SOPHOS
Cybersecurity evolved.

INFORME DE AMENAZAS 2021 DE SOPHOS

Gestionar la ciberseguridad en un mundo incierto

Por **SophosLabs, Sophos Managed Threat Response, Sophos Rapid Response, Sophos AI y Cloud Security**

CONTENIDO

EL PODER DE COMPARTIR

Joe Levy, director tecnológico de Sophos

"Si quieres ir rápido, ve solo; si quieres llegar lejos, ve acompañado".

Este proverbio africano no podría ser más cierto para la industria de la ciberseguridad. Trabajando juntos, con un marcado sentido del trabajo en equipo, podemos lograr mucho más que luchando contra la ciberdelincuencia como proveedores individuales.

Pero solo si mejoramos nuestro enfoque y compartimos la información sobre amenazas de manera más exhaustiva, y si ampliamos el grupo de participantes que contribuyen a (y se benefician de) este intercambio y colaboración, podremos los proveedores de ciberseguridad continuar elevando los costes para los atacantes y lograr un cambio impactante y duradero.

En el espíritu de ese enfoque de trabajo en equipo, en 2017 Sophos se unió a la *Cyber Threat Alliance*, una organización dedicada a romper las barreras que, durante años, obstaculizaban cualquier posibilidad de colaboración entre los competidores de la industria de la seguridad de la información. La CTA ha conseguido, más allá de su mandato inicial, servir de repositorio de intercambio de información sobre amenazas y de lugar de resolución de diferencias, y se ha convertido en una especie de ONU para la industria de la ciberseguridad.

A través de nuestra asociación con la CTA, en Sophos podemos proteger mejor a nuestros clientes, gracias a las alertas tempranas y al intercambio de datos entre los proveedores fruto de la alianza. Sophos también comparte la responsabilidad de proteger a los clientes de los otros proveedores aportando su propia información sobre amenazas.

En marzo de 2020, mientras los confinamientos para contener la propagación de la COVID-19 se decretaban rápidamente en todo el mundo, Joshua Saxe, científico jefe de Sophos, hizo un llamamiento en Twitter. Consternados por el hecho de que grupos de delincuentes empezaran a incorporar referencias a la COVID-19 en diversas campañas delictivas, más de 4000 analistas de seguridad de la información se unieron en una muestra colectiva de desafío y formaron la coalición COVID-19 Cyber Threat Coalition (CCTC) en un canal de Slack creado ese mismo día. Este canal está elaborando un "patrimonio común" duradero para que la comunidad lo utilice en tiempos de crisis, y está cerca de alcanzar la condición de organización sin ánimo de lucro bajo los auspicios de la CTA.

En última instancia, estas historias sobre el intercambio de información sobre amenazas nos hablan de algo más que las propias organizaciones. Como nos enseña otra parábola, la del ciego y el elefante, ningún proveedor puede ofrecer una verdad completa o absoluta solo a través de sus experiencias subjetivas. La forma real de las cuestiones complejas surge de la unión de nuestras experiencias. Estas iniciativas de colaboración han evitado que millones de personas se conviertan en víctimas de la ciberdelincuencia, pero no es esa la única ***razón*** por la que han tenido éxito. Han prosperado porque la motivación principal de sus miembros y fundadores ha sido, ante todo, proteger de todo daño a cualquiera que pudiera correr peligro. No hay afán de lucro, solo el deseo de defender a los que lo necesitan mientras parece que el peligro les acecha tras la puerta.

Esto demuestra que el modelo es correcto, y salva las lagunas críticas en la cobertura que ninguno de nosotros podría generar por sí solo, pero podemos hacer más con él. Como industria, es posible que en el futuro nos convenga compartir modelos de Machine Learning o entrenar conjuntos de datos de la misma manera que hoy compartimos listas de bloqueados o reglas de Yara. También podríamos consolidar y contribuir a los estándares emergentes como STIX y la plataforma Mitre ATT&CK. Y podríamos participar en los centros y organizaciones de análisis e intercambio de información (ISAC e ISAO) específicos del sector.

El futuro estará más conectado, y todos saldremos mejor parados (y estaremos mejor protegidos) por ello.

RESUMEN EJECUTIVO

El informe de amenazas 2021 de Sophos cubre temas sobre los que Sophos ha adquirido conocimientos gracias al trabajo realizado durante los últimos 12 meses por SophosLabs en el análisis de malware y spam, y por los equipos de Sophos Rapid Response, Cloud Security y Data Science. Estos aspectos de nuestro trabajo diario protegiendo a clientes ofrecen una visión del panorama de amenazas que puede servir de guía a los gestores de respuesta a incidentes y a los profesionales de seguridad TI para saber dónde deben centrar sus esfuerzos a fin de proteger las redes y los endpoints durante el próximo año.

Hemos dividido el informe en cuatro partes principales: debate sobre cómo se ha transformado el ransomware y hacia dónde se dirige esta amenaza; análisis de los ataques más comunes a los que se enfrentan las grandes empresas y por qué estos indicadores de peligro inminente siguen siendo amenazas importantes; cómo la aparición de una pandemia mundial ha afectado a la seguridad de la información en 2020; y un estudio sobre el alcance de los ataques dirigidos a plataformas que tradicionalmente no se consideran parte de la superficie de ataque de una empresa.

A continuación se resumen las principales conclusiones del informe:

Ransomware

- Los ejecutores del ransomware siguen innovando tanto su tecnología como su *modus operandi* delictivo a un ritmo acelerado.
- Cada vez más grupos de ransomware cometen robo de datos y extorsionan a sus víctimas amenazándolas con divulgar datos privados sensibles.
- A medida que los grupos de ransomware ponen más empeño en ataques activos contra empresas más grandes, los rescates que exigen han aumentado vertiginosamente.
- Además, los grupos específicos que cometen ataques de ransomware parecen colaborar más estrechamente con sus homólogos en la clandestinidad delictiva, comportándose más como cárteles de ciberdelincuentes que como grupos independientes.
- Los ataques de ransomware que antes tardaban semanas o días ahora solo tardan unas horas en completarse.

Amenazas "cotidianas"

- Las plataformas de servidores que ejecutan tanto Windows como Linux son el blanco constante de ataques y son utilizadas para atacar a las empresas desde dentro.
- Servicios comunes como los concentradores de RDP y VPN siguen siendo un foco de ataque en el perímetro de la red, y los delincuentes también utilizan el RDP para moverse lateralmente dentro de las redes vulneradas.
- Incluso el malware genérico menos sofisticado puede provocar filtraciones graves, ya que cada vez más familias de malware se ramifican para convertirse en "redes de distribución de contenido" para otro malware.
- Se ha descubierto que la falta de atención a uno o más aspectos de la higiene de seguridad básica es la causa principal de muchos de los ataques más dañinos que hemos investigado.

COVID-19

- El teletrabajo plantea nuevos retos, ya que amplía el perímetro de seguridad de una empresa a miles de redes domésticas, protegidas por sistemas de seguridad de niveles muy diversos.
- La informática en la nube ha asumido con éxito el peso de múltiples necesidades empresariales de entornos informáticos seguros, pero aun así presenta sus propios retos, distintos de los de una red empresarial tradicional.
- Los ciberdelincuentes han intentado limpiar su reputación prometiendo no atacar a las organizaciones involucradas en operaciones sanitarias que salvan vidas, pero más tarde han renegado de esas promesas.
- Las empresas delictivas se han ramificado en una economía de servicios que acoge fácilmente a nuevos infractores.
- Profesionales de la ciberseguridad de todo el mundo se han organizado en 2020 en una fuerza de intervención rápida, a fin de combatir las amenazas que se aprovechan del potencial en ingeniería social que les brinda todo lo relacionado con el nuevo coronavirus.

Plataformas no tradicionales

- Ahora, los atacantes sacan partido sistemáticamente de las numerosas herramientas y utilidades de los equipos rojos que empezaron a utilizar los técnicos de pruebas de penetración durante los ataques activos.
- A pesar de los esfuerzos de los operadores de plataformas móviles por supervisar las aplicaciones en busca de código malicioso, los atacantes siguen trabajando para buscar alternativas y desarrollar técnicas para eludir esos escaneados de código.
- El software clasificado anteriormente como "no deseado" porque distribuía numerosos anuncios (pero por lo demás no era malicioso) ha estado utilizando tácticas que cada vez cuestan más de distinguir del malware explícito.
- Los científicos de datos han aplicado enfoques tomados del mundo de la epidemiología biológica a los ataques de spam y a las cargas de malware como un método para colmar las lagunas en la detección.

EL FUTURO DEL RANSOMWARE

Los ataques de ransomware lanzados a lo largo de 2020 magnificaron el sufrimiento de una población ya recelosa. A medida que la pandemia destrozaba vidas y medios de sustento, también lo hacía una multitud de familias de ransomware, cuyos esfuerzos no dejaron de dirigirse a los sectores de la sanidad y la educación, incluso cuando los hospitales se convertían en campos de batalla contra la COVID-19 y las escuelas se esforzaban por inventar una forma totalmente nueva de enseñar a los niños durante marzo y los meses siguientes.

No se puede recaudar suficiente dinero con una pequeña venta benéfica durante una pandemia para pagar un rescate, pero algunas escuelas lograron recuperarse de los ataques que parecían dirigidos al primer día de clase gracias a las copias de seguridad que mantenían.

Los operadores del ransomware fueron pioneros en el diseño de nuevas formas de eludir los productos de seguridad de endpoints, se extendieron rápidamente e incluso encontraron una solución al problema (desde su punto de vista) de que los empleados o empresas atacados tuvieran copias de seguridad en buen estado, almacenadas de forma segura donde el ransomware no pudiera dañarlas.

Pero lo que parecía ser una amplia variedad de ransomware podría no ser tan extensa a fin de cuentas. A medida que pasaba el tiempo, e investigamos un número cada vez mayor de ataques, los analistas de Sophos descubrieron que el código de algunos programas de ransomware parecía haberse compartido entre familias, y que algunos de los grupos de ransomware parecían colaborar en lugar de competir entre sí.

En vista de todo esto, es difícil predecir con suficiente fiabilidad cómo procederán los delincuentes del ransomware. Los creadores y operadores de ransomware han invertido mucho tiempo en construir defensas contra los productos de seguridad para endpoints. Nosotros contrarrestamos sus contramedidas. Ellos muestran creatividad y versatilidad en el diseño de nuevas tácticas; nosotros mostramos tenacidad en el estudio de lo que hacen y en la búsqueda de formas inteligentes de detenerlos.

El robo de datos crea un mercado de extorsión secundario

Hasta este año, la creencia generalizada entre las empresas de seguridad que tenían algo de experiencia en ransomware era bastante uniforme: había que bloquear los métodos de entrada obvios, como los puertos RDP abiertos a Internet; mantener copias de seguridad en buen estado sin conexión; y ocuparse rápidamente de las infecciones de programas de malware pequeños e inocuos como Dridex o Emotet, antes de que pudieran liberar su carga letal.

Varios ataques de ransomware de alto perfil, por ejemplo, contra distritos escolares en todo EE. UU., fracasaron al menos en parte porque los responsables de TI habían mantenido una copia de seguridad intacta de los datos críticos.

Como medida para contrarrestar la preparación de sus víctimas, varias familias de ransomware se percataron de que podían aumentar la presión sobre sus víctimas de forma paralela para que pagaran el rescate, aunque todas las copias de seguridad con datos esenciales estuvieran a salvo. No solo secuestrarían los equipos, sino que también robarían los datos de esos dispositivos y amenazarían con publicarlos si los destinatarios no pagaban una recompensa.

