo e intentará borrar los rastros del mismo, pero esta acción nunca es infalible y depende de la astucia de los profesionales de seguridad de la información evitar los ciberdelincuentes puedan avanzar entre las fases de una APT.

V. IMPACTO DE LAS APT EN LATINOAMÉRICA

Desde hace algunos años la economía y los conflictos geopolíticos han hecho cada vez mas interesante a Latinoamérica para los ciberdelincuentes, esto ha generado una serie de ataques sofisticados en los que algunos países de la región se han visto afectados.

La compañía ESET en 2018 mediante un estudio a 2.500 empresas y mas de 4.500 participantes en Latinoamérica, dio a conocer que Venezuela y Ecuador eran de los países con más afectación por malware, principalmente con un tipo de malware de secuestro de información conocido como ransomware. Hablando específicamente de Colombia, se posiciona de séptimo en el top 10 con una participación del 19%. El principal vector de ataque en todos lo casos fue el correo electrónico mediante técnicas de ingeniería social, una de las principales técnicas usadas en las APT actualmente.

Ilustración 2. Porcentaje de malware por país [14].

Dentro de los eventos de APT más recientes en Latinoamérica se encuentra la APT Machete y la APT38, bautizada con este identificador por una de las empresas más importantes de investigación en el mundo, FireEye. Machete fue una APT que dejó más 778 víctimas en Latinoamérica [15]. Su objetivo principal era el ciberespionaje y sus primeras apariciones en 2010 con mejoras en 2012, la empresa Kaspersky Labs asegura que los creadores de Machete son de América Latina, pero no es posible determinar exactamente el país de procedencia. Su interés en los documentos diplomáticos generó que hasta una embajada en Rusia sea destino de la maliciosa operación. De los países con mayor porcentaje de presencia de esta APT fueron Venezuela con un 42%, Ecuador con un 36% y Colombia con un 11% [16].Machete fue distribuida a través de phishing que contenían malware capaz de realizar diversas funciones, como la copia de archivos en un servidor remoto, secuestrar el contenido del portapapeles, detectar las pulsaciones teclado al registrarse en la sesión de la máquina comprometida (keyloger), capturar el audio en el micrófono, tomar capturas de pantalla, obtener datos de geolocalización y hacer fotos con la cámara web de la máquina comprometida [17].

Ilustración 3. Afectacion APT Machete [15]

Como se ha mencionado a lo largo de este artículo las APT buscan siempre un objetivo específico, dentro de estos objetivos y siendo de los mas relevantes, esta lucrarse a través de robos a sistemas informáticos bancarios.A finales de 2018 se presentó un conocido incidente perpetrado a la banca chilena, este incidente fue bautizado por FireEye Inc. como APT38, el cual intentó robar al menos USD $1.100 millones en todo el mundo[18], esta conocida APT a logrado robar un estimado de USD $100 millones, con un estimado del 10% únicamente en en el Banco de Chile [19], a este país se suman países en Latinoamérica como el Banco del Austro en Ecuador y otros bancos en Brazil, Paraguay y México[19]. Esta APT presuntamente se orquestó desde Korea del Norte y aún se desconoce si este grupo hace parte del conocido grupo Lazarus a quien presuntamente se le atribuyeron los ataques a la empresa Sony en 2014.De lo que se tiene certeza es que este grupo es uno de los mejores ejemplos de la ejecución del ataque en el momento adecuado mediante herramientas de evasión, escalamiento de privilegios, fuerza bruta y herramientas de password cracking, esperando en algunos casos meses y hasta años de reconocimiento y vigilancia antes de dar el golpe final.

