Ministerio del Interior y Seguridad Pública

AMENAZAS PERSISTENTES AVANZADAS

un enemigo en las sombras

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

colaborador de contenidos de la semana

Contenido

Autor: Juan Roa Salinas.
Director: Carlos Landeros C.
Editor: Katherina Canales M.
Diseño: Jaime Millán G.
Corrección: Ramón Rivera N.
Correo: comunicaciones@interior.gob.cl
Santiago de Chile, 29 de Diciembre de 2020

Presentación

La actual edición 26 de Análisis de Amenazas Cibernéticas estuvo liderado por Juan Roa Salinas, quien junto a su equipo nos entrega una mirada de un enemigo en las sombras: Las Amenazas Persistentes, Juan Roa es Ingeniero informático con una trayectoria de 18 años en áreas relacionadas con Seguridad de la información, Magister en Seguridad de la información y Protección de datos, quien actualmente se desempeña como Gerente de Ciberseguridad y Defensa en Redbanc.

En el transcurso de la presente investigación —Amenazas Persistentes Avanzadas (APT): un enemigo en las sombras—, el autor y su equipo explican qué es una APT y cómo se diferencian de otros tipos de amenazas más comúnmente enfrentadas por los sistemas informáticos en el día a día.

La inmersión continúa con una detallada explicación de las características y principales objetivos de un APT, para luego explicar los distintos pasos que requiere, en general, implementar una operación de tipo APT: la preparación y el acceso inicial, expansión, persistencia y Asset Targeting, exfiltración y limpieza.

Asimismo, describen los principales grupos APT y cierra con las principales conclusiones y consejos para evitar en el mayor grado posible ser víctimas de las operaciones de uno de estos poderosos grupos.

1. Amenazas Persistentes Avanzadas (APT): qué son y cómo se clasifican

El medio ambiente de Ciberseguridad cambio drásticamente, no cabe duda de aquello, durante los últimos años, las ciberamenazas han evolucionado rápidamente en cantidad, sofisticación e impacto, en comparación con las capacidades de defensa de organizaciones, Estados y países. Esta relación se ha vuelto cada día más asimétrica, dejando en evidencia un problema sin una solución aparente y que mantiene en constante preocupación a una parte importante de la sociedad.

En este contexto, una nueva clase de amenazas, conocidas como amenazas persistentes avanzadas (APT), ha atraído cada vez más la atención de los investigadores del sector de la Ciberseguridad.

Las APT son ataques cibernéticos ejecutados por adversarios sofisticados y con una gran cantidad de recursos a disposición, que tienen como objetivo principal obtener información específica de empresas y gobiernos. Desde ciberdelincuentes que buscan información financiera personal y propiedad intelectual hasta ciberataques patrocinados por Estados, diseñados para robar datos y comprometer infraestructuras críticas, las APT pueden evadir las medidas de defensa de ciberseguridad y causar daños graves a cualquier organización.

Estas amenazas pueden usar múltiples vectores y puntos de entrada para navegar alrededor de las defensas, violar su red en minutos y evadir la detección durante meses. Las APT representan un desafío mayor para los esfuerzos de ciberseguridad de organizaciones y países en general. Originalmente utilizado para describir intrusiones cibernéticas contra organizaciones militares, la APT ha evolucionado y ya no se limita al dominio militar. Como se destaca en varios incidentes de ciberseguridad a gran escala, las APT ahora se enfocan a una amplia gama de industrias y gobiernos.

Las APT son ampliamente reconocidas, como una de las amenazas de ciberseguridad más sofisticadas y poderosas que existen hoy en día, en particular se refieren a grupos de atacantes con importantes capacidades ofensivas, normalmente muy bien organizados en base a estructuras jerárquicas y altamente sofisticados y motivados para lograr sus objetivos en contra de países y organizaciones públicas o privadas. Este tipo de atacantes representan una amenaza para la propiedad intelectual, los activos financieros y la reputación de las organizaciones, y en algunos casos, estas amenazas tienen como objetivo la infraestructura crítica de un país.

Las estrategias, herramientas, procedimientos y otros controles defensivos que comúnmente se implementan para manejar las amenazas de Ciberseguridad, son ineficaces contra este tipo de ataques ya que los atacantes detrás de este tipo de intrusiones están enfocadas en objetivos específicos pudiendo personalizar y adaptar sus tácticas, técnicas y procedimientos (TTP) para identificar y eludir controles de ciberseguridad y prácticas estándar de respuesta a incidentes.

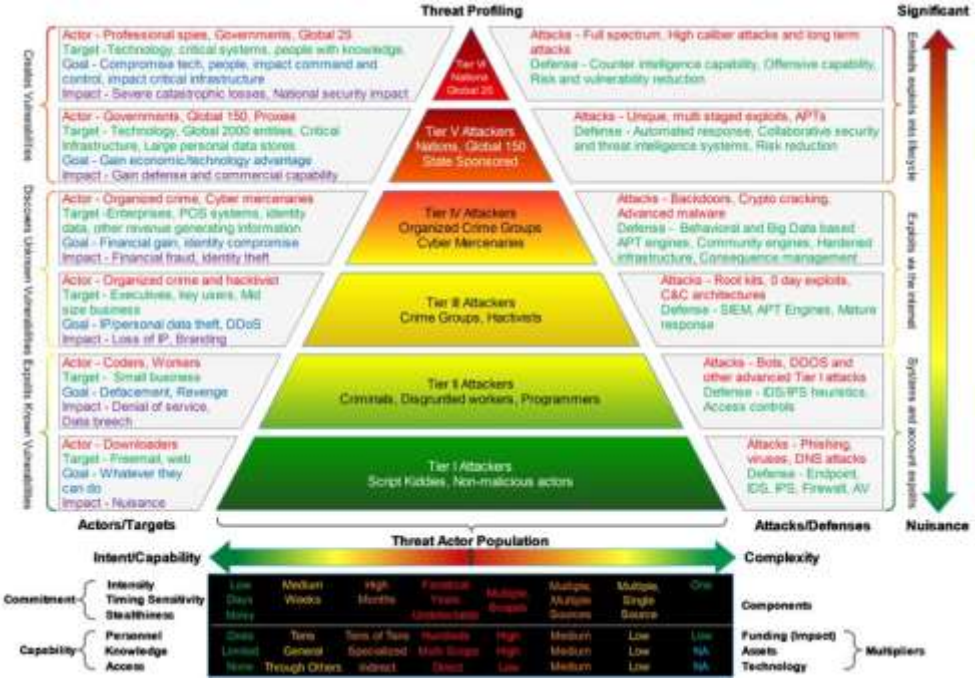

Figura 1: Pirámide de actores relacionados a las ciberamenazas y sus capacidades.