Durante el último semestre, los analistas de Sophos han observado que los adversarios del ransomware se han decidido por un conjunto de herramientas común (y que aumenta lentamente) que utilizan para exfiltrar los datos de la red de sus víctimas. Este conjunto de herramientas con utilidades conocidas y legítimas que cualquiera podría tener no será detectado por los productos de seguridad de los endpoints. La lista de familias de ransomware que se dedican a esta práctica sigue creciendo, y ahora incluye a Doppelpaymer, REvil, Clop, DarkSide, Netwalker, Ragnar Locker y Conti, entre muchos otros. Los atacantes operan sitios de "filtraciones", donde publican los datos que han robado; REvil, por ejemplo, permite que cualquiera compre los datos directamente de su sitio web.

Los delincuentes utilizan el conjunto de herramientas para copiar información interna sensible, comprimirla en un archivo y transferirla fuera de la red, y fuera del alcance de la víctima. Estas son algunas de las herramientas que hemos visto usar, hasta ahora:

- Total Commander (administrador de archivos con cliente FTP incorporado)
- 7zip (software para comprimir archivos)
- WinRAR (software para comprimir archivos)
- psftp (cliente SFTP de PuTTY)
- cURL para Windows

En cuanto al robo de datos, los atacantes son mucho menos quisquillosos y exfiltran carpetas enteras, independientemente de los tipos de archivo que contengan. (En la fase de cifrado del ataque, el ransomware suele priorizar tipos de archivo clave y excluye muchos otros.)

El tamaño no importa. Parece que no les importa la cantidad de datos que se exfiltran. Las estructuras de directorios son únicas para cada empresa, y algunos tipos de archivo pueden comprimirse mejor que otros. El tamaño mínimo de datos comprimidos que hemos visto robarse a una víctima antes del despliegue del ransomware es de 5 GB y, el máximo, 400 GB.

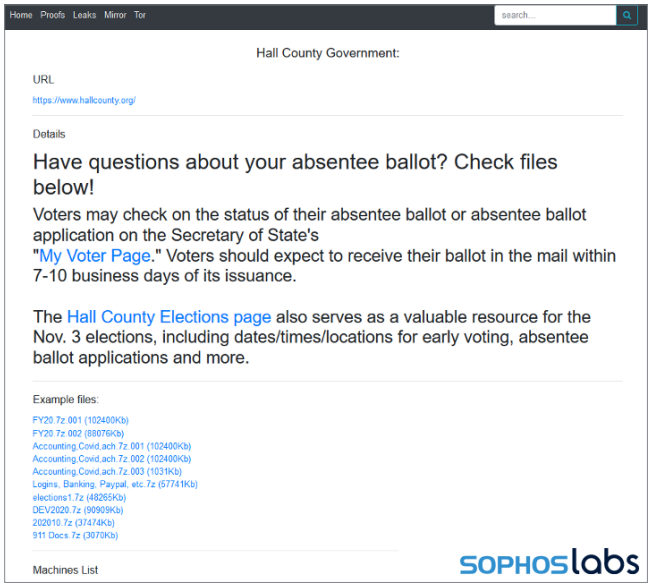


Fig. 1. En octubre de 2020, la página de filtraciones del ransomware Doppelpaymer reveló que los atacantes habían accedido a las redes del Condado de Hall, en Georgia, EE. UU. La filtración hacía referencia a un archivo llamado "elecciones", que incluía papeletas de muestra para las elecciones primarias estatales en 2020 y listas de agentes electorales y sus números de teléfono de las elecciones de 2018, entre otros archivos sensibles. La agencia Associated Press informó de que el ransomware cifró la base de datos de verificación de firmas que el condado usa para validar las papeletas electorales. Fuente: SophosLabs.

Los delincuentes suelen enviar los datos exfiltrados a servicios legítimos de almacenamiento en la nube, lo que hace que esta actividad sea más difícil de detectar, ya que se trata de destinos comunes y corrientes del tráfico de red. Los servicios de almacenamiento en la nube a los que los atacantes han acudido más para almacenar los datos exfiltrados son los siguientes:

- Google Drive
- Amazon S3 (Simple Storage Service)
- Mega.nz
- Servidores FTP privados

En un acto final de destrucción, los atacantes del ransomware buscan cada vez más los servidores locales que contienen copias de seguridad de datos críticos; cuando los encuentran, eliminan esas copias de seguridad (o las cifran por separado) justo antes del ataque de cifrado de toda la red.

Es más importante que nunca mantener una copia de seguridad de los datos clave fuera de la red. Si los ciberdelincuentes logran encontrarla, la destruirán.

Los rescates aumentan a medida que aumentan los ataques

Cuesta creer que, hace solo dos años, los analistas de Sophos se maravillaron ante el botín de 6 millones de dólares que se embolsaron los operadores del ransomware conocido como SamSam. En un ataque al que Sophos respondió en 2020, los operadores del ransomware iniciaron sus negociaciones partiendo de un importe en dólares de más del doble de lo que la banda del SamSam ganó en 32 meses de funcionamiento.

Hoy día el ransomware puede clasificarse en las siguientes categorías: pesos pesados que atacan las redes de grandes empresas, pesos wélter que atacan a la sociedad civil (seguridad pública y gobierno local) y a las pymes, y pesos pluma cuyo blanco son los ordenadores individuales y usuarios domésticos. Aunque ganar la dudosa distinción de ser el peso pesado más pesado impresiona, no es justo comparar las altas exigencias de rescate con las que se originan en el extremo inferior del espectro del ransomware.

Sophos tiene un equipo dedicado que investiga los ataques de ransomware y a menudo trabaja con sus víctimas. El equipo puede reconstruir desde un punto de vista forense los eventos de un ataque después de los hechos, y a veces interrumpir los ataques mientras aún se están produciendo. El equipo de Sophos Rapid Response interviene en los casos en que existe la posibilidad de detener o limitar el daño, pero a veces el ataque ocurre tan rápido, que no hay nada que pueda hacer, y el destinatario debe entonces decidir si paga o no el rescate, momento en el que Sophos deja de intervenir.

Ahí es donde entran en escena empresas como Coveware. La compañía representa a destinatarios de ransomware como negociador de alto nivel con sus atacantes. El director tecnológico de Coveware, Alex Holdtman, confirmó nuestra sospecha de que los pesos pesados del ransomware son el factor principal en la generación de demanda de rescates astronómicos.

Promedio de los pagos de rescate, por trimestre

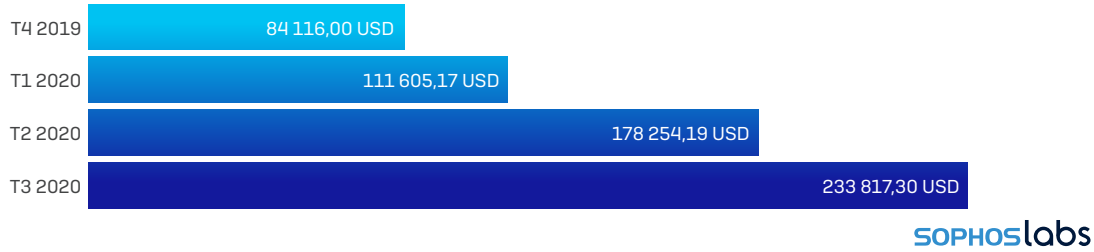


Fig. 2. La exigencia de rescate media ha aumentado un 21 % en el último trimestre y casi se ha triplicado en el último año. Fuente: Coveware.

Solo en el último trimestre, el promedio de los pagos de rescate ha aumentado un 21 %, pero Coveware cree que las medias pueden estar sesgadas por solo uno o dos ataques de ransomware que han exigido rescates muy elevados. El pago medio de rescate en el trimestre que acaba de terminar es ahora el equivalente a 233 817,30 dólares, pagaderos en criptodivisas. Hace un año, el pago medio era de 84 116 dólares.

Los ejecutores del ransomware entienden lo caro que puede ser el tiempo de inactividad, y han estado poniendo a prueba el límite máximo de lo que pueden conseguir en un ataque con rescate.

Varias familias de ransomware han adoptado el chantaje como actividad complementaria para ayudar a cerrar el trato. Como se ha mencionado anteriormente en nuestro informe, grupos como Netwalker y otros usan esta táctica. De esta manera, aunque el destinatario del ataque tenga copias de seguridad perfectamente recuperables de sus datos, es posible que se vea obligado a pagar con la esperanza de que los delincuentes no publiquen su información interna.

En el extremo inferior del espectro del ransomware, las demandas han ido aumentando, pero Holdtman afirma que distan muchísimo de alcanzar al pez gordo. Hay muchas pequeñas empresas y particulares que sufren ataques, pero para ellas las exigencias de rescate se han mantenido relativamente estables.

Día a día en la vida de un gestor de respuesta rápida al ransomware

Cuando una empresa sufrió un ataque del entonces todavía activo ransomware Maze, recurrió al equipo de Sophos Rapid Response. Investigamos y contrarrestamos activamente el ataque mientras aún se estaba produciendo. A continuación, presentamos un resumen diario del ataque tal y como se desarrolló.

Antes del día 1
En algún momento antes de activar el ataque, los delincuentes atacan un ordenador en la red del destinatario.

Este equipo se utiliza como "punto de desembarco" en la red. En múltiples ocasiones, el atacante se conectará desde aquí a otros equipos usando el protocolo de escritorio remoto (RDP).

Día 1
La primera prueba de actividad maliciosa aparece cuando se instala una señal SMB de Cobalt Strike como servicio en un controlador de dominio (DC) desprotegido. Los atacantes logran controlar el DC desde el ordenador previamente atacado explotando una cuenta de administrador de dominio con una contraseña poco segura.

Día 2
Los atacantes crean y ejecutan una serie de tareas programadas y scripts por lotes y luego los eliminan. Según las pruebas observadas por los investigadores, las tareas eran similares a una técnica utilizada más adelante para desplegar los ataques de ransomware. Es posible que los atacantes estén probando el método que planean utilizar.

Usando la cuenta de administrador de dominio comprometida y el acceso RDP, los atacantes se mueven lateralmente a través de la red a otros servidores críticos.

Utilizan Advanced IP Scanner, una herramienta legítima de escaneado de red, para empezar a trazar la red y hacer listas de direcciones IP a las que posteriormente se desplegaría el ransomware. Los atacantes crean una lista aparte con las direcciones IP de los ordenadores que usan los administradores de TI del destinatario.

A continuación, utilizan la herramienta de Microsoft ntdsutil para volcar la base de datos de credenciales con hash de Active Directory.

Los atacantes ejecutan varios comandos WMI para recopilar información sobre los equipos afectados, y luego su atención se centra en la exfiltración de datos. Identifican un servidor de archivos y, usando la cuenta de administrador de dominio comprometida, acceden a él de forma remota a través del RDP. Después, empiezan a comprimir las carpetas que se encuentran en él.

Los atacantes mueven los archivos al DC y luego tratan de instalar en él la aplicación de almacenamiento en la nube Mega. Esta está bloqueada por seguridad, así que cambian a la versión basada en web y suben los archivos comprimidos.

Día 3
La exfiltración de datos a Mega continúa a lo largo del día.

Días 4 y 5
No se observa ninguna actividad maliciosa durante este periodo. En incidentes anteriores, hemos observado que los atacantes de ransomware esperan para lanzar el ataque durante un fin de semana o día festivo, cuando el equipo de seguridad TI no está trabajando o prestando mucha atención a lo que ocurre en la red.

Día 6
Domingo. Se lanza el primer ataque de ransomware Maze, usando una cuenta de administrador de dominio comprometida y las listas de direcciones IP que se han identificado. Más de 700 ordenadores se ven afectados por el ataque, que el equipo de seguridad detecta y bloquea rápidamente. O bien los atacantes no se dan cuenta de que se ha evitado el ataque, o bien esperan tener suficiente con los datos robados para extorsionar a la víctima, ya que en ese momento emiten una petición de rescate por 15 millones de dólares.

