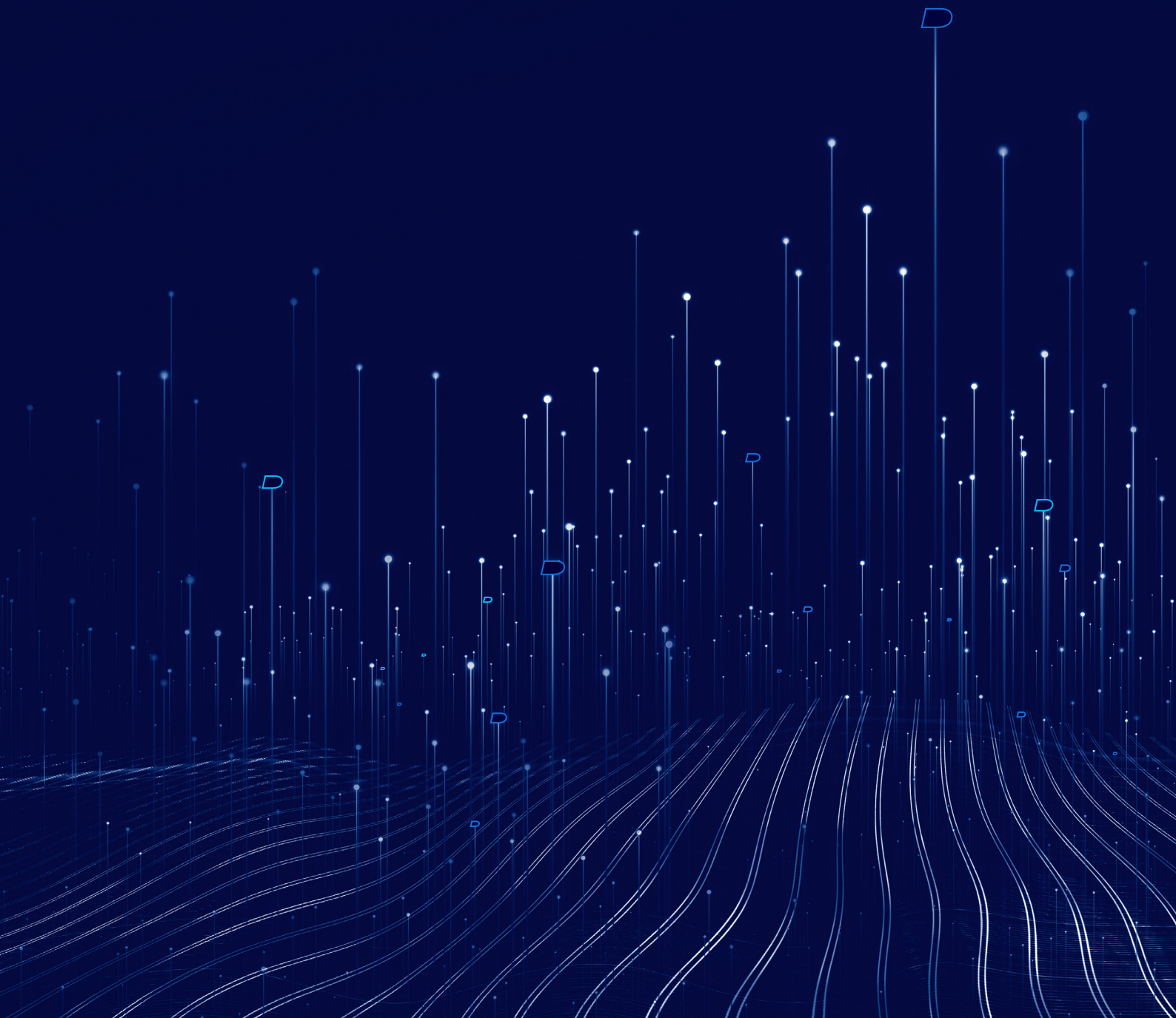
BlackBerry. Intelligent Security. Everywhere.

2022 INFORME DE AMENAZAS



CONTENIDO

INTRODUCCIÓN

El Informe de amenazas 2022 de BlackBerry no es una simple mirada retrospectiva de los ataques cibernéticos del 2021. Se trata de un enfoque de alto nivel de los problemas que afectan la ciberseguridad en todo el mundo, tanto de manera directa como indirecta. Aborda elementos de la explotación de infraestructura crítica, la inteligencia artificial (IA) adversarial, los agentes de acceso inicial (IAB), la gestión de eventos críticos (CEM), la detección y respuesta extendidas (XDR), y otros problemas que dan forma al entorno de seguridad actual.

En este informe, se analizan los principales eventos de seguridad del 2021 y cómo pueden dar forma al panorama de la ciberseguridad en el futuro.

En este informe, se analizan temas que enfrentan las personas y las organizaciones de todo el mundo. Como siempre, representa nuestra pieza única del rompecabezas de seguridad general. Nuestro objetivo es mejorar la postura de seguridad global compartiendo nuestra información, nuestras predicciones y nuestras experiencias con todos. Para lograrlo, en el informe se analizan los principales eventos de seguridad del 2021 y cómo pueden dar forma al panorama de la ciberseguridad en el futuro. Se profundiza en los problemas de seguridad cibernética que enfrentamos hoy en día y se ofrece a los lectores información adicional y contexto para que realicen su propio análisis reflexivo.

Dicho esto, los lectores que ansían nuestro análisis anual de los 10 principales ataques de malware que BlackBerry observó durante el año que pasó no se sentirán decepcionados. Tampoco aquellos que aguardan con gran expectativa nuestra revisión del año respecto de respuesta ante incidentes (IR), las actualizaciones legislativas anuales en materia de seguridad cibernética y las predicciones a corto plazo. Volvimos a incluir muchas de las secciones que nuestros lectores disfrutaron en entregas previas de los informes de amenazas de BlackBerry. Además, este año abordamos los ataques a la cadena de suministro, los nuevos y peligrosos lenguajes de programación, la seguridad en el metaverso, la informática cuántica, las campañas de ransomware y otros temas emergentes de relevancia.

Es posible que la fluidez de los ataques cibernéticos modernos exija a las organizaciones reconsiderar con frecuencia su enfoque respecto de la ciberseguridad y analizar nuevas opciones. Deben evaluar constantemente tecnologías y enfoques innovadores que superen a las soluciones de antivirus (AV) tradicionales, lo que va desde la IA con prioridad en la prevención hasta la adopción de una arquitectura de confianza cero. En consecuencia, el Informe de amenazas 2022 de BlackBerry ofrece sugerencias sobre las estrategias y tecnologías de seguridad cibernética que podrían haber evitado las principales fallas de seguridad del año pasado.

Esperamos sinceramente que la información incluida en este documento ayude a proteger a los usuarios y a mantener seguras a las organizaciones durante 2022 y en el futuro.

RESUMEN EJECUTIVO

Los eventos cibernéticos más publicitados del 2021 incluyeron ataques de ransomware a infraestructura crítica y compañías de tecnología. El grupo de amenazas de ransomware REvil atacó a Acer, a JBS Foods y a otras compañías, mientras que DarkSide paralizó las tareas de Colonial Pipeline y Avaddon se infiltró en los sistemas de AXA. En pocas palabras, el alcance y el éxito de diferentes grupos de amenazas el año pasado, en particular contra compañías del sector privado consideradas parte de la infraestructura nacional, resultaron inquietantes. Los gobiernos respondieron a los ataques: los países del G7 y los aliados de la OTAN dieron prioridad a la seguridad cibernética en la agenda de políticas públicas. El presidente de los EE. UU., Joe Biden, aprobó un decreto para "Mejorar la ciberseguridad de la nación", mientras que el Departamento de Justicia conformó el grupo de trabajo de extorsión digital y ransomware.

A medida que avanzaba el año, una vulnerabilidad de día cero en servidores de Microsoft® Exchange se transformó en una crisis después de que el grupo HAFNIUM explotara la falla. Otros atacantes aprovecharon rápidamente la oportunidad, aplicaron ingeniería inversa al parche y atacaron a organizaciones de todo el mundo. La rápida proliferación de ataques similares al del grupo HAFNIUM reforzó la importancia de que tanto las organizaciones como las personas mantengan el software actualizado. Sin embargo, actualizar el software como práctica reactiva no evita el ataque a una víctima inicial, o sea, al "cordero ofrecido en sacrificio". Esto hace que muchas organizaciones busquen enfoques de seguridad alternativos, como el marco de confianza cero, la XDR y la IA con prioridad en la prevención.

A fines del 2020, un ataque a la cadena de suministro de SolarWinds fue noticia internacional. El mismo estilo de ataque resurgió en el 2021, cuando el software VSA de Kaseya se vio comprometido y, en última instancia, afectó a más de 1000 empresas. Los ataques a la cadena de suministro suelen aprovechar la confianza ya establecida entre los proveedores y los clientes a fin de propagarse, otro motivo para adoptar un marco de confianza cero. Si bien los ataques a las grandes organizaciones predominaron entre las noticias del 2021, las pequeñas y medianas empresas también sufrieron innumerables ataques, tanto directamente como a través de la cadena de suministro. Los investigadores de amenazas de BlackBerry descubrieron que estas empresas presentaban un promedio de 11 a 13 amenazas por dispositivo, un número mucho más elevado que las empresas de mayor tamaño.

Los atacantes deben su éxito del 2021 a diversos factores. Muchos aprendieron a adoptar e imitar las capacidades del sector privado mediante el uso de proveedores de servicios como los de ransomware como servicio (RaaS), infraestructura como servicio (IaaS) y malware como servicio (Maas) con el fin de sacar ventaja de los ataques maliciosos. Otros crearon una capa de ofuscación entre ellos y sus objetivos haciendo uso de agentes de acceso inicial (IAB) y haciéndose pasar por otros grupos de amenazas. Se aprovecharon las vulnerabilidades de seguridad de los nuevos lenguajes de programación para lograr algún efecto, y Go, D, Nim y Rust fueron parte del panorama de amenazas. Cobalt Strike se mantuvo activo como herramienta fundamental para las redes de comando y control con el fin de propagar malware y ataques.

300 %

Los ataques de phishing por SMS (smishing) aumentaron un 300 % en América del Norte durante el último año.

Se avanzó en la integración de la seguridad a los vehículos conectados con la Organización Internacional de Normalización (ISO), la Sociedad de Ingenieros Automotrices (SAE) y la Organización de las Naciones Unidas (ONU) al proporcionar orientación firme a las empresas automotrices. Las aplicaciones móviles siguieron siendo notoriamente inseguras. La aplicación vulnerable SHAREit, que permitía la ejecución de código de manera remota, se descargó más de 1000 millones de veces. Estudios recientes determinaron que el 63 % de las aplicaciones móviles probadas emplean código abierto, el cual se sabe que es vulnerable. Además de los inconvenientes de los usuarios de teléfonos inteligentes, los ataques de phishing por SMS (smishing) aumentaron un 300 % en América del Norte durante el último año.

Los ataques cibernéticos del 2021 afectaron a personas de todos los niveles, desde grandes organizaciones hasta propietarios individuales de teléfonos móviles. Los informes internos de BlackBerry demuestran que todas las industrias son susceptibles a ataques cibernéticos. Los mismos problemas de ciberseguridad que amenazan a las organizaciones sin fines de lucro también representan riesgos para las compañías de transporte, las organizaciones públicas, los servicios públicos, las organizaciones de atención médica, las instituciones financieras, etc. Fue un recordatorio de que nadie está a salvo. Cuando se trata de ciberataques, no existe la inmunidad total. Sin embargo, existe una serie de innovaciones y enfoques de seguridad cibernética que ofrecen a las organizaciones una protección más sólida. Por ejemplo, las organizaciones que buscan nuevas medidas de seguridad efectivas deberían analizar la adopción de un marco de confianza cero. También podrían usar tecnología con prioridad en la prevención, migrar a una plataforma de XDR o contratar a un equipo de XDR administradas.

FEBRERO

Una planta de potabilización de agua en Oldsmar, Florida, se vio comprometida cuando un atacante intentó envenenar el suministro de agua.

CD Projekt Red se vio atacada por el ransomware HelloKitty.

MARZO

La cadena Channel Nine de Australia vio interrumpidas sus transmisiones debido a ataques cibernéticos.

La University of Highlands and Islands fue atacada por Cobalt Strike.

CNA Insurance recibió el ataque de Evil Corp.

Escuelas públicas en Buffalo, Nueva York fueron golpeadas con ransomware.

Servidores de Microsoft Exchange se vieron vulnerados por el grupo HAFNIUM.

ABRIL

El equipo de baloncesto Houston Rockets (NBA) fue afectado por Babuk.

MAYO

Colonial Pipeline fue víctima de un ataque de DarkSide.

AXA fue atacada por Avaddon.

Brenntag (distribuidor de productos químicos) fue víctima de DarkSide.

Acer fue atacada por REvil.

JBS Foods fue atacada por REvil.

El Ejecutivo de Servicios de Salud (HSE) de Irlanda fue afectado por Conti.

JULIO

Se lanzaron ataques de ransomware en Chile, Italia, Taiwán y el Reino Unido por parte del grupo de amenazas LockBit.

Kaseya sufrió un ataque a la cadena de suministro por parte de REvil.

NOVIEMBRE

La plataforma de inversiones Robin Hood sufrió una filtración que afectó la información de siete millones de cuentas de usuarios.

DICIEMBRE

Las vulnerabilidades de Log4j fueron reveladas y explotadas por múltiples atacantes.

CRONOLOGÍA DE ATAQUES CIBERNÉTICOS DE ALTO PERFIL DEL 2021

Entre los numerosos ataques cibernéticos de alto perfil que fueron noticia en el 2021, algunos de los incidentes más notables informados incluyen los siguientes:

Estos reconocidos incidentes fueron noticia a nivel nacional o internacional debido a su considerable escala, sofisticación, crueldad o demandas de rescate. Sin embargo, estas historias no representan el verdadero número de víctimas afectadas por el delito cibernético en organizaciones públicas y privadas. Más del 70 % de las pequeñas y medianas empresas han sufrido ciberataques, según un estudio del Ponemon Institute. De las organizaciones atacadas, el 60 % cierra sus actividades de forma definitiva en un plazo de seis meses. Los organismos gubernamentales y las grandes compañías pueden sobrevivir a un ataque cibernético; sin embargo, esto suele ser una sentencia de muerte para las empresas pequeñas y medianas.

Los ataques cibernéticos del 2021 afectaron a múltiples industrias y organizaciones de todos los tamaños, y son un claro recordatorio de que nadie está a salvo. No existe la inmunidad total ante los atacantes dedicados y cualquiera que opere en el espacio digital puede ser el próximo objetivo. Teniendo en cuenta que los intentos de piratería maliciosos ocurren cada 39 segundos, una organización desaparecerá por completo si emplea medidas de seguridad reactivas. Afortunadamente, las herramientas con prioridad en la prevención, las tecnologías de IA predictiva y los marcos de confianza cero pueden ofrecer a las organizaciones una alternativa eficaz a las soluciones de ciberseguridad tradicionales.

LAS AMENAZAS CIBERNÉTICAS

COBALT STRIKE

Ningún informe de amenazas estaría completo sin al menos una mención pasajera sobre Cobalt Strike. Este año, BlackBerry recopiló información y tendencias de un conjunto de datos interno de más de 7000 servidores de equipo y 60 000 balizas de Cobalt Strike.

El seguimiento y el monitoreo de los servidores de equipo de Cobalt Strike que se encuentran en circulación pueden ayudar en gran medida al ciclo de vida de la inteligencia sobre amenazas. Hacer esto proporciona información invaluable para adaptar las soluciones de seguridad y ayudar con las investigaciones de incidentes. Encontrará un desglose detallado de la inteligencia sobre amenazas obtenida a partir del análisis de Cobalt Strike en el nuevo libro electrónico del equipo de Investigación e Inteligencia de Amenazas de BlackBerry, *"Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence"* (Balizas en la oscuridad: guía de inteligencia sobre amenazas cibernéticas).

Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence (Balizas en la oscuridad: guía de inteligencia sobre amenazas cibernéticas)

Nuestra revisión anual de la actividad de Cobalt Strike comienza con algunas de las estadísticas más interesantes relacionadas con los despliegues del servidor de equipo.

Por ejemplo, observe los 10 principales números de sistema autónomo (ASN) y bloques de red (rangos de direcciones IP consecutivas) responsables de alojar la carga de balizas de gran versatilidad de Cobalt Strike. Esto demuestra una tendencia fascinante: es cada vez más probable que los atacantes empleen proveedores en la nube legítimos para el alojamiento. Esto permite que los operadores de malware oculten su tráfico de los sistemas de monitoreo, lo que dificulta la tarea de bloqueo automático. Además de las dificultades de detección, entre los 20 principales proveedores se incluyen diferentes compañías grandes y de buena reputación. En la Figura 1, se muestran los 10 principales ASN que alojan la baliza de Cobalt Strike:

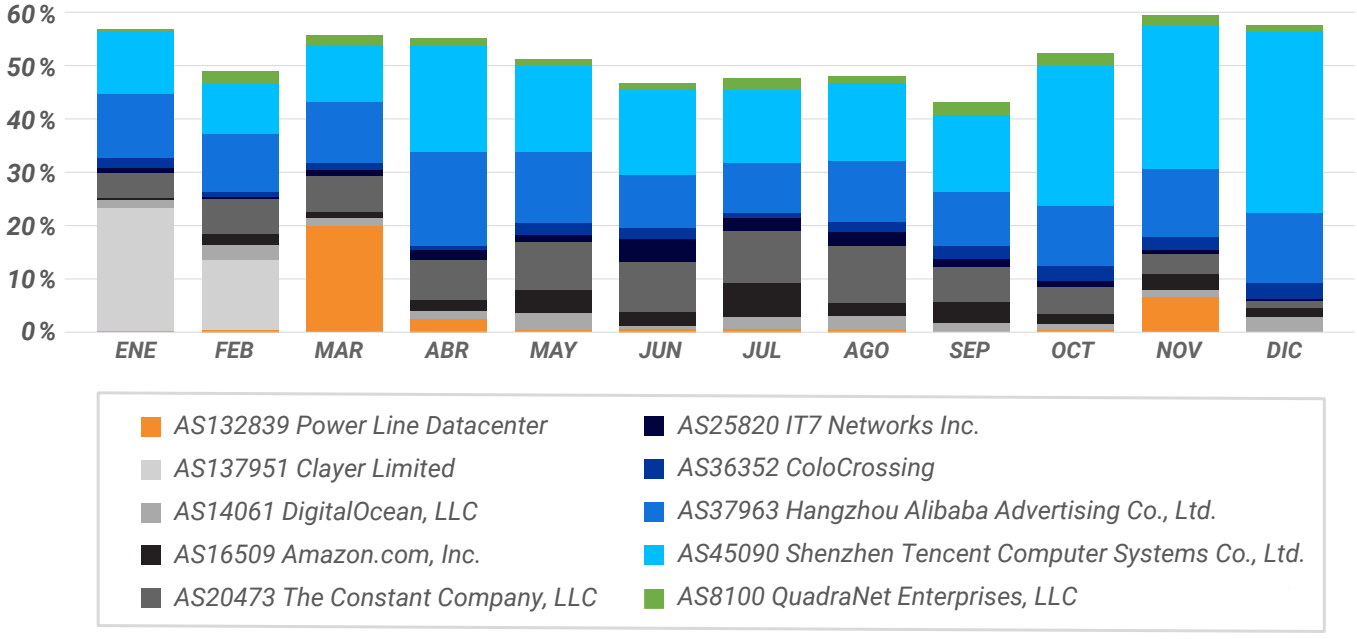


Figura 1: Los 10 principales ASN responsables de alojar la carga (baliza) de Cobalt Strike

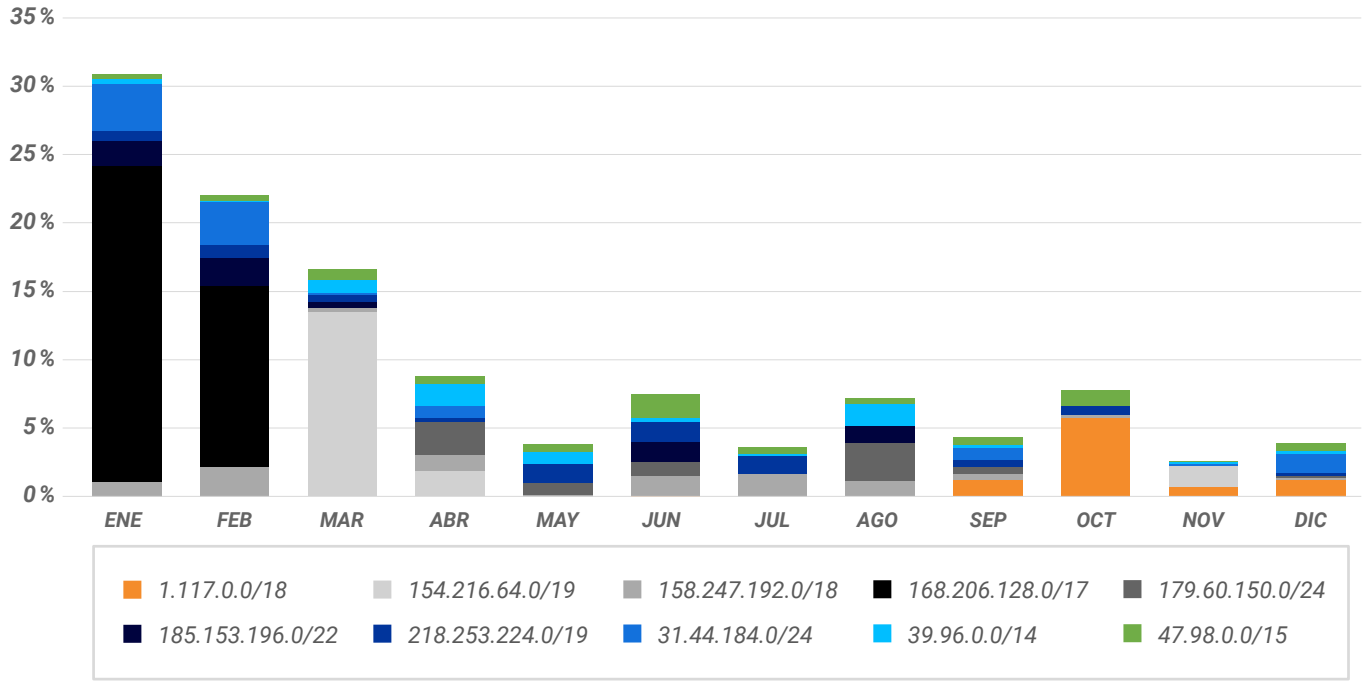


Figura 2: Los 10 principales bloques de red responsables de alojar las balizas

Desde el punto de vista geográfico, los siguientes países son los 10 principales utilizados para alojar balizas:

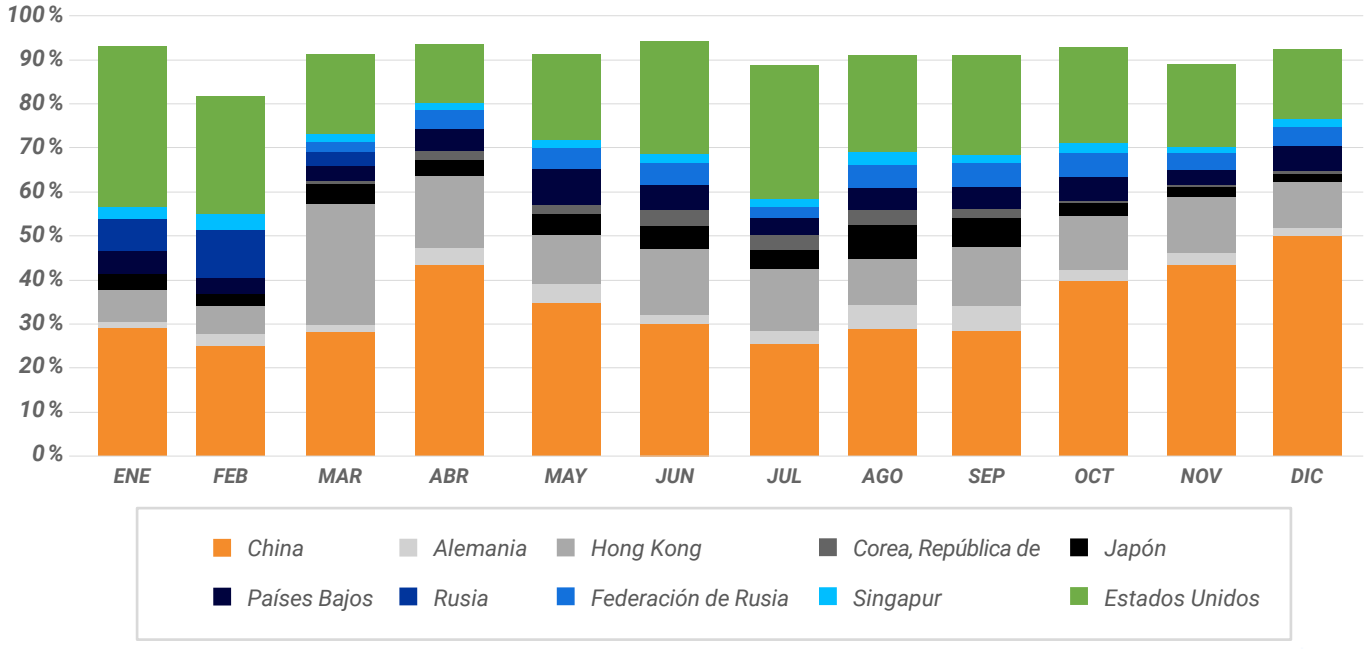


Figura 3: Los 10 principales países que alojan servidores de equipo de Cobalt Strike

Los puertos 80, 443 y 8080 son los más activos (como se observa en la Figura 4) que presentan balizas de los servidores de equipo. Por lo general, estos puertos están abiertos en la mayoría de los entornos, lo que los convierte en una opción obvia para enrutar el tráfico de comando y control (C2).

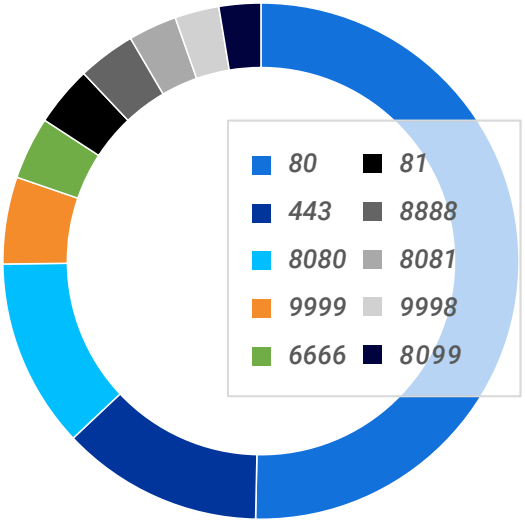


Figura 4: Los 10 principales puertos que presentan cargas de balizas

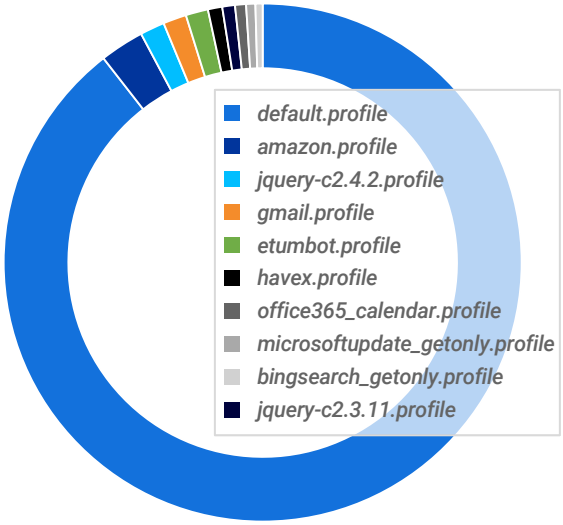


Figura 5: Los 10 principales perfiles adaptables utilizados por la baliza de Cobalt Strike

Las balizas de Cobalt Strike se pueden configurar en gran medida a través del uso de perfiles adaptables de C2, los cuales especifican las acciones y la apariencia de una baliza en el entorno de destino. Estos perfiles también especifican qué parámetros se emplean dentro de su protocolo de comunicación y el método que usa la baliza para infiltrarse en otros procesos. La Figura 5 muestra los 10 principales perfiles adaptables observados a lo largo del 2021.