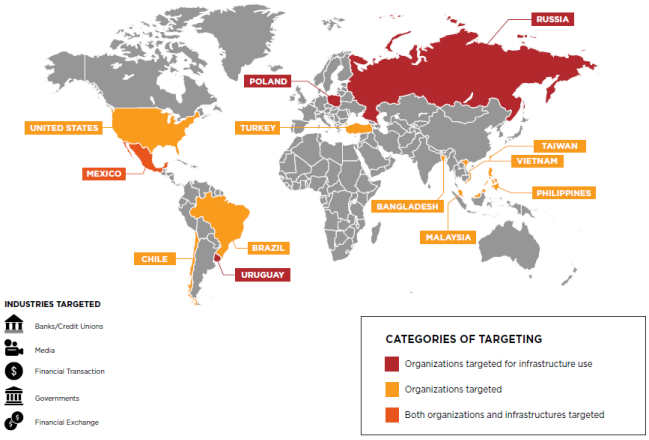

Ilustración 4 Paises afectados con APT38 [19]

VI. Mejores prácticas para hacer frente de defensa de una APT.

Conociendo las fases de una APT, los profesionales de seguridad de la información deben empezar a diseñar mecanismos de prevención orientados a la detección temprana de este tipo de amenazas, con el fin de reaccionar de manera oportuna en las fases iniciales.Estos controles siempre deben ir alineados con un esquema de defensa en profundidad, que se adapte a las políticas, procesos y la educación del personal en torno a la seguridad de la información siendo uno de los factores mas importantes para hacer frente a estas amenazas, adicional a los controles necesarios para proteger las capas subsecuentes hasta la protección del dato.

Existen métodos de defensa sugeridos por empresas reconocidas de seguridad. Estos métodos proponen el uso de herramientas que usen heurística, implementación de cifrado de

datos con algoritmos de cifrado fuertes, uso de tecnologías que usen algoritmos de inteligencia artificial, empresas como Symantec ofrecen una suite con todos las características mencionadas anteriormente, adicionalmente Palo Alto con su tecnología Traps, carbon black o FireEye EX si se trata de una plataforma de endpoint detection and response que ofrezca funcionalidades robustas de investigación e inteligencia de amenazas , también se pueden adoptar tecnologías open source como CimSweep o Wazuh, adicional se deben contemplar herramientas de sandboxing con el fin detectar comportamientos anómalos sobre archivos que se ejecutan sobre un sistema operativo, simulado antes de llegar a los equipos de cómputo reales en esta familia encontramos tecnologías destacadas como FireEye, PaloAlto, Fortinet y su complemento open source en caso de no contar con recursos suficientes para adquirir estas tecnologías como Cuckoo.

Las defensas efectivas requieren enfoques de factores múltiples, donde los analistas deben ser apoyados por técnicas analíticas de big data que sean capaces de detectar y priorizar eventos sutiles relacionados con las fases de una APT dentro de estas tecnologías se encuentra Splunk como una de las mas relevantes del mercado, en caso de tratarse de compañías pequeñas sin muchos recursos que quieran incursionar en el mundo del big data se recomienda el uso de Elasticsearch. El enfoque de estos métodos de detección debe ir orientado a la recolección de logs de todas las fuentes críticas o consideradas críticas en un análisis de riesgos previamente realizado, con el fin de que sean correlacionadas con indicadores de compromiso y detección mediante el uso de herramientas OSINT (Open Source Intelligence) la cuales ayudan a identificar y cuantificar toda la información relacionada con un ciberdelincuente asociado a un grupo y/o organización identificada por una fuente de inteligencia [20], dentro de estas fuentes de inteligencia de libre acceso las mas destacadas están shodan, DSHIELD, Abuse.ch y Pulsedive solo por mencionar algunas.

OSINT (Open Source Intelligence): Es un término acuñado y muy empleado entre militares, fuerzas del orden y personal de inteligencia de las agencias gubernamentales, para referirse a fuentes de inteligencia abiertas. Cualquier fuente abierta que aporte información a una investigación es considerada como OSINT.

VII. CONCLUSIONES

Las APT son una amenaza latente para todas las compañías en todos los sectores de la economía, tienen distintos objetivos desde dañar la reputación de una organización, como buscar beneficios económicos asociados a robos mediante técnicas y tácticas que día a día están en constante evolución.