¿Qué es una APT?

Una amenaza persistente avanzada (Advanced Persistent Threat o APT) es un ataque cibernético prolongado y dirigido en el que un intruso obtiene acceso a una red y permanece sin ser detectado por un período indeterminado de tiempo. Es realizado a través de distintas técnicas, tácticas y procedimientos como, por ejemplo: webshells, software de comando y control, software de acceso remoto (RAT), malware, spam o phishing, entre otros. El objetivo de un ataque APT puede ser variado, pero en general lo que se busca es obtener inteligencia y control sobre un grupo de individuos, una nación, gobiernos, instituciones privadas o públicas.

La definición dada por el Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU., permite comprender con mayor detalle la profundidad del concepto, básicamente establece que una APT es “un adversario que posee niveles sofisticados de pericia y recursos significativos que le permiten crear oportunidades para lograr sus objetivos al utilizando múltiples vectores de ataque (por ejemplo, cibernético, físico y engaño). Estos objetivos típicamente incluyen establecer y extender puntos de apoyo dentro de la infraestructura tecnológica de las organizaciones objetivo con el propósito de extraer información, socavar o impedir aspectos críticos de una misión, programa u organización; o posicionarse para llevar a cabo estos objetivos en el futuro. La amenaza persistente avanzada: (i) persigue sus objetivos repetidamente durante un período prolongado de tiempo; (ii) se adapta a los esfuerzos de los defensores para resistirlo; y (iii) está determinada a mantener el nivel de interacción necesario para ejecutar sus objetivos”.

Esta definición proporciona una buena base para distinguir entre amenazas tradicionales y APT. Las características distintivas de las APT son: (1) metas específicas y objetivos claros; (2) atacantes altamente organizados y con buenos recursos; (3) campaña a largo plazo con intentos repetidos; (4) técnicas de ataque furtivas y evasivas.

El término APT se define utilizando las siguientes propiedades del ataque:

• **Amenaza:** Identifica el uso de amenazas digitales para materializar el o los ataques.

• **Persistente**: indica que la naturaleza encubierta de la amenaza hace intentos reiterados de establecer el acceso a sistemas e información sensible de la organización.

• **Avanzada:** significa la capacidad de superar los sistemas de detección de intrusos y mantener un acceso constante a la red objetivo de manera segura.

Características de una APT

• Son altamente organizados: Involucran varias personas, tecnologías y técnicas.

• Son eficientes: Varían sus técnicas, tácticas y procedimientos según los objetivos, a veces técnicas básicas o ingeniería social, otras veces utilizaran RAT, exploits 0-day o spear phishing.

• Son Tenaces: invierten los recursos que sean necesarios para lograr el objetivo.

• Son Dirigidos: Principalmente se enfocan en organizaciones específicas, individuos, estados, naciones, etc.

• Son Persistentes: No se trata de un evento de ataque específico, más bien de actividades sistemáticas que permitan mantener el acceso a datos y sistemas la mayor cantidad de tiempo posible.

• Son Evasivos: Pueden fácilmente camuflarse con los productos de seguridad tradicionales.

• Son Complejos: Comprenden una mezcla de métodos de ataque dirigidos a distintas vulnerabilidades.

• Impacto: El impacto de un ataque del tipo APT es directamente proporcional al tiempo de permanencia de un atacante en la red, se estima que en promedio una amenaza de este tipo esta alrededor de 150 días en un objetivo.

Objetivos de una APT

• Políticos: Incluyen ataques a la población para alcanzar sus objetivos.

• Negocios / Económicos: además del robo directo de dinero y distintos tipos de divisas, incluyen el robo de propiedad intelectual para obtener ventajas competitivas.

• Militares: Buscan identificar y robar secretos militares de otros países para obtener ventajas geopolíticas.

Figura 2: Motivaciones de atacantes y adversarios relacionados a las Ciber Amenazas

2. Diferencia entre APT y ataques tradicionales

A diferencia de los ataques cibernéticos más comunes, las amenazas persistentes avanzadas tienden a llevarse a cabo a través de métodos que se han personalizado para el objetivo en lugar de utilizar herramientas más generales que pueden ser más adecuadas para atacar a un gran número de víctimas. Los APT también se llevan a cabo generalmente durante un período de tiempo mucho más largo, a diferencia de los ataques comunes, que pueden ser más obvios y, por lo tanto, más fáciles de defender.

La diferencia principal entre una APT y un ataque tradicional tiene que ver con que los ataques APT ocurren cuando alguien o alguna organización decide que usted tiene algo de valor, que ellos quieren y están dispuestos a invertir muchos recursos y tiempo para conseguirlo. No se trata de un objetivo genérico, se ha identificado como objetivo por una razón específica.

Comprender aquello es fundamental para entender, dimensionar y poder establecer estrategias para poder combatir ataques del tipo APT. El hecho de que un grupo de este tipo despliegue todas sus habilidades y recursos a disposición con el único objetivo de obtener sus activos cambia totalmente el panorama de riesgo. Significa que la amenaza se adaptará a situaciones específicas hasta que consigan su objetivo o el costo de la operación supere el valor percibido del objetivo.

	Traditional Attacks	APT Attacks
Attacker	Mostly single person	Highly organized, sophisticated, determined and well-resourced group
Target	Unspecified, mostly individual systems	Specific organizations, governmental institutions, commercial enterprises
Purpose	Financial benefits, demonstrating abilities	Competitive advantages, strategic benefits
Approach	Single-run, "smash and grab", short period	Repeated attempts, stays low and slow, adapts to resist defenses, long term

Figura 3: Diferencias entre un ataque del tipo APT Vs Ataques tradicionales.

3. Anatomía de un ataque APT

Los ataques APT se planifican meticulosamente y, por lo general, implican varios pasos. Si bien un ataque APT específico puede tener características únicas, las etapas de los ataques APT son similares y difieren principalmente en las técnicas utilizadas en cada etapa.