Mediante el uso de perfiles adaptables de C2, la baliza de Cobalt Strike se puede configurar para ejecutar una técnica llamada enmascaramiento de dominio (o domain fronting). Esta técnica se emplea para enrutar el tráfico HTTPS a través de redes de entrega de contenido de terceros confiables. Los 10 principales hosts utilizados para enmascaramiento de dominio en el 2021 fueron los siguientes:

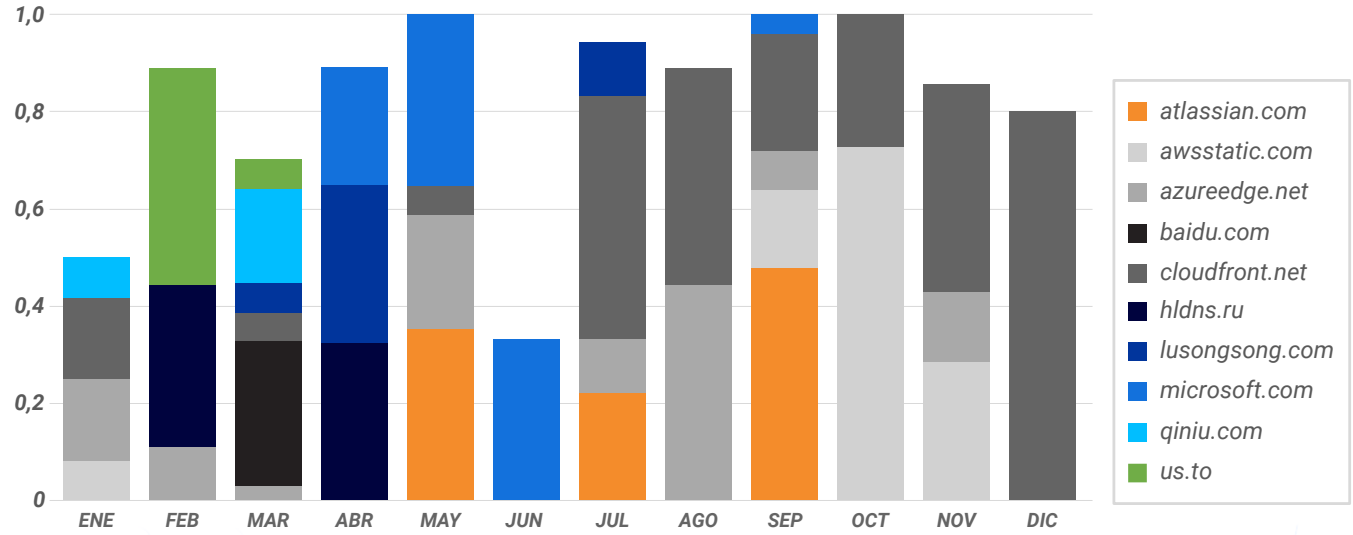


Figura 6: Los 10 principales hosts utilizados por la baliza de Cobalt Strike para enmascaramiento de dominio y general

La baliza de Cobalt Strike se puede configurar para que utilice redireccionador de DNS a fin de reenviar el tráfico de C2 a un servidor de equipo. En la Figura 7, se muestran los 10 principales protocolos de Internet (IP) de redireccionador de DNS del 2021.

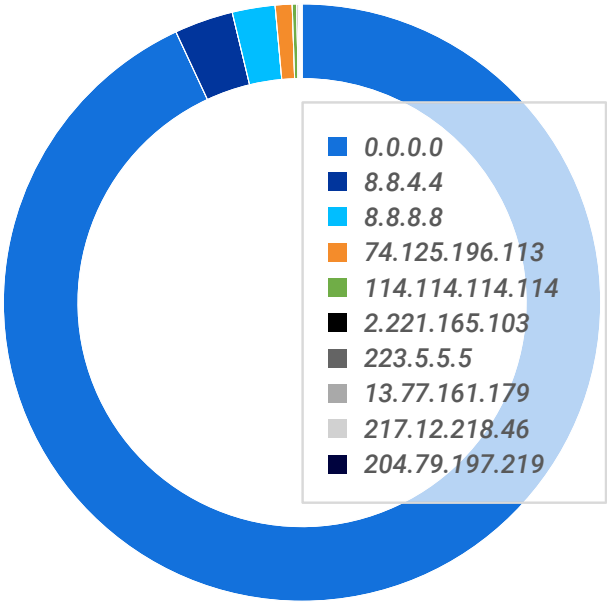


Figura 7: Los 10 principales IP de redireccionador de DNS empleados por Cobalt Strike

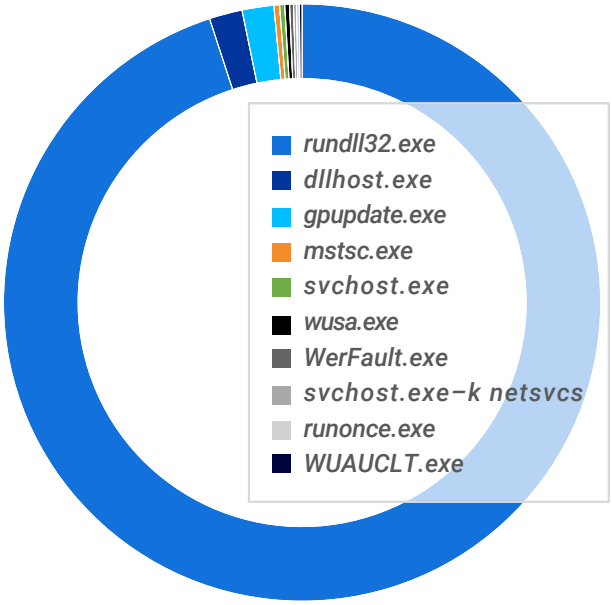


Figura 8: Procesos generados creados para las inyecciones de Cobalt Strike

La baliza de Cobalt Strike genera procesos y, luego, inyecta cargas de biblioteca de enlace dinámico en ellos. Estos procesos se pueden configurar para que funcionen en diferentes arquitecturas (x86/x64) a través de la opción SPAWNTO. El proceso predeterminado y la opción más elegida es rundll32.exe. Consulte la Figura 8.

Además de los certificados de capa de sockets seguros (SSL) implementados en el servidor de equipo, las balizas también se agrupan en paquetes con una clave pública de SSL adicional. Esto forma parte de un par de claves pública/privada que se genera en el servidor cada vez que alguien instala Cobalt Strike. La clave pública se incorpora posteriormente en todas las balizas generadas en el mismo servidor y se utiliza para los registros de C2. Es importante tener en cuenta que este par de claves es totalmente diferente del par de claves de SSL empleado para el certificado HTTPS del servidor de equipo.

A diferencia de las marcas de agua, la clave pública de SSL almacenada dentro de la configuración de una baliza ofrece un excelente medio para el agrupamiento de balizas. Está prácticamente garantizado que las claves son únicas por cada instalación de servidor de equipo; sin embargo, suelen reutilizarse, por ejemplo, a través de nuevos despliegues de máquinas virtuales. En otros casos, los atacantes utilizarán un único servidor de equipo con el fin de configurar las cargas para su despliegue desde otros servidores que tienen bajo su control. Esto facilita en gran medida la detección, el seguimiento y el monitoreo de su infraestructura.

Las 10 principales claves públicas de SSL pertenecen en su mayoría a compilaciones filtradas del servidor de equipo de Cobalt Strike:

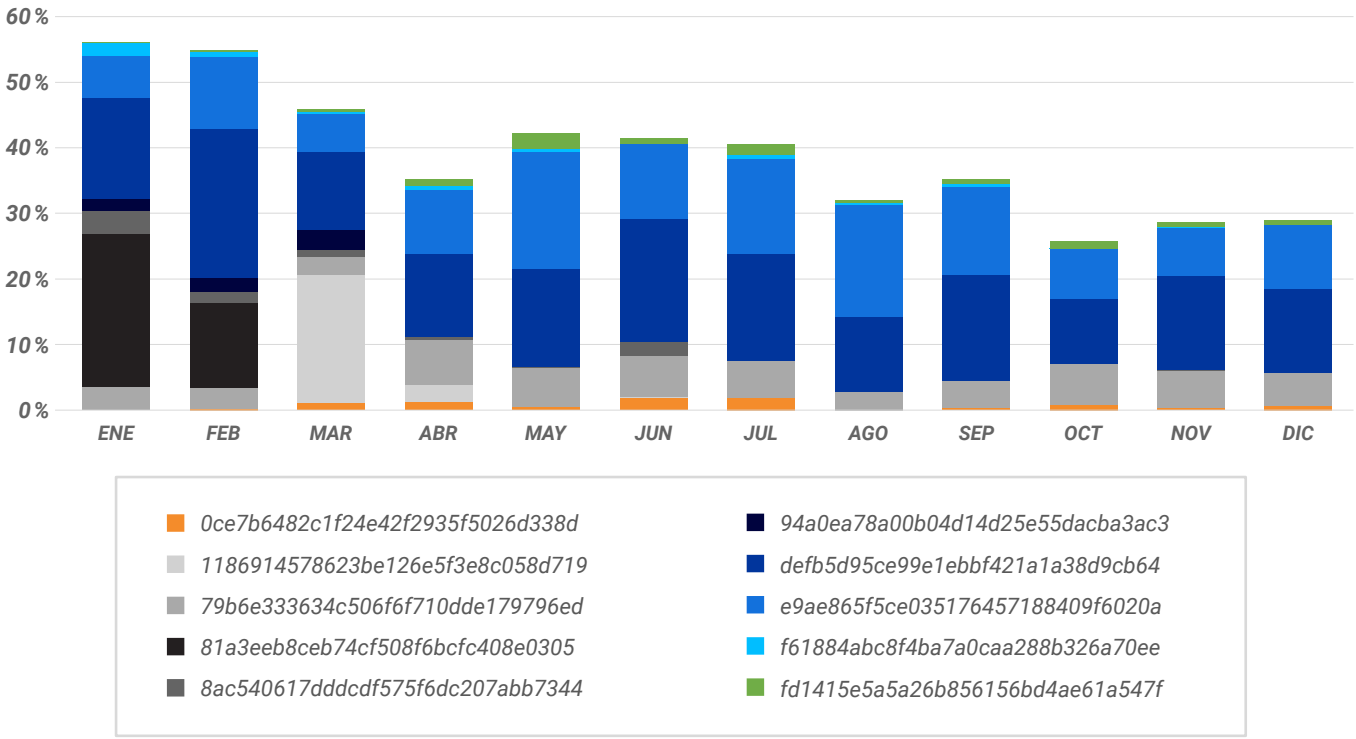


Figura 9: Las 10 principales claves públicas de los servidores de equipo de Cobalt Strike

Por último, es posible hacer un seguimiento de las compilaciones del servidor de equipo a través de una configuración llamada PROCINJ_STUB. Contiene un hash de algoritmo de resumen de mensaje (MD5) del archivo Java de Cobalt Strike (cobaltstrike[.]jar). Este archivo contiene el componente del lado del servidor que proporciona a los operadores del servidor de equipo una interfaz gráfica de usuario para generar, operar, desplegar y controlar las cargas de balizas.

El hash de MD5 del paquete cobaltstrike.jar nos permite determinar varias cosas. Al correlacionarlo con su archivo Java correspondiente, que comúnmente se encuentra en repositorios de malware en línea como VirusTotal, descubrimos:

- La versión exacta del servidor de equipo que se usó
- Si el servidor de equipo en funcionamiento es una versión filtrada, pirata o de prueba
- Si el servidor de equipo es una versión privada con licencia

Incluso si el archivo Java no está disponible para ayudar a identificar la versión, sigue siendo un mecanismo de agrupamiento de gran valor. Esto resulta particularmente cierto en el caso de compilaciones privadas y personalizadas.

Las 10 principales compilaciones del servidor de equipo en el 2021 (según el valor de hash PROCINJ_STUB) fueron las siguientes:

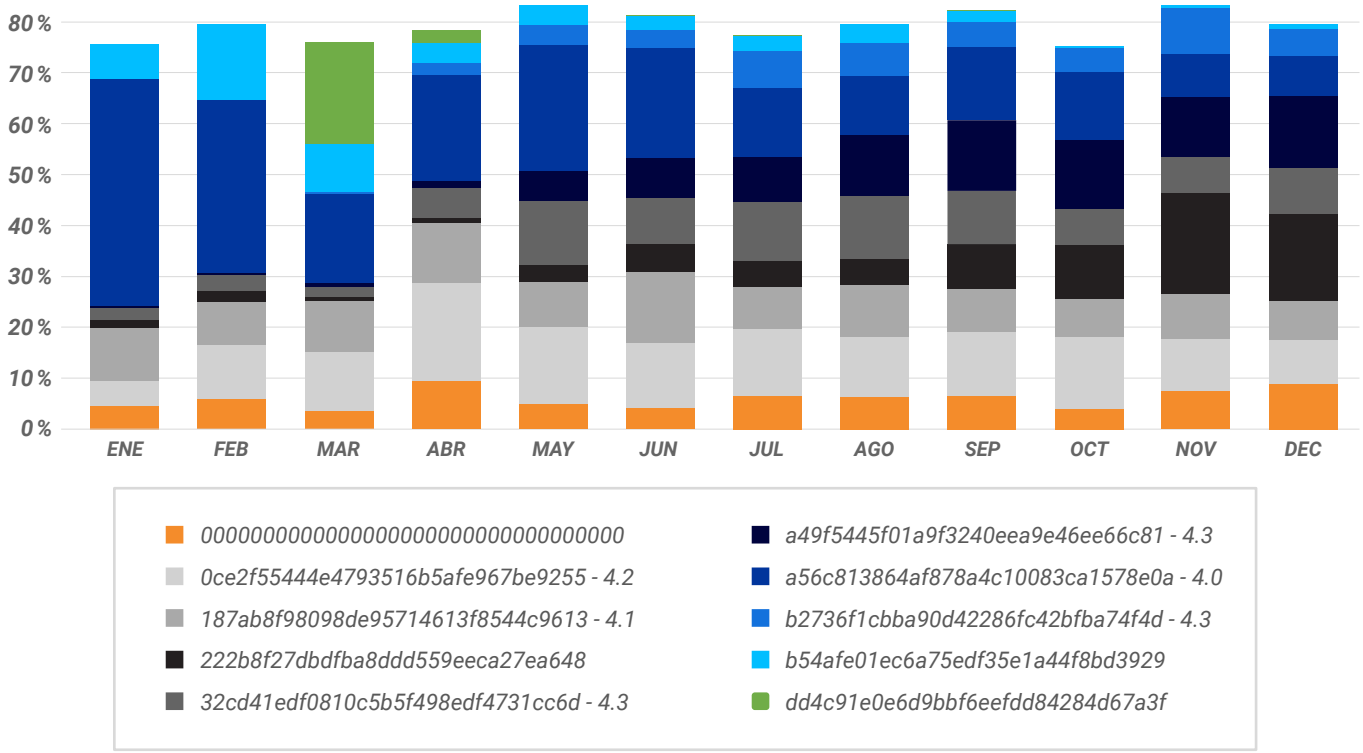


Figura 10: Las 10 principales compilaciones del servidor de equipo en el 2021

Además de nuestra investigación, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) del Departamento de Seguridad Nacional publicó un informe sobre la baliza de Cobalt Strike en mayo del 2021. Su documento incluye un listado de recomendaciones que los usuarios y las organizaciones pueden seguir a fin de minimizar la exposición a esta amenaza.

LOS ATAQUES A LA CADENA DE SUMINISTRO

Los ataques a la cadena de suministro no son un concepto reciente. Sin embargo, en los últimos años la cadena de suministro de software se ha utilizado cada vez más como vector de ataque. ¿A qué se debe esto? Por un lado, el impacto potencial y la propagación de un ataque a la cadena de suministro pueden ser mucho mayores que si el objetivo es una víctima individual. El potencial de daño varía según la base de clientes del producto en cuestión. La relación entre el fabricante y los consumidores es esencialmente de uno a muchos, con un único punto de falla. Esto significa que cuanto más grande sea la base de clientes, mayor será también la base de ataque potencial.

Los atacantes saben que explotar la confianza que las personas depositan en la integridad y seguridad de la cadena de suministro de estos fabricantes es más fácil que comprometer objetivos más protegidos. Los adversarios suelen buscar la vía de menor resistencia y la cadena de suministro representa la evolución más reciente en su oficio.

¿QUÉ ES UN ATAQUE A LA CADENA DE SUMINISTRO?

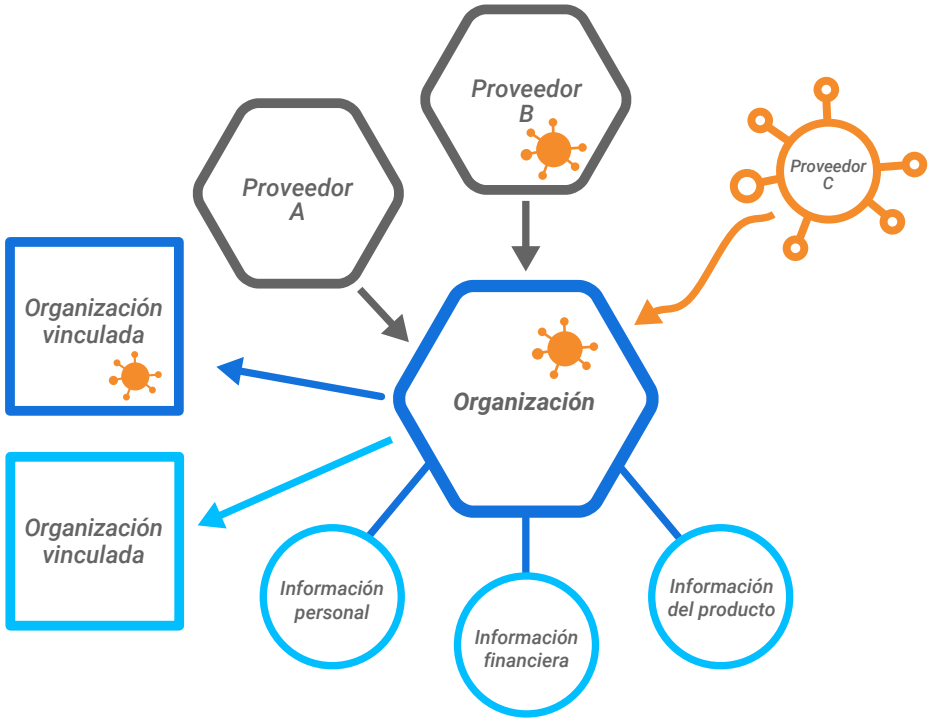


Figura 11: La topología de un ataque a la cadena de suministro

Para comprender mejor los ataques a la cadena de suministro, consulte la representación topológica de las interacciones empresariales en la Figura 11. Los ataques a la cadena de suministro ocurren cuando una organización depende de un tercero para el desarrollo de productos, hardware, software u otros servicios.

El Departamento de Defensa de los EE. UU. define un riesgo en la cadena de suministro como aquel en el que el adversario puede "sabotear, introducir maliciosamente una función no deseada o, de otro modo, subvertir el diseño, la integridad, la fabricación, la producción, la distribución, la instalación, la operación o el mantenimiento de un sistema para vigilar, denegar, interrumpir o, de otra manera, degradar la función, el uso o la operación de dicho sistema".

Observe nuevamente la Figura 11. La organización central depende de los proveedores A, B y C para cumplir con diferentes requisitos. Todo va bien hasta que el proveedor C es víctima de una filtración y se penetra su entorno. Se compromete el ciclo de vida de desarrollo del producto del proveedor C y se incluye un componente malicioso en su producto.

El producto, en su estado comprometido, se distribuye a la organización donde sirve como punto de entrada para que los adversarios maliciosos se infiltren y comprometan el sistema.

Una vez que los atacantes están adentro, toda la información a la que puedan acceder puede ser exfiltrada, incluida información de productos, información financiera y datos personales. Si la organización comprometida tiene una postura de seguridad débil, la propagación posterior de este ataque puede extenderse a organizaciones vinculadas y a su base de clientes.

EL IMPACTO POTENCIAL

En función del tamaño de la base de clientes de la organización comprometida, el impacto de un ataque a la cadena de suministro puede ser enorme.

Puede ser difícil determinar qué clientes fueron afectados y en qué medida. Como resultado, tan pronto como se identifique una filtración, se debe notificar a los clientes a fin de que puedan tomar sus propias medidas de remediación. Las organizaciones deben planificar para lo peor ante estas situaciones: suponer que sus clientes sufrieron una filtración y que el peligro de un mayor daño a la reputación es inminente. Cuanto más tarden en comunicar las amenazas y responder a ellas, mayor será el riesgo de que los atacantes logren penetrar de manera persistente los entornos de los clientes.

También existe la posibilidad de un efecto dominó: si la filtración no se contiene, otras organizaciones vinculadas también podrían verse afectadas.

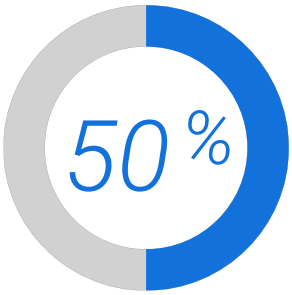
LOS ATAQUES RECIENTES A LA CADENA DE SUMINISTRO

Los ataques a la cadena de suministro suenan peligrosos, y lo son. Que el cliente potencial de una fuente confiable sea el punto inicial de compromiso es algo que muchos prefieren creer que no sucederá, pero sí sucede. Algunos ejemplos de ataques históricos a la cadena de suministro de software incluyen los siguientes:

- **Los ataques de ransomware de NotPetya en el 2017.** Los atacantes comprometieron el software fiscal ucraniano MEDoc y generaron miles de millones en daños a los gigantes farmacéuticos.
- **La filtración de SolarWinds en el 2020.** El software de monitoreo y administración de TI Orion se vio comprometido y se extendió a varias entidades de alto perfil.
- **Kaseya en el 2021.** Una vulnerabilidad de seguridad de día cero permitió a los atacantes implementar una actualización para cada cliente que ejecutaba su software de administración de servidores/sistemas virtual (VSA). La actualización era ransomware puro y cifró una gran parte de la base de clientes de VSA de Kaseya.

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) publicó recientemente un informe en el que se analizan 24 ataques a la cadena de suministro desde enero del 2020 hasta julio del 2021. El informe reveló algunas estadísticas crudas:

- Los proveedores no sabían o no informaron cómo se vieron comprometidos en el 66 % de los ataques a la cadena de suministro.
- A los grupos de amenazas persistentes avanzadas (APT) se les atribuyó la responsabilidad del 50 % de los ataques a la cadena de suministro.
- Casi el 62 % de los ataques a los clientes pudo concretarse debido a que se explotó la confianza depositada en el proveedor.



En 24 ataques recientes a la cadena de suministro, se atribuyó la responsabilidad del 50 % de los incidentes a grupos de amenazas persistentes avanzadas (APT).

¿DE QUÉ MANERA LOS ATAQUES A LA CADENA DE SUMINISTRO ELUDEN LA DETECCIÓN?

En esencia, un ataque a la cadena de suministro se basa en un abuso de la confianza. Se presume que un proveedor de confianza mantiene estrictos estándares de seguridad. Por ejemplo, un analista que responde a las alertas que muestran el tráfico de la red de C2 puede ser subjetivo basado en su nivel de confianza en una aplicación. Puede ver un dominio particular de su interés en el tráfico de la red o sus certificados de SSL. Sin embargo, como proviene de una aplicación confiable, se presume que el indicador de amenazas es legítimo.

Esta subjetividad resulta útil para resaltar los beneficios de un enfoque de confianza cero y cómo la confianza implícita puede ser una vulnerabilidad importante. También refuerza la necesidad de investigar y examinar con mayor profundidad las aplicaciones de terceros. Una cadena es tan fuerte como su eslabón más débil: si una parte se rompe, todo el sistema puede fallar.

¿CÓMO ES POSIBLE LOGRAR UNA MEJOR PROTECCIÓN?

Muchos problemas de seguridad se pueden abordar mediante un enfoque holístico de la seguridad y la adopción de los principios de confianza cero. Deben cubrirse todos los vectores de amenazas, incluidas las fuentes que, por lo general, se consideran benignas.

Muchos problemas de seguridad se pueden abordar mediante un enfoque holístico de la seguridad y la adopción de los principios de confianza cero.

El equipo de respuesta ante incidentes de seguridad de productos (PSIRT) de una organización también es un componente clave para mejorar su postura de seguridad. Por ejemplo, un PSIRT puede trabajar en estrecha colaboración con otros equipos y comunicarles valiosos conocimientos de seguridad a lo largo del ciclo de vida de desarrollo del software (SDLC). A medida que continúe su participación en el SDLC, el PSIRT alcanzará nuevos niveles de madurez y se volverá más proactivo. Esto ayuda a garantizar que los productos y los procesos de compilación sean lo más seguros posible. El riesgo de un ataque a la cadena de suministro disminuye cuando las líneas de comunicación entre los equipos son sólidas.

Para los analistas de seguridad, resulta importante reducir la subjetividad natural propia en pos de aplicaciones y servicios confiables. Si bien la firma de certificados, la procedencia, las herramientas de compilación y otros pasos que se pueden tomar tienen valor en términos de seguridad, resulta imperativo que los equipos de operaciones de seguridad (SecOps) sean siempre escépticos. La divulgación y contención rápidas de una filtración también es fundamental para proteger a las organizaciones y a los clientes que confían en sus productos o servicios.

LAS VULNERABILIDADES DE SEGURIDAD DE LOG4J/LOG4SHELL

Log4j es un paquete de registro de código abierto que se emplea en innumerables aplicaciones y marcos importantes, como Apache Struts2. Hacia fines del 2021, se descubrió una vulnerabilidad en este componente de software que los atacantes pueden aprovechar mediante el envío de texto especialmente redactado. Los ataques dirigidos a esta vulnerabilidad, también llamadas vulnerabilidades de seguridad de Log4Shell, permiten a los atacantes obtener el código de un servidor remoto y realizar la ejecución remota de código (RCE). Dado que Log4j no es un malware, no es susceptible de medidas y herramientas de seguridad cibernética enfocadas exclusivamente en la detección de código malicioso.

La vulnerabilidad de Log4j, informada por primera vez por Chen Zhaojun el 24 de noviembre, se describe con más detalle en CVE-2021-44228. El 10 de diciembre, la vulnerabilidad se hizo pública en la base de datos nacional de vulnerabilidades que lleva el Instituto Nacional de Normas y Tecnología (NIST). La revelación de esta vulnerabilidad dio como resultado un veloz aumento de los ataques que rápidamente sumaron millones por hora.

La vulnerabilidad de Log4j es particularmente problemática, ya que resulta difícil para las organizaciones saber qué aplicaciones y servicios están en riesgo. Una aplicación independiente en la que se usa Log4j puede ser fácil de identificar, pero ¿qué sucede con los casos en los que el paquete tiene seis niveles de profundidad en la cadena de dependencia? El uso generalizado de Log4j junto con la naturaleza compleja de las dependencias de software indica que esta vulnerabilidad representará una amenaza en los próximos años.

Si bien las medidas antimalware no son útiles para detectar y solucionar la vulnerabilidad de Log4j, otras estrategias de ciberseguridad pueden reducir la exposición de una organización a este riesgo. Por ejemplo, la adopción de un marco de confianza cero puede limitar el uso de la vulnerabilidad por parte de un atacante restringiendo el acceso de los procesos explotados. Los entornos de confianza cero pueden reducir aún más los riesgos mediante la implementación de políticas de acceso con privilegios mínimos en todo el entorno. Además, dado que muchos ataques cibernéticos se basan en la entrega de una carga maliciosa, en última instancia, las herramientas antimalware pueden evitar los ataques basados en archivos que resultan de la vulnerabilidad de seguridad.