Día 7
El equipo de seguridad implementa seguridad adicional y realiza una supervisión de amenazas 24/7. Comienza la investigación de respuesta a incidentes: se identifica rápidamente la cuenta de administrador comprometida, se detectan varios archivos maliciosos y se bloquea la comunicación entre el atacante y los equipos infectados.

Día 8
Se descubren otros instrumentos y técnicas utilizados por los atacantes, así como pruebas relacionadas con la exfiltración de datos. Se bloquean más archivos y cuentas.

Día 9
A pesar de la actividad defensiva, los atacantes mantienen su acceso a la red y a una cuenta comprometida diferente, y lanzan un segundo ataque. Este ataque es similar al primero: ejecutan comandos en un DC, recorriendo en bucle las listas de direcciones IP incluidas en archivos txt.

El ataque es identificado rápidamente. El ransomware se detecta automáticamente y tanto la cuenta comprometida como la carga de malware se desactivan y eliminan. No se ha cifrado ningún archivo.

Los atacantes, claramente lejos de rendirse, lo intentan de nuevo. El tercer intento se produce tan solo unas horas después del segundo ataque.

A estas alturas parece que están cada vez más desesperados, ya que este ataque se dirige a un solo ordenador. Se trata del servidor de archivos principal del que se exfiltraron los datos.

Los atacantes de Maze adoptan un enfoque diferente: despliegan una copia completa de un equipo virtual (VM) y un instalador de hipervisor VirtualBox, un ataque descrito en detalle en SophosLabs Uncut en septiembre de 2020.

El resultado del tercer intento es el mismo que antes: el equipo de Sophos Rapid Response detectó y frustró el ataque, sin que se cifraran archivos. El equipo ayudó al cliente a bloquear al grupo delictivo, y los atacantes ya no pudieron continuar con el ataque.

AMENAZAS DIARIAS A EMPRESAS: INDICADORES DE PELIGRO INMINENTE

Si todo lo que sabe sobre los ciberataques proviene de las noticias, se le podría perdonar que pensara que el mundo se acaba. Los ataques dirigidos a las grandes empresas ocurren todos los días, pero no son todos cisnes negros, como una gran filtración de datos, que pueden hacer que se desplome la fortuna de una empresa (o el precio de las acciones) y generar mala publicidad. Muchos de los ataques son mucho más rutinarios, con malware que el equipo de SophosLabs monitoriza en una especie de lista de "los más buscados" de "los sospechosos habituales".

Pero aunque estos ataques, y algunos de los programas de malware que distribuyen, se conocen bien y son fáciles de contener, cada ataque conlleva el peligro de empeorar mucho más si no se trata con rapidez y eficacia. Siguiendo con las metáforas ornitológicas, estos ataques rutinarios y cotidianos son como los canarios que se llevaban a las minas de carbón, cuya muerte revelaba de forma temprana una presencia tóxica que podía descontrolarse rápidamente.

Ataques dirigidos a servidores Windows y Linux

Si bien la gran mayoría de los incidentes de seguridad a los que respondimos en 2020 tenían que ver con ordenadores de sobremesa o portátiles con variaciones de Windows, vimos un aumento continuado de los ataques tanto a servidores Windows como a otros. En general, los servidores han sido durante mucho tiempo objetivos de ataque muy atractivos por diversas razones: suelen funcionar durante largos periodos sin vigilancia ni supervisión; suelen tener más capacidad de CPU y memoria que los portátiles individuales; y pueden ocupar un espacio privilegiado en la red, teniendo a menudo acceso a los datos más sensibles y valiosos del funcionamiento de una empresa. Así, pueden permitir a un atacante persistente establecerse en una posición de lo más atractiva. Estas características no cambiarán en 2021 y Sophos prevé que el volumen de ataques dirigidos a servidores seguirá aumentando.

La mayoría de los ataques dirigidos a servidores se ajustan a uno de estos tres perfiles: ransomware, criptomineros y exfiltración de datos, cada uno con su correspondiente y distintivo conjunto de tácticas y técnicas empleadas por los atacantes. Las prácticas recomendadas para los administradores de servidores consisten en evitar ejecutar desde el servidor aplicaciones de escritorio convencionales, como clientes de correo electrónico o navegadores web, como medida de protección contra las infecciones, por lo que los ataques dirigidos a los servidores requieren necesariamente un cambio de táctica.

Los servidores abiertos a Internet que ejecutan Windows reciben un aluvión interminable de intentos de acceso por fuerza bruta a través del RDP, una táctica de ataque que, al menos durante los últimos tres años, se ha asociado con mayor frecuencia a los ataques de ransomware (y se ha usado más para predecirlos). Según el equipo de Sophos Rapid Response, con frecuencia la causa raíz de los ataques de ransomware que investiga implica un acceso inicial a la red del destinatario a través del RDP, seguido del uso de esos equipos para afianzarse dentro de la red y tomar el control de servidores DC, desde los cuales pueden organizar el resto del ataque.

Por el contrario, los ataques de criptojacking tienden a dirigirse a una gama más amplia de vulnerabilidades en Windows y en las aplicaciones que normalmente se ejecutan en el hardware de los servidores, como el software de bases de datos.

Por ejemplo, un método utilizado por el criptominero Lemon_Duck implica un ataque por fuerza bruta contra los servidores conectados a Internet que ejecutan Microsoft SQL Server. Una vez que los atacantes adivinan la contraseña correcta de la base de datos, utilizan la base de datos misma para volver a ensamblar la carga del criptojacker, la escriben en el sistema de archivos del servidor y la ejecutan. Luego, el equipo infectado trata de explotar las vulnerabilidades de EternalBlue y/o SMBGhost en un intento de propagar el criptojacker.

Lemon_Duck es un atacante que fomenta la igualdad de oportunidades y puede infectar servidores Linux. El malware intenta atacar por fuerza bruta las contraseñas de SSH tomadas de una lista relativamente pequeña. Si lo consigue, los atacantes cargan un shellcode malicioso, que luego establece persistencia explotando las carencias de un servicio llamado Redis. El criptojacker también puede ocultarse ejecutando los comandos para iniciarse desde dentro de clústeres Hadoop.

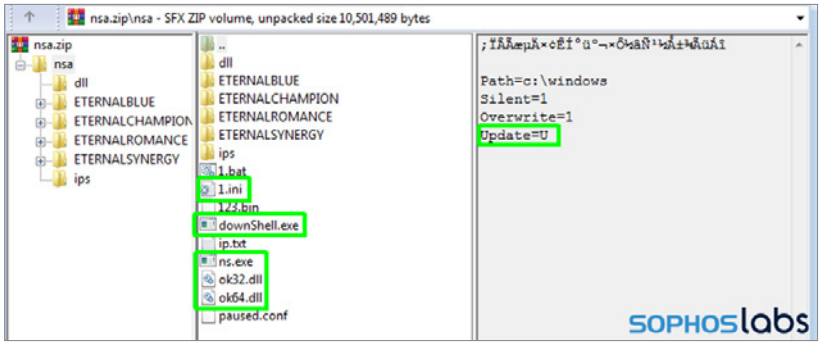


Fig. 3. Uno de los criptojackers más prolíficos, llamado MyKings, distribuyó los componentes necesarios para la instalación de la red de bots (resaltada en verde) dentro de un archivo zip junto con varios de los exploits filtrados de la NSA por The Shadow Brokers. Fuente: SophosLabs.

Ocasionalmente, los delincuentes atacan servidores porque, en lugar de obtener una paga rápida o un flujo constante de criptomonedas, quieren robar datos de valor almacenados en ellos. En 2020, Sophos descubrió un atacante que se dirigía a servidores Linux usando un malware que llamamos Cloud Snooper. Los servidores en cuestión estaban alojados en un clúster de informática en la nube, y eludieron la detección inventando un ingenioso sistema de retransmisión de mensajes, incorporando sus mensajes de comando y control en conexiones HTTP rutinarias.

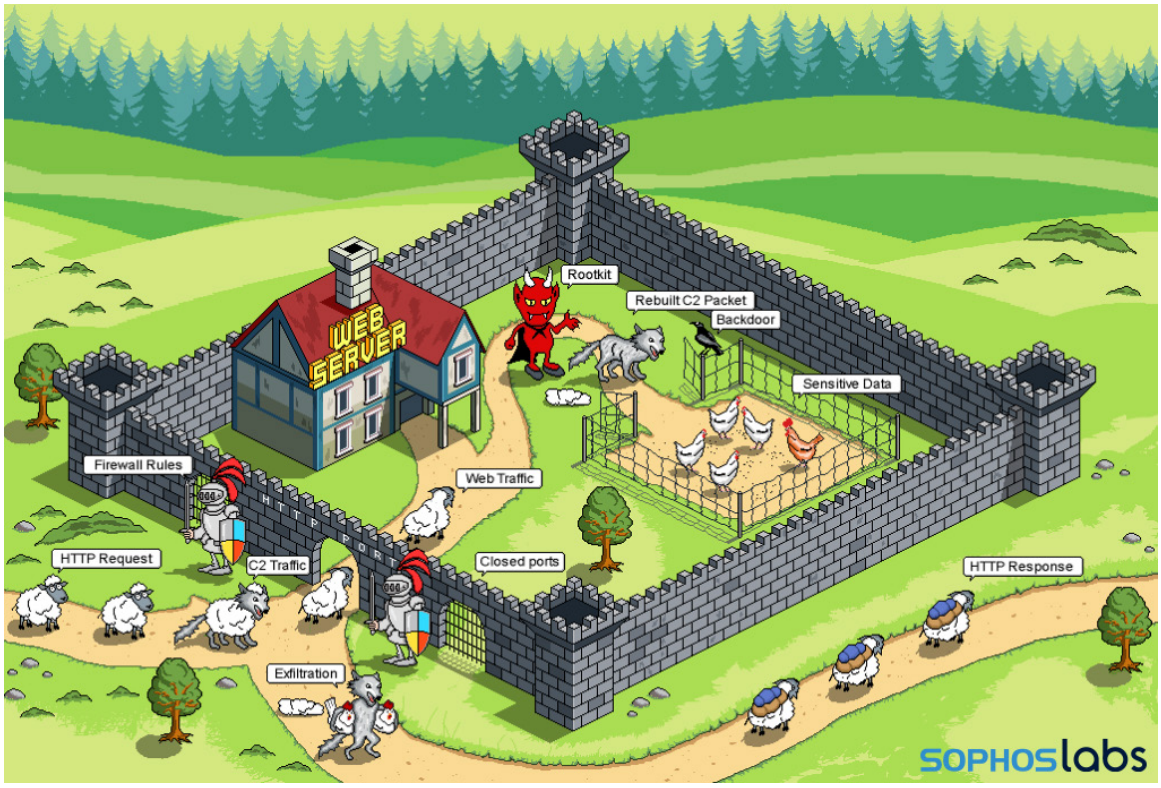


Fig. 4. Una ilustración de la metáfora del "lobo con piel de cordero" sobre cómo el malware de APT Cloud Snooper ocultaba sus comandos y exfiltraba datos en forma de solicitudes y respuestas HTTP convencionales, con la ayuda de una herramienta que monitorizaba el tráfico de red y reescribía los paquetes TCP/IP en tiempo real. Fuente: SophosLabs.

Históricamente, los administradores de servidores no instalaban productos de protección de endpoints en los servidores, pero con la llegada de este tipo de ataques, esta práctica generalizada ha cambiado.

Subestimar el malware "genérico" supone un riesgo

No todo el mundo se ve afectado por una vulnerabilidad de día cero de una amenaza avanzada recurrente (APT) patrocinada por un estado nacional. La mayoría de ataques tienen que ver con malware común y corriente distribuido por medios convencionales, que normalmente consisten en un correo de spam, un archivo adjunto o un enlace de aspecto benigno y grandes dosis de motivación para que el destinatario abra ese adjunto. Sophos recibe miles de coincidencias de telemetría al mes sobre este tipo de malware común, lo que normalmente indica que un ordenador protegido por uno de nuestros productos ha bloqueado el ataque.