A pesar de los métodos de defensa disponibles contra una APT, el alto porcentaje de ataques exitosos de las APT indica claramente que es necesario hacer esfuerzos adicionales para contraatacar este tipo de amenazas. Estos se deben centrar en la educación al personal y el buen uso de las herramientas tecnológicas de las que disponen las compañías, adicional, las organizaciones deberían informar a los centros de respuesta a incidentes autorizados cuando tengan información o indicios de que hay presencia de una APT, esto podría ayudar a los expertos en seguridad a proponer un mecanismo de defensa mucho mejor para contrarrestar dichos ataques en el futuro. Hay varias razones por las cuales la mayoría de las organizaciones no reportan violaciones de seguridad. Las razones pueden incluir la preocupación por la reputación de una organización, o en ocasiones las organizaciones ni siquiera son conscientes de que la red está siendo comprometida, lo cual es alarmante. Con el presente artículo se espera crear conciencia acerca de este tipo de amenazas y lograr generar un impacto en cómo las organizaciones y/o profesionales de la seguridad de la información se están preparando para este tipo de amenazas.

REFERENCIAS

[1] Symantec Internet Security Threat Report. Disponible: https://www.symantec.com/security-center/threat-report

[2] Understanding the advanced persistent threat. https://searchsecurity.techtarget.com/magazineContent/Understanding-the-advanced-persistent-threat

[3] Vilius Benetis, Jeimy J. Cano, Christos K. Dimitriadis, Jo Stewart-Rattray, Advanced Persistent Threat Awareness por ISACA con patrocinio TREND micro

[4] Raimund Genes, Operation Aurora and beyond How to avoid that this happens to How to avoid that this happens to your organisation https://www.eiseverywhere.com/file_uploads/b7b68ecce1c001adfeef8358fc7352e5_Tuesday_1110_Raimund_Genes.pdf

[5] Jamie Warren, OPERATION AURORA DETECT, DIAGNOSE, RESPOND Jan 27, 2010, Verdasys, Inc. https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2010/Aurora_HBGARY_DRAFT.pdf

[6] ¿Qué es Operación Aurora? https://www.welivesecurity.com/la-es/2010/01/21/que-es-operacion-aurora/

[7] Stuxnet, el misil más letal de la ciberguerra https://www.elconfidencial.com/tecnologia/2010-10-03/stuxnet-el-misil-mas-letal-de-la-ciberguerra_774229/

[8] Stuxnet https://www.ecured.cu/Stuxnet

[9] S T U D Y O F G H O S T N E T, Chalakkal sreepriya, publicado en Abril 2016, disponible https://priyachalakkal.files.wordpress.com/2016/06/ghostnet_sreepriyachalakkal.pdf

[10] Tracking GhostNet, Munk Centre for International Studies. Publicado en Marzo 29, 2009. Disponible https://www.f-secure.com/weblog/archives/ghostnet.pdf

[11] Advanced Persistent Threats: A Symantec Perspective. Disponible en https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf

[12] Anatomy of an APT Attack: Step by Step Approach, Disponible en https://resources.infosecinstitute.com/anatomy-of-an-apt-attack-step-by-step-approach/#gref

[13] Yadav, Tarun & Rao, Arvind. (2015). Technical Aspects of Cyber Kill Chain. Disponible en https://arxiv.org/pdf/1606.03184.pdf

[14] ESET SECURITY REPORT Latinoamérica 2018, disponible https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

[15] La APT Machete se hace fuerte en Latinoamérica, disponible https://www.muyseguridad.net/2014/08/23/apt-machete-latinoamerica/

[16] SAS LatAm: Operación Machete Espía a Los Gobiernos de América Latina, 19 Ago 2014, disponible https://latam.kaspersky.com/blog/sas-latam-operacion-machete-espia-a-los-gobiernos-de-america-latina/3708/

[17] "El Machete", 20 Ago 2014, https://securelist.com/el-machete/66108/

[18] El Toro: Firma que adjudicó a Corea del Norte hackeo al Chile entrega detalles de APT38, disponible, https://www.latercera.com/pulso/noticia/toro-firma-adjudico-corea-del-norte-hackeo-al-chile-entrega-detalles-apt38/347377/

[19] APT38 Un-usual Suspects, 2018 FireEye, Inc. Disponible en https://content.fireeye.com/apt/rpt-apt38

[20] Mirco Marchetti, Fabio Pierazzi, Alessandro Guido, Michele Colajanni, COUNTERING ADVANCED PERSISTENT THREATS THROUGH SECURITY INTELLIGENCE AND BIG DATA ANALYTICS