LOS TRUCOS NUEVOS DE LOS ATACANTES CONOCIDOS: LENGUAJES DE PROGRAMACIÓN POCO CONOCIDOS

El equipo de Investigación e Inteligencia de Amenazas de BlackBerry ha estado rastreando y monitoreando el panorama de amenazas en busca de la aparición de cuatro lenguajes de programación poco conocidos:

- **Go**
- **D**
- **Nim**
- **Rust**

Estos lenguajes se observan en la actualidad a fin de rastrear su uso y adopción por parte de los atacantes. La selección de estos lenguajes se debió, en parte, a un repunte en su uso indebido para concretar actividades maliciosas. Otro factor es su rol cada vez mayor en las familias de malware creadas y reveladas dentro del panorama general de amenazas.

Por lo general, se suelen desarrollar nuevos lenguajes de programación con el fin de mejorar diferentes aspectos o deficiencias de los lenguajes actuales. En consecuencia, esto también los convierte en una opción atractiva para el abuso por parte de los atacantes. Los nuevos lenguajes se pueden usar como contenedor o cargador de una familia de malware existente, para reescribir malware existente, o bien con el fin de desarrollar malware completamente nuevo. Esta tendencia se ha observado en el pasado con el uso de VB6 y Delphi a fin de desarrollar contenedores para el malware vigente en ese momento.

Los trucos nuevos de los atacantes conocidos: los atacantes adoptan lenguajes de programación exóticos

Más recientemente, en marzo del 2021, la familia de malware BazarLoader se reescribió en el lenguaje de programación Nim y se denominó Nimzaloader. Varios meses después, en mayo, apareció RustyBeur, que fue una variante del malware Buer Loader reescrita en Rust.

Desde el punto de vista de un atacante, el uso de lenguajes de programación exóticos ofrece muchas ventajas. Estas incluyen lo siguiente:

- Mejor rendimiento
- Falta de herramientas de análisis disponibles
- Desconocimiento de los analistas sobre su composición
- Mayor capacidad para evadir la detección de antivirus basados en firmas

Se podría argumentar que estos lenguajes actúan como una capa de ofuscación. Su novedad y la falta de herramientas de análisis disponibles hacen que puedan parecer bastante extraños para los investigadores inexpertos.

BlackBerry observó que estos lenguajes se usaban en el desarrollo de una cantidad cada vez mayor de "depositadores" (droppers) y cargadores. Se usaron como piezas nuevas e iniciales de malware diseñadas para depositar/decodificar, cargar y desplegar familias de malware actualmente producido habituales. Las amenazas que actualmente utilizan estos nuevos lenguajes incluyen los troyanos de acceso remoto Remcos y NanoCore, y las balizas de Cobalt Strike.

Muchos de estos lenguajes también se pueden compilar de forma cruzada a fin de apuntar a múltiples sistemas operativos. Los atacantes han abusado incansablemente de esta poderosa funcionalidad. Específicamente, el grupo APT29 con sede en Rusia y su malware Wellmess, que fue escrito en Go y compilado para atacar los sistemas operativos Windows® y Linux®. Otro ejemplo de esto fue la aparición del malware ElectroRAT en enero del 2021. También se desarrolló en Go y, luego, se compiló de forma cruzada para atacar todos los principales sistemas operativos: Windows, macOS® y Linux.

Nim y Go se han empleado en diferentes partes de la misma cadena de ataque con el fin de mejorar la capacidad de evasión de detección del atacante. Por ejemplo, el grupo de amenazas APT28 aprovechó un descargador basado en Nim para recuperar una carga basada en Go en su malware Zebrocy.

Los beneficios y la popularidad de estos lenguajes han impulsado su adopción de parte de la comunidad de seguridad. Debido a sus ventajas ofensivas, son de particular utilidad en el desarrollo de herramientas de Red Team. A fines del 2020, FireEye reveló que un atacante había obtenido acceso no autorizado a algunas de sus herramientas de Red Team. Como contramedida, publicó una declaración junto con un repositorio de GitHub formado por varias firmas de detección para ayudar a identificar las herramientas robadas. En este repositorio, FireEye reveló que su Red Team había estado empleando una combinación de herramientas modificadas disponibles al público y herramientas personalizadas internas. Algunas de estas herramientas de Red Team se escribieron en DLang, Rust y Go.

Los binarios maliciosos creados en estos lenguajes actualmente son solo una pequeña parte de los que utilizan los atacantes. Sin embargo, su uso en los ataques cibernéticos es una tendencia que, probablemente, escale en la próxima década.

LOS AGENTES DE ACCESO INICIAL

El equipo de Investigación e Inteligencia de Amenazas de BlackBerry ha estado rastreando un agente de acceso inicial (IAB) previamente no documentado que BlackBerry llamó Zebra2104. Nuestra investigación reveló una gran cantidad de infraestructura maliciosa interconectada que mostraba una conexión inusual entre diferentes grupos de amenazas aparentemente no relacionados.

La primera revelación ocurrió en abril del 2021, con el descubrimiento de un dominio que presentaba balizas de Cobalt Strike que también funcionaba como servidor de C2. Si seguimor el rastro de la red, encontramos numerosas superposiciones con la infraestructura malspam documentada previamente. Esta infraestructura funcionó con varias cargas, incluido Dridex, durante el año pasado. También se asoció con una campaña de phishing dirigida a entidades con sede en Australia, tanto privadas como gubernamentales.

Las investigaciones posteriores descubrieron enlaces adicionales a una intrusión del ransomware MountLocker en marzo del 2021, a través de cierta información de registro de dominio compartido para el dominio supercombinating[.]com. Otros análisis revelaron otro dominio relacionado, mentiononecommon[.]com, que se resolvió en la misma IP de manera alterna como supercombinating[.]com durante varios meses. La inteligencia de código abierto confirmó que este dominio había sido etiquetado anteriormente como un servidor StrongPity de C2 en junio del 2020.

Promethium (también denominado StrongPity) es un grupo de APT que ha estado activo desde el 2012. Por lo general, el grupo usa ataques de abrevadero como un mecanismo para entregar versiones troyanizadas de utilidades de uso común. WinRAR, CCleaner e Internet Download Manager son algunas de las utilidades que se han reutilizado de manera maliciosa para distribuir el malware del grupo.

Mientras nuestros investigadores buscaban más evidencia para demostrar que estos dos grupos dispares cooperaron de alguna manera, encontraron otro hallazgo interesante. Un tuit de The DFIR Report en agosto del 2020 señaló que se estaba distribuyendo ransomware adicional desde supercombinating[.]com. Esta vez, el malware pertenecía a la familia Phobos, no a MountLocker.

Esto planteó más interrogantes sobre la conexión entre estos grupos de amenazas. ¿Estaban relacionados o simplemente compartían la misma infraestructura? ¿Habíamos descubierto algún tipo de sistema de distribución? ¿Un IAB era el eslabón perdido que unía a estos grupos?

Un IAB es una entidad cuya finalidad es obtener acceso ilegal a la red de una organización. Establece un punto de penetración, generalmente mediante la instalación de una puerta trasera y, luego, vende su acceso ilegal en la web oscura. El precio de sus servicios puede variar desde USD 25 hasta miles de dólares. Tras obtener acceso, los compradores a menudo despliegan malware dentro del entorno de la víctima.

Aunque diferentes grupos de ransomware pueden compartir infraestructura, nuestros sondeos durante esta investigación indican que este no fue el caso. En numerosas instancias, se observó un retraso entre el compromiso inicial que utilizaba Cobalt Strike y la distribución de ransomware adicional. Estos factores nos llevaron a determinar que la infraestructura superpuesta no es la de MountLocker, Phobos ni Promethium. En cambio, pertenece a un cuarto grupo que ha actuado como intermediario para facilitar las operaciones de los tres primeros. Este arreglo se logró al brindar/vender acceso inicial, o mediante la provisión de IaaS.

Además, los dominios encontrados a lo largo de esta infraestructura superpuesta empleada para resolver las direcciones IP fueron proporcionados por un único ASN búlgaro que pertenece a Neterra LTD.

El hecho de que todas las IP estuvieran agrupadas en el mismo ASN da más credibilidad a la teoría de que pertenecen a un grupo de amenazas. Es probable que este grupo también sentara las bases para que los otros atacantes accedieran a las redes filtradas por el IAB.

CHACHI

El equipo de Investigación e Inteligencia de Amenazas de BlackBerry ha estado rastreando un troyano de acceso remoto (RAT) Golang previamente sin nombre dirigido a sistemas de Windows. Lo denominamos RAT ChaChi. Este RAT ha sido empleado por operadores del ransomware PYSA (también llamado Mespinoza) como parte de su conjunto de herramientas para atacar a víctimas en todo el mundo. Recientemente, el malware se ha dirigido a organizaciones educativas.

PYSA adora a ChaChi: un nuevo RAT GoLang

ChaChi se ha observado en circulación desde la primera mitad del 2020 sin recibir mucha atención por parte de la industria de la ciberseguridad. La primera variante conocida de ChaChi se utilizó en ataques a las redes de las autoridades del Gobierno local en Francia. Fue incluido como indicador de compromiso (IOC) en una publicación de CERT France al momento de los ataques.

Desde entonces, los analistas de BlackBerry han visto versiones mejoradas de ChaChi desplegadas por los operadores del ransomware PYSA. Su campaña se centró en instituciones educativas de los EE. UU., lo cual es evidente debido a un aumento reciente en la actividad, según lo informado por el FBI.

TIPOS DE ATAQUES

RANSOMWARE

REVIL

El FBI nombró al grupo de RaaS afiliado a Rusia REvil (también conocido como Sodin o Sodinokibi) como el responsable de los ataques contra el proveedor de carne más grande del mundo, JBS. Estos ataques amenazaron a la cadena de suministro de alimentos global y sirvieron como recordatorio del estado vulnerable en que se encuentra la infraestructura crítica de todo el mundo.

REvil se publicitó por primera vez en foros de delincuentes cibernéticos en idioma ruso y se lo asocia con el atacante conocido como Unknown (también, UNKN).

El malware actúa como un RaaS, y se volvió prolífico cuando otro grupo de RaaS, GandCrab, cerró sus operaciones. Los investigadores de seguridad identificaron muchas similitudes y reutilización de código entre REvil y GandCrab. REvil se publicitó por primera vez en foros de delincuentes cibernéticos en idioma ruso y se lo asocia con el atacante conocido como Unknown (también, UNKN).

REvil es popularmente conocido por los recientes ataques a la industria de los seguros de viaje, Acer, y fabricantes de computadoras. Al actuar como un RaaS, REvil depende de que afiliados o socios realicen sus ataques. Los desarrolladores de REvil reciben un porcentaje de todas las ganancias de los pagos de rescate. Dado que el ransomware se distribuye a distintas entidades, el vector de infección inicial puede variar. Normalmente, la infección se logra mediante campañas de phishing, ataques de fuerza bruta para comprometer el protocolo de escritorio remoto (RDP) o a través de vulnerabilidades de software. REvil además puede ser distribuido por otro malware, como IcedID.

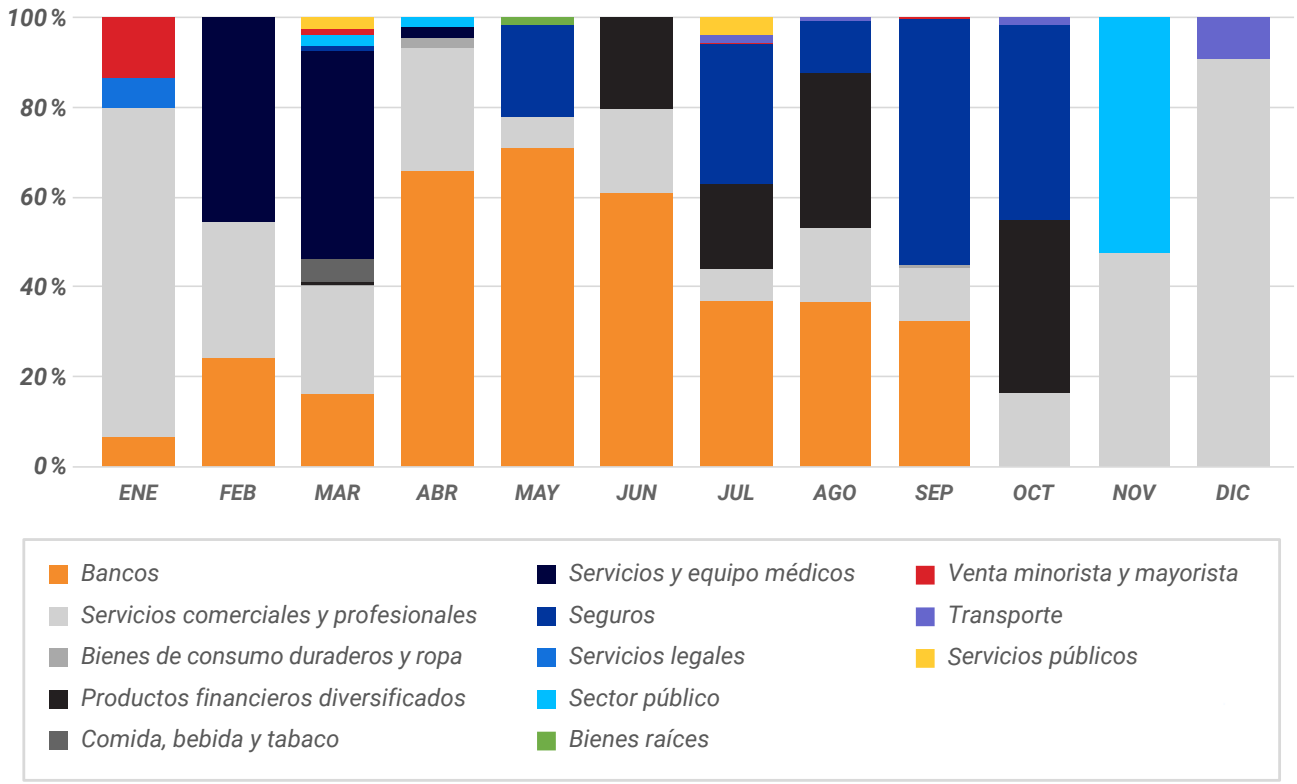


Figura 12: Industrias atacadas por REvil en el 2021

DARKSIDE

La variante de ransomware DarkSide apareció por primera vez a mediados del 2020. Se distribuye como un RaaS que se utiliza para realizar ataques dirigidos. DarkSide apunta tanto a máquinas que operan con Windows como con Linux. Acaparó los titulares en el 2021 con su ataque al sistema de oleoductos Colonial Pipeline de los EE. UU.

DarkSide emplea un esquema de doble extorsión, en el que los datos se encriptan localmente y se exfiltran antes de exigir el rescate. Si la víctima se niega a pagar, los datos se publican en un sitio de la "internet oscura".

Después del ataque a Colonial Pipeline, el grupo DarkSide declaró que no planeaba afectar sistemas de hospitales o instalaciones médicas, instituciones educativas, organizaciones sin fines de lucro o gubernamentales. Según se informó, el grupo DarkSide fue desmantelado en mayo del 2021, posiblemente por el Cibercomando de las Fuerzas Armadas de los EE. UU.

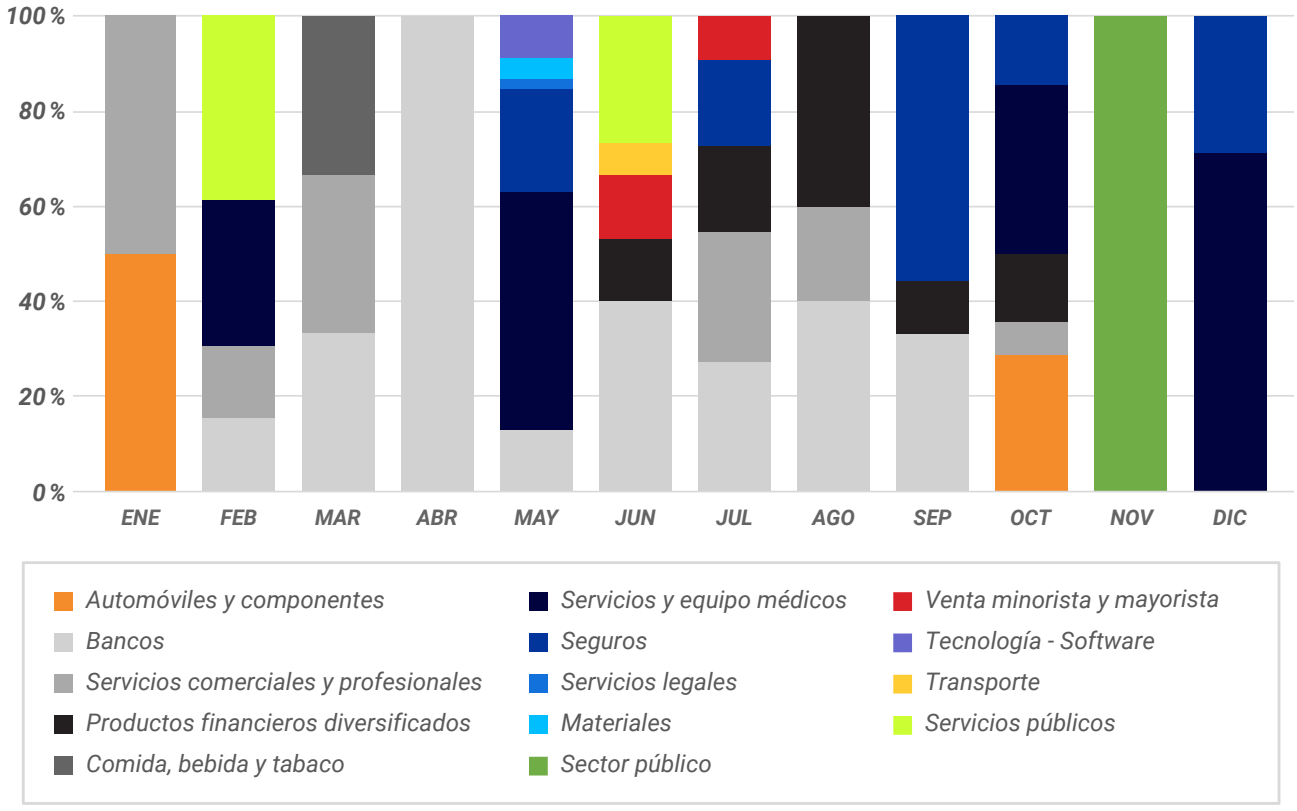


Figura 13: Industrias atacadas por DarkSide en el 2021

Muchos analistas afirman que Conti es el ransomware que reemplazó a Ryuk, y lo consideran como una de las amenazas más preocupantes en circulación.

CONTI

El ransomware Conti apareció en los titulares de noticias internacionales tras haber sido descubierto a mediados del 2020. Los investigadores de BlackBerry observaron los ataques de Conti contra proveedores de servicios de las áreas de fabricación, seguros y salud en Japón, Europa y los EE. UU.

Conti se ofrece como un RaaS, que los atacantes suelen utilizar para distribuir y vender sus servicios maliciosos en foros clandestinos. Dado que esta amenaza se ofrece como un servicio vendible, puede personalizarse alterando su funcionalidad de una infección a otra. Los atacantes lanzaron un descifrador para esta amenaza en mayo del 2021, que puede ayudar a recuperar archivos alterados por una variante específica de Conti.

La popularidad de Conti está en ascenso desde que el infame ransomware Ryuk parece haber dejado de operar. Muchos analistas afirman que Conti es el ransomware que reemplazó a Ryuk, y lo consideran como una de las amenazas más preocupantes en circulación.

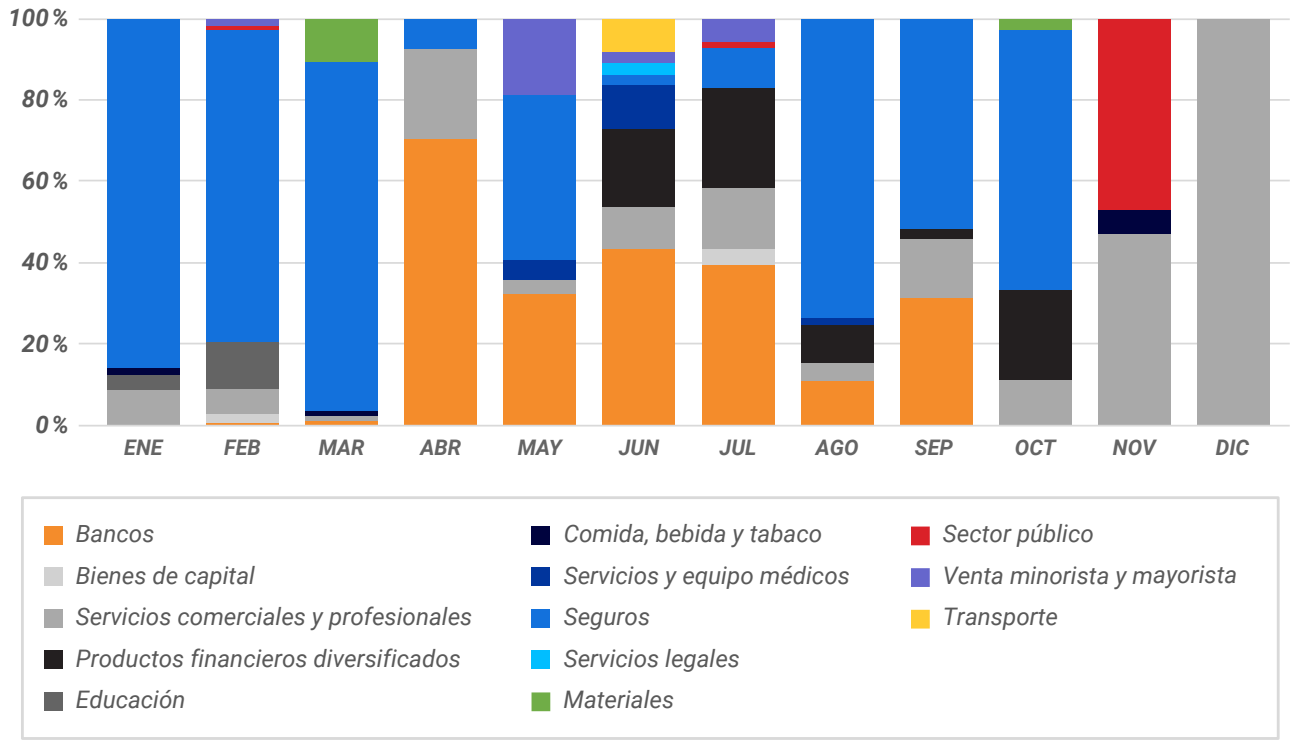


Figura 14: Industrias atacadas por Conti en el 2021

AVADDON

La variante de ransomware Avaddon apareció por primera vez a principios del 2020. Llegó a los titulares internacionales debido a ataques recientes contra organizaciones australianas y la compañía de seguros cibernéticos con sede en Asia, AXA. Tanto el FBI como el Centro de Seguridad Cibernética Australiano (Australian Cyber Security Center, ACSC) emitieron advertencias sobre un ataque en curso de parte de esta familia de malware.

Al igual que los ransomware DarkSide y REvil, Avaddon emplea un esquema de doble extorsión, en el que los datos se encriptan localmente y se exfiltran antes del pedido de rescate. Si la víctima se niega a pagar, los datos se publican en un sitio de la "internet oscura". Sin embargo, Avaddon va un paso más allá. Para alentar todavía más a las víctimas a acatar sus demandas, los atacantes también las someten a un ataque de denegación de servicio (DDoS) hasta que realicen el pago del rescate.

Después de atraer atención a causa de su papel en varios incidentes de ransomware de alto perfil, el grupo detrás de Avaddon parece estar cerrando sus operaciones actuales. Los esfuerzos de las agencias de cumplimiento de la ley de perseguir a los operadores de malware aumentaron visiblemente después del ataque a Colonial Pipeline, que, a su vez, hizo que DarkSide cerrara sus operaciones. Avaddon publicó los descifradores de la última versión de su amenaza.

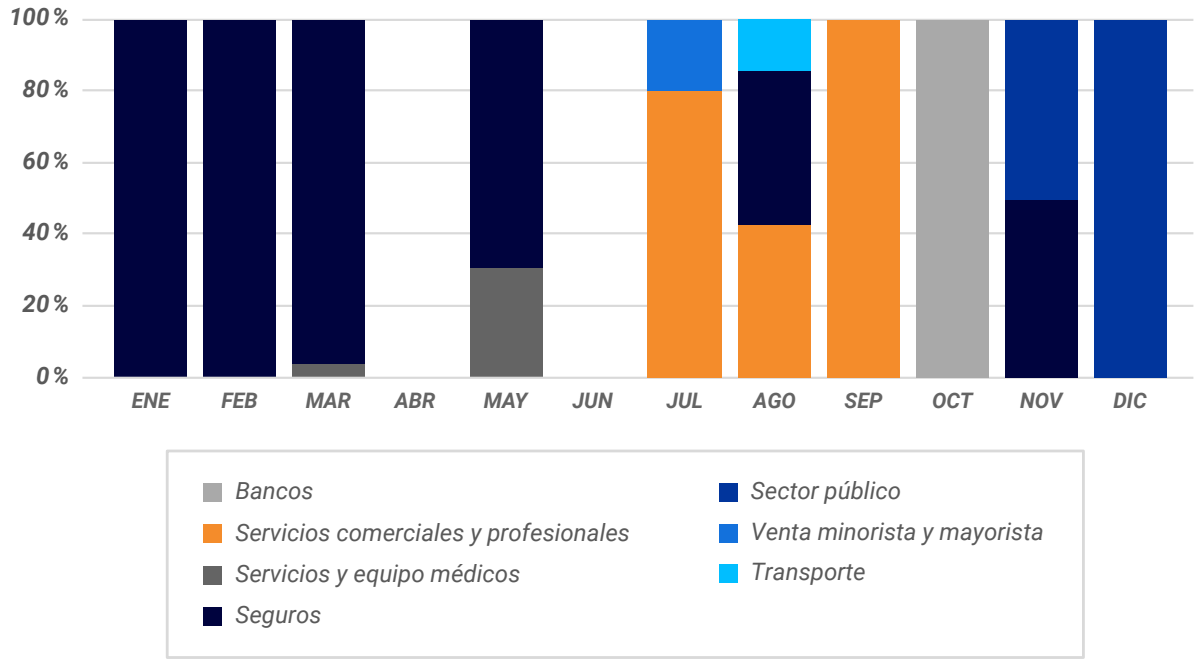


Figura 15: Industrias atacadas por Avaddon en el 2021

RAGNAR LOCKER

El ransomware Ragnar Locker apareció en los titulares internacionales por sus ataques contra un fabricante taiwanés de productos de memoria flash NAND y módulos de memoria DRAM de alto desempeño. La primera variante de esta familia apareció a fines del 2019.

1,5 TB

Ragnar Locker afirma haber exfiltrado 1,5 TB de datos de una sola víctima de alto perfil.

Al igual que muchas otras variantes de ransomware conocidas (como DarkSide, Avaddon y REvil), la variante actual de Ragnar Locker también utiliza una técnica de doble extorsión para alentar a las víctimas a pagar.

El sitio de la internet oscura de Ragnar Locker enumera sus víctimas más recientes en una autodenominada "pared de la vergüenza". El grupo de amenazas actualmente afirma haber exfiltrado 1,5 TB de datos de una víctima de alto perfil. Según su sitio web, esta información se recopiló de manera sigilosa durante un largo período.

HIVE

La familia de ransomware Hive, que apareció por primera vez en junio del 2021, protagonizó las noticias tras atacar a la empresa de software para bienes raíces comerciales Altus Group. Esta amenaza también emplea la técnica de doble extorsión. Las víctimas que se niegan a cooperar con el atacante, corren el riesgo de que se publiquen sus datos en el sitio del grupo, Hive Leaks.

Las muestras de Hive están escritas en el lenguaje de programación Go y se compilan para máquinas de 32 y 64 bits. Las muestras en sí se empaquetan con UPX para reducir su tamaño, dado que los binarios de Go tienden a ser bastante grandes.