En equipos desprotegidos, en los que el malware puede ejecutarse por completo, generará un perfil del ordenador del destinatario; extraerá las credenciales de inicio de sesión o las contraseñas guardadas de los sitios web que controlan algo de valor (por lo general, aunque no exclusivamente, cuentas bancarias o de servicios financieros); a continuación, enviará esa información a sus operadores y esperará nuevas instrucciones, que pueden llegar en cuestión de segundos... o varios días después.

Pero no deje que el hecho de que estas familias de malware sean *simplemente ordinarias* le genere una falsa sensación de seguridad. Estos programas maliciosos de batalla pueden causar enormes problemas si se les permite establecer persistencia. Como hemos mencionado anteriormente en este informe, el equipo de SophosLabs mantiene una lista del malware "más buscado", con analistas dedicados a aquellas familias que siguen siendo obstinadamente recurrentes. A continuación incluimos un breve resumen de algunas de ellas.

Dridex y Zloader

Uno de los tipos de malware más comunes es el *cargador*. Los cargadores tienen características centradas en la distribución de otra carga de malware en nombre de sus operadores o de las personas que contratan con sus operadores. Las familias de malware Dridex y Zloader son plataformas de cargadores maduras y consolidadas. Los atacantes utilizan tanto Dridex como Zloader para recopilar información sobre el sistema objetivo y enviarla a los delincuentes, que pueden decidir a su antojo qué componentes o cargas van a distribuir, en función de la información que devuelve el bot.

La función principal del cargador Dridex es contactar con su servidor de comando y control (C2), recuperar una o más cargas cifradas y desplegarlas. Para los analistas es muy difícil conseguir esas cargas porque los ejecutores solo las distribuyen en función de sus necesidades, como un VNC oculto (una aplicación de control remoto) o un proxy SOCKS. Estas cargas permiten a los atacantes hacer cosas en el contexto del dispositivo de un usuario. También permiten a los delincuentes acceder a recursos del sistema de la víctima a los que no pueden acceder directamente desde su propio sistema.

La lógica del lado del servidor que determina lo que sucede durante una infección puede ser inescrutable, pero podemos inferir algunas reglas porque los bots no quieren infectar los ordenadores que utilizan los analistas de malware. El bot envía a sus operadores una lista de programas instalados; si hay herramientas de análisis o componentes de equipos virtuales, los bots no entregan cargas a ese ordenador. En el caso de Zloader, los operadores del bot propagan el malware a través de un mensaje de spam; si tarda demasiado en infectar su ordenador, en un plazo de ocho a doce horas después de que se envíe el correo de spam, dejan de enviar cargas.

También debe ser un equipo muy limpio, pero tampoco demasiado limpio. Una simple instalación de Windows no permitirá la activación, pero tampoco un equipo muy lleno con muchas herramientas.

Agent Tesla y RATicate, ladrones de información y RAT

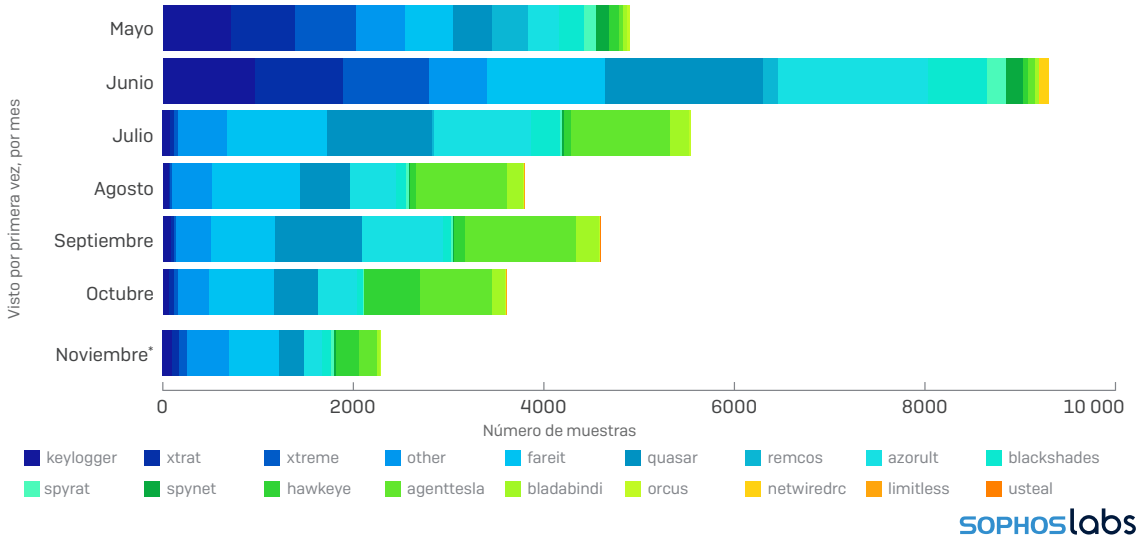


Fig. 5. Ejecutamos todas las muestras de malware de RAT recién descubiertas a través de nuestro sistema interno de espacio seguro. Esta tabla ilustra el número de muestras nuevas y únicas que detectamos a lo largo de un periodo de siete meses y que luego clasificamos en una de las 18 familias de RAT más comunes, desglosadas por apellidos. * Datos de mes parcial. Fuente: SophosLabs.

Los troyanos de acceso remoto (RAT) y los ladrones de información figuran entre las formas más antiguas de malware. Como su nombre indica, los RAT ofrecen al atacante la posibilidad de controlar el ordenador infectado de forma remota. Los ladrones de información se dedican a robar y exfiltrar credenciales, certificados y otra información sensible. Dos de las familias "más buscadas" a las que nos hemos enfrentado durante el último año son Agent Tesla (un ladrón de información) y RATicate (un RAT).

Al igual que los cargadores, los RAT también suelen tener un mecanismo por el que pueden distribuir cargas adicionales, incluidas versiones actualizadas de ellos mismos. Hemos visto a RATicate distribuir otro malware, por ejemplo, Agent Tesla. También hemos visto a estas familias de RAT ser servidas desde las mismas direcciones IP o servidores o comunicándose con ellos, lo que sugiere algo compartido entre grupos por lo demás no relacionados.

Caída del Trickbot

El Trickbot ha sido un molesto malware persistente durante al menos cuatro años. La infame red de bots fue pionera en muchos de los que ahora son comportamientos y características comunes: por ejemplo, se comunicaba con su infraestructura C2 mediante TLS. El bot ha intervenido en varios ataques de ransomware de alto perfil y es un ladrón de credenciales competente por mérito propio.

```
    "type"   :  "TEXT",
    "size"   :  101
},
"controllers"   :  [   {
    "url"   :  "https://127.0.0.1.1"
}  ],
"controllers"   :  {
```

SOPHOSlabs

Fig. 6. Una sola línea de código venció al Trickbot. Fuente: SophosLabs.

En octubre de 2020, mientras preparábamos este informe, Microsoft y el Departamento de Justicia de los Estados Unidos anunciaron que habían incautado varios servidores y enviado un comando a través del sistema de comando y control de la red de bots que hizo que alrededor del 90 % de la red de bots dejara de comunicarse con la infraestructura C2.

Los investigadores lograron subir una configuración "envenenada" en la infraestructura del Trickbot que cada bot descargó. La configuración engañó a la red de bots haciéndole creer que su principal servidor de comando y control era el equipo infectado en el que se estaba ejecutando. La red de bots perdió entonces el contacto con los servidores C2 reales y ya no pudo obtener cargas ni instrucciones.

El esfuerzo tuvo un impacto drástico en el operador del Trickbot, pero se espera que poco a poco, con el tiempo, vuelvan a su funcionamiento normal.

Mecanismos de distribución

Hay un número limitado de formas en que el malware o los atacantes pueden llegar a un equipo específico o penetrar en una red. Los métodos de la mayoría de ataques de malware siguen un camino trillado que puede incluir el empleo de correo electrónico con enlaces o un archivo adjunto malicioso, o el delincuente puede asumir un papel más activo atacando el RDP o algún otro servicio vulnerable alojado en el perímetro de la red, abierto a la Internet pública.

RDP, principal vector de ataque del ransomware

El protocolo de escritorio remoto (RDP) de Windows es un servicio estándar disponible en todas las versiones actuales de Windows. Con muy poco esfuerzo, el RDP permite a los administradores de TI o a los usuarios acceder a un equipo cuando no están físicamente delante del mismo, lo que puede ser muy práctico en el caso de una pandemia en la que todo el mundo se ve repentinamente obligado a trabajar desde casa. Por desgracia, durante los últimos tres años, los responsables del ransomware han estado abusando (a un ritmo acelerado) de esa misma plataforma de acceso remoto como forma de afianzarse y causar daños de gran magnitud a las empresas, ganándose un sueldo cada vez mayor de las compañías víctimas de los ataques.

Intentos de inicio de sesión a través del RDP por cebo

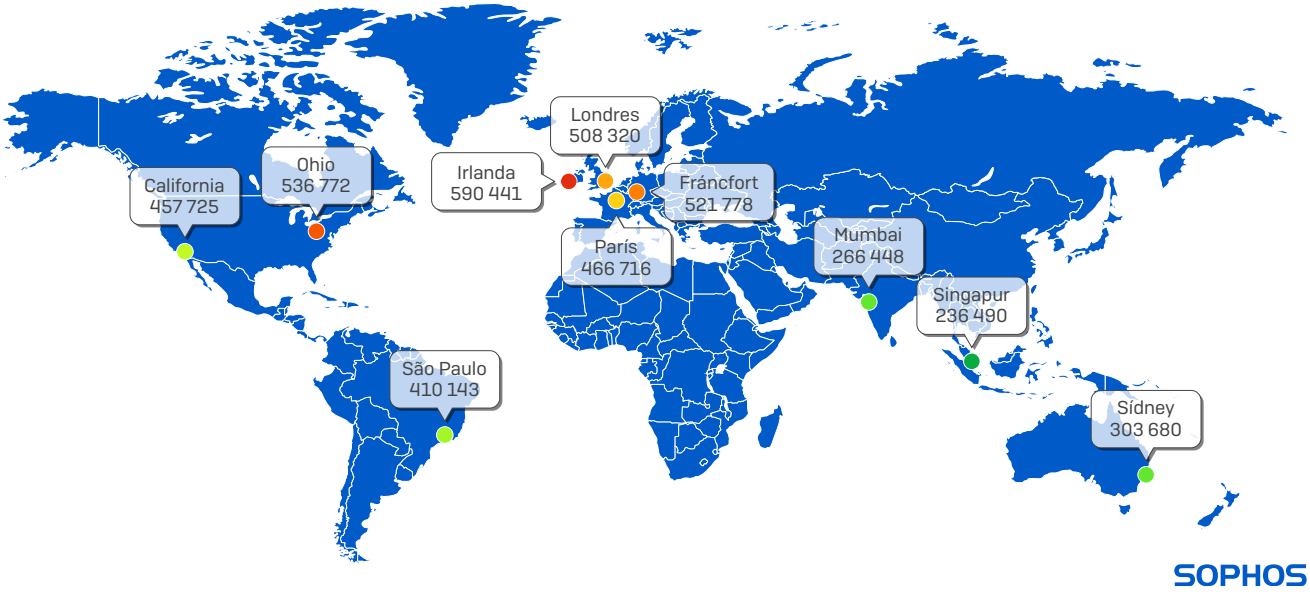


Fig. 7. Distribuimos cebos en centros de datos de todo el mundo y permitimos que los atacantes intentaran entrar por fuerza bruta. Los equipos trampa fueron detectados de forma "natural", sin anunciarse de ninguna manera. Durante el periodo de 1 mes que duraron nuestras pruebas, este mapa ilustra cuántos ataques recibió cada cebo.