Para describir las fases de un ataque APT, se presenta un modelo de seis etapas basado en el concepto de una "cadena de intrusión" El uso de este modelo de cadena de intrusión, ayuda a comprender las técnicas de los actores en cada etapa y también proporciona una guía para la defensa contra ataques APT.

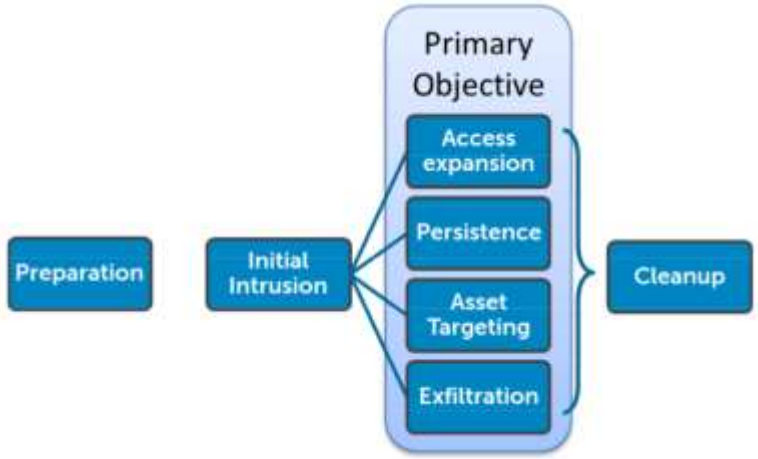

Figura 4: Ciclo de vida general de una amenaza persistente avanzada (APT).

Según la naturaleza del objetivo y el propósito que se busca, un ataque del tipo APT utiliza distintas metodologías para lograr su objetivo. Sin embargo, en la mayoría de los ataques se identifican etapas que son comunes. Estas etapas definen el nivel de penetración en el sistema de destino. En general, se visualizan las siguientes etapas básicas en este tipo de ataques.

a. Preparación y Acceso Inicial:

Las operaciones tipo APT implican un alto grado de preparación, por lo que, en esta fase, se identifican y detallan todos los componentes necesarios para la ejecución del plan y comienza el proceso de reconocimiento y obtención de estos componentes, suelen incluir: información de vulnerabilidades, infraestructura, herramientas, datos, información sobre el entorno de los objetivos, personas, cargos y otros activos necesarios. Los atacantes también recopilan inteligencia sobre los controles y procedimientos de seguridad que probablemente encontrarán, para crear planes de evasión y respuesta.

Ejemplo de estos componentes son por ejemplo el registro de nuevos dominios o dominios en proveedores de DNS dinámico, configuraciones de servidores de comando y control (C2C), de

malware en sitios de hosting o en sistemas previamente comprometidos, asignación de servidores web y FTP (transferencia de archivos) para alojamiento de phishing o exploits, adquisición de servidores de correo electrónico para transmisión de correo no deseado o para la exfiltración de datos, etc.

Incluso, se han visto casos en donde se han utilizado servicios públicos como Google, documentos, chat, Twitter, IRC (Internet Relay Chat) y sitios de blogs configurados como canales C2C. Como se mencionó anteriormente, los atacantes asociados a grupos APT son tenaces y persistentes. No es de extrañar que algunas operaciones puedan durar años, ya que están enfocadas en objetivos de tan alto valor que el tiempo empleado en la fase de preparación representa una pequeña inversión en la operación general.

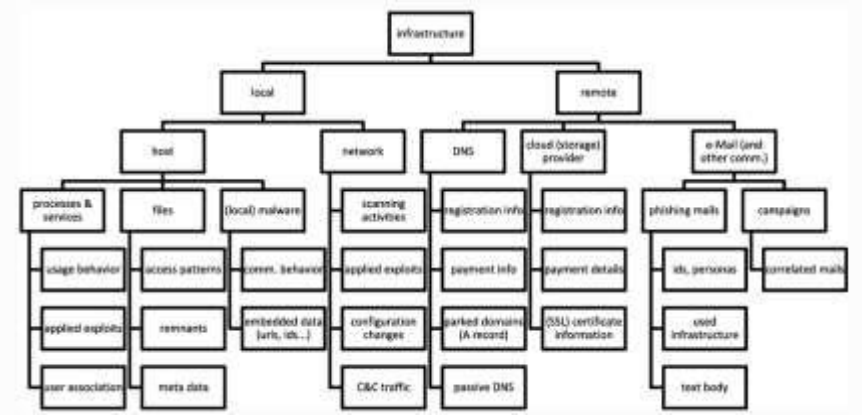

Figura 5: Tipos de artefactos obtenidos en fase de preparación.

Una vez que el atacante completa la fase de preparación, el siguiente paso es intentar mantenerse o ganar "persistencia" en el objetivo. Para esto, una táctica de entrada extremadamente común es el uso de correos electrónicos de phishing que contienen un enlace web o un archivo adjunto malicioso. Los enlaces de correo electrónico generalmente conducen a sitios donde el navegador web del objetivo y el software relacionado puedan ser explotados a través de alguna vulnerabilidad o donde los atacantes intentan obtener información de ingeniería social de la víctima que se puede utilizar más tarde.

Si se produce una explotación exitosa, se instala un malware de fase inicial en el equipo de la víctima. La Figura 6 ilustra un ejemplo de un correo electrónico del tipo "spear phishing" que contiene un archivo adjunto malicioso. Estos correos electrónicos de phishing suelen ser muy convincentes y difíciles de distinguir de los mensajes de correo electrónico legítimos. Las tácticas para aumentar su credibilidad y efectividad incluyen la modificación de documentos válidos o relacionados con la organización o con algún proveedor de confianza. En ocasiones, los documentos son robados a la organización o sus colaboradores durante operaciones de explotación previas y

utilizados posteriormente, en este caso, los atacantes modifican los documentos agregando exploits y códigos maliciosos y luego los envían a las víctimas.

La explotación de vulnerabilidades en servidores expuestos a internet es también otra técnica muy utilizada por algunos grupos APT, esto se puede lograr utilizando exploits conocidos o adquiriendo vulnerabilidades de día cero en el mercado negro según sea necesario.

Figura 6: Atacante APT envía correos del tipo "spear phishing" al objetivo con contenido malicioso.