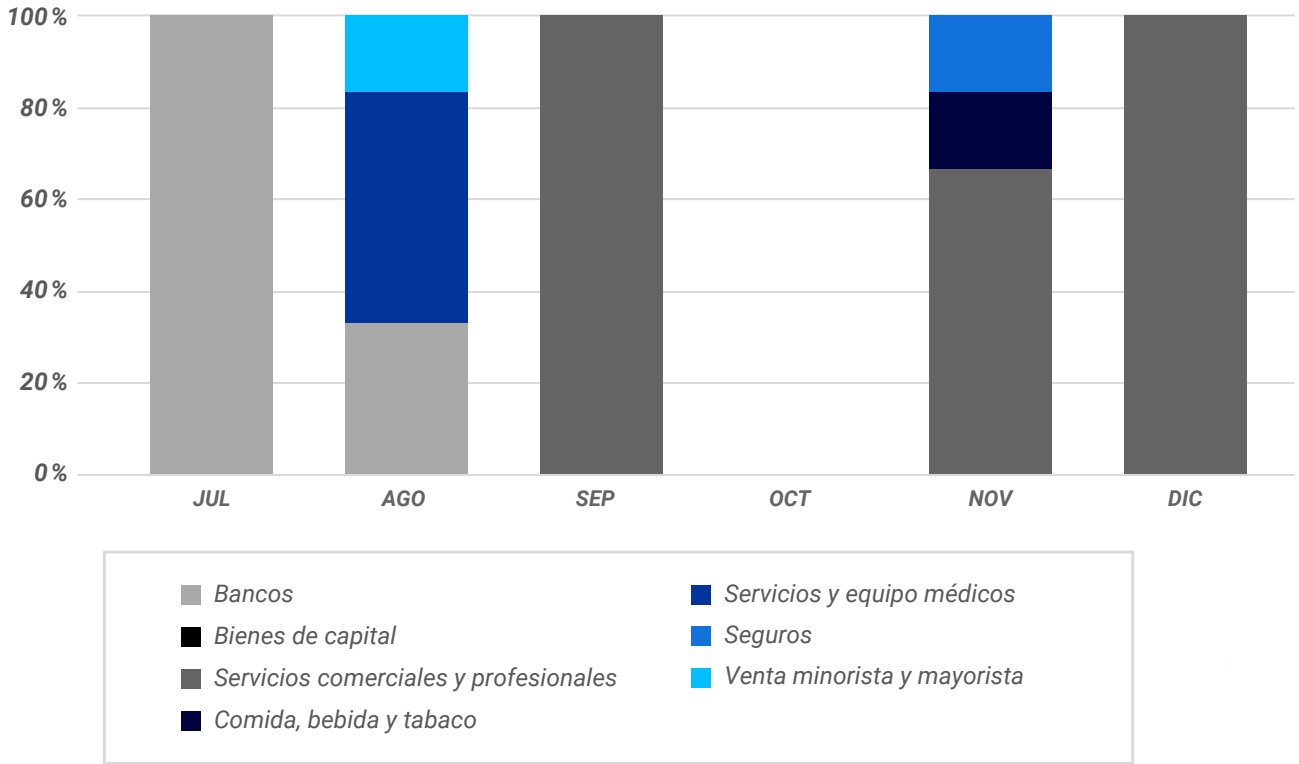


Figura 16: Industrias atacadas por Hive en el 2021

INFOSTEALERS

RedLine es una familia de malware infostealer que se distribuye mediante campañas de correo electrónico de phishing que hacen referencia a la COVID-19.

REDLINE

RedLine es una familia de malware infostealer que se distribuye mediante campañas de correo electrónico de phishing que hacen referencia a la COVID-19. Fue una amenaza activa durante todo 2020. En el 2021, se entregó mediante publicidades maliciosas de Google y campañas de phishing dirigidas a artistas digitales o de 3D que usaban tokens no fungibles (NFT). Los NFT son tokens digitales ligados a activos que pueden comprarse, venderse o intercambiarse.

RedLine es sumamente versátil y apareció como distintos servicios, juegos, cracks y herramientas troyanizados. Muchas muestras de RedLine también aparecen con certificados digitales que lucen legítimos.

Una vez que se establece la conexión con su panel de C2, el malware RedLine tiene una amplia gama de aplicaciones y servicios. En todos los casos, intenta exfiltrar los datos de la víctima. El malware recopila información de navegadores web, clientes de protocolo de transferencia de archivos (FTP), mensajeros instantáneos, billeteras de criptomonedas, servicios de red privada virtual (VPN) y clientes de videojuegos. También cuenta con funcionalidad remota para depositar y ejecutar otro malware en la máquina de la víctima.

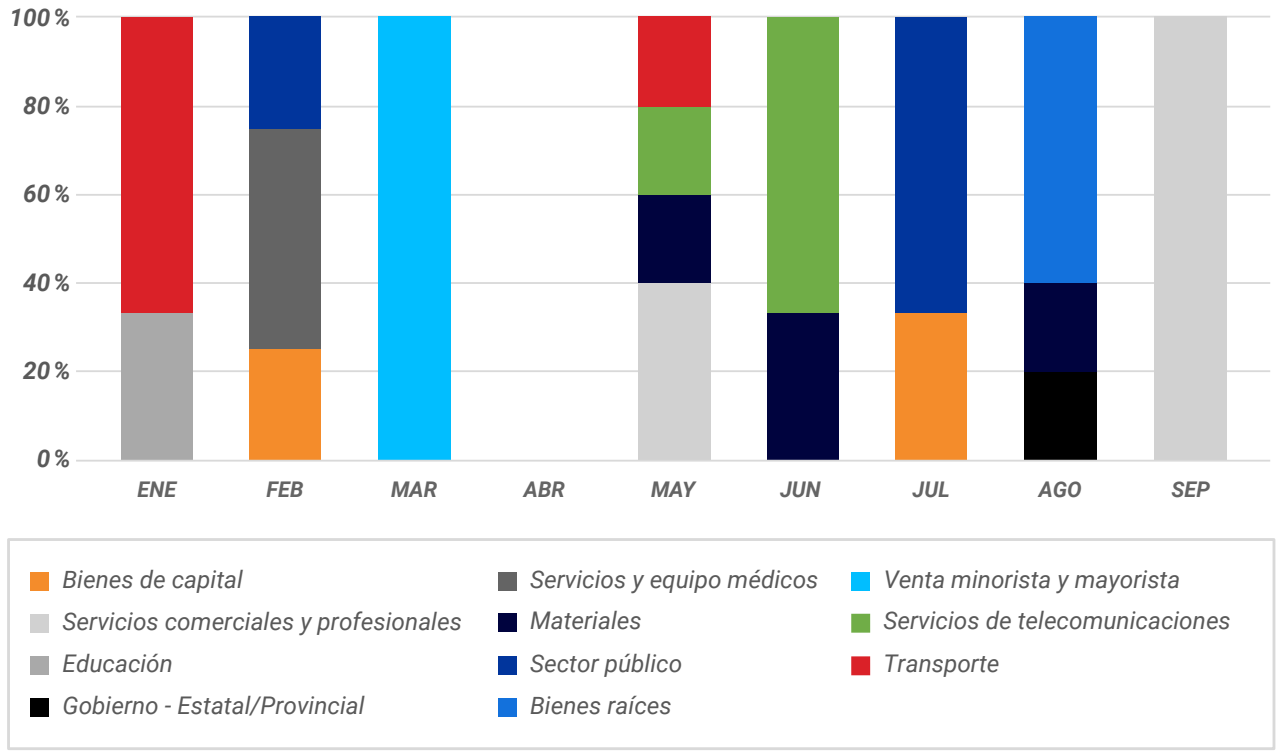


Figura 17: Industrias atacadas por RedLine en el 2021

El infostealer Agent Tesla fue utilizado sistemáticamente por delincuentes cibernéticos en distintas campañas, con frecuencia usando correos de spam para posibilitar la infección.

AGENT TESLA

Visto en circulación por primera vez en el 2014, Agent Tesla está compilado con .NET y contiene una serie de funciones de infostealing poderosas. Inicialmente, estaba disponible para la compra mediante un sitio web, en el que el autor del malware ofrecía varias licencias de plazo fijo para su uso.

Desde entonces, el infostealer Agent Tesla fue utilizado sistemáticamente por delincuentes cibernéticos en distintas campañas, con frecuencia usando correos de spam para posibilitar la infección.

El malware evolucionó para recopilar información sobre el perfil de Wi-Fi de un usuario, potencialmente como un mecanismo de propagación. Esta actualización sigue a una mejora similar a la variante de malware Emotet, que también recibió un módulo de distribución por Wi-Fi.

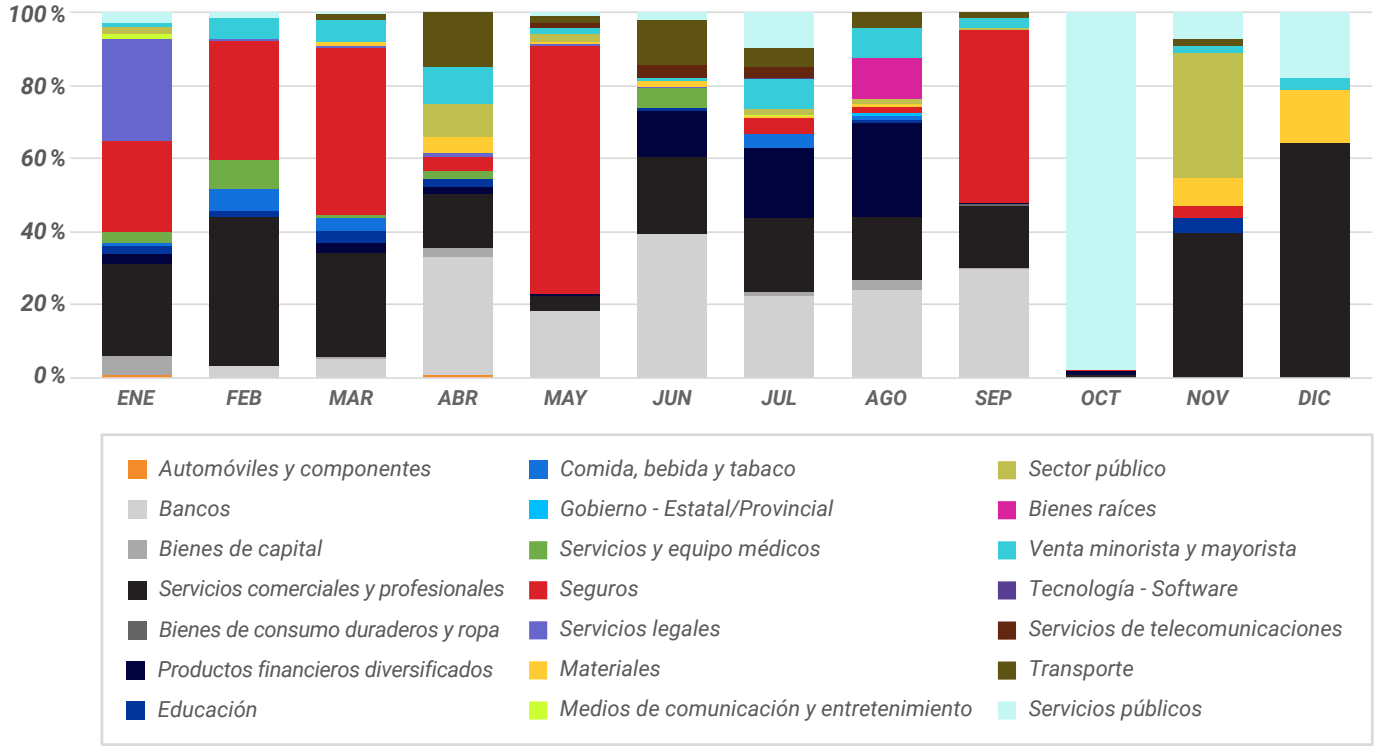


Figura 18: Industrias atacadas por Agent Tesla en el 2021

Ficker es un infostealer malicioso que dirige a las víctimas a páginas que supuestamente ofrecen descargas gratis de servicios pagos legítimos, como Spotify y YouTube Premium™.

FICKER

Ficker es un infostealer malicioso que un delincuente de amenazas bajo el alias [@]ficker vende y distribuye en foros clandestinos rusos. Este MaaS se descubrió por primera vez en circulación en el 2020.

Ficker se distribuyó anteriormente mediante enlaces web troyanizados y sitios web comprometidos. Por ejemplo, podía dirigir a las víctimas a páginas que supuestamente ofrecían descargas gratis de servicios pagos legítimos, como Spotify y YouTube Premium™. También se desplegó mediante el conocido descargador de malware Hancitor.

Notablemente escrito en Rust, Ficker tiene diversos objetivos para sus actividades de robo de información, entre los que se incluyen los siguientes:

- Navegadores web
- Información de tarjetas de crédito
- Billeteras de criptomonedas
- Clientes de FTP
- Otras aplicaciones

Ficker utiliza verificaciones antianálisis y puede desplegar más funcionalidad y descargar malware adicional una vez que un sistema se ve exitosamente comprometido.

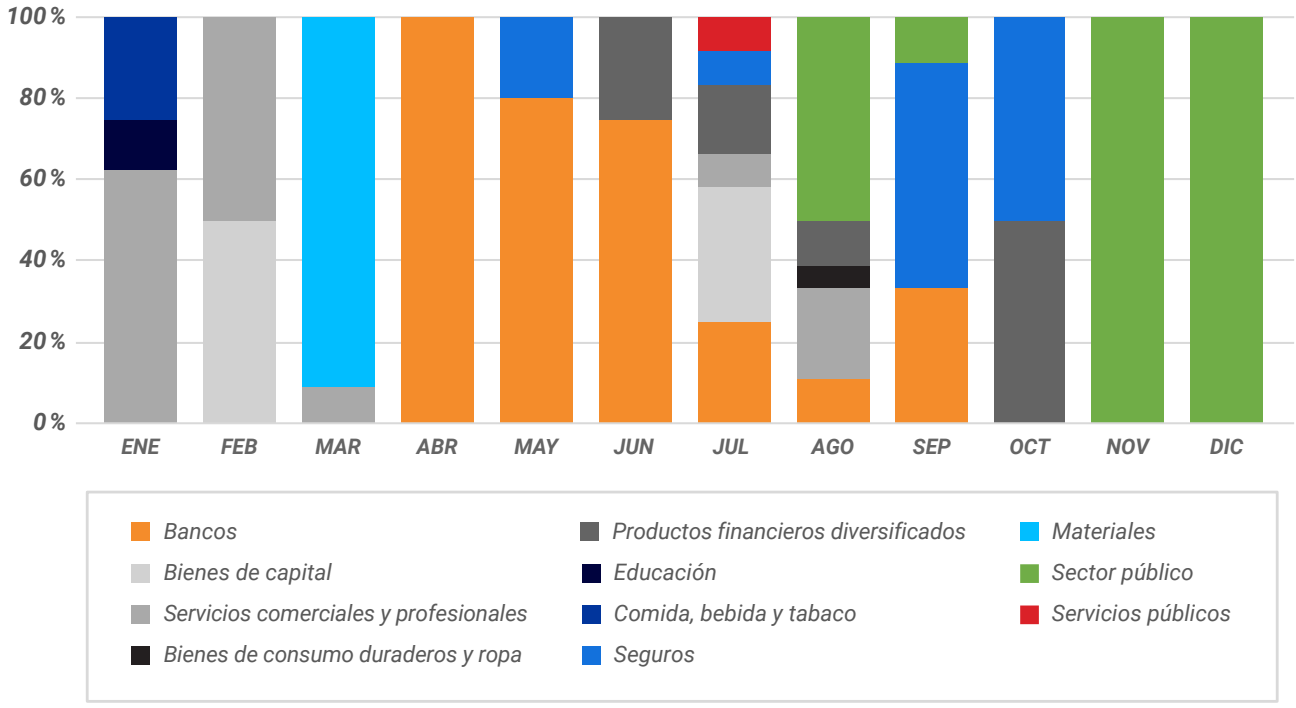


Figura 19: Industrias atacadas por Ficker en el 2021

HANCITOR

Hancitor (también conocido como, Chanitor) se descubrió por primera vez en circulación en el 2013. Se distribuye mediante técnicas de ingeniería social, como aparentar provenir del servicio legítimo de firma de documentos DocuSign®. Una vez que se engaña a las víctimas para que permitan que se ejecute este macrocódigo malicioso, infecta sus sistemas.

Hancitor entonces se conecta con su infraestructura de C2 e intenta descargar una amplia gama de componentes maliciosos, según las necesidades de la campaña de los operadores. Este año, se observó que Hancitor descargó la popular familia de malware Ficker (también conocida como, FickerStealer), así como una carga de baliza de Cobalt Strike.

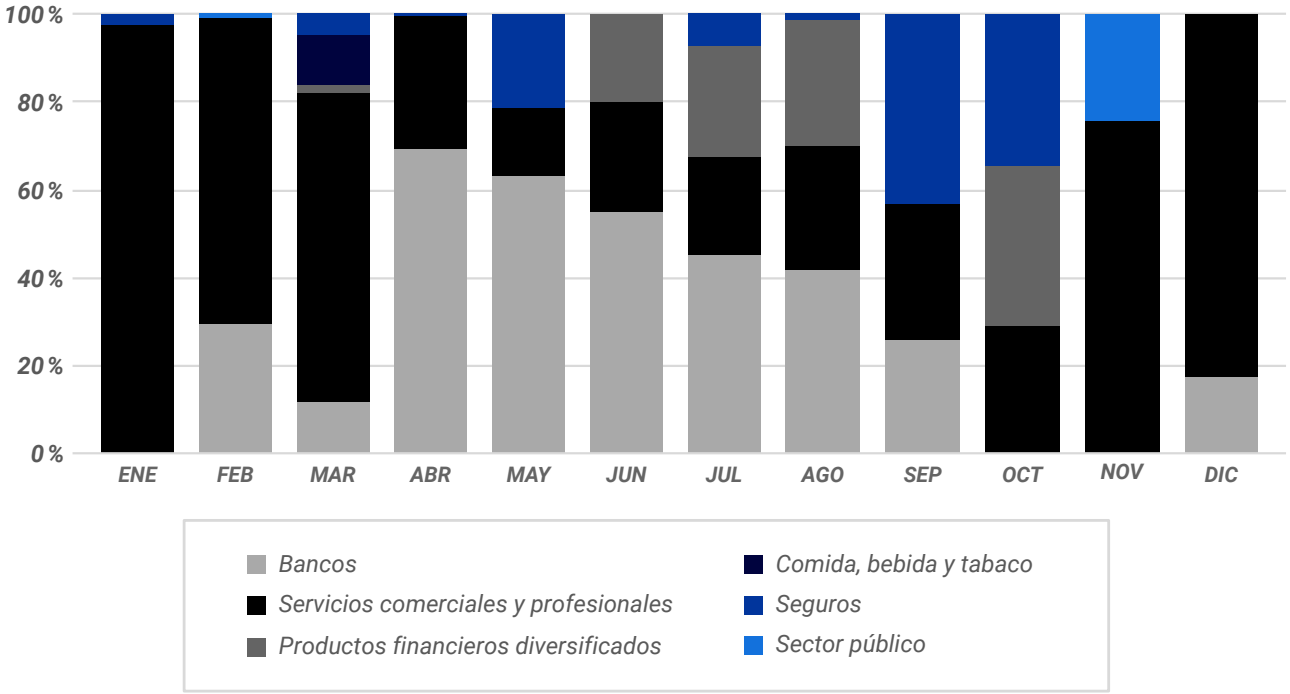


Figura 20: Industrias atacadas por Hancitor en el 2021

LAS 10 PRINCIPALES AMENAZAS

INSTANCIAS DE LAS 10 PRINCIPALES AMENAZAS EN EL 2021

La Figura 21 muestra la prevalencia mensual de cada una de las familias de malware según datos internos de BlackBerry.

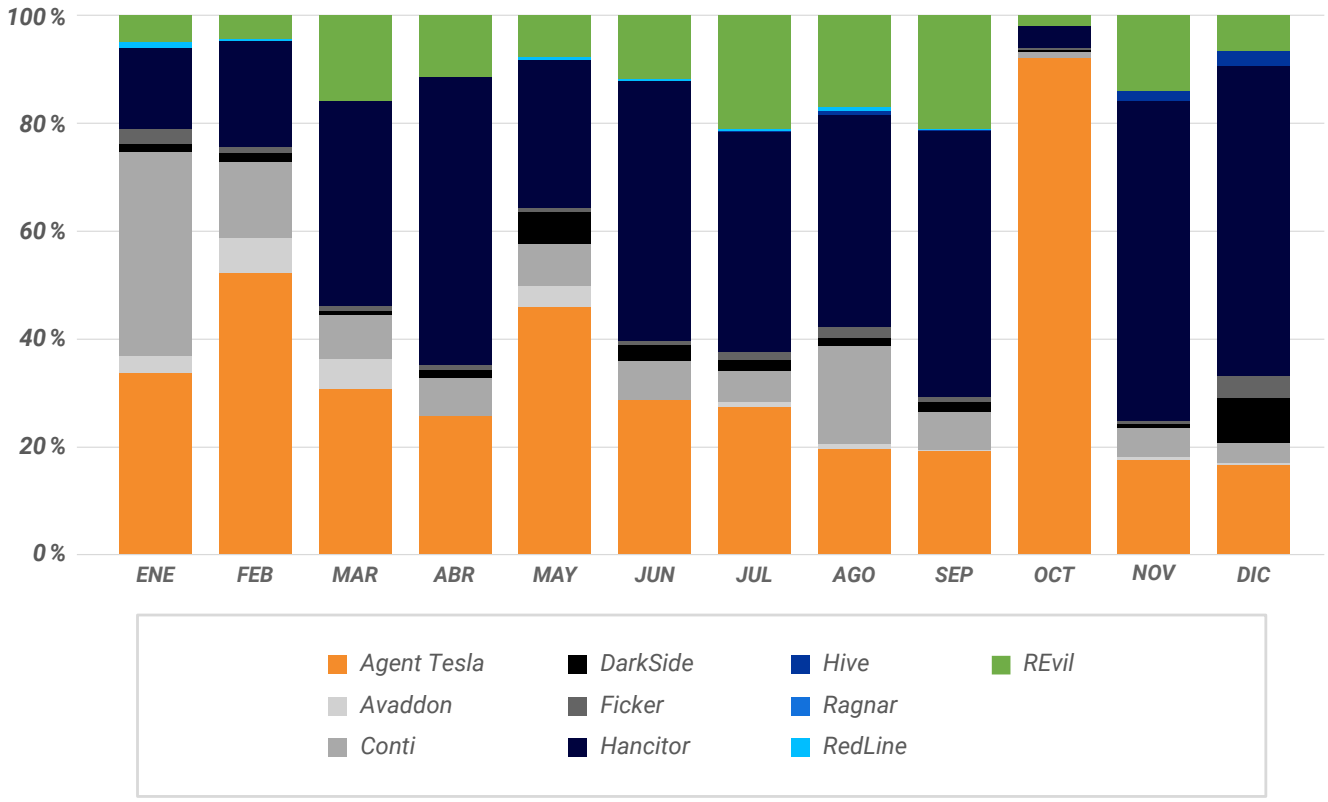


Figura 21: Prevalencia de las 10 principales amenazas de malware en el 2021

LAS 10 PRINCIPALES VERSUS LA VENTAJA PREDICTIVA DE BLACKBERRY

Nadie quiere ser el paciente cero de una nueva amenaza. Las organizaciones no tienen por qué serlo si aprenden las lecciones cotidianas del amplio mundo de las amenazas.

Gracias a los modelos de detección de amenazas predictivos, los modelos de seguridad cibernética de vanguardia pasaron de métodos de detección tradicionales a técnicas impulsadas por aprendizaje automático (AA). Entrenar a los modelos de AA exhaustivamente sobre el malware actual permite que las soluciones impulsadas por IA predigan cómo las amenazas aparecerán y se comportarán en el futuro. Las soluciones de BlackBerry®, basadas en la IA Cylance®, aprenden a predecir variantes y familias de malware emergentes mediante el entrenamiento con muestras existentes tomadas del panorama de amenazas. Este enfoque le da a la seguridad cibernética impulsada por IA la capacidad de detectar amenazas conocidas y de día cero antes de que lleguen a sus objetivos.

La ventaja predictiva mide retroactivamente el tiempo en que un modelo impulsado por IA hubiera detectado y prevenido una nueva amenaza antes de su descubrimiento.

¿QUÉ ES LA VENTAJA PREDICTIVA?

La ventaja predictiva mide retroactivamente el tiempo en que un modelo impulsado por IA hubiera detectado y prevenido una nueva amenaza antes de su descubrimiento. Por ejemplo, si un modelo de AA protege contra una amenaza que aparece un año después de la creación del modelo, tendrá una ventaja predictiva de 12 meses. La medida se utiliza como un algoritmo de predicción local sin conexión para realizar pruebas, sin actualizaciones o conexión a internet. Esto garantiza que el modelo de AA se desempeñe exactamente como lo hizo en su fecha de lanzamiento original, sin mejoras ni actualizaciones.

BlackBerry realizó una prueba de ventaja predictiva para calificar nuestras detecciones contras las 10 principales familias de malware descriptas en este informe anual. Esto ilustra con cuanta anticipación el modelo de IA ofreció protección contra las amenazas más significativas que enfrentaron nuestros clientes en el 2021.

El modelo de IA representado en esta prueba se creó en octubre del 2015. Fue desplegado con la versión 1320 del agente BlackBerry® Protect. Las cifras de la Figura 22 muestran con cuántos meses de antelación nuestro modelo podría haber protegido a los clientes de cada amenaza antes de que fuera descubierta.

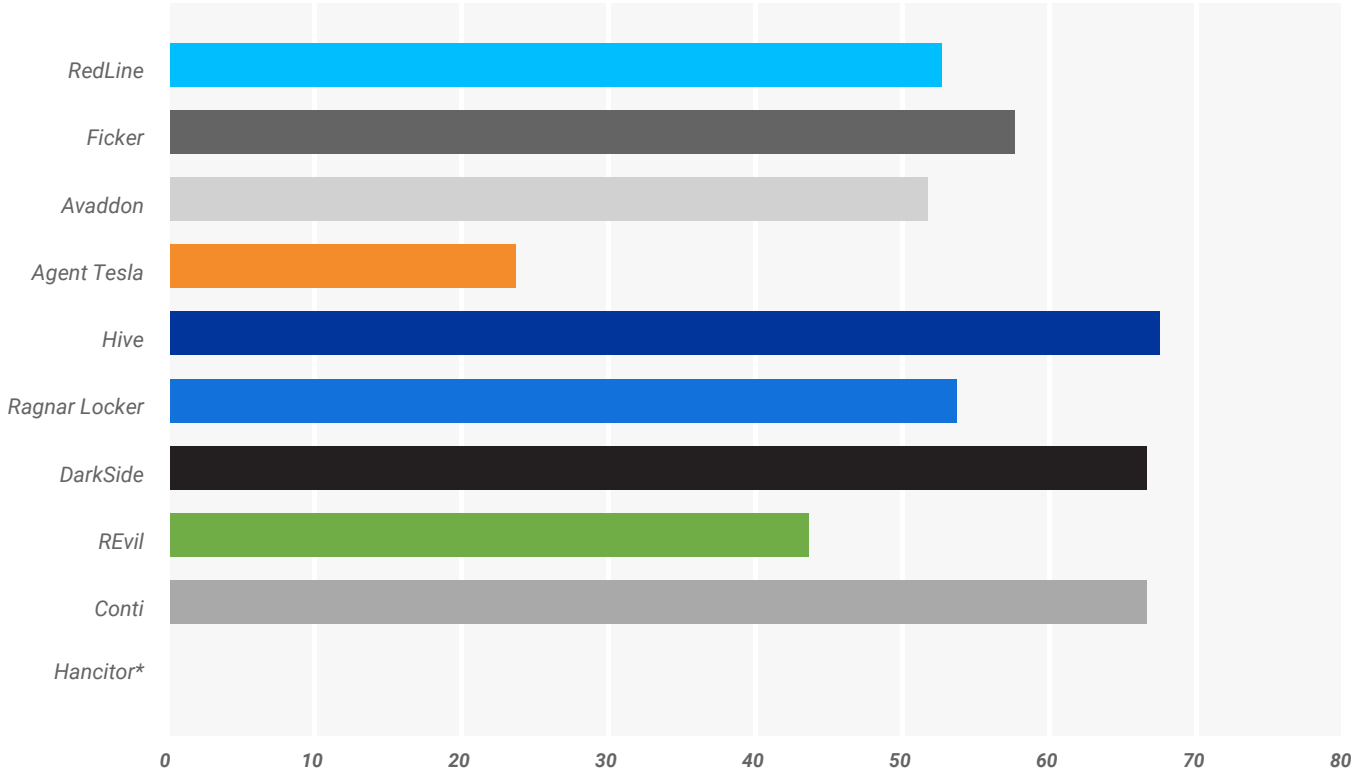


Figura 22: Ventaja predictiva de BlackBerry, en meses, respecto de las 10 principales amenazas a nuestros clientes
** NOTA: Hancitor no está representada en el gráfico dado que su descubrimiento es anterior a octubre del 2015.*

CIENCIA DE DATOS

LA IA Y LOS ATAQUES ADVERSARIALES

Tal como indican los ejemplos anteriores de ventaja predictiva, la inteligencia artificial y el aprendizaje automático pueden ser armas poderosas en la lucha contra los delitos cibernéticos. Desafortunadamente, también tienen el potencial de abuso o uso indebido en manos de individuos inescrupulosos y sofisticados con intenciones maliciosas.