El impacto de la era del confinamiento por la COVID-19 no ha hecho más que exacerbar el problema, ya que cada vez más empresas y empleados se ven obligados por las circunstancias a depender del RDP para poder seguir funcionando. El principal riesgo en este caso es que el RDP nunca fue concebido para hacer frente al tipo de ofensiva que puede recibir de la Internet de cara al público. Si la contraseña de RDP es poco segura, fácil de adivinar o atacada por fuerza bruta mediante intentos de acceso automatizados, el atacante se afianza en la red y puede explotarla a su antojo.

El equipo de Sophos que gestiona la respuesta a incidentes graves asegura que el RDP sigue siendo una de las principales "causas raíz" de los eventos de ransomware que atienden. El consejo a los responsables de TI sigue siendo el mismo de siempre: el RDP nunca debería estar expuesto a la Internet pública, sino que debería colocarse detrás de un firewall que requiera que los usuarios se conecten primero a través de una VPN u otro método de confianza cero; y los administradores deberían reforzar las políticas de contraseñas de Windows para requerir contraseñas más largas y un token o aplicación de autenticación multifactor.

En una investigación realizada antes de que se hiciera efectivo el confinamiento, Sophos instaló cebos en 10 centros de datos de todo el mundo para comprender mejor la gravedad del problema. Durante un periodo de 30 días, los cebos registraron un promedio de 467 000 intentos de inicio de sesión a través del RDP, o unos 600 por hora en cada ubicación. La investigación reveló que los intentos de acceso en cada cebo fueron aumentando progresivamente en frecuencia e intensidad hasta que finalmente los desconectamos.

Los 5 principales nombres de usuario utilizados en todos los intentos de inicio de sesión fallidos

NOMBRE DE USUARIO	INTENTOS DE INICIO DE SESIÓN FALLIDOS
administrator	2 647 428
admin	376 206
user	79 384
ssm-user	53 447
test	42 117

Fig. 8. Los intentos de acceso por fuerza bruta al escritorio remoto se sirven de los nombres de usuario más comunes de Windows, incluida la cuenta predeterminada "administrador".
Fuente: SophosLabs.

Estafas por correo electrónico corporativo comprometido y falsificación de correo corporativo

La estafa por correo electrónico corporativo comprometido (BEC) es el nombre formal que se da a un tipo específico de spam que se centra en una petición fraudulenta de dinero. En un ataque de estafa BEC, un spammer envía mensajes que han sido elaborados para que parezcan proceder de un alto ejecutivo dentro de una compañía, pidiendo a un empleado de nivel inferior que realice algún tipo de transferencia financiera o efectúe una compra importante en nombre de ese directivo. Para ello, los atacantes reproducen el aspecto de correos electrónicos internos (método a veces llamado "falsificación de correo corporativo") o intentan hacerse con el control de las cuentas en el propio servidor de correo de la empresa y utilizan una cuenta para enviar la petición fraudulenta.

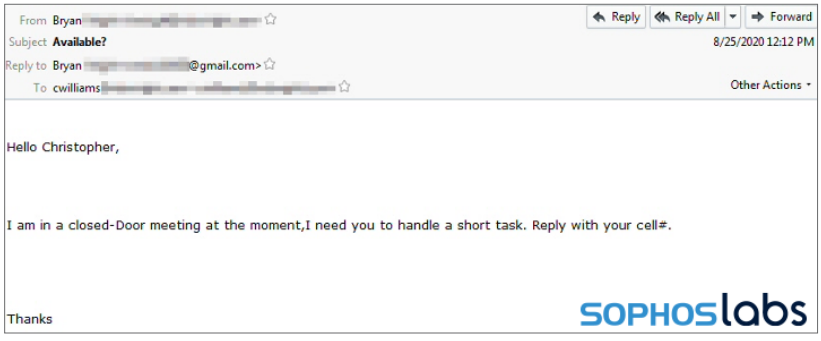


Fig. 9. En este ejemplo real de un intento de estafa por correo electrónico corporativo comprometido, el estafador se hace pasar por un ejecutivo que pide a un empleado que responda a una petición urgente. El correo tiene una dirección de respuesta (de una cuenta de Gmail) diferente a la del campo "De:", un claro indicio de que algo va mal, si el destinatario presta atención a los encabezados del mensaje. Fuente: SophosLabs.

Los atacantes de estafas BEC, al hacerse pasar por un directivo, pueden pedir a un empleado que compre tarjetas regalo de alto importe o que acelere una transacción financiera de algún tipo. Los ataques suelen estar específicamente adaptados a las personas y empresas a las que van dirigidos. Los mensajes de estafas BEC no se parecen en nada al spam malicioso, ya que no siguen patrones similares a los del correo basura. No suelen contener archivos adjuntos ni enlaces maliciosos, e intentan que parezca que se originaron dentro de la empresa víctima de la estafa; a veces incluso incorporan las típicas "firmas" de correo de la empresa objetivo u otros elementos que pueden ser familiares para los empleados, a fin de que resulten más convincentes para el destinatario que el spam malicioso convencional.

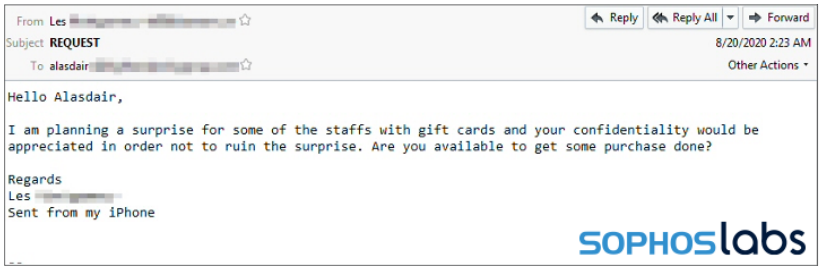


Fig. 10. Después de que la víctima acuse recibo del mensaje inicial, el estafador hace la "petición", facilitando un pretexto que parece creíble. Fuente: SophosLabs.

Las estafas BEC dependen de que el objetivo de la estafa (el empleado) se encuentre físicamente lejos del sujeto de la misma (el ejecutivo) y también de que el destinatario actúe rápidamente, antes de que alguien pueda averiguar lo que está pasando y evitar que la víctima compre tarjetas regalo o haga transferencias bancarias. Es posible que los estafadores BEC elaboren un mensaje cuando saben que el directivo está fuera de la oficina por negocios.

Este tipo de peticiones fraudulentas a menudo implican algún tipo de interacción entre el atacante y el objetivo. La conversación puede comenzar con una solicitud sencilla para que el empleado responda al estafador y continuar con una serie de mensajes que desembocan en una "petición importante" de realizar una compra basada en un pretexto que resulta bastante convincente.

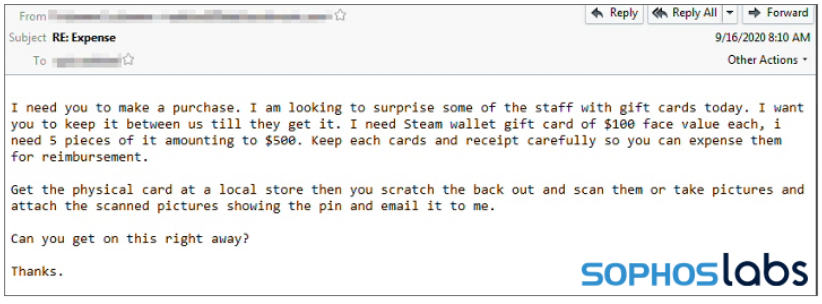


Fig. 11. En algún momento durante el ataque, el estafador BEC hará una petición que va claramente en contra del sentido común, como hacer una transferencia bancaria urgente de una cantidad elevada a una cuenta desconocida para el destinatario de la estafa. Para un empleado cauteloso, esto presenta otra oportunidad de cuestionar la naturaleza de la petición: ¿para qué necesitaría el ejecutivo una fotografía del reverso de una tarjeta regalo con el PIN rascado cuando las tarjetas van a ser regalos? Fuente: SophosLabs.

Cuando la mayoría de nosotros trabajaba en oficinas, la proximidad física entre el objetivo y el sujeto habría hecho la estafa inmediatamente evidente. Pero nuestro actual entorno de trabajo distribuido, donde es poco probable que el ejecutivo y el empleado estén físicamente cerca, reduce las oportunidades de que la gente se acerque a la mesa de alguien y le pida que confirme la petición.

Las estafas BEC existían antes de la era COVID-19, pero a medida que más gente teletrabaja, los estafadores BEC están al acecho. Como ataque contra la buena disposición de las personas que solo quieren ayudar y prestar apoyo, es un tipo de estafa particularmente ofensiva. Si se encuentra con correos electrónicos como estos, confíe en su instinto y hable con la persona en cuestión directamente, si es posible, o pida consejo a alguien más si no puede ponerse en contacto con ella. Cuantos más empleados reales intervengan en la gestión de estas peticiones, más probable será que se destape la estafa antes de que se produzca algún daño.

Cosas de la ciencia: un fallo retro de Office ataca de nuevo

En cuanto a los documentos maliciosos de Office y los exploits que intentan desplegar, lo que es antiguo se utiliza una y otra vez, desaparece después de que Microsoft publique una actualización y, después, (a veces) resurge. Durante años, SophosLabs ha analizado cómo los atacantes incrustan una amplia y cambiante variedad de exploits en los documentos maliciosos. Las vulnerabilidades recién descubiertas tienen muchos partidarios entre los delincuentes que utilizan documentos maliciosos como trampolín para distribuir cargas de malware, porque no todo el mundo instala los parches de inmediato, y a veces las empresas de seguridad tardan un poco en crear una medida de protección eficaz basada en el comportamiento u otras características de un vector novedoso.

La mayoría de los documentos maliciosos que hemos visto a lo largo del año pasado han sido elaborados utilizando herramientas llamadas generadores, que dan a los atacantes un sistema de menú de "apuntar y hacer clic" literal que les permite decidir exactamente qué exploits incorporan en el documento malicioso. A medida que las herramientas de protección de endpoints mejoran en la identificación de estos exploits más modernos, que por lo general consisten en un script incrustado en el documento, los creadores de documentos maliciosos parecen haber buscado mucho para encontrar un error muy, muy antiguo que ayuda a ocultar las macros y otro contenido malicioso en los documentos.

El error se conoce coloquialmente como exploit **VelvetSweatshop**, aunque en realidad no es un exploit en absoluto. De hecho, VelvetSweatshop fue introducido por Microsoft en Microsoft Office 2003, aunque no vimos que se abusara de él hasta 2013, cuando los libros de Excel que explotaban la vulnerabilidad CVE-2012-0158 fueron camuflados con la ayuda del fallo. Una hoja de cálculo de Excel o un documento de Word marcado como "de solo lectura" es solo un documento protegido por contraseña cuya contraseña por defecto es, efectivamente, "VelvetSweatshop".

Hemos visto que este año se han distribuido muchas hojas de cálculo de Excel maliciosas que utilizan la técnica como una forma de burlar la detección de amenazas avanzadas. Debido al cifrado, el verdadero contenido malicioso se esconde detrás de una fuerte criptografía que los escáneres no pueden descifrar ni escanear a menos que admitan el último algoritmo utilizado por los atacantes. Debido al uso de la contraseña predeterminada, Excel abre el contenido descodificado sin solicitar la contraseña, por lo que, desde el punto de vista de la ejecución, el cifrado es transparente. Los programas de seguridad de endpoints añadieron soporte para el cifrado y la contraseña predeterminada, pero los atacantes siguen encontrando otros algoritmos criptográficos que tienen la misma función y que (todavía) no han sido implementados por los escáneres AV.