Lograr un punto de persistencia en el destino es el objetivo principal de la fase de intrusión inicial. Una vez que se explota un sistema, el atacante generalmente coloca malware en el sistema comprometido y lo usa como un punto de salto o proxy para acciones posteriores. El malware inyectado durante la fase de intrusión inicial suele ser el código de un downloader simple, un troyano de acceso remoto básico o un shell simple.

La Figura 7 ilustra un sistema recién infectado que inicia una conexión saliente para notificar al atacante APT que la intrusión inicial fue exitosa y que está listo para aceptar comandos.

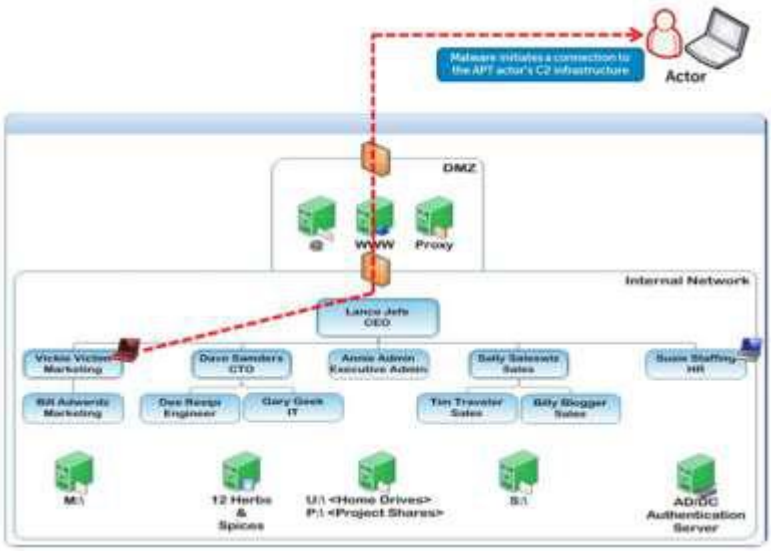

Figura 7: Malware inicia una conexión desde el equipo victima a un servidor de comando y control (C2C).

b. Expansión:

Después de ejecutar la fase de preparación y acceso inicial de un sistema en la red del objetivo, el atacante APT usa el sistema comprometido como puente hacia distintos segmentos de la red y como un mecanismo de instalación y ejecución de herramientas adicionales que le permitirán moverse con facilidad dentro de la red atacada.

En algunos casos, el objetivo de la explotación es un único sistema, al que se puede atacar directamente. Si la intrusión inicial logra el acceso a este objetivo directamente, es posible que no sea necesario continuar con esta fase. Sin embargo, en la mayoría de los casos, lograr el o los objetivos que están detrás del ataque requiere acceso a más de un sistema o plataforma. En estas instancias, una de las primeras acciones realizadas por los atacantes después de la intrusión inicial es una expansión del acceso y elevación de privilegios.

El objetivo de esta fase es obtener acceso a sistemas y plataformas adicionales e información de cuentas de usuarios y de sistemas que generalmente centralizan o provisionan el acceso a la red. Un patrón común para obtener privilegios administrativos a nivel de dominio es:

- Obtener permisos de administrador local del equipo vulnerado inicialmente.
- Capturar credenciales almacenadas en caché, de administradores de dominio o usuarios con mayor privilegio que han hecho “logon” en esta máquina comprometida.
- Utilizar la técnica “pass the hash” con las credenciales administrativas almacenadas en caché capturadas para obtener acceso a otros sistemas.

Como se muestra en la Figura 8, una vez que se ha obtenido el acceso con privilegios, uno de los objetivos iniciales predilectos por los atacantes es el controlador de dominio (Domain Controller) del entorno o el servidor de “Active Directory” que cumple esta función.

Desde estos sistemas, los atacantes pueden capturar y exfiltrar la cuentas y hashes de información y contraseña para todas las cuentas de usuario y así poder descifrarlas “offline”. Una vez que los atacantes poseen las credenciales de las distintas cuentas que son utilizadas en los sistemas, el movimiento a través de la red se vuelve mucho más difícil de rastrear, esto debido a que cuando se tiene el nombre de usuario y la contraseña correcta, la actividad ocurre bajo el concepto de inicio de sesión, lo que dificulta la identificación. Cuando esta actividad se realiza desde los sistemas correctos y en los patrones correctos, puede ser muy difícil diferenciar entre acceso autorizado y no autorizado hasta que el ataque ya haya sido ejecutado y se esté desarrollando el análisis forense.

En muchos casos, las organizaciones responden a este tipo de incidentes forzando a que sus usuarios cambien sus contraseñas. Si bien esta acción es una buena práctica, no mitiga el riesgo en su totalidad debido a que los atacantes mantienen acceso administrativo que les permite evadir esta medida de control. Se debe ejecutar un proceso de “erradicación” al más alto nivel.

Los atacantes pueden usar los datos que obtuvieron para obtener acceso incluso después de que se hayan realizado los cambios de cuenta. Esto es importante porque si los atacantes detrás de las intrusiones no han terminado sus tareas, es seguro que volverán en el futuro para completar sus objetivos.

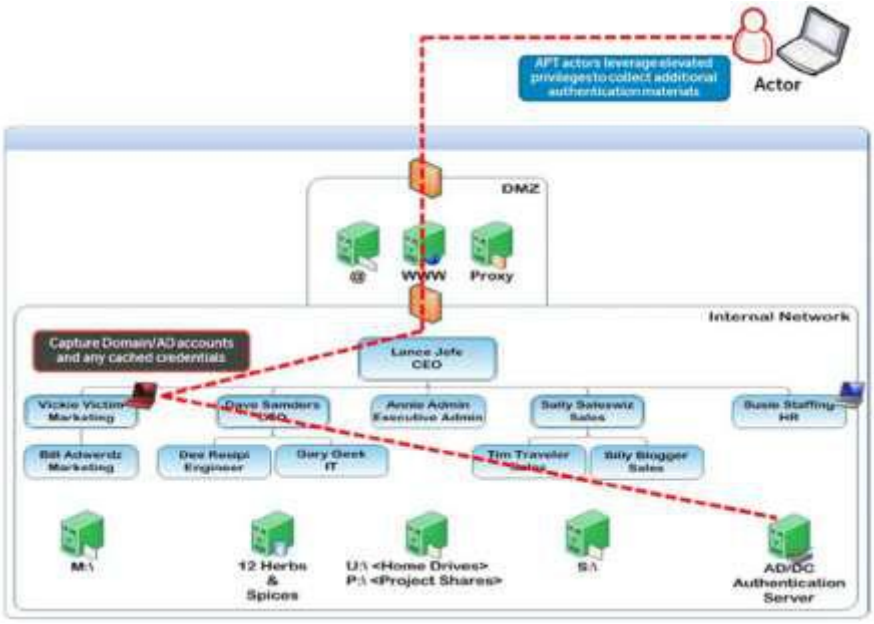

Figura 8: Obtención de credenciales de autenticación desde el objetivo.