Considere el caso del aprendizaje profundo, una de las tecnologías más publicitadas de la última década. A pesar de lo que promete a la industria, también introduce otro objetivo que los atacantes pueden comprometer.

EL APRENDIZAJE PROFUNDO Y LOS ATAQUES ADVERSARIALES

Durante la última década, el surgimiento del aprendizaje profundo (también conocido como redes neuronales) brindó un impulso masivo a las industrias técnicas. Esta tecnología disruptiva permitió a las empresas mejorar productos y optimizar indicadores de desempeño clave mediante el descubrimiento de patrones previamente ocultos en sus datos internos. Estos algoritmos permitieron a las empresas separar a los trabajadores de tareas analíticas tediosas: en particular, aquellas en las que se generaban manualmente enormes cantidades de conjuntos de reglas u otras tareas heurísticas.

Todo un campo conocido como aprendizaje adversarial surgió como amenaza a todos los productos que emplean algoritmos predictivos.

Lamentablemente, este progreso tuvo un costo. Todo un campo conocido como aprendizaje adversarial surgió como amenaza a todos los productos que emplean algoritmos predictivos. El objetivo principal de este campo es descubrir maneras en las que se puede enseñar a las redes neuronales a engañar a otros algoritmos predictivos cambiando sutilmente los datos de entrada. Por ejemplo, se utilizaron algoritmos adversariales con el objeto de determinar cómo aplicar parches pequeños de cinta a un letrero de alto para hacerlo invisible para los algoritmos de clasificación. En el caso de las imágenes o el audio, los ataques adversariales pueden utilizarse para hacer cambios casi imperceptibles a una muestra a fin de engañar a algoritmos de predicción que, de lo contrario, son altamente precisos.

En el campo de la ciberseguridad, estos algoritmos se utilizaron con el objeto de modificar archivos maliciosos para que pudieran evadir defensas heurísticas y asistidas por AA. No resulta simple hacer cambios arbitrarios a archivos (que tienen su propia estructura y reglas estructurales), de modo que la mayoría de estos ataques emplean una estrategia iterativa en masa. Mediante esta técnica, los algoritmos realizan miles (o incluso cientos de miles) de pequeñas adiciones a un archivo que individualmente no tienen impacto en su funcionalidad. Sin embargo, cada cambio puede impulsar las decisiones de un algoritmo predictivo respecto de la clasificación de amenazas en la dirección adecuada. Resulta preocupante que los archivos generados por estos algoritmos adversariales sean capaces de transferirse entre modelos. Esto significa que un ataque entrenado para una defensa puede ser capaz de evadir decenas de productos de seguridad cibernética comerciales.

A pesar del peligro que implican estos algoritmos, el ritmo de la investigación en esta área está aumentando, en gran medida debido a que los incentivos están desalineados. El aprendizaje profundo es un campo sumamente popular y competitivo, lo que motiva a académicos y grandes empresas de tecnología a publicar tanta investigación como sea posible. Como resultado, el campo de los ataques adversariales es extremadamente activo. Por ejemplo, una búsqueda de ataques adversariales en Google Scholar™ para el 2020 devuelve miles de entradas, de las cuales unos pocos cientos se centran en la ciberseguridad.

De manera similar, se suele alentar a los ingenieros de AA que buscan postularse en empresas de tecnología de alto nivel a crear paquetes de código abierto útiles para demostrar sus habilidades. Una búsqueda rápida de aprendizaje adversarial en GitHub arroja casi 5000 repositorios individuales, algunos con más de 1000 estrellas (o Me gusta). Los incentivos basados en el desarrollo profesional han tenido el efecto neto de democratizar y transformar los algoritmos adversariales en un producto, haciéndolos ubicuos y reduciendo su barrera de acceso.

DEFENSAS ALGORÍTMICAS

Poco tiempo después de que se descubrieran los ataques adversariales, se creó un campo secundario llamado aprendizaje adversarial o defensas adversariales. Estas defensas suelen enfocarse en maneras de diseñar o entrenar modelos, o de preprocesar datos de antemano, para mitigar los efectos de los ataques adversariales.

Esta disciplina aún tiene mucho por delante respecto de su eficacia general. Ninguna defensa adversarial parece ser sólida ante ataques de "caja blanca" en los que el atacante tiene total conocimiento del tipo de modelo y las defensas que se emplean. Sin embargo, muchas defensas adversariales parecen bastante sólidas frente a los ataques de "caja negra". Por lo tanto, las organizaciones pueden evitar los ataques de "caja blanca" y forzar a los atacantes a confiar en ataques de "caja negra" menos eficientes mediante el uso de un par de técnicas. Pueden ofuscar el resultado de una defensa, por lo general, reduciendo su precisión, o limitar la capacidad de los atacantes de realizar una consulta en masa de una defensa.

Como se mencionó anteriormente, los ejemplos adversariales suelen ser transferibles, y posiblemente puedan evadir numerosas defensas, tal como lo confirmaron publicaciones recientes.

Sin embargo, estos ataques solo evadieron productos que no emplearon defensas adversariales generadas por aprendizaje profundo. BlackBerry verificó internamente que es poco probable que los ataques generados de esta manera evadan modelos que utilizan varios esquemas defensivos de aprendizaje profundo robustos.

Además, los ataques adversariales a los archivos necesitan confiar en enfoques iterativos que no se utilizan comúnmente en otras áreas (como en modelos visuales o auditivos). Como resultado, muchos kits de herramientas de ataques adversariales de código abierto no pueden modificarse fácilmente para centrarse en defensas de ciberseguridad. Desafortunadamente, una búsqueda en GitHub arroja algunas páginas que contienen lo que parecen ser esfuerzos aficionados de generar ejemplos adversariales. Esto no es un buen presagio para lo que puede seguir a medida que este campo madure.

PRONÓSTICO

A corto plazo, el pronóstico en esta área es mixto. El campo de los ataques adversariales sigue siendo candente, y el software de código abierto redujo enormemente la barrera de acceso para las personas que buscan generar ejemplos adversariales. La cantidad de experiencia necesaria para generar evasiones sigue siendo bastante alta. Por ello, no se espera un uso generalizado de esta tecnología en los siguientes uno o dos años.

Es probable que cualquier paquete adversarial de código abierto todavía necesite confiar en enfoques en masa para generar ataques. Esto significa que las empresas de seguridad cibernética tienen un camino por recorrer razonable que puede resumirse de la siguiente manera:

- Contratar personal que entienda el aprendizaje profundo adversarial
- Emplear varios esquemas defensivos sólidos (incluso para productos que utilicen defensas heurísticas)
- Mantener los esquemas defensivos secretos/exclusivamente internos
- Evitar que los atacantes consulten rápidamente las defensas para encontrar baches sutiles

En lo que respecta a la seguridad, nada está garantizado. Sin embargo, para las organizaciones que sigan estas reglas, los ataques adversariales deberían ser un vector de amenazas manejable a corto plazo.

PERSPECTIVAS SOBRE LA SEGURIDAD CIBERNÉTICA

REPASO DEL AÑO RESPECTO DE RESPUESTA ANTE INCIDENTES Y TENDENCIAS

Durante el último año, el ransomware siguió siendo protagonista según el equipo de Respuesta ante incidentes de BlackBerry. Como se analizó en el Informe de amenazas 2021 de BlackBerry, la estrategia de doble extorsión de pedido de rescate y exfiltración de datos se convirtió en la norma. De hecho, la tendencia incluso se escaló, con instancias de triple (sumando el acoso) y cuádruple (con ataques disruptivos como DDoS) extorsión. Como resultado de estas estrategias de ataque en expansión, la filtración de datos públicos es cada vez mayor.

Los métodos de extorsión en evolución crearon una alineación cercana entre las tácticas utilizadas por los atacantes de amenazas avanzadas persistentes (APT) de estados nacionales y las organizaciones delictivas que buscan ganancias. Sus enfoques y objetivos operativos son notablemente similares, a pesar de que sus motivaciones centrales, niveles de experiencia técnica y métodos de ejecución suelen variar. Por lo tanto, la amplia mayoría de ataques en la actualidad siguen un patrón similar, como se detalla en la Figura 23.

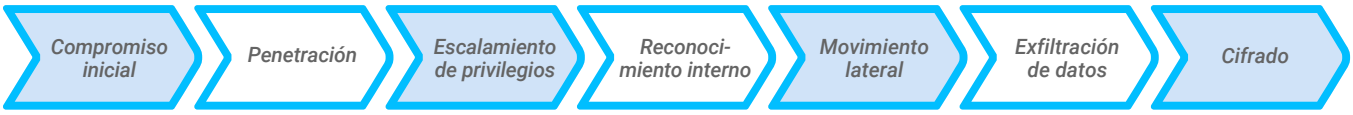


Figura 23: Flujo de ataque típico de un atacante

Una de las principales diferencias entre los grupos de APT y las organizaciones de ransomware es cuánto tiempo planea cada grupo permanecer activo en el entorno. Esto, a su vez,, afecta qué tan furtivamente se comportan. Los grupos de APT con frecuencia planean residir a largo plazo en el entorno de la víctima. Los grupos de ransomware suelen tomar lo que pueden para luego desaparecer.

Por ejemplo, los APT a menudo prefieren ataques del tipo “living-off-the-land” (LotL) donde usan recursos legítimos del sistema para que su actividad sea difícil de distinguir de las operaciones cotidianas. Se toman el tiempo de estudiar detenidamente un entorno y entender sus medidas de seguridad antes de ejecutar acciones maliciosas. Los ataques de ransomware son más oportunistas y, por lo tanto, operan de manera más rápida e imprudente. Como resultado de esto, suelen generar más ruido de entre el cual deben detectar las herramientas de plataforma de protección para puntos finales (EPP) y detección y respuesta para puntos finales (EDR). Por ejemplo, pueden utilizar herramientas como PowerShell, script por lotes de Windows o WMI para intentar desactivar productos antivirus, soluciones de copias de seguridad y otros procesos del sistema.

Otra diferencia clave es que los grupos de estados nacionales suelen buscar información específica para exfiltrar. Pueden utilizarla con fines de inteligencia, generalmente en busca de una ventaja política o económica. Por el contrario, los grupos de ransomware suelen buscar cualquier cosa de valor que pueda aumentar la probabilidad de obtener un pago. Entre los favoritos frecuentes está apuntar a bases de datos que puedan contener información de clientes o financiera.

En lo que respecta a la opinión pública, el tamaño realmente importa en lo referente a titulares y fugas de datos. Por lo tanto, los atacantes que buscan obtener ganancias intentarán tomar todo lo que puedan mientras estén dentro del sistema o la red.

Como resultado de esto, BlackBerry observó algunos enfoques indiscriminados automatizados respecto de la exfiltración de datos de parte de grupos de ransomware durante el último año. Algunos cuentan con scripts bien diseñados que apuntan a tipos de archivos específicos a recopilar: por lo general, documentos de Microsoft® Word, Excel® y PDF con menos de un año de antigüedad. Después, se cargan los datos robados a la infraestructura del atacante. En otras instancias, BlackBerry identificó a atacantes que buscaban comprimir unidades compartidas enteras del nivel más alto dentro de las empresas en un intento por hacerse con todo lo que esté disponible.

Junto con grupos de ransomware como Conti, DarkSide, BlackMatter y otros que actualmente acaparan los titulares, existe una nueva afluencia de operaciones de ransomware que ocurren mediante RaaS. BlackBerry observó distintos incidentes en los que las empresas fueron atacadas usando una variante de un ransomware muy conocido. Sin embargo, las tácticas, técnicas y procedimientos (TTP) utilizados por el atacante carecían de sofisticación o profundidad. En varios incidentes, BlackBerry identificó a atacantes que dejaban atrás archivos de texto de tácticas que contenían indicadores de compromiso (IOC) con comandos exactos, direcciones IP, listas de objetivos y más. Esto sugiere que los autores de estas familias de ransomware sofisticadas no son quienes de hecho ejecutan los ataques.

Los atacantes con motivaciones financieras continúan teniendo en la mira a presas fáciles en lo que respecta a la fase de compromiso inicial de su ataque.

Los atacantes con motivaciones financieras continúan teniendo en la mira a presas fáciles en lo que respecta a la fase de compromiso inicial de su ataque. Desafortunadamente, el año pasado abundaron los objetivos debido al uso continuo de infraestructura y tecnologías más antiguas en los entornos de las víctimas, como los servidores en las instalaciones. Por ejemplo, ProxyLogon y ProxyShell, nombres comunes para dos conjuntos de vulnerabilidades que afectan a muchos servidores de Microsoft Exchange en las instalaciones, fueron vulnerados ampliamente durante el 2021. El grupo de APT HAFNIUM fue el primero en explotar las vulnerabilidades en varias organizaciones. Después de la publicación de la vulnerabilidad ProxyLogon y las vulnerabilidades de seguridad de prueba de concepto, otros atacantes comenzaron a explorar e infectar rápidamente numerosos hosts de Exchange en las instalaciones. Los atacantes que explotaban estas vulnerabilidades solían implantar puertas traseras adicionales, comúnmente como shells web China Chopper, un shell web cada vez más popular y que es muy poderoso a pesar de su tamaño pequeño.

El protocolo de escritorio remoto (RDP) accesible externamente sigue siendo un favorito que persiste; sin embargo, se está haciendo menos común en comparación con otras técnicas. Las vulnerabilidades que afectan los aparatos de proveedores, especialmente VPN, firewalls y dispositivos de red de perímetro, siguen siendo la causa raíz de muchos incidentes. Si bien estas vulnerabilidades suelen ser anticuadas y estar bien documentadas, BlackBerry observó varios incidentes en los que los dispositivos no contaban con parches instalados.

En otros casos, se instalaron parches a aparatos de red anteriormente vulnerables, pero recién después de que fueran comprometidos. Estos incidentes desembocaron en el robo de credenciales o la instalación de puertas traseras. La enorme cantidad de credenciales y entornos comprometidos impulsaron los mercados de la internet oscura, en donde se aplica un valor a las cuentas de administrador de dominio. Sin embargo, no es difícil también encontrar credenciales empresariales o privadas disponibles de forma gratuita.

Además de las técnicas mencionadas antes, BlackBerry observó varios incidentes con ataques de abrevadero. Los ataques de abrevadero brindan una manera única de penetrar y establecer acceso persistente en un entorno. Estos ataques apuntaron a usuarios que realizaban búsquedas legítimas de material relacionado con su negocio, una práctica común del lugar de trabajo. En estos incidentes, los resultados de las búsquedas arrojaron la URL del abrevadero cerca de la parte superior de la primera página de resultados de la búsqueda en Google™. El sitio del ataque de abrevadero presentaba al usuario lo que parecía ser una publicación útil de un foro con un enlace a exactamente lo que necesitaba. Incluía varios comentarios falsos afirmando que el archivo del enlace era una coincidencia exacta de su consulta.

Sin embargo, si los usuarios abrían el documento usado como arma, un malware descargaba e instalaba una baliza de Cobalt Strike, permitiendo así que los atacantes penetraran el entorno.

REvil es uno de los grupos de atacantes más conocidos actualmente que utilizan esta técnica. Este grupo de amenazas fue identificado inicialmente en el 2019. Son uno de los grupos de ransomware dominantes, atribuyéndose la responsabilidad por algunos de los ataques de ransomware más infames de los últimos años. También estuvieron muy ligados al grupo DarkSide, responsable del ataque a Colonial Pipeline. El grupo vinculado a Rusia estuvo bajo escrutinio recientemente y en varias ocasiones pasó a operar desde la clandestinidad, solo para volver a emerger después.

El aumento en el uso de Cobalt Strike es otra tendencia observada en el último año. BlackBerry fue testigo de cómo se lo aprovechó como un kit de herramientas posterior a una explotación sumamente eficaz y popular durante varios años. Su abuso siguió en aumento al punto de que es común encontrar pruebas de su uso durante una intervención de respuesta ante incidentes. Para quienes estén familiarizados con él, BlackBerry recomienda revisar nuestro nuevo y acreditado libro sobre Cobalt Strike, publicado por el equipo de Investigación e Inteligencia de Amenazas de BlackBerry en noviembre del 2021.

Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence (Balizas en la oscuridad: guía de inteligencia sobre amenazas cibernéticas)

EL CICLO DE VIDA DE UN ATAQUE

El Red Team de BlackBerry analiza el ciclo de vida completo de un ataque como parte de nuestra misión y cartera de ofertas de servicios. Nuestra simulación de adversarios de extremo a extremo ofrece una perspectiva única de los atacantes, al permitirnos observar la eficacia de distintas defensas en una serie de organizaciones. Estas experiencias nos instaron a revelar algunos de los ataques más comunes y las defensas más eficaces que encontramos.

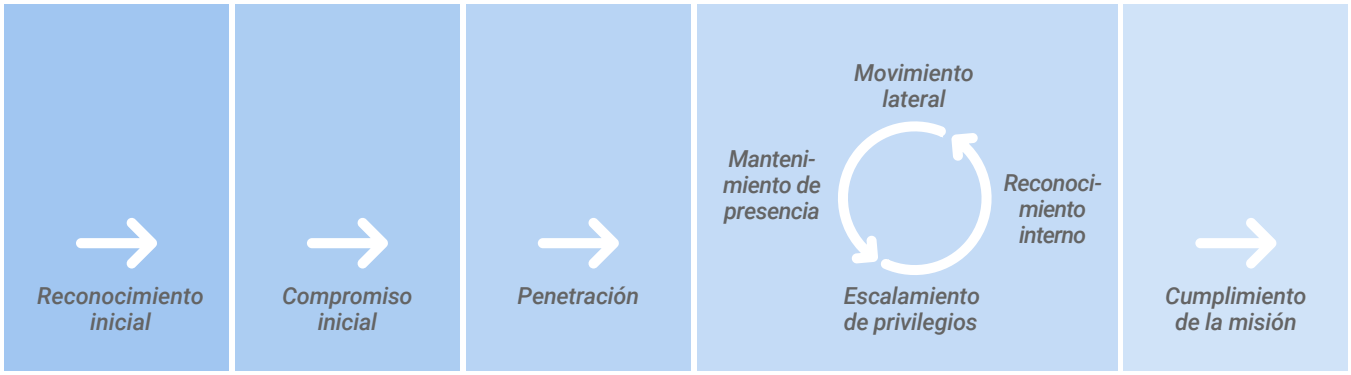


Figura 24: Ciclo de vida de un ataque típico

RECONOCIMIENTO INICIAL

El reconocimiento inicial que lleva a cabo un atacante puede ser pasivo, activo o ambos. Dado que el reconocimiento pasivo no afecta a los sistemas objetivo, puede ser difícil de detectar. Sin embargo, una vez que el reconocimiento pasa a actividades más activas e intrusivas, como sondear los sistemas en busca de vulnerabilidades, los defensores deben ser alertados. Las estrategias de defensa clave para esta fase implican conocer los activos de su organización, explorar de manera proactiva, instalar parches, monitorear y reducir la superficie de ataque.

COMPROMISO INICIAL Y PUNTO DE PENETRACIÓN

Una vez que se descubre una vulnerabilidad durante la fase de reconocimiento, los atacantes la explotan y establecen su presencia en el host. Desde ahí, los atacantes pueden recuperar el acceso más adelante y pasar a otros sistemas en la red. Esta actividad es algo que las organizaciones deben detectar y bloquear mediante una defensa por capas de visibilidad de host y red basada en IA, y técnicas de bloqueo.

ESCALADA

Los atacantes normalmente obtienen un acceso equivalente al de la aplicación que vulneraron, y lo utilizan para comprometer al host. Esta es una de las muchas razones por las que el principio de privilegios mínimos es importante. Además de seguir las prácticas recomendadas, el software de EPP debe contar con capas de defensa para incluir bloqueo de scripts y protección de la memoria. El objetivo es hacer que sea sumamente difícil que

un atacante logre alcanzar cada paso del ciclo de vida de un ataque. Ralentizar el avance del adversario también les permite a los defensores ganar tiempo para detectar y bloquear el ataque.

RECONOCIMIENTO INTERNO Y MOVIMIENTO LATERAL

Una vez que el atacante consigue suficientes privilegios, avanza por la red y se posiciona para lograr su objetivo. Una de las mejores defensas en esta situación es emplear segmentación de red y procurar detectar anomalías consecuencia del uso de las credenciales robadas. En esta fase, los equipos de defensa pueden beneficiarse enormemente del uso de tecnología de defensa impulsada por IA, como autenticación continua mediante información biométrica pasiva. Esta información biométrica pasiva son las actividades del usuario de baja carga, como los patrones de uso del teclado y el mouse, que identifican a los usuarios de manera única. Se puede aplicar un algoritmo de AA a estos metadatos para crear una puntuación de riesgo. Luego, las organizaciones pueden utilizar acciones, como forzar una nueva autenticación o bloquear a un usuario, cuando la puntuación de riesgo supera el umbral definido por la organización.

CUMPLIMIENTO DE LA MISIÓN

Antes de que el Red Team de BlackBerry realice un ejercicio de simulación de adversarios, definimos los objetivos junto con nuestros clientes. Esto casi siempre incluye algún tipo de exfiltración de datos (o indicadores), dado que muchos atacantes tienen motivos financieros. Los atacantes pueden recibir pagos de diversas formas, como con la venta de los datos robados o el desbloqueo de los datos cifrados.

Maneras en que los atacantes reciben pagos

Vendiendo datos robados

Amenazando con vender datos robados

Desbloqueando datos cifrados

APRENDIZAJE

Estas son algunas verdades universales útiles para recordar sobre el ciclo de vida de un ataque y la cadena de ataque cibernética:

- Sea proactivo. Cuanto más a la izquierda esté en el ciclo de vida de un ataque (ver la Figura 24), más fácil y económico será descubrirlo y defenderse ante él.
- Cualquier alternativa al monitoreo constante las 24 horas será insuficiente.
- La misión de la mayoría de los atacantes de hoy en día es exfiltrar datos y lanzar ransomware en busca de ganancias.
- Las defensas basadas en IA ayudan a las organizaciones a evitar convertirse en el paciente cero y son inmunes al retraso de la escritura de firmas que ocurre con las defensas tradicionales.
- Los esfuerzos de defensa siempre deben ser continuos, debido a las vulnerabilidades recientemente descubiertas y el panorama de amenazas en constante evolución.
- La prevención es clave. La capacidad de recuperarse a partir de copias de seguridad no aborda la táctica de doble extorsión derivada de los atacantes que amenazan con vender los datos robados.

LA PROTECCIÓN DE LA INFRAESTRUCTURA CRÍTICA

Cada organización, en cada sector vertical de la industria, queda expuesta a fugas de datos, despliegues de ransomware y extorsión. Sin embargo, pocas corren el mismo riesgo del mundo real de sufrir un ataque cibernético que las que están en el sector de la infraestructura crítica. El público espera que servicios necesarios como la electricidad, el gas, el agua y el tratamiento de desechos siempre puedan prestarse. Como resultado, estas organizaciones están significativamente motivadas a cumplir con estas expectativas, lo que las hace objetivos lucrativos para el pedido de rescates y la extorsión.

Desafortunadamente, los desafíos para este sector exceden el hecho de que se traten de objetivos de alto valor. Los siguientes factores complican más el problema:

- Los dispositivos más antiguos, inherentemente más vulnerables y sensibles
- Los sistemas operativos heredados
- La necesidad de contar con entornos fuera de línea/desconectados

Cada organización, en cada sector vertical de la industria, queda expuesta a fugas de datos, despliegues de ransomware y extorsión. Sin embargo, pocas corren el mismo riesgo del mundo real de sufrir un ataque cibernético que las que están en el sector de la infraestructura crítica.

Numerosos dispositivos y sistemas de infraestructura crítica se utilizan desde hace mucho tiempo y, originalmente, fueron diseñados para la comunicación secuencial, pero más tarde se adaptaron a redes de TCP/IP ubicuas. Esta adaptación de la conectividad no necesariamente incluyó una actualización de seguridad. Dado que estos entornos pueden ser difíciles y costosos de modernizar, normalmente admiten sistemas operativos más viejos y, por lo general, sin soporte.

Con frecuencia, la necesidad de proteger los entornos tiene como consecuencia la segmentación de otras redes, y, con suerte, de internet también. Sin embargo, esta segmentación presenta desafíos de gestión y protección adicionales.

En resumen, las protecciones necesitan ampliarse a dispositivos más antiguos con sistemas operativos heredados, desconectados de las redes e internet. Una solución posible es el uso de protección de puntos finales basada en aprendizaje automático que resida en el punto final mismo. Este tipo de software de plataforma de protección para puntos finales (EPP) puede ejecutarse en sistemas operativos heredados como Windows XP/2003. Si es ligero, no sobreexigirá al hardware anticuado. El modelo matemático localizado debe estar diseñado para evitar la necesidad constante de desplegar actualizaciones de firmas.

El software AV tradicional necesita que se escriban firmas para las amenazas más recientes y que estas se publiquen incluso cada hora. Esto resulta difícil de mantener, aun con hardware moderno y hosts conectados a internet. De modo que es una mala elección para la infraestructura crítica que está desconectada y requiere un enfoque de transferencia de datos con medios físicos o “sneakernet” para distribuir actualizaciones de firmas. Las defensas basadas en IA ofrecen un tiempo de espera mucho más largo entre actualizaciones, ya que identifican las amenazas usando millones de atributos, y no mediante firmas conocidas.

Proteger un entorno de infraestructura crítica es un gran desafío, pero no imposible. Al igual que otros sectores de la industria, simplemente necesita evolucionar más allá de la dependencia en tecnología de defensa heredada que no puede escalarse para evitar ataques cibernéticos modernos.

LA IA CON PRIORIDAD EN LA PREVENCIÓN

La IA y el AA ofrecen muchas capacidades y ventajas para proteger a las organizaciones de los ataques cibernéticos. Si bien los términos IA y AA suelen usarse indistintamente, son conceptos diferentes en ciertos aspectos clave. La IA describe la capacidad de las computadoras o máquinas de realizar actividades que imitan el comportamiento humano inteligente. El AA es un subconjunto de la IA que se basa en algoritmos matemáticos para alcanzar la funcionalidad y el comportamiento de la IA. El proceso que respalda el entrenamiento del AA requiere acceso a enormes cantidades de datos históricos como base para el aprendizaje. Mediante múltiples fases, se introducen nuevos datos para mejorar las funciones de aprendizaje del modelo de AA antes de que, finalmente, se convierta en un componente de la IA.