Fue una gran sorpresa descubrir un error tan antiguo que, si fuera humano, estaría en su último curso en la escuela. Pero no es de extrañar que los autores de generadores de documentos armados con malware traten de aprovecharse de él.

Seguridad de la información: una retrospectiva de 20 años

Si bien un informe anual nos permite mirar hacia atrás a los acontecimientos importantes del año pasado, pensamos que remontarnos aún más –a las dos últimas décadas– ofrecería un mayor contexto sobre cómo hemos llegado al panorama actual de amenazas. El cambio de milenio marcó un hito, cuando la seguridad de la información se convirtió en una disciplina profesional y una industria legítima. Esta cronología de amenazas y eventos representa momentos significativos y representativos en la evolución del comportamiento de las amenazas.

A medida que las empresas y los particulares adoptaron Internet tanto para los negocios como para el entretenimiento, las grandes redes se convirtieron en objetivos fáciles para los gusanos (malware que se autopropaga) que proliferaban. Acumulativamente, los gusanos infectaron decenas de millones de sistemas en todo el mundo y costaron más de 100 000 millones de dólares en daños y costes de remediación.

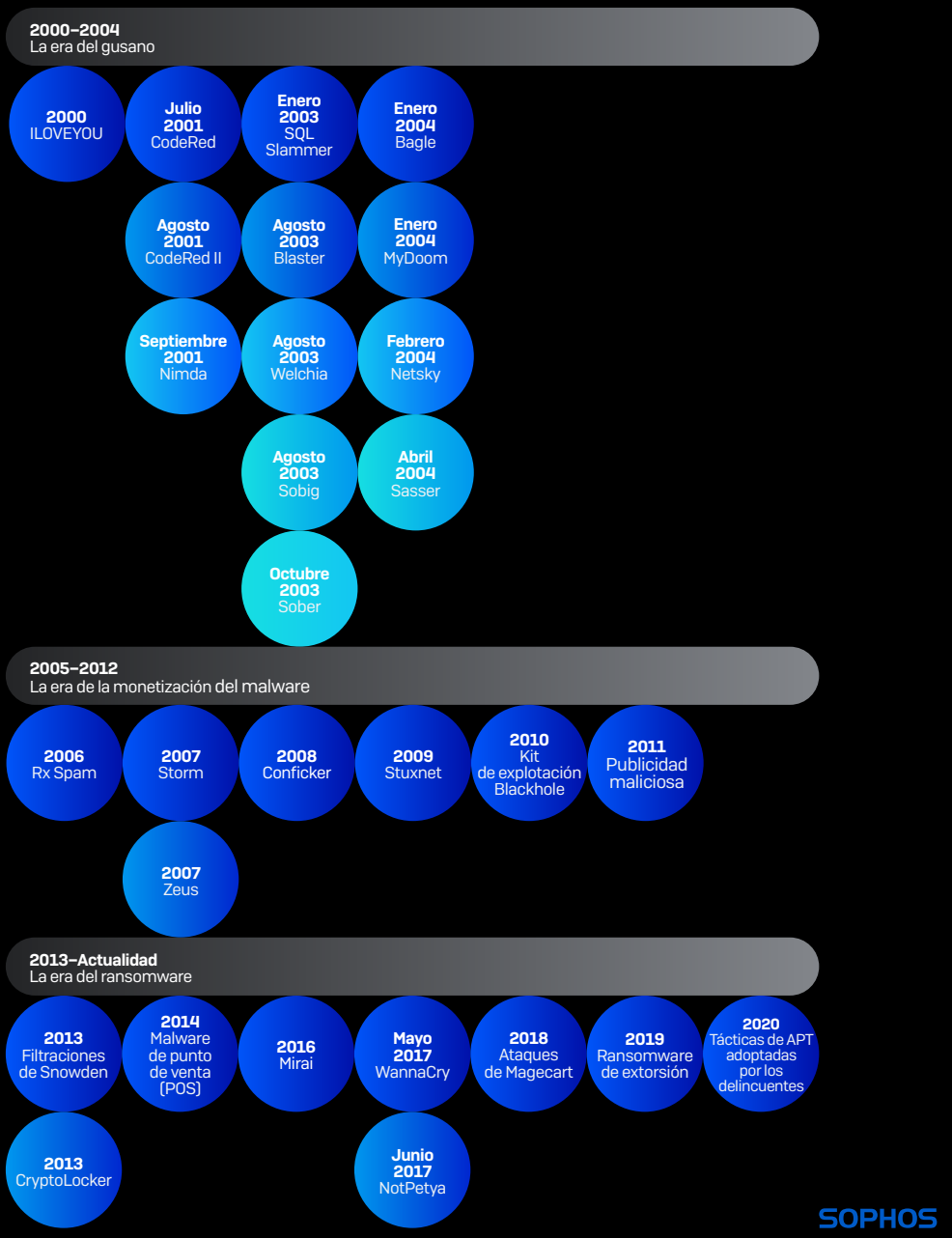


Fig.12. Fuente: Sophos

2000–2004 - La era del gusano

2000 - ILOVEYOU
El gusano ILOVEYOU usaba un truco de ingeniería social que aún hoy persiste: en forma de archivo adjunto en un correo de spam, llegó a infectar cerca del 10 % de todos los equipos Windows conectados a Internet.

Julio de 2001 - CodeRed
CodeRed, cuyo nombre procede del sabor del refresco Mountain Dew que sus descubridores estaban bebiendo en ese momento, explotaba una vulnerabilidad de desbordamiento del búfer en IIS para autopropagarse y modificar sitios web. Fue seguido un mes después por una versión mejorada que instalaba una puerta trasera en los ordenadores en red.

Agosto de 2001 - CodeRed II

Septiembre de 2001 - Nimda

Enero de 2003 - SQL Slammer
Con solo 376 bytes, Slammer explotaba un desbordamiento del búfer en las aplicaciones de bases de datos de Microsoft. Duplicando sus infecciones cada 8,5 segundos, Slammer derribó grandes partes de Internet en solo 15 minutos.

Agosto de 2003 - Blaster
Blaster fue creado mediante ingeniería inversa de un parche de Microsoft un par de meses antes del primer Patch Tuesday. Explotaba una vulnerabilidad de desbordamiento del búfer en el servicio RPC de los sistemas Windows XP y 2000 y lanzaba un ataque DDoS contra windowsupdate.com si el día del mes era mayor de 15, o el mes era septiembre o posterior.

Agosto de 2003 - Welchia

Agosto de 2003 - Sobig

Octubre de 2003 - Sober

Enero de 2004 - Bagle

Enero de 2004 - MyDoom
Se estima que el 25 % de todos los correos electrónicos enviados en 2004 se originaron con el gusano MyDoom, que se enviaba prolíficamente por correo electrónico a nuevas víctimas y llevaba a cabo un ataque de denegación de servicio (DDoS).

Febrero de 2004 - Netsky

Abril de 2004 - Sasser

2005-2012 - La era de la monetización del malware
Hasta aproximadamente 2005, los incidentes de malware podían atribuirse a la curiosidad o al deseo de producir interrupciones. A partir de entonces, dominó el malware de las redes de bots, diseñado para pasar desapercibido y obtener beneficios. Esta era también vio el comienzo del llamado spam farmacéutico. Los exploits contra las vulnerabilidades de software se convirtieron en componentes clave del malware, que permitía la publicidad maliciosa. Allí donde existía la posibilidad de obtener beneficios económicos, los ciberdelincuentes aprovechaban esas oportunidades.

2006 – Spam Rx
Lo que había sido una mera molestia (o una forma de propagar gusanos), se convirtió en un lucrativo negocio que vendía principalmente medicamentos con receta falsificados que se anunciaban a través de mensajes de spam. Se estima que los spammers farmacéuticos se embolsaron miles de millones de dólares vendiendo medicamentos que la mayoría de la gente solo podía conseguir yendo a su médico.

2007 - Storm

2007 - Zeus

2008 - Conficker
Conficker infectó rápidamente millones de ordenadores en todo el mundo, pero no causó muchos daños. Aún no sabemos el verdadero propósito del gusano, pero miles de hosts siguen infectados hasta el día de hoy, y el tráfico de escaneado del Conficker se detecta rutinariamente como parte de la "radiación de fondo" de Internet.

2009 - Stuxnet
Stuxnet fue una de las primeras armas digitales en apuntar a un sistema físico: centrifugadoras de refinamiento nuclear utilizadas por Irán para enriquecer uranio. El legado perdurable de Stuxnet es que abrió permanentemente la puerta al uso de malware como instrumento de guerra por parte de los estados nacionales.

2010 - Kit de explotación Blackhole
Los kits de explotación (kits de herramientas que se aprovechan de las vulnerabilidades de software) unieron diferentes partes del ecosistema de los ciberataques. La ciberdelincuencia como servicio nació cuando los creadores del kit de explotación Blackhole comenzaron a ofrecer sus servicios.

2011 - Publicidad maliciosa

2013–Actualidad - La era del ransomware
El ransomware ha tenido un tremendo impacto en esta era. Aunque los gusanos, los troyanos bancarios, la publicidad engañosa y el spam persisten, nada se ha acercado a la fuerza destructiva del ransomware. Se estima que los daños causados por los ataques de ransomware en los últimos siete años ascienden a billones de dólares. El ransomware también es muy probablemente la primera forma de malware relacionada con la muerte de un ser humano. Además, muchas de las amenazas actuales acaban distribuyendo ransomware y, al igual que los kits de explotación, este ha dado un enorme impulso a un ecosistema de ciberdelincuencia ya de por sí próspero.

2013 - Filtraciones de Snowden

2013 - CryptoLocker
Durante su breve existencia, CryptoLocker proporcionó a los futuros atacantes una fórmula ganadora al unir dos tecnologías existentes: el cifrado y las criptodivisas. CryptoLocker cambió para siempre el panorama de las amenazas, y sus réplicas todavía se sienten hoy en día. Tres meses después de su lanzamiento, la cartera de bitcoins usada por CryptoLocker contenía casi 30 millones de dólares.

2014 - Malware de punto de venta (POS)

2016 - Mirai

Mayo de 2017 - WannaCry
WannaCry, el híbrido de gusano y ransomware más extendido que se ha visto, demostró (de nuevo) cómo un lapsus en la aplicación de parches puede tener consecuencias nefastas. Se basaba en exploits robados de la NSA y publicados por The Shadow Brokers. Los ataques obligaron a Microsoft a publicar actualizaciones fuera de banda para productos no soportados.

Junio de 2017 - NotPetya
NotPetya paralizó algunas de las mayores empresas de transporte y logística del mundo y causó, supuestamente, más de 10 000 millones de dólares en daños. Algunas de las empresas afectadas aún no se han recuperado totalmente.

2018 - Ataques de Magecart

2019 - Ransomware de extorsión
En un ataque contra la ciudad de Johannesburgo (Sudáfrica), los ejecutores del ransomware Maze fueron los primeros en usar el chantaje. No solo cifraron y robaron datos, sino que también amenazaron con publicar los datos robados si las empresas no pagaban. Esta táctica ha sido copiada por muchos otros grupos de ransomware como cobertura contra los objetivos con copias de seguridad en buen estado.

2020 - Tácticas de APT adoptadas por los delincuentes
La adopción de herramientas y tácticas de los estados nacionales, que comenzó en los últimos dos años, se generalizó en 2020. Las bandas de ciberdelincuentes profesionales utilizan herramientas sofisticadas como Cobalt Strike con un efecto devastador, mientras que algunos grupos (Dharma) integran las tácticas en kits de herramientas de fácil uso para principiantes.