No todos los sistemas aprovechan las credenciales de Windows para el proceso de autenticación. Es por esto que los atacantes utilizan herramientas como keyloggers y formularios web maliciosos para poder capturar estas credenciales. Estas herramientas permiten capturar y almacenar cada "string" que se ingresa al presionar una tecla o capturar la información que se digita y envía a través de formularios web. Los keyloggers pueden capturar credenciales de acceso, contraseñas a archivos y muchos otros datos valiosos de la organización destino.

Cuando las credenciales de acceso no están disponibles o son ineficaces, los atacantes pueden utilizar métodos alternativos como, por ejemplo: explotación de vulnerabilidades, ingeniería social, distribución de medios físicos infectados como memorias USB, CD, tarjetas de memoria, sobornar personas, utilitarios de captura de pantalla y otras técnicas. Para los atacantes detrás de estas intrusiones, los TTP (Técnicas, Tácticas y Procedimientos) son solo un medio para un fin, ya que utilizarán cualquier medio a su alcance para completar su misión.

c. Persistencia y Asset Targeting

Vulnerar las defensas perimetrales de un objetivo y establecer un punto de acceso dentro de la red requieren de un esfuerzo relevante, por lo que el concepto de mantener "persistencia" es muy importante durante todo el proceso en el cual los atacantes se mantienen dentro de la red, realizando sus actividades maliciosas asociadas a la operación. Para llevar a cabo este concepto, los atacantes utilizan distintas estrategias, técnicas, tácticas y procedimientos para para mantener el acceso.

Los delincuentes saben que la mayoría de las organizaciones utiliza herramientas de seguridad en sus entornos, por lo que extreman todas las medidas para garantizar que sus herramientas no sean detectadas. Esto en la práctica significa producir o personalizar malware y reescribir o reempaquetar herramientas de uso común. Luego, estas herramientas personalizadas se prueban contra los motores de antivirus actualizados y otras herramientas de seguridad para evaluar si son detectadas. Dado que los adversarios pueden acceder a las mismas herramientas de seguridad que los objetivos atacados, es que tienen ventaja para poder desplegar este tipo de herramientas en los objetivos atacados y así generar la persistencia deseada.

Una vez detectada una intrusión, la organización objetivo puede examinar los sistemas afectados, recuperar malware y herramientas maliciosas, analizar el tráfico de red y recopilar otros indicadores de compromiso. Una vez que se recopilan estos indicadores, es posible desarrollar contramedidas y posteriormente verificar los sistemas en busca de archivos comprometidos conocidos, entradas de registro, patrones de memoria y otros artefactos del sistema. La actividad de la red se puede monitorear en búsqueda de tráfico a direcciones IP que se sabe están involucradas en la intrusión. Estas técnicas si bien son útiles, se limitan a detectar indicadores y patrones conocidos recopilados de incidentes actuales o anteriores.

Los atacantes están familiarizados con estas técnicas de respuesta, por lo que planifican e implementan una estrategia de persistencia basada en la diversidad de código malicioso y conexiones hacia el exterior. Esto se logra mediante el uso de una variedad de malware personalizado en forma de ejecutables, servicios y controladores adicionales colocados en múltiples sistemas en todo el entorno atacado, como se muestra en la Figura 9. Las piezas de malware son configuradas para comunicarse con una variedad de hosts de C2C (Comando y Control), dificultando el proceso de detección.

Las piezas maliciosas a menudo no son activadas todas de una vez, más bien son configuradas y activadas solo después de transcurrido un intervalo muy largo de días, semanas o incluso meses. Asimismo, se han identificado campañas que incluyen código que monitorea el estado de otros sistemas infectados en el entorno del objetivo. Si se determina que el sistema o los sistemas infectados primarios están inactivos o ya no están infectados, el malware se desconecta del servidor de comando y control, activando un nuevo punto de entrada para los atacantes.

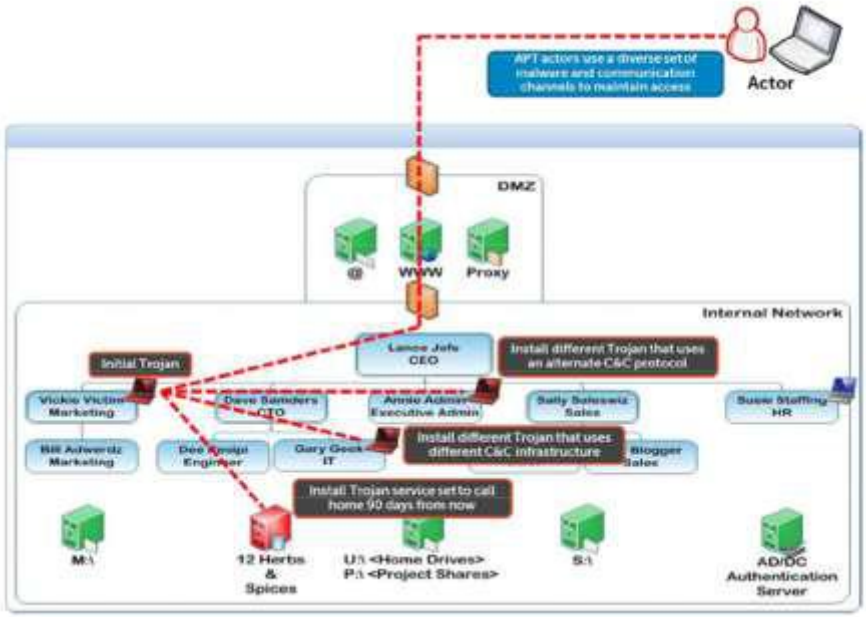

Figura 9: Instalación de Malware Adicional u otro método de persistencia en el objetivo.