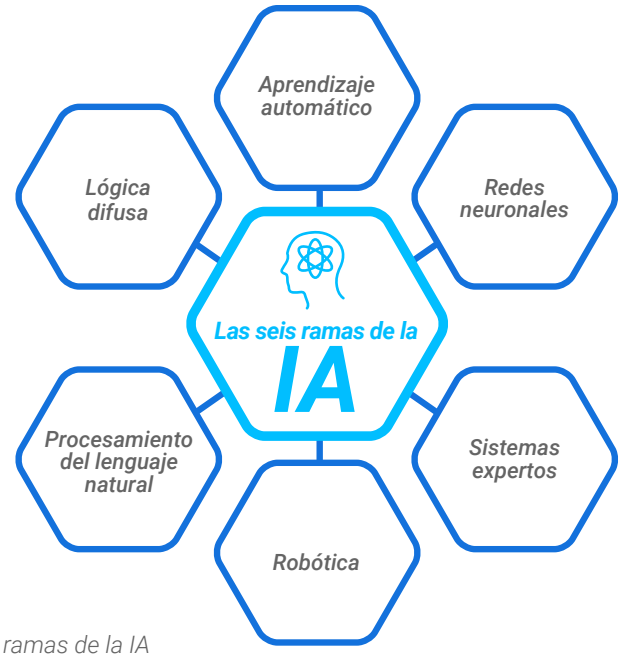


Figura 25: Las seis ramas de la IA

De hecho, el AA representa solo una de las seis ramas de la IA. Las otras ramas son las redes neuronales, los sistemas expertos, el procesamiento del lenguaje natural, la lógica difusa y la robótica. Por ejemplo, la IA Cylance de BlackBerry combina AA y redes neuronales para identificar y prevenir ataques cibernéticos antes de que se ejecuten. Dado que los agentes de seguridad de IA están bien entrenados y son sumamente livianos, pueden residir en los puntos finales de los usuarios sin afectar a los recursos. Los agentes de seguridad instalados en los dispositivos los mantienen protegidos ya sea que tengan conexión o no. BlackBerry dedicó esfuerzos y fondos de investigación y desarrollo considerables a profundizar su IA Cylance. Contamos con cientos de patentes de IA, AA, seguridad e investigación forense, lo que nos ubica junto con otras empresas líderes centradas en la IA como Google, Facebook y Amazon.

El AA se clasifica en dos categorías diferentes: supervisado y no supervisado. Estas clasificaciones describen las maneras en las que los modelos de AA aprenden a clasificar datos de entrada en los supuestos de salida correctos. En otras palabras, cómo hacen predicciones precisas.

El aprendizaje supervisado es un proceso asistido en el que se guía al algoritmo matemático para predecir los resultados de la entrada de un conjunto de entrenamiento de datos. Con este método, las personas supervisan al AA etiquetando manualmente los conjuntos de datos de entrenamiento. El AA supervisado es como un niño que aprende a montar en bicicleta con ruedas de soporte. El padre lo ayuda hasta que el niño está listo para quitar las ruedas de soporte y montar por su cuenta. El aprendizaje supervisado requiere de cantidades increíblemente grandes de datos de entrenamiento y guía antes de que los modelos matemáticos puedan evaluar las entradas y arrojar los resultados deseados.

El AA no supervisado clasifica los datos en los supuestos de salida correctos sin intervención humana ni datos etiquetados. El aprendizaje no supervisado suele ser la segunda etapa del entrenamiento de los modelos matemáticos, después de ingerir grandes cantidades de datos de entrada de conjuntos de entrenamiento supervisados. Esta fase permite a los científicos de datos ver cómo los modelos matemáticos funcionan por su cuenta, y qué tan bien crean los resultados deseados. Volviendo a la alegoría de la bicicleta, el aprendizaje no supervisado es cuando el padre quita las ruedas de soporte para ver qué tan bien el niño puede montar la bicicleta sin ayuda.

IA + AA

En BlackBerry, nuestros modelos matemáticos de IA utilizan AA supervisado y no supervisado para entrenarse sobre cómo identificar un binario bueno y diferenciarlo de uno malo.

En BlackBerry, nuestros modelos matemáticos de IA utilizan AA supervisado y no supervisado para entrenarse sobre cómo identificar un binario bueno y diferenciarlo de uno malo. Los conjuntos de datos son amplios y se basan en millones de características de archivos. Al determinar el peligro que implica un archivo, sus características (todo lo que compone el archivo) se extraen para, esencialmente, brindar su ADN digital. Estas características se correlacionan con aproximadamente otras 2,7 millones con las que nuestros modelos matemáticos se entrenaron antes. Al entrenarse con un conjunto tan grande de características de archivos, la IA Cylance aprendió a diferenciar rápidamente un archivo bueno de uno malo (o sea, malicioso).

BlackBerry Protect, creado usando la IA Cylance, puede llevar a cabo esta correlación de características en 100 milisegundos o menos y, lo que es más importante, puede lograrlo antes de la ejecución. Esto significa que detiene a la amenaza antes de que pueda ejecutarse. De esta manera, BlackBerry Protect evita que se ejecuten archivos maliciosos, ya sea que se trate de malware conocido o de una amenaza nunca antes vista. Esta capacidad de detener malware de día cero y emergente es lo que llamamos la ventaja predictiva de BlackBerry. Se alcanza gracias a la precisión de nuestros modelos matemáticos, que pueden identificar correctamente archivos maliciosos, con frecuencia años antes de que se los vea en circulación.

¿CÓMO SE LOGRA LA EXTRACCIÓN DE CARACTERÍSTICAS/VECTORIZACIÓN?

Para que las máquinas interpreten las asociaciones del AA de la extracción de características y produzcan un resultado, debe efectuarse la vectorización. La vectorización es el proceso de convertir los datos de entrada en vectores matemáticos usando un formato que las computadoras y los algoritmos de AA puedan leer.

La vectorización existe desde que se construyeron las primeras computadoras. Es la manera en la que los modelos matemáticos de AA pueden correlacionar y agrupar las características de archivos buenos, diferenciándolas de los malos. Formatea la información de características de los archivos de manera tal que las computadoras y los modelos matemáticos la entiendan, y les permite brindar un resultado. Cuando la característica

de un archivo, como código que se espera en un área específica de la memoria, se extrae de un archivo, se convierte en un valor matemático de unos y ceros. Esto permite que los algoritmos de AA de BlackBerry Protect determinen si un archivo es seguro. De ser así, se autoriza su ejecución, pero los archivos maliciosos se bloquean y ponen en cuarentena.

Cabe mencionar que BlackBerry Protect, en las fases iniciales del proceso de aprendizaje de algoritmos, identificó aproximadamente 300 millones de características de archivos. Desde entonces, esto se depuró a 2,7 millones de características críticas que puede utilizar para categorizar y etiquetar la seguridad de un archivo. Las características se refieren tanto a lo que se encuentra en los archivos como lo que se espera. Por ejemplo, si se espera que aparezcan datos en particular en una parte específica del ADN del archivo, pero no están ahí, eso también es una característica.

Una IA bien entrenada ofrece una ventaja increíble respecto de sus contrapartes humanos en la realización de este tipo de análisis y trabajo predictivo. Un analista humano puede demorarse un tiempo considerable en identificar de 150 a 200 características de un archivo. Los algoritmos de AA entrenados pueden identificar, correlacionar y evaluar millones de características y determinar la probabilidad de amenaza de un archivo en tan solo milisegundos.

UN ENFOQUE QUE PRIORIZA LA PREVENCIÓN PARA PROTEGER UNA FUERZA LABORAL CADA VEZ MÁS HÍBRIDA

Resulta tentador culpar a la pandemia de la COVID-19 y el cambio consecuente a una fuerza laboral distribuida por el aumento masivo de ataques cibernéticos de los últimos 18 meses. Una encuesta de IBM reciente parece respaldar esta visión:

$1,07 M

de aumento en costos de fugas (de $3,89 M a $4,96 M) cuando el trabajo remoto fue un factor.

58 días

más de tiempo en identificar y contener una fuga cuando el 50 % o más de los empleados trabajan de manera remota.

Es cierto que expandir la red corporativa para incluir el entorno hogareño y los dispositivos personales crea brechas de seguridad que los adversarios pueden explotar. Sin embargo, si nuestras prácticas y tecnologías de seguridad actuales fueran lo suficientemente sólidas como para poder escalarse fácilmente, la transición podría haber sido mucho menos disruptiva para muchas organizaciones de lo que resultó ser.

El phishing dirigido y el abuso de credenciales ya eran problemas mayores antes de la pandemia. Siguen representando la mayoría de las filtraciones en la actualidad. Los productos de infraestructura de escritorios virtuales y VPN ya eran vulnerables a explotaciones antes de la COVID-19. Y lo siguen siendo hoy. Lo mismo ocurre con los servidores sin parches y las amenazas causadas por empleados maliciosos, o por usuarios con malas prácticas de higiene cibernética.

El problema real es que los enfoques de seguridad actuales son insostenibles porque, inherentemente, son reactivos y poco realistas. No puede esperarse que un empleado de recursos humanos responsable de examinar currículums todo el día sepa cuándo un documento está siendo usado como un arma, y evite abrirlo. Tampoco se debe esperar que los profesionales de SecOps y NetOps responsables de proteger una infraestructura compleja y en rápida evolución anticipen e impidan manualmente cada potencial ataque.

El problema no puede resolverse capacitando a cada empleado para que también se convierta en un experto en ciberseguridad. No se puede arreglar sumando otra capa o herramienta de seguridad más a una arquitectura de seguridad que es fundamentalmente reactiva. BlackBerry cree que una solución más realista es transicionar a una estrategia de seguridad con prioridad en la prevención. Al sacar provecho de soluciones inteligentes que se centran en perjudicar y obstaculizar ataques cibernéticos, los empleados pueden concentrarse en los trabajos para los que se los contrató.

A nivel de los dispositivos, esto significa el tradicional bloqueo y enfrentamiento. Los sistemas vulnerables deben emparcharse y actualizarse. Las defensas reactivas basadas en firmas deben reemplazarse por protección de puntos finales impulsada por IA que evite la ejecución de malware de día cero y conocido.

Luego, se deben desplegar controles de seguridad enfocados en los usuarios en cada punto de ingreso a redes empresariales y aplicaciones en la nube que eviten que los empleados remotos puedan abusar de sus credenciales o violar políticas de seguridad, ya sea intencional o accidentalmente. El acceso de cada usuario a los recursos debe controlarse dinámicamente, basándose en evaluaciones del riesgo en tiempo real de su comportamiento actual. Para preservar la productividad, este proceso continuo de autenticación debe ser lo más transparente posible para los usuarios, pero no permitir soluciones alternativas o evasiones.

Las herramientas que dependen de análisis basado en reglas estáticas no pueden lograr esto. No resulta posible elaborar reglas que anticipen cada gradación de comportamiento riesgoso o anómalo. Y el análisis retrospectivo que suelen producir llega demasiado tarde como para evitar la explotación. Esto requiere de soluciones diseñadas con IA que aprendan cómo evaluar los riesgos y evitar la explotación de manera proactiva, en lugar de responder después de los hechos cuando el daño ya ha comenzado.

Si se implementa debidamente, la estrategia con prioridad en la prevención preserva los beneficios de flexibilidad y productividad de contar con una fuerza de trabajo híbrida o remota en primer lugar.

El equilibrio entre la prevención y la productividad: lo mejor de ambos mundos.

DETECCIÓN Y RESPUESTA EXTENDIDAS

En la actualidad, los equipos de seguridad enfrentan muchos desafíos. Los atacantes ejecutan rápidamente ataques más sofisticados, imperceptibles y de múltiples vectores en distintas superficies de ataque como puntos finales, la nube, redes, aplicaciones y dispositivos móviles. Las soluciones de detección y respuesta para puntos finales (EDR) crearon un plano de defensa brindando capacidades potentes de detección de amenazas y respuesta ante incidentes para los puntos finales. Sin embargo, se necesita de una protección más proactiva e integral que cubra toda la superficie de ataque.

Esta demanda impulsó la creación de la detección y respuesta extendidas (XDR). Se trata de una evolución de la EDR que unifica la protección en el punto final con otras herramientas de seguridad. Optimiza la visibilidad y detección para los analistas, y ofrece capacidades de correlación, investigación y respuesta más eficaces.

La XDR es una evolución de la EDR que unifica la protección en el punto final con otras herramientas de seguridad. Optimiza la visibilidad y detección para los analistas, y ofrece capacidades de correlación, investigación y respuesta más eficaces.

¿QUÉ ES LA XDR?

Los productos de XDR, en esencia, son estrategias de enriquecimiento e inclusión. Esto significa que incorporan información recogida de sus propias plataformas de productos, y la integran con datos de telemetría ingeridos de socios y otras fuentes. Estos datos se combinan para crear contexto adicional, que se comparte como inteligencia de amenazas cibernéticas (CTI) procesable dentro del producto.

Cuando se la aprovecha para la detección de amenazas, combinar esta nueva inteligencia permite a los proveedores de XDR mejorar las capacidades de los productos e incrementar sus oportunidades en el mercado. Esta inteligencia de amenazas posibilita que los productos remedien riesgos de manera proactiva y, luego, informen a los clientes de las medidas tomadas para proteger a sus organizaciones. Una mejor inteligencia sobre amenazas también permite que el desarrollo de productos sea dinámico respecto de las necesidades y las exigencias del cliente.

¿CUÁLES SON LOS BENEFICIOS DE LA XDR?

La inteligencia sobre amenazas enriquecida, que se recopila de toda la superficie de ataque, puede contextualizarse para mejorar las medidas de respuesta humanas y automatizadas. Por ejemplo, un analista de seguridad puede perder mucho tiempo sorteando alertas y datos de amenazas informados por muchas fuentes. Una plataforma de XDR puede correlacionar de manera inteligente los datos de amenazas de todo el entorno y reenviar la información de alto valor a los analistas mientras filtra el ruido. Con datos de XDR enriquecidos, el analista puede comprender mejor el entorno y dispone de más tiempo para tomar decisiones de seguridad fundamentadas y efectivas.

Los proveedores de XDR como BlackBerry entienden los datos y lo que significan para la comunidad de seguridad y nuestros clientes, independientemente de la estructura, el origen o la ubicación. Hacemos que los datos perduren en una estructura que admite el acceso y procesamiento compartidos con facilidad, de modo que puedan ser utilizados por la totalidad de nuestra plataforma.

Los proveedores de XDR pueden garantizar que ofrecen alertas de eventos de la más alta fidelidad si cuentan con expertos que entienden y aprueban los datos que fluyen desde varios sensores. Los datos seleccionados profesionalmente posibilitan respuestas automáticas para evitar amenazas y brindan remediación que sigue mejorando incluso cuando los ataques se hacen más sofisticados.

¿EN QUÉ SE DIFERENCIA LA XDR DE LA SIEM?

El enfoque típico del equipo del centro de operaciones de seguridad (SOC) respecto de tener administración de eventos e información de seguridad (SIEM) además de todos los productos de detección tiene muchas contras. Las soluciones de SIEM son buenas para recopilar y almacenar registros que son útiles en casos de uso forenses y de cumplimiento, pero no pueden generar alertas de detección de alta fidelidad.

Las soluciones de SIEM no producen y recopilan datos de forma nativa. Simplemente consumen datos, sin recopilar ni considerar el contexto. Los equipos de SOC deben recopilar y correlacionar manualmente los datos de telemetría producidos de forma aislada, lo que da como resultado alertas de baja fidelidad.

Se requiere de un nuevo enfoque respecto de la arquitectura para resolver algunos de estos problemas modernos de los SOC. En este punto interviene la XDR. El agente de seguridad y sensor de un proveedor producen y recopilan la mayoría de los datos de telemetría de toda la superficie de ataque y los centralizan en una plataforma en la nube. Esto brinda un repositorio de datos de amenazas valiosos sin la necesidad de ingestión, correlación y enriquecimiento de datos manual.

Cuando ocurren incidentes, los analistas de los SOC con frecuencia se ven forzados a malgastar tiempo de respuesta crítico compilando datos de telemetría manualmente para crear una línea temporal de resumen necesaria a fin de determinar las intenciones del atacante. Las soluciones de XDR permiten la detección automatizada de amenazas con historias de ataques creadas previamente. Esta automatización reduce el tiempo necesario para la detección y respuesta.

¿QUÉ DEBE TENER UNA BUENA SOLUCIÓN DE XDR?

La XDR es una plataforma que unifica las capacidades de muchos productos distintos en una única experiencia personalizable, simple y robusta. Representa la fusión de la inteligencia de productos nativos y de terceros que posibilita capacidades de respuesta necesarias. En resumen, los productos de XDR eficaces deben:

Por supuesto, las mejores soluciones de XDR no pueden detener las amenazas por sí solas. Algunas plataformas de XDR pueden incluir tecnologías con prioridad en la prevención, análisis asistido por IA y automatización, pero siguen siendo los especialistas humanos quienes deben determinar qué califica como una amenaza en su entorno. Todos los

datos de telemetría de amenazas que recopila la XDR a partir de soluciones principales y de terceros deben ser, en última instancia, interpretados por analistas capacitados. Esto puede hacer que los servicios de XDR administradas sean una opción atractiva para las organizaciones que operan con presupuestos de ciberseguridad más pequeños.

600 %

Incremento en los delitos cibernéticos debido a la COVID-19

LA EVOLUCIÓN DE LOS SERVICIOS DE DETECCIÓN Y RESPUESTA ADMINISTRADAS

Las amenazas cibernéticas cada vez más complejas y sofisticadas están cambiando la forma en que las organizaciones abordan la seguridad cibernética. Algunos atacantes han virado el enfoque y pasaron de comprometer infraestructura a explotar a personas mediante el aumento de campañas de phishing dirigidas. Este cambio, entre otros, implica que las defensas tradicionales resulten inadecuadas para abordar la multitud de vectores de amenazas vulnerados por los adversarios contemporáneos. Las organizaciones que hoy buscan socios de detección y respuesta necesitan proveedores que puedan hacer frente a una amplia variedad de ataques cibernéticos avanzados. Un vistazo al panorama de amenazas muestra que las organizaciones enfrentan una batalla cuesta arriba:

- Se descubrieron 667 millones de nuevas detecciones de malware en todo el mundo en el año 2020.
- Hubo un aumento del 600 % en delitos cibernéticos debido a la pandemia de la COVID-19.
- Se necesitan 4 millones de trabajadores de ciberseguridad adicionales a nivel global.
- Se ven 1 millón de alertas de seguridad diarias en el 25 % de los SOC.

Las organizaciones operan en un entorno en constante cambio mientras que los atacantes los observan sigilosamente, buscando la oportunidad para atacar. Las organizaciones deben encontrar la manera de salir adelante sin quedar expuestas a ataques cibernéticos oportunistas. Los servicios de detección y respuesta administradas (MDR) pueden ayudar a las organizaciones a navegar de manera segura las aguas turbulentas de la tecnología insegura de una fuerza laboral híbrida o móvil. Las plataformas de MDR ofrecen soporte profesional 365x24x7 para la detección de intrusiones, la respuesta ante incidentes y la eliminación de amenazas.

El ataque de HAFNIUM de enero del 2021 es un ejemplo perfecto de cómo una plataforma de MDR ayuda a las organizaciones. Durante la campaña, al menos 30 000 organizaciones en los EE. UU. se vieron comprometidas por una unidad de espionaje cibernético china, conocida como HAFNIUM. Estos ataques fueron en su mayoría automatizados y estuvieron dirigidos a servidores de Microsoft Exchange sin parches instalados.

Un equipo de MDR podría combatir HAFNIUM si reúne e investiga exhaustivamente todas las fuentes de distribución de inteligencia de amenazas disponibles. La información recopilada puede incluir indicadores de compromiso (IOC), líneas de comandos, procesos en ejecución, claves de registro, solicitudes de DNS y más. Luego, el equipo de MDR realizaría la detección de amenazas adicional. Por ejemplo, los equipos de BlackBerry seguirían buscando amenazas mediante el uso de herramientas como InstaQuery, a través de API.

Mediante la recopilación de información y la detección de amenazas, un equipo de MDR experimentado puede identificar rápidamente una amenaza cibernética específica. Brindan a sus clientes instrucciones de remediación y prácticas recomendadas rápidamente, así como actualizaciones a medida que cuentan con más información. Los equipos de MDR proactivos incluso pueden establecer una serie de reglas específicas para HAFNIUM directamente en una herramienta de EDR; reglas que apliquen las técnicas del marco MITRE ATT&CK®, por ejemplo.

Dado el panorama de amenazas cambiante y sofisticado, la necesidad de los analistas de contar con telemetría y visibilidad integral de todas las herramientas de seguridad es mayor. Las soluciones de XDR administradas se basan en el marco de servicios de MDR mediante la incorporación de visibilidad de XDR en toda la empresa. Las plataformas de XDR unifican las detecciones de puntos finales relevantes para la seguridad mediante la recopilación y contextualización de los datos de telemetría de amenazas de las herramientas de terceros. Por ejemplo, una plataforma de XDR puede recoger y analizar datos de fuentes de la red y SIEM, seguridad de correo electrónico, administración de identidades y acceso, firewall de última generación y más. Una solución de XDR administradas es nativa en la nube y se basa una infraestructura de grandes volúmenes de datos para brindar flexibilidad, escalabilidad y oportunidades de automatización a los equipos de seguridad. Una solución de XDR administradas puede ofrecer a las pequeñas y medianas empresas un nivel de protección que, de lo contrario, pocas organizaciones podrían costear. Por ejemplo, una solución de XDR administradas puede proporcionar:

Una solución de XDR administradas puede ofrecerles a las organizaciones acceso ininterrumpido a profesionales de ciberseguridad avezados que utilizan herramientas de detección y respuesta de última generación. Esto puede dar a las organizaciones una gran tranquilidad y permitirles centrarse en su misión principal, en lugar de tener que preocuparse por ataques cibernéticos.

LA AMPLIACIÓN DEL ROL DE LA SEGURIDAD DE REDES Y LA IA/EL AA EN LA PREVENCIÓN DE ATAQUES DE DÍA CERO

La red fue la portadora de las vulnerabilidades de seguridad más atacadas y explotadas del 2020 y 2021. En el 2020, varias de estas vulnerabilidades afectaron el trabajo remoto, las VPN o las tecnologías basadas en la nube. En el 2021, los atacantes cibernéticos maliciosos siguieron apuntando a dispositivos de perímetro y comprometiéndolos. Se descubrieron vulnerabilidades altamente explotadas en muchas plataformas cibernéticas populares, como las de Microsoft, Pulse, Accellion, VMware y Fortinet. Esta ola de ataques exitosos hizo que se incrementara el enfoque en proteger la conectividad de la red.

Las organizaciones están optando por estrategias de ciberseguridad más nuevas como acceso a la red de confianza cero (ZTNA), perímetro de servicio de acceso seguro y XDR. A nivel macro, el marco MITRE ATT&CK también brindó recursos que mejoran la cobertura de los ataques respecto de vulnerabilidades específicas de la red. Los ataques de día cero alentaron a los analistas de seguridad a combinar defensas y tecnologías para reforzar las medidas de seguridad. Entre las estrategias utilizadas se pueden mencionar:

- Tecnología con prioridad en la prevención
- Enfoques con prioridad en la protección
- Análisis basado en firmas
- Detección de amenazas y anomalías basada en IA y AA en la capa de red
- Correlación avanzada de varias fuentes de datos de telemetría

El tejido de la red también enfrenta grandes cambios. Las soluciones de VPN basadas en IPSec fueron un punto álgido de varias vulnerabilidades de seguridad recientes, destacando la necesidad de contar con pilas de protocolos TCP/IP seguras y modernas. De manera similar, una estrategia respecto del malware basada exclusivamente en firmas requiere que al menos un usuario se infecte para poder así obtener una muestra maliciosa. Esto ha multiplicado los enfoques basados en IA y AA, que pueden analizar amenazas en la capa de red y evitar ataques de día cero.

EL ROL DE LA IA Y EL AA

Cuando hablamos de detección de amenazas a la red, la IA y el AA desempeñan un rol importante, ya que ejemplifican el comportamiento normal de la organización y sus usuarios. Pueden detectar anomalías que no se condicen con el comportamiento de ningún usuario autorizado. También pueden predecir si es más o menos probable que cierto comportamiento de la red esté asociado con un usuario específico. Esto brinda una manera eficaz de identificar balizas de C2, por ejemplo, y diferenciarlas de procesos benignos y de uso de la red iniciado por un usuario. Esta capacidad de detección de anomalías basada en modelos e impulsada por IA y predicción específica de cada usuario puede reducir tanto los falsos positivos como los falsos negativos.

EL EMPLEADO MALICIOSO

Para los empleados maliciosos, los modelos de comportamiento predictivo y detección de acceso anómalo pueden ser menos eficaces. El empleado malicioso por lo general seguirá con su propio comportamiento anterior y puede compartir muchas características con el acceso de la organización y los usuarios que de otra forma resultaría normal. Sin embargo, el comportamiento abiertamente malicioso, anormal o sospechoso todavía puede llamar la atención.

EL EXTRAÑO MALICIOSO

Los modelos de IA son sumamente eficaces contra extraños maliciosos, como quienes acceden subrepticiamente a un dispositivo desbloqueado u obtienen acceso ilícito a credenciales de usuario legítimas. Es mucho menos probable que el comportamiento de un extraño malicioso siga continuamente el comportamiento modelado del usuario comprometido. También es probable que el comportamiento del extraño entre en conflicto con el de la organización como un todo. Es posible que inicien sesión fuera del horario laboral habitual, accedan a recursos nuevos o realicen acciones atípicas, como intentar descargar bases de datos que rápidamente los identifican como amenazas.

MALWARE

Al igual que en el caso de los extraños maliciosos, el acceso a puntos finales anómalo o poco probable de parte de malware puede disparar detecciones. Alertar al usuario legítimo sobre la actividad maliciosa le permite detener el acceso y denunciar el problema a su SOC. Además, el malware y su C2 asociado exhiben patrones de redes que son atípicos del comportamiento legítimo de los usuarios. Para una protección adicional, se pueden desarrollar modelos del comportamiento de amenazas por separado a fin de optimizar la detección. La configuración de acciones de respuesta automatizadas para el comportamiento de amenazas modelado protege al entorno en los casos en los que el usuario legítimo no rechaza los intentos de acceso sospechosos.

DETECCIÓN DE AMENAZAS A LA RED BASADA EN REGLAS

La protección holística de la red incluye una combinación de tecnología de IA y AA y detección de amenazas a la red basada en reglas. Por ejemplo, el tráfico IDS/IPS puede usarse para analizar, evaluar y filtrar comunicaciones. El tráfico puede evaluarse mediante reglas creadas previamente, como SNORT, y, luego, desplegarse para prevenir y detectar tráfico malicioso. Una regla puede asociarse con una acción de respuesta correspondiente, como alertar, permitir o bloquear. Por lo general, los administradores del SOC mantienen visibilidad de las acciones realizadas por SNORT o reglas similares. La detección basada en reglas por sí sola puede aumentar significativamente la cobertura de MITRE ATT&CK en áreas como el escalamiento de privilegios, movimiento lateral, comando y control, exfiltración de datos, etc.

MICROSOFT Y HAFNIUM

El atacante patrocinado por el estado HAFNIUM utilizó vulnerabilidades de parche en servidores de Microsoft Exchange en las instalaciones para comprometer cuentas de correo electrónico. En apenas días, delincuentes más allá de HAFNIUM comenzaron a atacar sistemas sin parches y a instalar malware para obtener acceso a largo plazo a entornos comprometidos.

Una combinación de seguridad cibernética que prioriza la prevención y tecnología de detección rápida puede frustrar ataques del estilo de HAFNIUM. Específicamente, las vulnerabilidades de seguridad que explotó HAFNIUM podrían haberse protegido mediante lo siguiente:

- Principios de ZTNA
- Un enfoque de privilegios mínimos respecto del acceso
- Una plataforma de red consciente de la identidad
- Autenticación continua y tecnología de acceso adaptativo
- Soluciones de trabajo remoto que autentican el acceso a aplicaciones individuales, en lugar de a toda la red

LAS VULNERABILIDADES DE SEGURIDAD DE VPN

Las vulnerabilidades de seguridad de VPN de día cero castigaron a la industria en el 2021, desde Sonic VPN y Pulse Secure a Fortinet VPN. Si bien varias de estas vulnerabilidades existían desde hacía ya un tiempo, las tendencias recientes de trabajo desde casa y acceso remoto hicieron que ganaran más atención. A medida que una tecnología atrae más usuarios y organizaciones, se vuelve más valiosa para los atacantes.