CÓMO LA COVID-19 MULTIPLICA LA FUERZA DE LOS ATAQUES

El nuevo coronavirus COVID-19 afectó radicalmente a todos los aspectos de la ciberseguridad. Los atacantes se sintieron envalentonados para atacar a los empleados de oficinas recién confinados en casa. El ya elevado nivel de ansiedad y miedo que impregnaba la esfera pública se vio agudizado por oleadas de campañas de spam, ransomware dirigido a instituciones debilitadas o destrozadas o a la sociedad civil que ya estaba bajo presión económica, y todo tipo de fraudes para captar rentas y especular con la escasez de recursos, desde equipos de protección individual (EPI) hasta papel higiénico.

Nuestros hogares son el nuevo perímetro

La normalidad tal y como la conocíamos terminó en marzo de 2020, cuando los empleados que podían teletrabajar y los alumnos de casi todos los niveles fueron enviados a casa en una carrera desenfrenada para detener la propagación de la COVID-19 y aliviar la presión de los hospitales saturados. De repente, ya no trabajábamos en casa, sino que vivíamos en el trabajo.

Mucha gente tuvo dificultades para encontrar la nueva normalidad sin desplazarse a la oficina. Se disparó la demanda de acceso a redes VPN y servicios de autenticación multifactor. Los Chromebooks se convirtieron en bienes escasos. Zoom registró unos diez años de crecimiento evolutivo en tan solo dos meses. Y en medio de todo esto, Microsoft, Adobe, Apple y Google publicaban actualizaciones y parches de mantenimiento para una multitud de plataformas.

Aumentan las estafas por correo electrónico relacionadas con el coronavirus y la COVID-19

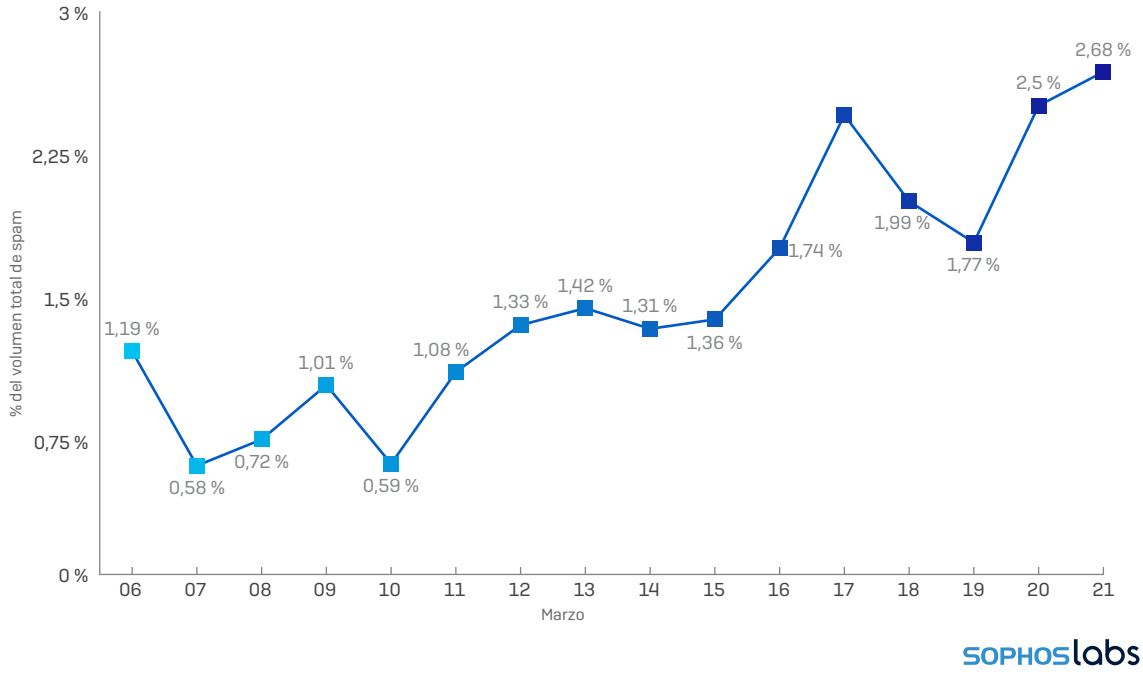


Fig. 13. En las semanas posteriores al confinamiento, una parte significativa de los correos de spam mencionaban la COVID-19 o el coronavirus a escala mundial. Fuente: SophosLabs.

La COVID-19 nos convirtió a todos en nuestros propios departamentos de TI, gestionando parches, actualizaciones de seguridad y problemas de conectividad que nos impedían acceder a reuniones o que impedían que nuestros hijos pudieran asistir a una clase virtual. Aumentó la demanda de auriculares, micrófonos, productos para mejorar la iluminación y soluciones de seguridad tanto en la red como en el endpoint. E incluso significó dar a los niños un curso intensivo de phishing, spam, troles online, ciberacoso y malware camuflado en un ejemplar gratuito de su juego favorito, listo para jugar.

No ha sido fácil, y todavía no estamos funcionando como en febrero de 2020, pero mucha gente considera que la nueva normalidad podría, de alguna manera, representar una mejora. Muchas oficinas han decidido seguir permitiendo el teletrabajo incluso después de que terminen los confinamientos y las personas puedan regresar al lugar de trabajo, lo que supondrá un beneficio significativo tanto para el medio ambiente como para la calidad de vida de las personas.

A medida que los perímetros de esos lugares de trabajo se amplían para abarcar gran parte de las plantillas en sus ubicaciones remotas, las circunstancias han hecho que nos tomemos más en serio el papel de las redes domésticas como última línea de defensa. El módem en el armario del pasillo es ahora el perímetro de la red. Necesitamos replantearnos completamente cómo proveer a esa estructura de una defensa exhaustiva.

Ciberdelincuencia como servicio

Puede ser útil pensar en los creadores de malware como una especie de empresa emergente de software. Un tanto desorganizados al principio, con el tiempo prosperan y ganan fieles seguidores. Y puede haber tantos modelos de negocio para el software malicioso como para el software legítimo.

El término "crimeware" o software delictivo es intencionadamente amplio; algunos creadores de malware, o de las herramientas que permiten distribuirlo fácilmente o mejorarlo con nuevas funciones, no venden su producto directamente, sino que conceden licencias, del mismo modo que se vende una licencia de un año de Adobe Creative Suite. Hemos llamado a esta clase de modelo de negocio "ciberdelincuencia como servicio" (CaaS), y todo parece indicar que formará parte de la nueva normalidad.

Uno de los ejemplos más notorios del malware CaaS es el Emotet. Este troyano distribuido a través del spam existe desde hace años, ya que parece ofrecer una experiencia sin complicaciones al delincuente en potencia. El Emotet es uno de los tipos de malware que los investigadores de seguridad denominan cargadores. Su objetivo fundamental es distribuir otro malware al ordenador de la víctima. Lleva a cabo esta tarea con una sofisticada red que distribuye correos electrónicos de spam armados con malware a una gran cantidad de destinatarios.

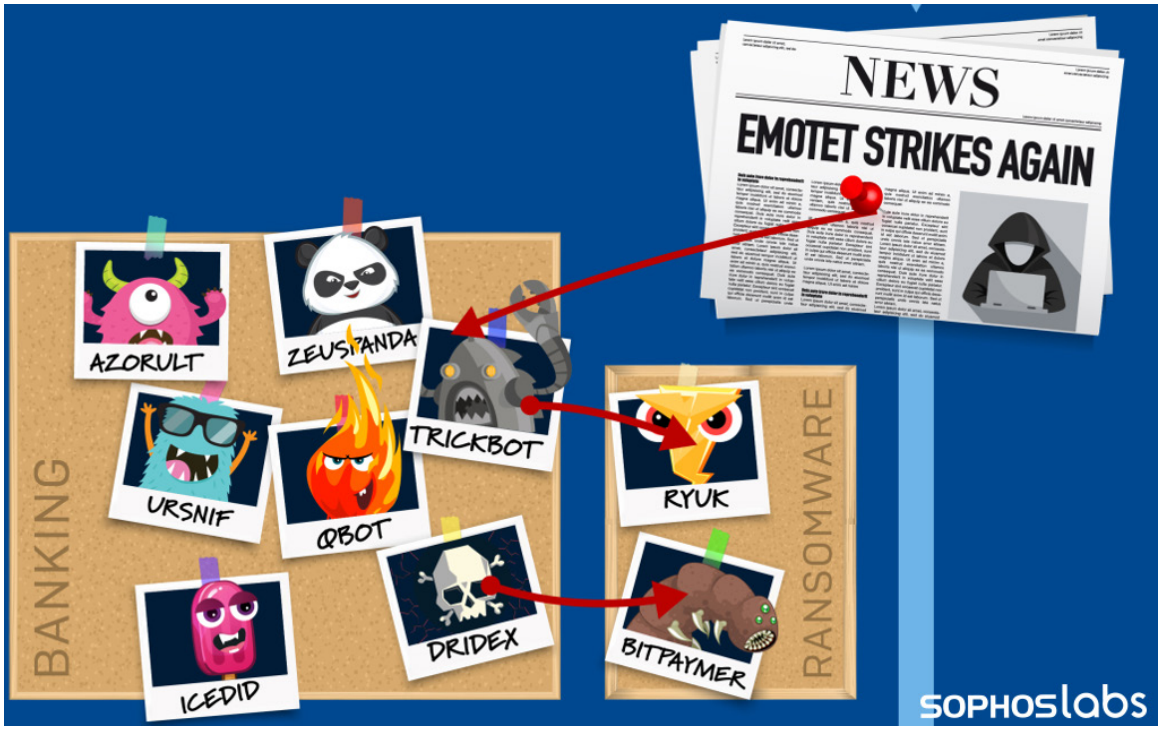


Fig. 14. Fuente: SophosLabs.

El Emotet, sin embargo, ha tenido dos periodos de inactividad en lo que va de año. El malware permaneció en comunicación con sus servidores C2 durante un periodo de casi cinco meses, durante los cuales los mensajes de spam que normalmente distribuyen ataques se evaporaron por completo. Los correos de spam que propagan el Emotet se reanudaron misteriosamente en julio.

El ransomware Dharma es otro malware CaaS que destacar. A diferencia de sus parientes más caros, Dharma mantiene un rescate bajo fijo. La razón se reduce al modelo de negocio de Dharma: es el ransomware con ruedines para delincuentes en ciernes que necesitan aprender lo básico. Básicamente, estos principiantes pagan una cuota de suscripción para obtener cargas de los creadores de Dharma y se reparten los beneficios de cualquier ataque con ellos.

A medida que los atacantes se ramifican en especialidades y subespecialidades, no parece que el modelo de negocio en que los delincuentes trabajan con contratistas independientes, autónomos y asociados vaya a desaparecer pronto.

Spam, estafas y promesas rotas

Los confinamientos en todo el mundo fueron acompañados por un aluvión de estafas instigadas por correos de spam. En el mejor de los casos, las campañas de spam más eficaces crean una sensación de urgencia para exigir que el destinatario actúe. Es un truco psicológico muy conocido, porque si nos tomamos unos segundos para analizar el contenido del mensaje de spam, probablemente nos daremos cuenta de que es falso. Si el spammer provoca una reacción de miedo, actuamos antes de pensar y quedamos atrapados en la trampa.

La COVID-19 ya tenía a todo el mundo en un estado de alerta permanente, así que los spammers ni siquiera tuvieron que esforzarse mucho.