La diversidad de técnicas, tácticas y procedimientos utilizadas por los atacantes pueden dificultar la identificación de los sistemas comprometidos. Por eso es importante aprovechar los recursos disponibles para responder a este tipo de incidentes, tales como análisis de logs, netflow, y análisis forenses de disco. Esto recursos pueden ayudar en el proceso de detección, pero no hay que dejar de lado que los atacantes conocen este tipo de tecnología de respuesta y, en algunos casos, pueden eludir el monitoreo o destruir los registros de su actividad de manera de dificultar aún más el proceso de detección.

También es muy importante poder identificar los puntos no tradicionales para la instalación de componentes maliciosos, tales como servidores, routers, firewalls, impresoras, y puntos de acceso inalámbricos, cuya utilización es otra forma en que los atacantes mantienen la persistencia.

d. Exfiltración

La exfiltración de datos es una técnica utilizada por atacantes maliciosos que permite copiar y transferir datos confidenciales de manera ilícita desde una red comprometida. La exfiltración de datos se realiza normalmente de forma remota, y puede ser extremadamente difícil de detectar, dado que se “camufla” dentro del tráfico de red valido o "normal”. Esto permite a los atacantes poder realizar este tipo de actividades sin ser detectados, hasta que ya se haya logrado parcial o completamente el objetivo buscado. Los principales tipos de datos que se buscan extraer incluyen registros financieros, información de clientes y propiedad intelectual / secretos comerciales, entre otros.

En muchos casos, los atacantes maliciosos tienen como objetivo documentos o tipos de datos específicos, previo a que se lance el ataque. En otros casos, saben que es probable que existan datos valiosos en la red, pero no hay seguridad de donde residen, por lo tanto requieren de tiempo para poder identificar la ubicación de este tipo de información.

Un método popular de búsqueda y exfiltración es tomar todo lo que pueda ser de interés desde la red, esto incluye todo tipo de documentos, correos electrónicos y otros archivos identificables en la red. Algunas ubicaciones examinadas con frecuencia incluyen carpetas de documentos del usuario comprometido, unidades compartidas ubicadas en file servers, archivos locales de correo electrónico y el correo electrónico del servidor de correo electrónico central. Identificar y recopilar documentos asociados a la extensión del archivo también es una táctica popular para este tipo de actividades. Las extensiones comúnmente revisadas son .DOC, .DOCX, .XLS, .XLSX, .PPT, .PPTX y .PDF.

También se han identificado campañas donde los atacantes buscan tipos de extensiones específicas (si los atacantes conocen aplicaciones personalizadas o atributos únicos de interés en el entorno de destino). Tomar todos los documentos no es necesariamente un indicador de que los atacantes no saben lo que buscan.

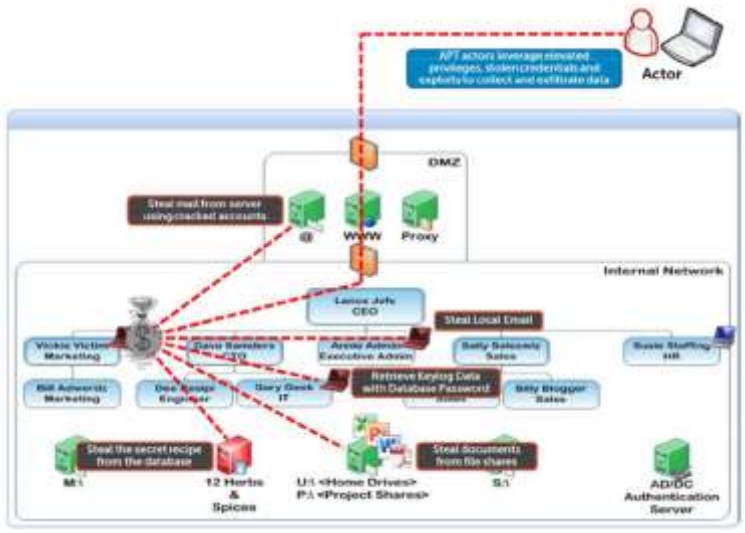

Figura 10: proceso de exfiltración de datos desde una red comprometida por un atacante APT

Tomar todos los datos disponibles de una red puede ser demasiado "ruidoso", creando grandes flujos de datos y otro tipo de indicadores que podrían alertar la existencia de un atacante malicioso operando dentro de la red. Para evitar esta situación, algunos atacantes adoptan un enfoque más específico, buscan documentos a través de palabras clave y metadatos que indiquen que el documento puede ser de interés para el atacante. Varias muestras de malware recuperadas y analizadas de intrusiones específicas han incluido capacidades de búsqueda de palabras claves.

Incluso, algunos programas maliciosos pueden preprogramarse para buscar tipos de palabras clave y extensiones sin interacción de control externo, esta capacidad permite al malware implementado encontrar y filtrar datos automáticamente.

En el caso de que el atacante solo tenga acceso a la cuenta del usuario y, por lo tanto, a su nivel de privilegios en el sistema, la obtención de información puede estar limitada solamente al equipo comprometido. Sin embargo, si el atacante tiene la capacidad de elevar los privilegios (ya sea a través de técnicas de hash o de obtener credenciales para cuentas de mayor privilegio), podría acceder a todos los archivos que se encuentran en carpetas dentro de los servidores de archivos administrados de forma centralizada y para muchas estaciones de trabajo utilizando el mismo acceso privilegiado obtenido previamente.

Un caso similar es el del correo electrónico. Con la contraseña de la cuenta de usuario de un individuo, el atacante puede obtener los archivos de correo electrónico locales, como los archivos PST (carpeta personal) utilizados por Microsoft Outlook. Así, cuando la autenticación de correo electrónico central está controlada por la cuenta de usuario de Windows, la cuenta de usuario comprometida también permite al atacante obtener todos los mensajes de correo electrónico, incluidos los archivos adjuntos del servidor de correo central. Si el atacante obtiene acceso privilegiado al servidor de correo electrónico, es posible que instale software malicioso para monitorear y capturar todos los mensajes entrantes y salientes. Este acceso permite tener visibilidad de todo el correo electrónico dentro de la organización.