Para evitar las vulnerabilidades de seguridad de VPN y a la vez posibilitar una fuerza laboral remota y móvil, las organizaciones deben considerar adoptar lo siguiente:

- Una arquitectura de red de confianza cero definida por software
- Una red basada en una pila de protocolos TCP/IP sólida
- Protección de la conectividad a través de los principios de acceso de privilegios mínimos
- Soluciones que ofrecen control de acceso a la red segmentado para separar el tráfico de red profesional del personal
- Controles de acceso dinámico que puedan brindar acceso cuando es necesario a una plataforma que ofrezca visibilidad plena del tráfico de la red de los recursos en las instalaciones y en la nube

LAS AMENAZAS MÓVILES Y LA SEGURIDAD

76 %

Según estudios recientes, un increíble 76 % de las aplicaciones móviles probadas almacenan los datos de manera insegura.

La seguridad de dispositivos móviles debe ser una cuestión seria para toda organización. Considere el estado actual del mercado de teléfonos inteligentes, que se divide entre dispositivos Android™ y iPhone®. Según estudios recientes, un increíble 76 % de las aplicaciones móviles probadas almacenan los datos de manera insegura. Las aplicaciones inseguras amenazan a las organizaciones con políticas de "use su propio dispositivo" (BYOD), y a las que admiten trabajadores móviles o remotos. El peligro surge del aumento en el uso de parte de los empleados de dispositivos personales no administrados para realizar tareas profesionales. Cuando los recursos empresariales y las aplicaciones vulnerables ocupan el mismo dispositivo y se conectan a redes múltiples, aparecen oportunidades para que ocurran desastres.

Las aplicaciones vulnerables no son la única amenaza móvil a la que se enfrentan las organizaciones. Cuando dispositivos personales almacenan y acceden a recursos de la organización, existe riesgo de que los datos empresariales se expongan accidentalmente. Las filtraciones podrían ser simples, como reenviar correos electrónicos confidenciales a la dirección equivocada, o graves, como revelar credenciales de usuario e información de identificación personal. Las fugas de datos pueden ocurrir a través de otras vías también, por ejemplo, al emparejarse con dispositivos de la Internet de las cosas (IoT) y puntos de acceso a la red sin administrar (como una Wi-Fi pública).

El software sin parches instalados y desactualizado también implica un riesgo grave para los dispositivos móviles. En marzo del 2021, se reveló que la aplicación de uso compartido de archivos SHAREit de Android contenía vulnerabilidades que posibilitaban la ejecución remota de código. Los investigadores de amenazas descubrieron el problema y lo notificaron a los desarrolladores en diciembre del 2020, pero no se publicaron actualizaciones. Para el momento en que los investigadores hicieron públicas las vulnerabilidades, SHAREit ya contaba con más de 1000 millones de descargas.

En América del Norte, los ataques de smishing —es decir, ataques de phishing mediante SMS— a dispositivos móviles se incrementaron en un 300 % durante el tercer trimestre del 2020. Este aumento saltó al 700 % en los primeros seis meses del 2021. Los ataques de smishing llegan como un mensaje de texto de SMS, presuntamente de un contacto de confianza, y suelen contener enlaces maliciosos. Por ejemplo, una víctima podría recibir un mensaje de texto que supuestamente proviene de su banco, que indica que su cuenta está sobregirada. El mensaje de texto contiene un enlace malicioso e insta a la víctima a cliquearlo para conocer más detalles. Si hace clic en el enlace, la víctima puede iniciar una descarga de malware o permitir que capturen su información. Estos ataques son fáciles de realizar dado que lo único que necesita el atacante es el número de teléfono de la víctima. Además, los mensajes de SMS truncan las URL, lo que dificulta inspeccionarlas visualmente en busca de señales de advertencia.

Recientemente, las prácticas engañosas de phishing y smishing evolucionaron para convertirse en una amenaza más grande: la de aplicaciones maliciosas que se hacen pasar por programas legítimos. Esta tendencia se notó en particular con aplicaciones de banca, criptomoneda y bursátiles. Las aplicaciones maliciosas instaladas por los usuarios cuentan con el beneficio de la confianza implícita del usuario. Dado que la aplicación recibe permiso del usuario para instalarse y ejecutarse, las estrategias tradicionales de ciberseguridad no siempre logran detectarla. Esto es incluso más complicado cuando las aplicaciones maliciosas se descargan de plataformas de confianza.

LA IA ABORDA LAS AMENAZAS MÓVILES

Las organizaciones se enfrentaron a muchos desafíos de seguridad al intentar admitir una fuerza laboral remota y móvil con la llegada de los confinamientos a causa de la COVID-19. Desde entonces, la fuerza laboral se mantuvo fluctuante, y muchas organizaciones quedaron en la búsqueda de maneras eficaces de combatir las amenazas móviles.

Un enfoque prometedor es la adopción de soluciones impulsadas por IA que emplean modelos matemáticos y análisis predictivo para detectar y prevenir muchos tipos de amenazas. Por ejemplo:

- **Código vulnerable en aplicaciones.** La IA puede extraer características de archivos de una aplicación antes de que se ejecute, y bloquear las que contengan código explotable o malicioso. Esto protege a los usuarios del malware y de aplicaciones plagadas de errores que confían en código abierto o de terceros vulnerable.
- **Fugas de datos.** Las plataformas de gateway inteligentes pueden ofrecer capacidades de túnel completo y dividido que cifran las comunicaciones para los datos confidenciales, pero dejan abiertas las comunicaciones triviales. La IA desempeña un papel esencial en la selección de cómo se clasifica el tráfico de la red, eliminando el riesgo del error humano que causa fugas de datos accidentales.
- **Software desactualizado.** La IA puede monitorear dispositivos en busca de versiones de software desactualizadas y malas configuraciones. Estas verificaciones garantizan que el sistema operativo, las bibliotecas del sistema y el firmware permanezcan actualizados.
- **Puntos de acceso vulnerables.** La IA puede analizar la seguridad de puntos de acceso de Wi-Fi para garantizar que el tráfico móvil no transite por redes privadas o públicas inseguras.
- **Ataques de phishing/smishing.** La IA puede determinar rápidamente la seguridad de las URL, evitando que los usuarios naveguen a ubicaciones inseguras sin saberlo.
- **Aplicaciones maliciosas.** La IA puede detectar aplicaciones maliciosas antes de que se carguen o ejecuten en un dispositivo móvil. Esta capacidad proactiva de detener el malware es una función de la seguridad cibernética que prioriza la prevención.

Si bien ninguna solución es 100 % efectiva contra todos los ataques, la IA puede abordar de manera eficaz muchas de las amenazas que enfrenta la tecnología móvil. La IA puede tomar decisiones fundamentadas en relación con la seguridad de manera continua en segundo plano, permitiendo a los usuarios enfocarse en la productividad. Además, la IA puede monitorear conexiones y tráfico de la red para garantizar que las comunicaciones permanezcan protegidas mientras los usuarios viajan a donde requiera su trabajo, o desempeñan sus tareas desde donde lo requieran sus viajes. Dado que la IA es una tecnología adaptativa, resulta ideal para responder a amenazas conocidas como las que emergen durante épocas de crisis.

LOS VEHÍCULOS CONECTADOS: AVANZANDO HACIA LA SEGURIDAD

En términos de los sistemas electrónicos críticos para la seguridad, cualquier modificación a su comportamiento para evitar ataques maliciosos (incluso la introducción de una nueva prevención) requiere que el sistema vuelva a certificarse.

Los cambios transformacionales que ocurrieron en el transporte personal resaltan la necesidad de tratar los requisitos de seguridad de estas plataformas de datos de red sobre ruedas. La industria automotriz explora usos constructivos de IA, incluso su capacidad de realizar tareas de ciberseguridad críticas.

La mejor manera de entender cómo la seguridad cibernética de la IA con prioridad en la prevención se integra con la conducción conectada es desglosar la tecnología en los componentes individuales de la prevención y la IA. Cada uno puede implementarse independientemente del otro. De la misma manera, se debe trabajar en cada elemento para desplegarlo debidamente en la conducción conectada.

LA PREVENCIÓN DE ATAQUES DE CIBERSEGURIDAD

El primer paso para proteger cualquier sistema es diseñarlo y construirlo de manera tal de minimizar las vulnerabilidades de seguridad. Esta postura se refleja en algunas de las pautas recientes establecidas por la ISO y la ONU:

- La normativa ISO/SAE 21434, publicada en agosto del 2021, establece la norma para manejar la seguridad durante el diseño, la fabricación, el uso y el desguace de un vehículo.
- El reglamento de la ONU R155 contempla la seguridad cibernética no solo en las plataformas automotrices sino también en la infraestructura que las rodea.

Sin embargo, la prevención y detección de amenazas no son cosas diametralmente opuestas. Existen vulnerabilidades que no se encontrarán durante el diseño y desarrollo del sistema. Evitar la explotación de estas vulnerabilidades no identificadas implica detectar un ataque contra el sistema y detener su avance. Las posibilidades de prevenir comportamiento malicioso se verán afectadas por el hecho de que el sistema electrónico sea crítico para la seguridad.

Algunos sistemas electrónicos de los vehículos modernos deben contar con un certificado de seguridad. La normativa ISO 26262 define el nivel de integridad de la seguridad automotriz (ASIL) de A a D. Los eventos peligrosos se clasifican según su gravedad, exposición y capacidad para controlar el vehículo en caso que ocurra el evento. En términos de estos sistemas electrónicos críticos para la seguridad, cualquier modificación a su comportamiento para evitar ataques maliciosos (incluso la introducción de una nueva prevención) requiere que el sistema vuelva a certificarse. La recertificación implica efectuar un análisis de riesgos para cada acción preventiva que pueda realizarse. En el caso de los sistemas electrónicos que no son críticos para la seguridad, cambiar el comportamiento del sistema para prevenir actividad maliciosa en marcha resulta más sencillo.

Normalmente, la implementación de detección de intrusiones precede a la prevención de intrusiones en los entornos nuevos. Permite monitorear y ajustar el sistema sin padecer consecuencias adversas, hasta que sea posible confiar en su operación y habilitar enfoques basados en la prevención.

EL USO DE LA IA

Con la IA, surge la misma distinción importante entre sistemas críticos para la seguridad y otros sistemas del vehículo. Todavía se debate el uso de IA dentro de sistemas críticos para la seguridad. Uno de los desafíos de utilizar IA en un contexto de seguridad es entender el comportamiento del sistema resultante. La garantía de la seguridad depende de entender cómo el sistema responderá a sus entradas. Un sistema de IA basado en AA, en el que el comportamiento no se entiende bien, introduce deuda intelectual. Un sistema con deuda intelectual es una enorme preocupación para los ingenieros de seguridad responsables de la certificación. Los ataques, como los de aprendizaje automático adversarial, destacan la incapacidad del diseñador de entender plenamente cómo todas las entradas pueden afectar las acciones del sistema de IA. Los datos que se emplearon para entrenar al sistema también pueden quedar en la mira del ataque, o no ser representativos de las condiciones del mundo real en constante cambio. Por lo tanto, resulta fundamental no tratar a los nuevos sistemas de IA como infalibles y entender por qué fallan cuando lo hacen.

Reconstruir el estado de un sistema que utiliza IA para ejecutar un análisis posterior al incidente y descubrir por qué falló requerirá de significativamente más recursos en muchas áreas. Todavía queda mucho por hacer en lo que respecta a reducir la deuda intelectual relacionada con la IA. El Safety of Autonomous Systems Working Group (SASWG) publicó pautas sobre las medidas de seguridad de los sistemas autónomos. La normativa ISO TC 22/SC 32 cuenta con varios grupos de trabajo (WG13 y WG14) que están examinando la seguridad de la IA y la conducción autónoma. Entre los problemas de usar IA basada en AA en un sistema crítico para la seguridad se incluyen las amenazas a la IA misma y a los datos que se utilizan para entrenarla o en la producción.

El vehículo es solo uno de los componentes de la red del vehículo conectado. Otros sistemas incluyen la infraestructura de carga, las intersecciones conectadas e incluso la búsqueda de rutas.

Por lo tanto, esperamos que la seguridad cibernética basada en la IA logre hacer avances fuera de los componentes críticos para la seguridad del vehículo antes de su inclusión como componente crítico para la seguridad. La plataforma IVY™ de BlackBerry está diseñada para posibilitar la introducción de IA al vehículo, brindando perspectivas inteligentes para mejorar las experiencias del conductor y el pasajero.

OTRAS ÁREAS QUE REQUIEREN ATENCIÓN

El vehículo es solo uno de los componentes de la red del vehículo conectado. Otros sistemas en la red del vehículo conectado incluyen la infraestructura de carga, las intersecciones conectadas e incluso la búsqueda de rutas. Actualmente, la mayor parte de las búsquedas de rutas se realizan mediante teléfonos inteligentes en lugar de estar integradas en el vehículo. La conducción autónoma a niveles más altos requerirá que la búsqueda de rutas esté integrada en el vehículo. En todas estas redes de apoyo, la IA puede utilizarse para tomar decisiones basadas en los datos. Todas estas redes también presentan el potencial de ataques cibernéticos. Factores como la seguridad seguirán influenciando las decisiones sobre cómo proteger estas redes de la mejor manera contra las amenazas de ciberseguridad.

La seguridad cibernética de IA con prioridad en la prevención no tiene que enfocarse exclusivamente en los entornos de producción. Evitar la introducción de vulnerabilidades durante el diseño y desarrollo del software, incluso el de sistemas de IA, es otra alternativa para mejorar la ciberseguridad. El uso de IA sigue siendo investigado para técnicas de fuzzing y otras herramientas de análisis de pruebas de seguridad de aplicaciones estáticas/dinámicas (SAST/DAST).

Tanto la ISO como la SAE trabajan para determinar el nivel de garantía de seguridad cibernética necesario para distintos componentes del vehículo, basándose en las amenazas cibernéticas que podrían enfrentar. La garantía más alta viene de un mayor enfoque en el diseño, desarrollo y pruebas adecuados de los sistemas. Esto asegurará que se minimice la posibilidad de que queden vulnerabilidades sin descubrir.

El creciente enfoque en el diseño, desarrollo y pruebas adecuados del software no es exclusivo de los vehículos conectados. Dadas las campañas cibernéticas maliciosas lanzadas contra los sectores público y privado, la intención de mejorar la ciberseguridad se hace extensiva a todo el software crítico.

LA GESTIÓN DE EVENTOS CRÍTICOS: PREPARARSE PARA CUALQUIER COSA

A muchas organizaciones la pandemia les recordó la realidad de que los eventos críticos sumamente disruptivos pueden ocurrir en cualquier momento. Sin embargo, la pandemia no fue la única crisis de los últimos 12 meses. Instancias de interrupciones en la cadena de suministro, disturbios civiles, apagones energéticos, desastres naturales y causados por el hombre, e incluso clima extremo se sucedieron de manera recurrente a lo largo del año, y en todo el mundo. Además de eventos físicos, los ataques cibernéticos y otras interrupciones de TI golpearon a sistemas críticos para las empresas, según un informe de Aberdeen. Las interrupciones en la cadena de suministro y los apagones del pasado solían ser consecuencia de la logística "ascendente y descendente" o de problemas de transmisión de electricidad. Hoy, los ataques cibernéticos tienen un rol cada vez mayor en este tipo de interrupciones.

La empresa Colonial Pipeline, propietarios del oleoducto más grande de los EE. UU., fue víctima del ransomware DarkSide en mayo del 2021, lo que forzó a la compañía a cerrar su sistema de oleoductos durante varios días.

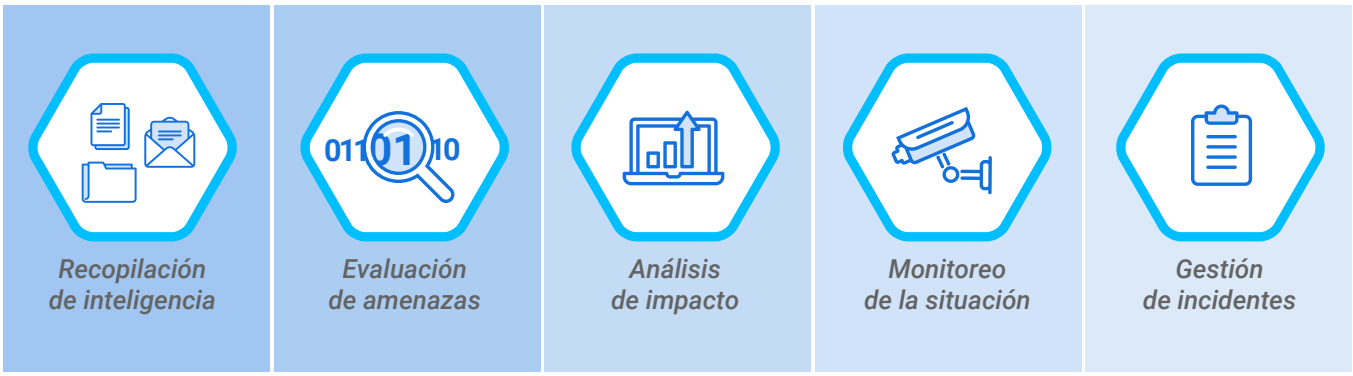
Durante la primera mitad del 2021, se denunciaron una serie de incidentes de ciberseguridad de alto perfil, entre ellos:

- **Colonial Pipeline.** La empresa Colonial Pipeline, propietaria del oleoducto más grande de los EE. UU., fue víctima del ransomware DarkSide en mayo del 2021. Los ataques interrumpieron las operaciones y forzaron a la empresa a cerrar su sistema de oleoductos durante varios días. Colonial Pipeline pagó $5 millones de rescate, de los cuales $2,3 millones se recuperaron más adelante.
- **Suministro de agua de Florida.** En febrero del 2021, un delincuente cibernético infiltró el sistema de la planta de agua de la ciudad de Oldsmar. El atacante intentó envenenar a los residentes de la ciudad aumentando el contenido de hidróxido de sodio del suministro de agua a niveles peligrosos. Un operario de la planta notó los altos niveles de hidróxido de sodio y revirtió el ataque antes de que nadie saliera lastimado. Las autoridades federales todavía están buscando al atacante.

- **Channel Nine de Australia.** En marzo del 2021, un ataque cibernético interrumpió la transmisión de los programas de la cadena de televisión australiana Channel Nine. La empresa batalló con el problema durante varias horas antes de hallar una solución alternativa que les permitiera volver a transmitir.
- **Ataque a la cadena de suministro de Accellion.** Los atacantes infiltraron el sistema de transferencia de archivos Accellion a comienzos del 2021. Mediante esta fuga, los delincuentes cibernéticos pudieron robar datos de varias organizaciones.

Desafortunadamente, muchas organizaciones estaban mal preparadas para este tipo de evento crítico. Los ataques a las cadenas de suministro y la infraestructura crítica, que protagonizaron las noticias en el 2021, plantearon serios interrogantes para las organizaciones de todo el mundo. ¿Se pueden prevenir estos tipos de ataque en el futuro? De ser así, ¿cómo? ¿Qué medidas podrían haber tomado las organizaciones para estar mejor preparadas a fin de responder ante ellos?

Para abordar incidentes cibernéticos similares, las organizaciones con visión de futuro invierten en reclutamiento, capacitación y equipamiento de sus analistas de seguridad para proveer personal a centros de operaciones "fusión". Estos centros pueden gestionar eventos críticos relacionados con la ciberseguridad y TI, así como problemas no técnicos. Sus responsabilidades fusionadas se extienden a eventos críticos que tradicionalmente gestionaba un centro de operaciones de emergencia, como disturbios civiles, desastres naturales e incidentes de seguridad. Trabajan ininterrumpidamente llevando a cabo tareas importantes, como:



Operar un centro de operaciones fusión bien dotado de personal es solo uno de los aspectos de la respuesta ante eventos críticos. Existen otros desafíos a tener en cuenta. Las organizaciones todavía necesitan garantizar que existan procesos confiables para comunicarse con las partes interesadas, sistemas de respuesta interoperables y sistemas que no sean del SOC integrados.

La gestión de eventos críticos (CEM) exitosa depende de la comunicación rápida y la colaboración con todas las partes interesadas afectadas. Todo el personal y los proveedores externos involucrados deben estar familiarizados con los procedimientos operativos estándar de la organización antes de que ocurra un evento crítico. Realizar ejercicios simulados de gestión de crisis puede crear consciencia, preparación y, en última instancia, reducir los impactos de los eventos críticos.

La CEM no se limita a los desastres de gran escala, sino que incluye el abordaje de eventos con el potencial de deteriorar y escalar a situaciones graves. Contar con una plataforma de CEM segura, confiable y de extremo a extremo ayuda a mitigar posibles descuidos que podrían resultar costosos más adelante. Garantiza que se entiendan y aborden los riesgos, que las partes interesadas estén bien preparadas, que las fuentes de distribución de monitoreo de amenazas estén integradas eficazmente y que los recursos puedan desplegarse de inmediato.

La gestión de eventos críticos (CEM) no se limita a los desastres de gran escala, sino que incluye el abordaje de eventos con el potencial de deteriorar y escalar a situaciones graves.

Tenga en cuenta el aumento en la frecuencia y la gravedad de los ataques de ransomware. Durante un ataque de este tipo, se cifran los datos críticos de una organización y, en algunas instancias, se exfiltran. Los atacantes exigen el pago de un rescate a cambio de la clave de descifrado para liberar los datos y una garantía de que no se harán circular más los datos. Si una organización no cumple con sus exigencias, los atacantes pueden usar los datos para extorsionarlos, o divulgarlos al público. Saber si los atacantes cumplirán con su palabra una vez pagado el rescate es, por supuesto, una apuesta.

Si se utilizara una plataforma de CEM en esta situación, las partes interesadas previamente identificadas ya estarían familiarizadas con los procedimientos de respuesta esperados. A medida que se desarrolla el incidente, los analistas de seguridad intentarán rastrear la fuente inicial e identificar los puntos finales afectados. Un flujo de trabajo automatizado puede enviar notificaciones a usuarios posiblemente afectados. Estas notificaciones pueden incluir la naturaleza del incidente, señales de advertencias específicas, maneras de informar problemas y medidas alternativas. Incluso se podría incorporar un estado de avance que permita contar con un vistazo rápido a modo de ayuda para el gerente de incidentes.

A nivel externo, se podría notificar a los entes reguladores, las agencias de cumplimiento de la ley, los usuarios del servicio identificados u otros socios sobre el avance actual del incidente. Supongamos que la organización afectada es un proveedor de atención crítica, como un hospital, o una organización de seguridad pública. Una plataforma de CEM significaría contar con la capacidad de garantizar eficazmente que los servicios críticos continúen operando. Por ejemplo, la terminal móvil de a bordo de una ambulancia podría estar integrada para garantizar el envío continuo de información crítica como los datos y la ubicación del paciente. Esto podría ocurrir mientras la organización, simultáneamente, se esfuerza por contener y resolver un evento disruptivo importante, como un incidente cibernético. Una plataforma de CEM brinda la capacidad de gestionar mejor interrupciones operativas y garantiza la entrega de servicio continua cuando las amenazas se materializan.

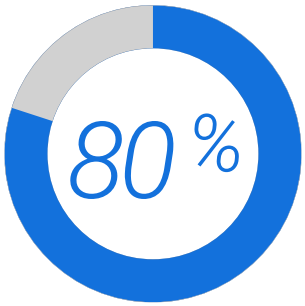
Según la encuesta a los CIO de Gartner del 2021, el 64 % de los empleados podrían trabajar desde casa y el 40 % ya lo está haciendo. Para este grupo de partes interesadas, la capacidad de comunicarse y recibir información vital durante un incidente cibernético u otro evento crítico es crucial. Si bien los riesgos no pueden eliminarse por completo, adoptar una tecnología de CEM permite optimizar la preparación actual y las iniciativas de prevención, y mejora la resiliencia de la organización.

Para las organizaciones sin una plataforma de CEM, o las que deseen ampliar sus capacidades, adquirir capacidades de CEM como un servicio administrado puede ser una opción interesante.

LAS NUEVAS INICIATIVAS REGULATORIAS Y LEGISLATIVAS DE SEGURIDAD CIBERNÉTICA Y EL PRONÓSTICO

La ciberseguridad se encuentra ahora a la cabeza de la agenda de políticas públicas para los países del G7 y los aliados de la OTAN. Los ataques cibernéticos sucesivos y en escalada a oleoductos, hospitales, aerolíneas, cadenas de suministro y servicios esenciales destacan la necesidad urgente de proteger la infraestructura crítica, las empresas y los ciudadanos. En el 2020/21, los Gobiernos de los EE. UU., Reino Unido, Francia, Japón, Italia, Australia y Alemania prometieron conjuntamente miles de millones de dólares e introdujeron nuevas medidas para reforzar su resiliencia cibernética.

En los EE. UU., la administración Biden firmó un decreto en mayo del 2021 diseñado para fomentar las iniciativas de ciberseguridad en todo el Gobierno federal. El presidente Biden nominó a un director cibernético nacional para supervisar las políticas de seguridad digital y anunció nuevas medidas para proteger los sistemas de información federales. Además, reforzó la autoridad de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) del Departamento de Seguridad Nacional (DHS) para responder ante incidentes cibernéticos graves. Mientras tanto, el Congreso aprobó legislación para codificar y financiar algunos de estos esfuerzos.



Más del 80 % de los CEO canadienses mencionan a la ciberseguridad como una de las principales amenazas para el potencial de crecimiento de su empresa.

La Unión Europea está considerando una legislación de seguridad cibernética amplia que cubra redes, infraestructura crítica y nuevas certificaciones de seguridad para productos de la IoT. En Canadá, el Gobierno federal se comprometió a redactar una nueva estrategia de ciberseguridad nacional, aprobar nuevas leyes para llevar ante la justicia a los delincuentes cibernéticos y ampliar las capacidades cibernéticas federales. Sin embargo, las empresas y los grupos de la industria piden que el Gobierno federal haga más y que considere a la ciberseguridad como una prioridad de política principal. El apoyo a medidas más fuertes es alto y un 92 % de los canadienses afirma que el Gobierno debe priorizar la inversión en seguridad cibernética. Más del 80 % de los CEO canadienses mencionan a la ciberseguridad como una de las principales amenazas para las perspectivas de crecimiento de su empresa.

De hecho, la implementación de leyes aprobadas en el 2021, lo que incluye la implementación de inversiones significativas en seguridad cibernética, continuará en el 2022 e incluirá lo siguiente:

- Requisitos de seguridad del software de la cadena de suministro
- Programas de etiquetado de ciberseguridad orientados al consumidor
- Cumplimiento relacionado con la protección de sectores de la infraestructura crítica
- Medidas para proteger infraestructura crítica y redes gubernamentales frente a ataques cibernéticos
- Mejoras en la colaboración entre los sectores público y privado respecto de iniciativas de seguridad cibernética
- Aceleramiento de los esfuerzos por equipar a las agencias gubernamentales con las capacidades cibernéticas que necesitan para responder ante las amenazas cibernéticas y los riesgos cibernéticos en rápida evolución

Es posible que los contratistas del Gobierno y las empresas en industrias reguladas como las de energía, transporte, finanzas, salud y defensa sean las primeras en ver que se implementan requisitos de seguridad cibernética adicionales. Los Gobiernos tienden a considerar a estos sectores de alto riesgo para los ataques cibernéticos que podrían dar como resultado un impacto generalizado en lo económico, de seguridad nacional y social.

ESTADOS UNIDOS

El año 2021, al igual que el 2020, marcó otro hito en lo que respecta a incidentes de ciberseguridad y, en consecuencia, en iniciativas de políticas de ciberseguridad en los EE. UU. Como se mencionó anteriormente, el presidente Biden firmó un decreto para "Mejorar la ciberseguridad de la nación" (EO 14028). El decreto convocó a la creación nuevas pautas para mejorar la seguridad del software de la cadena de suministro, entre otras iniciativas de seguridad cibernética clave. Lanzó un proceso que incluyó a varias agencias federales con el objeto de determinar el marco adecuado para requerir una Lista de materiales de software vendido al Gobierno federal. Este decreto instruyó a las agencias del Gobierno federal a realizar la transición a una arquitectura de TI de confianza cero más segura, entre otras cosas.

Otras de las acciones del Gobierno de los EE. UU. en el 2021 incluyeron los nuevos requisitos de ciberseguridad para operadores y propietarios de oleoductos críticos, operadores de transporte de carga y pasajeros de alto riesgo, aeropuertos importantes y operadores de aeronaves; una iniciativa de ciberseguridad de sistemas de control industriales por parte del DHS, en coordinación con el Departamento de Comercio; el establecimiento de un grupo de trabajo de extorsión digital y ransomware por parte del Departamento de Justicia; y una serie de iteraciones de 60 días para lidiar con problemas de ransomware y seguridad cibernética de la fuerza laboral. El Presidente también convocó a representantes de 30 países a una cumbre en la Casa Blanca para discutir medidas colaborativas con el fin de contrarrestar el ransomware.

A raíz de las vulnerabilidades cibernéticas masivas expuestas por los ataques a SolarWinds, Microsoft Exchange, JBS Foods, Colonial Pipeline, Log4j y otros de alto perfil y alto impacto, el Congreso sigue dispuesto a profundizar las exigencias de ciberseguridad para proteger tanto al sector público como al privado.

Algunos de los desarrollos de políticas públicas de los EE. UU. más destacados que los encargados de la toma de decisiones en materia de seguridad empresarial deben tener en cuenta incluyen los siguientes:

- **Disposiciones relacionadas con la seguridad cibernética en la Ley de Autorización de Defensa Nacional para el año fiscal 2022** cuyo fin apunta a mejorar la capacidad del Departamento de Defensa (DOD) y el DHS de identificar, detener, brindar protección, detectar y responder ante campañas cibernéticas maliciosas que amenacen al sector público, así como a infraestructura crítica de propiedad privada. Esto incluye exigir al DOD que desarrolle una arquitectura basada en un modelo y estrategia de confianza cero para su red de información y expandir la elegibilidad a fin de recibir financiación y soporte técnico del DOD a los propietarios de infraestructura crítica. El DHS, incluso la CISA, también ampliará sus esfuerzos por abordar los riesgos cibernéticos y mejorar la respuesta ante incidentes cibernéticos, en especial los que se relacionen con sistemas de control industriales. Implementará un programa que establezca monitoreo y detección continuos de riesgos de ciberseguridad a entidades de infraestructura crítica, y estipulará un programa nacional de ejercicios cibernéticos diseñado para ayudar con la planificación de respuesta ante incidentes tanto industrial como gubernamental.
- **Requisitos de seguridad cibernética para reforzar a los sectores de los oleoductos, ferroviario y de la aviación** contra amenazas en el espacio cibernético. Por ejemplo, en diciembre del 2021, la Administración de Seguridad en el Transporte (TSA) implementó nuevas reglas que instan a los operadores de aeronaves, aeropuertos

grandes y ferroviarios de alto riesgo a adoptar nuevos procesos. Estos incluyen denunciar incidentes cibernéticos a la CISA, identificar a un coordinador de seguridad cibernética, realizar evaluaciones de vulnerabilidad y desarrollar planes de recuperación tras una contingencia a implementar en caso de un ataque cibernético.

- **Nuevos requisitos de seguridad del software de la cadena de suministro** incluidos en el decreto del Presidente que están empezando a tomar forma a medida que distintas agencias del Gobierno comienzan a abordar este difícil problema. Inicialmente, estas reglas afectarán a los contratistas federales. Si bien se enfocan en el abastecimiento a nivel federal, es posible que los requisitos de seguridad de software más exigentes se apliquen también a los requerimientos y las prácticas del sector privado.

$1000 M

Monto autorizado según la Ley de Empleo e Inversión en Infraestructura con el fin de financiar subvenciones de ciberseguridad para los gobiernos estatales y locales

Entre las iniciativas gubernamentales que posiblemente tomen impulso en el 2022 están el desarrollo de requisitos de ciberseguridad adicionales para los sectores de transporte, energía, telecomunicaciones y finanzas. En el caso de que se materialicen nuevas reglas o leyes, los propietarios y operadores de estos sectores estarán obligados a dedicar más recursos para cumplir con los requisitos de seguridad cibernética. Algunos miembros del Congreso promoverán una mayor consulta a nivel federal con partes interesadas de la industria en el desarrollo de estos requisitos. La industria también puede esperar propuestas bipartidarias para establecer mandatos de informe y notificación de incidentes de ciberseguridad para propietarios y operadores de infraestructura crítica y, posiblemente, para otros también. Durante el 2021 se debatieron muchas propuestas de este tipo y, es probable, que se las vuelva a tratar en el 2022.

Por último, se espera que el Gobierno en todos los niveles siga avanzando en cuanto a las inversiones para modernizar su TI, lo que abarca la ciberseguridad. Estos fondos se obtienen mediante la Ley del Plan de Rescate Estadounidense firmada en marzo del 2021, que amplió el Fondo de Modernización Tecnológica, y la Ley de Empleo e Inversión en Infraestructura aprobada en noviembre del 2021. Varias disposiciones de esta nueva ley plantean que la financiación para infraestructura dependa de la inversión y la planificación en seguridad cibernética por primera vez en la historia. De la misma manera, los Gobiernos estatales y locales se beneficiarán de $1000 millones autorizados a través de la Ley de Empleo e Inversión en Infraestructura con el objetivo de financiar subvenciones de ciberseguridad para los gobiernos estatales y locales.

CANADÁ

Al igual que ocurre en los EE. UU., la seguridad cibernética es uno de los desafíos más importantes que enfrenta Canadá. Durante décadas, los expertos han advertido sobre los peligros de los ataques cibernéticos. Hoy, las fugas cibernéticas se han vuelto preocupantemente rutinarias. Los canadienses están legítimamente preocupados. En particular, ser víctima de un ataque cibernético ahora ocupa el segundo lugar después de perder el trabajo en la lista de cosas que más preocupan a los canadienses. Durante el último año, empresas, hospitales, universidades, sistemas de transporte, ciudades y servicios gubernamentales canadienses experimentaron ataques cibernéticos significativos.

Abordar las deficiencias de seguridad cibernética es una prioridad alta para los canadienses, dado que resulta esencial para crear una economía más resiliente, innovadora, inclusiva y dinámica. Algunos grupos de la industria están planteando inquietudes sobre el creciente

conjunto de amenazas cibernéticas. Están exigiendo al Gobierno invertir en ciberseguridad a un nivel similar al de los pares de Canadá del G7, y desarrollaron recomendaciones detalladas sobre cómo pueden colaborar los sectores público y privado para mejorar la seguridad cibernética en Canadá.

El Gobierno de Trudeau se comprometió a redactar una nueva estrategia nacional de ciberseguridad y a desarrollar un plan de acción nacional de seguridad cibernética. Esto promoverá leyes para contrarrestar los delitos cibernéticos y mejorar la protección a la privacidad, y equipará al Centro de Seguridad en las Telecomunicaciones de Canadá (CSE) con las herramientas que necesita para responder ante un panorama de amenazas cibernéticas en rápida evolución. Sin embargo, muchos en la industria, incluso la Cámara de Comercio Canadiense, están presionando al Gobierno de Canadá a tomar más medidas que protejan la infraestructura crítica, las empresas y las comunidades. Entre estas recomendaciones, se llama al Gobierno a hacer lo siguiente:

- **Aumentar la resiliencia cibernética de la infraestructura crítica.** Como se indicó en el Informe de amenazas 2021 de BlackBerry, la estrategia de infraestructura crítica de Canadá es antigua, creada en 2009. La agencia de Seguridad Pública de Canadá inició consultas para renovar y actualizar su estrategia, pero esto puede demorar varios años en concretarse. Mientras tanto, la agencia de Infraestructura de Canadá está avanzando hacia una evaluación nacional de infraestructura que establece prioridades de inversión gubernamental para los próximos años. Los ataques cibernéticos contra el sistema de salud de Terranova y Labrador y la autoridad de transporte de Toronto en el 2021 sirvieron como alarma para que Canadá incrementara su inversión en seguridad cibernética para la infraestructura crítica. La agencia de Transporte de Canadá ha logrado avances en la ciberseguridad vehicular mediante la publicación de pautas concretas y la caracterización de la seguridad cibernética como un elemento esencial de la seguridad vial. Sin embargo, se esperan más reglamentaciones y pautas relacionadas con las ciberseguridad para los sectores ferroviario, marítimo y de aviación dada la falta de atención al tema a la fecha.
- **Ayudar a empresas canadienses a invertir en ciberseguridad.** En abril del 2021, el Gobierno federal prometió $4000 millones de dólares al Programa de Adopción Digital de Canadá. Estos fondos tienen como objetivo ayudar a 160 000 empresas pequeñas y medianas a comprar y adoptar las nuevas tecnologías que necesitan para crecer. Muchos dieron la bienvenida a esta iniciativa, dado que la epidemia de la COVID-19 empujó a las empresas a depender de manera sin precedentes en la tecnología digital para admitir el trabajo remoto y el comercio electrónico. Sin embargo, estas mismas empresas experimentaron un auge nunca antes visto de ataques cibernéticos. Para aprovechar al máximo el potencial del Programa de Adopción Digital, la ciberseguridad debe convertirse en un elemento esencial del programa. Mediante el aprovechamiento del talento y la vasta experiencia del sector privado canadiense, el país puede elevar las exigencias de ciberseguridad y equipar a pequeñas y medianas empresas con las prácticas recomendadas y herramientas que necesitan para prosperar en una economía impulsada por los datos. Esto también ayudará a las empresas canadienses a cumplir con una nueva ley federal de protección de los datos y la privacidad, que probablemente se proponga en el 2022.
- **Mejorar las acciones y la coherencia respecto de la seguridad en todo el Gobierno.** En la actualidad, las responsabilidades cibernéticas del Gobierno federal están distribuidas entre 12 departamentos y agencias federales. Crear coherencia en el Gobierno para garantizar que todos los departamentos operen en pos del mismo propósito es esencial

para promover la resiliencia cibernética. BlackBerry, junto con otras empresas líderes en tecnología, solicitó a Canadá que considere establecer un puesto gubernamental sénior como el del nuevo Director Cibernético Nacional en los EE. UU. Este cargo ayudaría a elevar la ciberseguridad en lo que respecta a políticas gubernamentales y a promover la resiliencia cibernética mediante la mejora de la coherencia y la colaboración entre los distintos departamentos del Gobierno. En el 2022, esperamos ver una mayor atención al desarrollo de estrategias y mecanismos que posibiliten la implementación de una estrategia de seguridad cibernética cohesiva en todo el Gobierno. Hacer esto ayudará al Gobierno a pasar de una mentalidad de respuesta ante incidentes reactiva a un enfoque con prioridad en la prevención que posicionará a Canadá como un líder en ciberseguridad.

UNIÓN EUROPEA

En el 2021, la UE continuó con su enfoque proactivo para abordar las vulnerabilidades de ciberseguridad. La Estrategia de Ciberseguridad de la UE, publicada a fines del 2020, introdujo nuevas medidas con el objeto de perfeccionar las capacidades cibernéticas colectivas. Los pasos para lograrlo incluyen la creación de un nuevo centro de operaciones de seguridad conocido como la Unidad Cibernética Conjunta en el que autoridades públicas de la UE pueden conectarse y colaborar para responder ante los ataques cibernéticos. Además de nuevas iniciativas y requisitos de seguridad cibernética para los Gobiernos, la industria se verá afectada por las revisiones a la Directiva sobre la Seguridad de las Redes y la Información (NIS) y la legislación que regula los requisitos de informe de incidentes cibernéticos para operadores críticos.

En el 2022, continuará el enfoque en lo siguiente:

- Una propuesta de la Comisión para abordar las deficiencias de la Directiva sobre la Seguridad de las Redes y la Información (NIS). Entre los cambios más destacados se incluyen la expansión del alcance de las entidades cubiertas bajo esta directiva. Estas ahora incluirán a proveedores de servicios basados en la nube, telecomunicaciones y comunicaciones electrónicas, sistemas de transporte inteligentes y vehículos autónomos, y tecnología espacial. La directiva también incluirá normas de gestión del riesgo y de ciberseguridad más restrictivas. Los cambios afectan la seguridad del cifrado y de la cadena de suministro y, además, exigen el informe obligatorio de incidentes cibernéticos dentro de plazos estrictos. También se anticipa que habrá nuevas medidas de certificación de productos para el sector privado. La falta de cumplimiento podría tener como consecuencia multas equivalentes a las del Reglamento General de Protección de Datos (RGPD).
- Un marco de certificación de ciberseguridad para toda la UE, que especificará niveles de garantía de seguridad para productos y servicios basados en tecnologías de la información y comunicación (TIC) tanto para aplicaciones de consumo como industriales. Las áreas de enfoque actuales incluyen la seguridad en la nube, la seguridad 5G, la IoT y la inteligencia artificial.
- También se espera que la UE anuncie una nueva *ley de resiliencia cibernética de la UE* con miras a establecer nuevos requisitos de obligación de diligencia respecto de los datos y el software en los dispositivos de TIC para los fabricantes. Esta propuesta incluye software y dispositivos de la IoT. El objetivo es garantizar la seguridad durante todo el ciclo de vida de los productos de TIC, desde el desarrollo hasta el final de la vida útil.

PREDICCIONES: CON VISTAS AL 2022 Y MÁS ALLÁ

Si bien es imposible predecir el futuro, les pedimos a nuestros experimentados expertos de BlackBerry que compartan sus opiniones sobre temas que pronto podrían afectar a la seguridad cibernética. Estos son algunos de los temas a los que nuestros profesionales estarán atentos a medida que nos adentramos en el año 2022.

LA INFORMÁTICA CUÁNTICA

El avance continuo de la informática cuántica puede ser tan disruptivo para el espacio de la ciberseguridad como la IA lo es actualmente, en particular cuando computadoras cuánticas futuras puedan descifrar esquemas de encriptación modernos en tan solo minutos o segundos. Resulta difícil dimensionar el impacto general de la informática cuántica en la seguridad cibernética, pero podríamos comenzar por imaginar que el cifrado dejará de ser un factor. Esto podría ser catastrófico, dado que organizaciones privadas y públicas perderían una herramienta valiosa para proteger datos robados de los atacantes.

Sin embargo, existe otra forma de ver este problema. Los datos y las comunicaciones suelen cifrarse debido a la creencia general de que los atacantes motivados podrán acceder a ellos. Esto desestima la posibilidad de que otros aspectos de la ciberseguridad puedan mejorar al punto que los datos permanezcan totalmente protegidos. Por ejemplo, las tecnologías que fomentan una estrategia sólida con prioridad en la prevención respecto de la seguridad, que permita identificar y frustrar ataques antes de que se ejecuten. Si los atacantes nunca pueden acceder a los datos, entonces no importa si estos están cifrados o no. De esta manera, el avance de otras tecnologías podría compensar la inminente pérdida del cifrado debido a la informática cuántica.

No es ilógico suponer que las tecnologías de seguimiento de la COVID, que se desarrollaron e implementaron rápidamente durante la pandemia, son objetivos atractivos para los atacantes.

LOS ATAQUES RELACIONADOS CON LA COVID-19

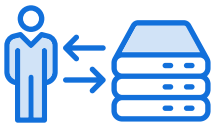
No resulta difícil predecir que los ataques relacionados con la COVID-19 continuarán durante lo que reste de la pandemia. Cuando ocurre un evento disruptivo, siempre existirán individuos oportunistas que quieran obtener una ganancia o beneficio del caos reinante. Resulta más complejo pronosticar cómo serán los ataques relacionados con la COVID-19 del 2022 cuando aparezcan. Una posibilidad es considerar que surgirán nuevas tecnologías relacionadas con la COVID-19, y anticipar los ataques cibernéticos en esos frentes.

Por ejemplo, no es ilógico suponer que se seguirán desarrollando tecnologías de seguimiento de la COVID durante la pandemia. Estas nuevas tecnologías se desarrollarán e implementarán rápidamente, lo que las convertirá en objetivos atractivos para los delincuentes. De la misma manera, si los pasaportes de vacunación o políticas similares se vuelven necesarios en ciertas regiones, la infraestructura tecnológica detrás de ellos puede captar la atención de los atacantes.

LOS GOBIERNOS URGIDOS A ADAPTARSE

Los gobiernos enfrentan una presión cada vez mayor para cambiar su enfoque frente a los ataques cibernéticos. Los atacantes están adoptando rápidamente nuevas tácticas, técnicas y procedimientos (TTP) para ofuscar sus operaciones y explotar sus objetivos. Los estados nacionales hostiles, que antes se contentaban con librar sus propias batallas cibernéticas, ahora suelen tercerizar sus ataques a grupos o servicios externos. Esto hace que atribuir un ataque en particular a un atacante específico sea cada vez más complejo. De forma similar, algunos grupos de atacantes estudian las TTP de otros adversarios y, luego, imitan sus comportamientos y utilizan sus herramientas para fomentar la identificación incorrecta.

Los gobiernos que confían en tecnología y enfoques de ciberseguridad tradicionales descubren que continuamente deben adoptar una postura defensiva. Al enfrentarse con una situación en la que sus atacantes son desconocidos y su tecnología es reactiva, es cada vez más probable que los gobiernos adopten medidas más agresivas en el futuro. Todavía no está claro cuáles serán esas medidas, pero podrían incluir herramientas de seguridad con prioridad en la prevención, marcos de confianza cero y monitoreo más intrusivo.



Los cambios futuros al SOC posiblemente se reduzcan a dos componentes separados pero relacionados: las personas y la tecnología.

LOS CAMBIOS AL SOC

Los cambios futuros al SOC posiblemente se reduzcan a dos componentes separados pero relacionados: las personas y la tecnología. Impulsando los cambios relacionados con las personas, los ataques cibernéticos se volvieron cada vez más sofisticados, lo que implica que los analistas dedicados a detectarlos deban, a su vez, evolucionar. Los días en los que el personal de seguridad podía considerarse calificado por simplemente entender cómo interpretar un SHA-256 quedaron atrás. Los analistas del SOC de hoy y en el futuro necesitan una comprensión más profunda de las técnicas adversariales. No solo deben poder detectar un ataque, sino además entender de dónde provino y a dónde se dirige.

Esta necesidad de un mayor conocimiento impulsará el cambio en la tecnología del SOC. Por ejemplo, los SOC modernos se enfocan menos en productos singulares y más en capacidades. Es por eso que los servicios de XDR y XDR administradas están captando más atención. La capacidad de una plataforma de integrar datos de telemetría de amenazas de distintas fuentes, incluso de soluciones de terceros, y entregarlos a los analistas es esencial. Es necesario contar con analistas que entiendan los ataques sofisticados y las soluciones que identifican y entregan información relevante, sin importar dónde residan los datos de la amenaza. Predecimos que en el 2022 el SOC seguirá favoreciendo a los analistas altamente capacitados y las plataformas de seguridad que prioricen las capacidades por sobre la fortaleza individual de un producto.

LA SEGURIDAD EN EL METAVERSO

Se puede decir mucho sobre la sabiduría de crear una realidad híbrida en la que las interacciones y el estado de los seres humanos existan principalmente en un sentido virtual. Desde una perspectiva de seguridad, es importante recordar una obviedad simple: las personas prefieren la conveniencia a la seguridad. Un ejemplo claro de esto puede observarse en la funcionalidad de GPS de los teléfonos inteligentes. Cualquiera puede denegar información sobre su ubicación geográfica a un atacante (o una empresa) con

solo desactivar los servicios de ubicación GPS de su teléfono. Sin embargo, quien lo intente pronto descubre que muchas aplicaciones dejarán de funcionar. Esto significa que, por mera conveniencia, las personas dejan activado el GPS de su teléfono, incluso cuando las aplicaciones móviles son notoriamente inseguras.

Para que la seguridad tenga éxito en el metaverso, deberá implementarse de manera tal que sea robusta sin afectar negativamente la conveniencia del usuario.

Ahora, piense cuánto mayor es el riesgo cuando no se trata solo de la ubicación de un teléfono móvil, sino de monitorear toda la vida de una persona. Si la información puede utilizarse indebidamente para obtener una ganancia o beneficio, siempre existirán personas a la espera de poder robarla o explotarla. El metaverso requiere de considerablemente más interacción del usuario que un teléfono móvil. Por lo tanto, no es ilógico suponer que recopilará mucha más información y atraerá a muchos más atacantes también. Para que la seguridad tenga éxito en el metaverso, deberá implementarse de manera tal que sea robusta sin afectar negativamente la conveniencia del usuario.

EL FUTURO DE LAS AMENAZAS CIBERNÉTICAS

Los atacantes seguirán explotando eventos que hacen que las organizaciones sean más vulnerables de lo habitual. Esto se aplica tanto a crisis globales imprevistas, como la pandemia de la COVID-19, y hechos más previsibles, como los desastres naturales o los días festivos programados. Cuando las operaciones de seguridad de una organización se ven interrumpidas, es más probable que esto capte la atención de los atacantes que ven una oportunidad.

Los delincuentes también seguirán imitando las estrategias exitosas y las tendencias que observaron en el mundo de los negocios. Por ejemplo, observamos la creación de más malware diseñado para ejecutarse en una arquitectura en la nube. Las ofertas como el RaaS y la IaaS maliciosa siguen creciendo. Los agentes de acceso inicial (IAB) surgieron para ayudar a los delincuentes comunes a ejecutar campañas más exitosas, y para ayudar a los estados nacionales y otras organizaciones poderosas que buscan realizar ataques cibernéticos de manera subrepticia y poder negarlo plausiblemente. Las organizaciones de amenazas están volviéndose cada vez más resilientes, como en el caso de Emotet, que regresó después de haber sido totalmente desmantelada por Gobiernos internacionales en enero del 2021. Basándonos en estos factores, predecimos que las tecnologías y tendencias cada vez más elegidas por las organizaciones probablemente sigan siendo objetivos principales para los atacantes en el 2022.

CONCLUSIÓN

CONCLUSIÓN

Los ataques organizados contra infraestructura crítica y grandes organizaciones acapararon los titulares durante el 2021 y el ransomware tuvo un rol clave en esto. Los atacantes demostraron su capacidad de adoptar e imitar las capacidades del sector privado valiéndose de servicios maliciosos (RaaS, IaaS, MaaS, etc.) y utilizando IAB. A medida que los atacantes siguen adoptando rápidamente nuevas tecnologías y explotando circunstancias en constante cambio, es cada vez más crítico que los analistas de amenazas puedan seguirles el ritmo. Esto puede requerir invertir en plataformas de tipo XDR o en servicios de XDR administradas que puedan recopilar datos de telemetría de amenazas de distintos productos y dispositivos, a la vez que aíslan la inteligencia útil del ruido.

Los ataques a la cadena de suministro fueron otro factor importante del panorama de amenazas durante el 2021. Los atacantes centraron su atención en los proveedores de servicios, comprometiéndolos para lanzar ataques descendentes sobre sus clientes. Dos ataques a la cadena de suministro, los de SolarWinds y Kaseya, captaron la atención pública, pero muchos más ocurrieron a lo largo del último año. Casi dos tercios de estos ataques dependieron de vulnerar la confianza del usuario en su proveedor de servicios, otro motivo por el cual las organizaciones deben considerar adoptar un marco de confianza cero.

Una vulnerabilidad en particular, la falla de los servidores de Microsoft Exchange, causó estragos en todo el mundo. Primero fue explotada por HAFNIUM y, después, diversos grupos identificaron la falla y lanzaron ataques usando las mismas tácticas contras distintas organizaciones. Si bien estos ataques dependieron de vulnerabilidades de seguridad de día cero, podrían haberse evitado con algunas tecnologías existentes. Contar con una plataforma de red consciente de la identidad, autenticación continua, acceso adaptativo y soluciones de trabajo remoto que autentiquen por aplicación, reduce enormemente los riesgos de este tipo de vulnerabilidad.

Los gobiernos siguen participando activamente del espacio de la ciberseguridad, y países del G7 y aliados de la OTAN la tienen como prioridad en sus agendas de políticas públicas. En los EE. UU. se firmó un decreto respecto de la mejora de la ciberseguridad nacional, creando nuevos requisitos para el informe de incidentes y la seguridad del software de la cadena de suministro. El Departamento de Justicia estableció un grupo de trabajo de extorsión digital y ransomware. La Unión Europea continúa con el trabajo establecido en la Estrategia de Ciberseguridad de la UE del 2020. Entre las medidas que se tomaron se enumeran la creación de un centro de operaciones de seguridad de la Unidad Cibernética Conjunta y la estandarización de un marco de certificación de ciberseguridad común. La agencia de Transporte de Canadá declaró la seguridad cibernética como un elemento esencial de la seguridad vial. Los fabricantes de automotores recibieron pautas de ciberseguridad de la ISO, la SAE y la ONU respecto del diseño, la fabricación y el uso de vehículos conectados.

Los eventos del 2021 sirven como recordatorio de que existe cero inmunidad contra los ataques cibernéticos, y que nadie está seguro. Las pequeñas y medianas empresas se vieron particularmente afectadas tras innumerables ataques con consecuencias financieras penosas que nunca llegaron a las noticias. Se produjeron ataques que afectaron a organizaciones de todos los tamaños tanto directamente como a través de sus cadenas de suministro. Los dispositivos móviles, que cada vez más ciudadanos de todo el mundo utilizan, cuentan con aplicaciones que son abrumadoramente inseguras. La vulnerable aplicación SHAREit para dispositivos Android, que permitía la ejecución de código de manera remota, fue descargada más de 1000 millones de veces antes de que se revelaran sus fallas. Cada participante del espacio digital, desde las corporaciones internacionales al propietario de un teléfono inteligente, sigue estando expuesto a riesgos cibernéticos.

BlackBerry está dedicada a brindar soluciones de ciberseguridad de avanzada a personas y organizaciones de todo el mundo. Seguimos entrenando y desplegando modelos de IA avanzados y eficaces que predicen amenazas y utilizan tecnología con prioridad en la prevención para evitar que se ejecuten. Los modelos de seguridad de nuestra IA Cylance, desplegados primero en puntos finales, fueron adaptados para detectar amenazas en la red, el comportamiento del usuario y más.

PARA CONOCER MÁS SOBRE CÓMO BLACKBERRY PUEDE PROTEGER SU ORGANIZACIÓN, VISITE BLACKBERRY.COM.

AGRADECIMIENTOS:
El Informe de amenazas 2022 de BlackBerry representa el esfuerzo conjunto de nuestros talentosos empleados y equipos. En particular, nos gustaría agradecerles a:

Adam Lancaster
Baldeep Dogra
Brent Nicorvo
Brian Robison
Dan Ballmer
David Relyea
Dean Given
Eoin Wickens
Eric Milam
Ethan Fleisher
Gary Ng
Gina Regan
Ginger Espanola
Glenn Wurster
Goran Gotev
Grace Hu
Heather Spring
Ieva Rutkovska
Jim Simpson
John McClurg
John de Boer
Kristofer Vandercook
Lysa Myers
Marc Cormier
Marisa Goodrich
Marjorie Dickman
Mark Mariani
Mark Stevens
Marta Janus
Michelle Haynes
Natasha Rohner
Nigel Thompson
Patrick Slattery
Rajesh Rajamani
Robert Nusink
Sabrina Forgione
Samuel Spector
Sriram Krishnan
Steve Kovsky
Thom Ables
Tony Lee
Tom Bonner
Tracey Swanson
William L. Savastano
Willy Vega
Yi Zheng

La información en el Informe de amenazas 2022 de BlackBerry se incluye únicamente con fines educativos. BlackBerry no garantiza ni se responsabiliza de la precisión, integridad y confiabilidad de la investigación o las declaraciones de terceros aquí citadas. El análisis expresado en este informe refleja el entendimiento actual de la información disponible de parte de nuestros analistas de investigación y puede estar sujeto a cambios a medida que se tome conocimiento de información adicional. Es responsabilidad de los lectores evaluar debidamente esta información al aplicarla a sus vidas profesionales y privadas. BlackBerry no justifica el uso malicioso o indebido de la información presentada en este informe en ningún caso.

BlackBerry Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) brinda servicios y software de seguridad inteligente a empresas y gobiernos alrededor del mundo. La compañía protege a más de 500 millones de puntos finales, lo que incluye a 175 millones de automóviles que están en las calles hoy en día. Con sede en Waterloo, Ontario, la compañía emplea IA y aprendizaje automático para brindar soluciones innovadoras en las áreas de la seguridad cibernética, soluciones de seguridad y privacidad de datos, y es líder en los campos de gestión de seguridad de puntos finales, cifrado y sistemas incorporados. La visión de BlackBerry es clara: garantizar un futuro conectado en el que pueda confiar.

Para obtener más información, visite BlackBerry.com y siga @BlackBerry.