También es posible recopilar otros datos mediante la instalación de “sniffers” o programas que permitan capturar tráfico de red. Este tipo de programas pueden recopilar la totalidad de la información que fluye por la red o un subconjunto, según la necesidad del atacante. Todos estos datos se recopilan y envían a una ubicación centralizada donde los atacantes pueden recuperarlos de manera parcial, evitando detecciones que podrían ser provocadas por muchos hosts que se ponen en contacto con un sitio de descarga remoto. También permite a los actores extraer datos en “partes”, asegurando que al menos una gran cantidad de datos puedan extraerse antes de que el personal de seguridad pueda responder.

Para eludir las tecnologías de prevención de pérdida de datos (DLP), que buscan palabras clave o patrones en los documentos que salen de la red, los atacantes almacenan los datos robados en archivos comprimidos cifrados o con contraseña, de manera de evitar este tipo de detección. La exfiltración de datos generalmente logra “bypassear” controles perimetrales tales como proxies web, reglas de firewall y listas de control de acceso. Los códigos maliciosos utilizados por los atacantes tienen capacidades avanzadas que inutilizan este tipo de controles.

4. Principales grupos APT

Los grupos APT generalmente reciben nombres asignados por sus descubridores, aunque muchos ataques avanzados de amenazas persistentes han sido descubiertos por más de un investigador, por lo que algunos son conocidos por más de un nombre.

Algunos ejemplos de amenazas persistentes avanzadas incluyen:

La familia de **malware Sykipot APT**, la cual aprovecha las fallas en Adobe Reader y Acrobat. Se detectó en 2006 y, según los informes, continuaron los ataques con malware hasta 2013. Los atacantes utilizaron la familia de malware Sykipot como parte de una serie de ataques cibernéticos de larga duración que apuntan principalmente a organizaciones estadounidenses y británicas, incluidas agencias gubernamentales, contratistas de defensa y compañías de telecomunicaciones. Los atacantes utilizaron un ataque de suplantación de identidad que incluía enlaces y archivos adjuntos maliciosos que contenían ataques de día cero en correos electrónicos específicos.

La operación de **ciberespionaje GhostNet** fue descubierta en 2009. Ejecutados desde China, los ataques se iniciaron a través de correos electrónicos de suplantación de identidad que contenían archivos adjuntos maliciosos. Los ataques comprometieron computadoras en más de 100 países. Los atacantes se centraron en obtener acceso a los dispositivos de red de los ministerios y embajadas del gobierno. Estos ataques permitieron a los atacantes controlar estos dispositivos comprometidos, convirtiéndolos en dispositivos de escucha y grabación al encender de forma remota sus cámaras y capacidades de grabación de audio.

El **gusano Stuxnet**, utilizado para atacar el programa nuclear de Irán, fue detectado por investigadores de ciberseguridad en 2010. Todavía se considera una de las piezas de malware más sofisticadas jamás detectadas. El malware apuntó a los sistemas SCADA (control de supervisión y adquisición de datos) y se propagó con dispositivos USB infectados. Los Estados Unidos e Israel han estado vinculados al desarrollo de Stuxnet, y aunque ninguna de las naciones ha reconocido oficialmente su papel en el desarrollo del gusano, ha habido confirmaciones no oficiales de que fueron responsables de Stuxnet.

APT28, Los investigadores de Trend Micro identificaron al APT28, el grupo de amenaza persistente avanzado ruso también conocido como Fancy Bear, Pawn Storm, Sofacy Group y Sednit en 2014. APT28 se ha relacionado con ataques contra objetivos militares y gubernamentales en Europa del Este, incluyendo Ucrania y Georgia, así como campañas dirigidas a organizaciones de la OTAN y contratistas de defensa estadounidenses.

APT29, el grupo ruso de amenaza persistente avanzada también conocido como Cozy Bear, se ha relacionado con una serie de ataques, incluido un ataque de spear phishing en 2015 en el Pentágono, así como los ataques de 2016 en el Comité Nacional Demócrata.

APT34, un grupo avanzado de amenazas persistentes vinculado a Irán, fue identificado en 2017 por investigadores de FireEye, pero ha estado activo desde al menos 2014. El grupo de amenazas se

ha dirigido a compañías en el Medio Oriente con ataques contra finanzas, gobierno, energía, productos químicos y empresas de telecomunicaciones.

APT37, también conocido como Reaper, StarCruft y Group 123, es una amenaza persistente avanzada vinculada a Corea del Norte, que se cree que se originó alrededor de 2012. APT37 se ha conectado a ataques de spear phishing que explotan una vulnerabilidad de día cero de Adobe Flash.

APT38, también conocido como Lazarus, es un grupo de amenaza persistente con motivaciones financieras que está respaldado por el régimen de Corea del Norte. El grupo tiene como objetivo principalmente a bancos e instituciones financieras y se ha dirigido a más de 16 organizaciones en al menos 13 países desde el año 2014.

APT41, también conocido como Doubledragon, es un es un avanzado grupo de cibercriminales que lleva a cabo actividades de espionaje asociado al estado chino, además de actividades con motivaciones financieras que potencialmente están fuera del control estatal.

Figura 11: Distintos grupos de amenazas persistentes avanzadas (APT)

5. Conclusiones

Las APT son amenazas sofisticadas, específicas y en evolución, sin embargo, ciertos patrones pueden identificarse en sus actividades maliciosas. En este artículo, nos enfocamos en la identificación de estos puntos en común. Si bien las medidas de ciberseguridad tradicionales son una buena práctica, son absolutamente insuficientes para poder enfrentar de manera seria la defensa contra organizaciones de este tipo. Para mitigar los riesgos que plantean las APT, los equipos de defensa deben trabajar en obtener conocimientos avanzados de las técnicas, tácticas y procedimientos involucrados en los ataques, y desarrollar nuevas capacidades que aborden las características específicas de los ataques APT.

Algunas consideraciones para enfrentar amenazas avanzadas del tipo APT:

• Es necesario tener en cuenta las capacidades de los actores detrás este tipo de amenazas avanzadas al planificar las estrategias de defensa que se desean implementar.

• Identificar todos los activos tecnológicos que componen el alcance a defender, es muy relevante para tener visibilidad total del equipamiento.

• En el desarrollo de arquitecturas de redes y sistemas se deben contemplar medidas de ciberseguridad avanzadas, ya que esto facilita la tarea de defender las infraestructuras tecnológicas de la organización.

• La segmentación de los recursos de la red ya sea por requisitos de acceso, servicios ofrecidos u otras estrategias compatibles con las necesidades de la organización, hace posible tener mejor visibilidad y control de los recursos de red, dificultando el trabajo a un atacante.

• Una correcta estrategia de registro y monitoreo de “logs” es clave para poder enfrentar un incidente del tipo APT. Una correcta gestión de los “logs” hará que sea mucho más difícil para los actores de la APT camuflar sus operaciones, eliminar sus huellas y hará que los esfuerzos de respuesta a incidentes sean más efectivos y eficientes.

• Un plan de comunicaciones bien desarrollado que ayude a los usuarios a comprender las amenazas y cómo identificarlas, también ayudará a mitigar los intentos de ingeniería social.

• Mantener el entorno de TI a través de la evaluación de vulnerabilidades y la gestión eficiente de parches es un paso importante para reducir al mínimo las oportunidades de intrusiones iniciales.

• Eliminar los privilegios administrativos locales de las cuentas de las estaciones de trabajo de los usuarios y limitar el acceso solo a lo necesario, ayuda a evitar el escalamiento de privilegios y los esfuerzos de movimiento lateral.

• Desarrollar pruebas de penetración y ejercicios prácticos de simulación de escenarios de ataque que emulan actores del tipo APT, son herramientas valiosas de autoevaluación y capacitación para el personal del equipo de defensa.

• Generar conciencia de estos riesgos dentro de la organización es fundamental para formar estrategias de defensa eficaces. Sin un conocimiento profundo de las amenazas, las estrategias defensivas y el gasto serán ineficaces.

Con todas estas técnicas de detección y mejores prácticas implementadas, las organizaciones estarán en una mejor posición para reaccionar proactivamente ante una amenaza del tipo APT, que de otra manera sería muy difícil abordar. Sin embargo, debido a la naturaleza persistente de estas amenazas, las organizaciones deben evaluar continuamente el entorno, invertir en capacidades de ciberinteligencia, constantemente evaluar las vulnerabilidades en las plataformas tecnológicas, afinar y mejorar de forma continua las capacidades de monitoreo para detectar intrusiones con capacidades, en lo posible lo más cercano al tiempo real, incluyendo alertas de cualquier tipo de anomalías encontrada en la red.

Es importante recordar que frente a este tipo de amenazas avanzadas no existe una “bala de plata” más bien una estrategia escalonada, permitirá mejorar la postura de ciberseguridad de la organización y así poder detectar, responder y erradicar en el menor tiempo posible.

6. Anexos y referencias

https://en.wikipedia.org/wiki/PLA_Unit_61398

http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

https://www.cfr.org/interactive/cyber-operations/pla-unit-61398

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

https://blog.trendmicro.com/trendlabs-security-intelligence/the-siesta-campaign-a-new-targeted-attack-awakens/

https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-oceansalt-delivers-wave-after-wave/

https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf

https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=f1265df5-6e5e-4fcc-9828-d4ddbbafd3d7&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

https://attack.mitre.org/groups/G0006/

https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html

7. Reconocimiento

El Equipo de Respuestas ante Incidentes de Seguridad Informática (CSIRT) del Gobierno de Chile quiere agradecer la especial colaboración entregada por Juan Roa Salinas, Gerente de Ciberseguridad y Defensa en Redbanc y su valioso equipo, y en especial por el constante aporte que hace al fortalecimiento y fomento de cultura de ciberseguridad en nuestro país.

8. Palabras del editor

Análisis de Amenazas Cibernéticas es un trabajo creado desde las inquietudes e intereses de quienes están comprometidos directamente en la primeria línea de la ciberseguridad. Durante sus 26 ediciones esta publicación brindó un espacio de expresión a los analistas y especialistas que administran, gestionan, crean, educan, fomentan y se forman en esta materia. En principio fueron investigaciones de nuestros profesionales en el CSIRT con el apoyo del área de comunicaciones de nuestra unidad, pero luego extendimos la invitación a quienes estaban vinculados con nosotros en convenios de colaboración, así como a investigadores cercanos y especialistas reconocidos. Nuestro objetivo fue involucrar a la comunidad cibernética de la que somos parte para que los especialistas pudieran reflejar en estas páginas el estado de la ciberseguridad nacional. Fue un gran esfuerzo que involucró muchas voluntades y nos permitió conocer fenómenos y tipos específicos de amenazas cibernéticas, así como herramientas que nos pueden ayudar a contenerlas. Pero además nos dio la posibilidad de explorar por primera vez nuestras propias capacidades de investigación. Fue un reto muy especial que abrió un espacio público para compartir y debatir, en forma escrita, sobre los riesgos cibernéticos que enfrentamos como sociedad. En síntesis, esta publicación buscó crear conciencia del enorme esfuerzo que realizamos y nos queda por delante como país.

Hoy tenemos que hacer una pausa en esta primera experiencia. La expectativa es volver a retomar este trabajo en el corto plazo, pero es necesario rediseñar su estructura, con un sentido multidisciplinario, pero sin perder el énfasis científico en su elaboración.

Queremos agradecer a todas las personas que colaboraron con esta publicación, entre los autores, las organizaciones que los respaldaron, así como los correctores, editores y por supuestos a los lectores. Queremos destacar especialmente a los investigadores Carlos Silva, Paula Moraga, Natalia Pérez, Gabriela Sepúlveda, Juan Moraga, Hernán Espinoza, Patricio Quezada, Andrés Godoy, Carlos Landeros, Benjamín Aravena, Carlos Montoya, Énida Casanova, Ching-Yuih Chiu, Pía Salas, Juan Pablo Arias, Miguel Kurte, Germán Fernández, Jaime Gómez, Jennifer Nilo, Elsa Bravo y Juan Roa. Un agradecimiento especial merece el investigador Nicolás Fica, cuyo trabajo no pudo ser compartido en esta colección. Sabemos que pronto se formará la consciencia suficiente para que todos los esfuerzos científicos puedan tener cabida en nuestra sociedad. Junto a todos ellos, queremos agradecer especialmente a quien diseñó cada una de las portadas que acompañaron estos trabajos, las que fueron producto del talento de Jaime Millán. También agradecemos la gestión editorial, de coordinación y el esfuerzo del equipo de comunicación, así como el respaldo entregado a este proyecto por nuestro Director, Sr. Carlos Landeros Cartes.

Esperamos que este trabajo haya sido de su agrado y que pueda servir como un aporte en perspectiva científico a la ciberseguridad de nuestro ecosistema nacional.