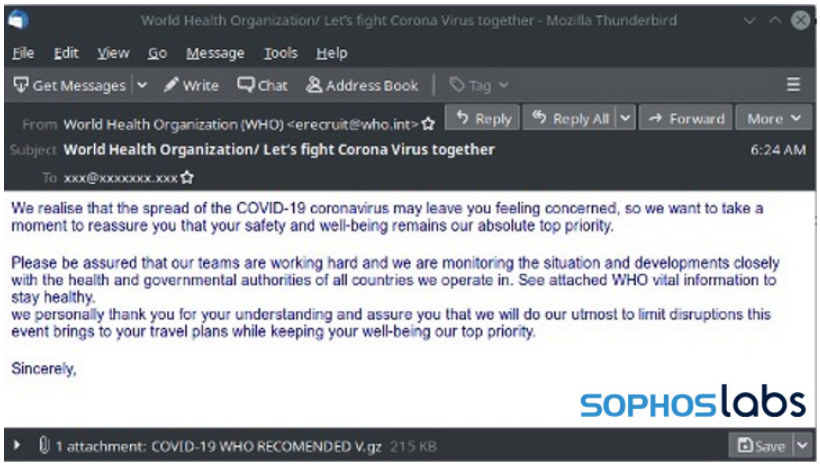


Fig. 15. Fuente: SophosLabs.

A las pocas semanas de confinamiento, decidimos echar un vistazo más de cerca a otro fenómeno creciente: los registros de dominio. En pocas semanas, se habían estado registrando miles de nombres de dominio nuevos al día que contenían cualquier combinación de las cadenas *COVID-19*, *corona* o *virus*.

Domain	First Seen	Nameserver	Ns Ip
coronavirusshaquilleoneal.com	2020-03-14 07:00:38	ns-cloud-b1.googledomains.com	216.239.32.107

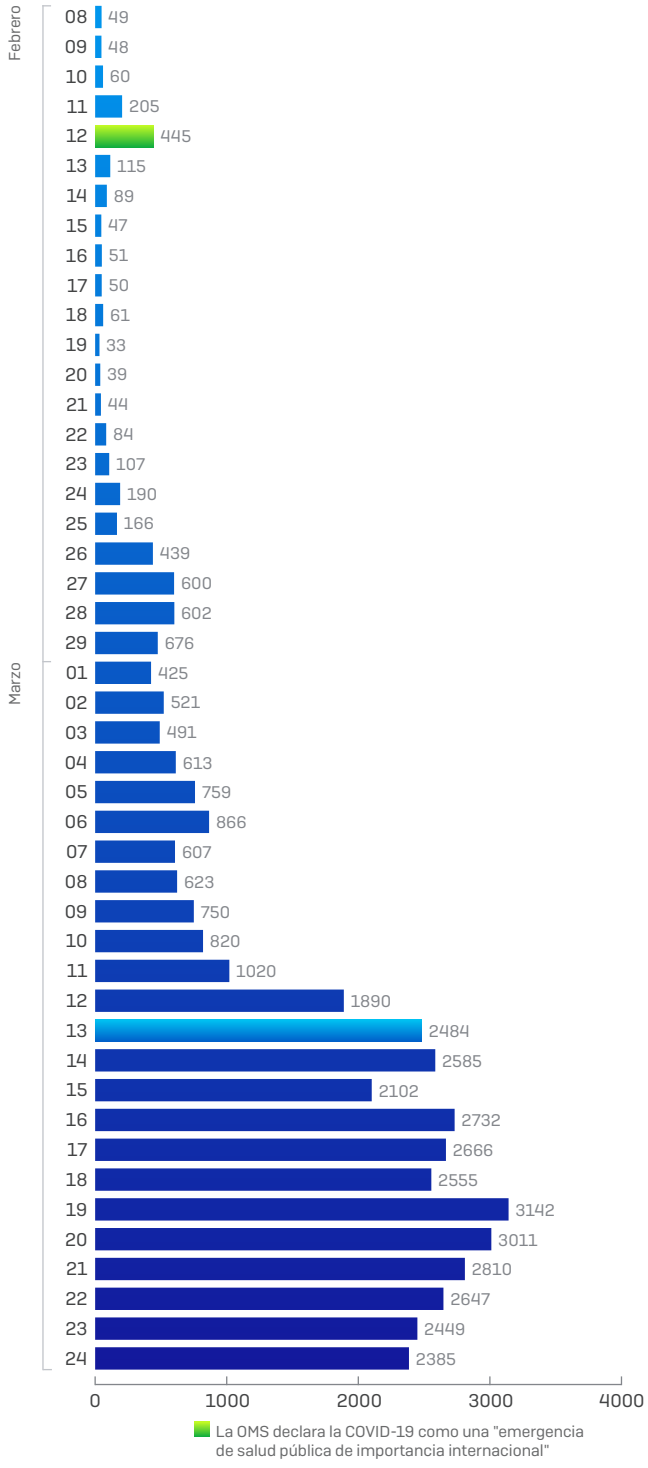
SOPHOSlabs

Fig. 16. Fuente: SophosLabs.

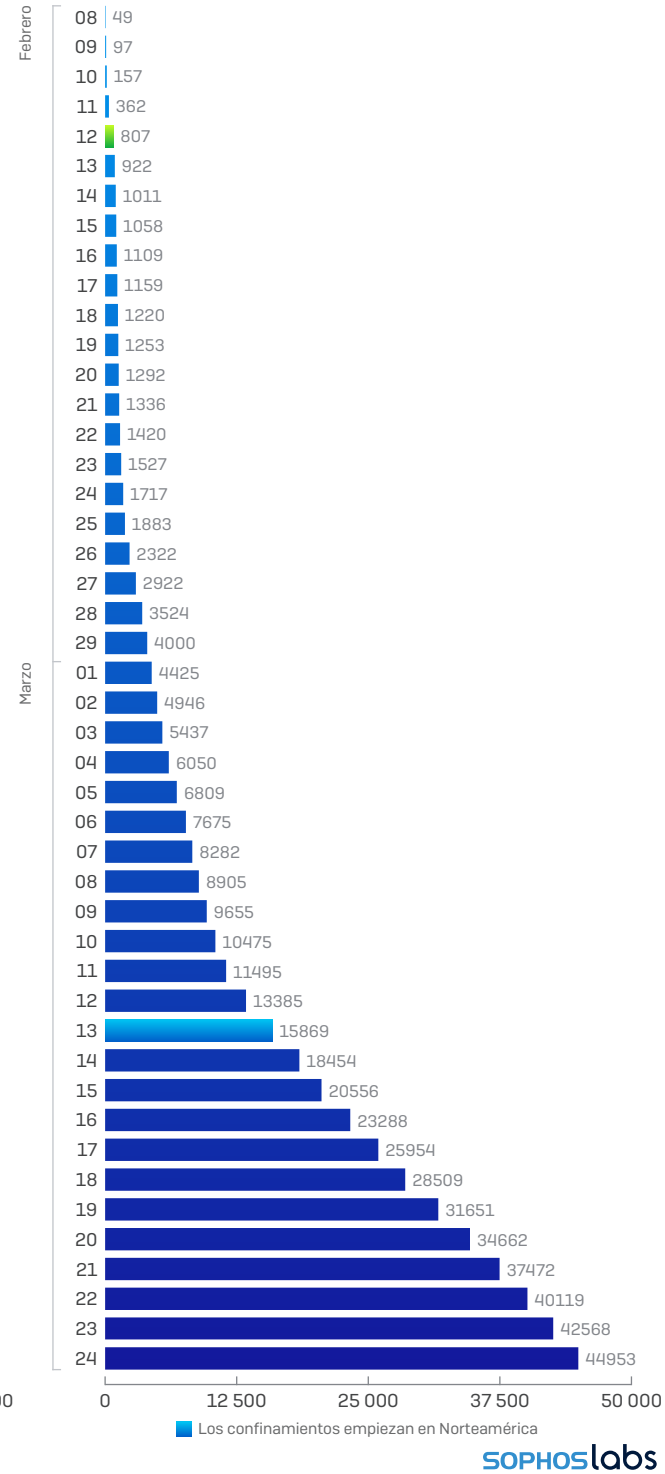
Algunos de los sitios eran evidentemente bromas, mientras que otros eran similares a los utilizados por las autoridades sanitarias regionales o nacionales legítimas hasta el punto de crear confusión.

También buscamos dominios y subdominios relacionados con la COVID-19 en los registros de transparencia de certificados TLS. Los registros de transparencia de los certificados son útiles para hacer un seguimiento de los subdominios que tienen sus propios certificados TLS (información que no aparece en los datos sin procesar de registro de los dominios) y nombres de dominio.

Nuevos registros de dominios COVID al día



Total de nuevos nombres de dominios COVID hasta la fecha



SOPHOSlabs

Fig. 17. Durante los primeros meses de la crisis de la COVID-19, se registraron al día miles de dominios cuyos nombres contenían la cadena "COVID-19" o "corona", y se concedieron licencias para una cantidad igual o mayor de certificados TLS. Fuente: SophosLabs.

Nuevos certificados TLS al mes con nombres de host "COVID-19" o "corona".

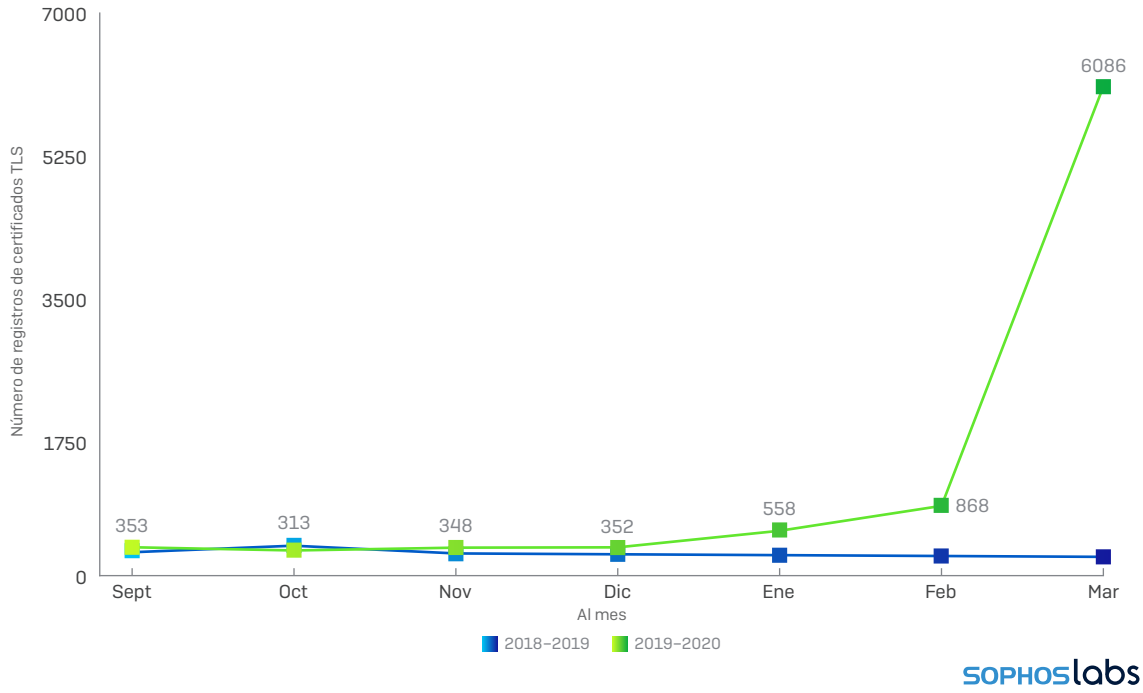


Fig. 18. Los registros de certificados TLS que se referían a la pandemia se dispararon más o menos al mismo tiempo que los registros de dominio.
Fuente: SophosLabs.

Vimos una media de más de 200 solicitudes de certificados para los dominios COVID-19 al día en marzo, y el índice siguió subiendo durante los meses posteriores. En junio, el promedio llegó a 625 solicitudes al día. En octubre, ese índice alcanzó un máximo de 951 nuevos certificados TLS que se solicitaban al día.

La mayoría de estos dominios siguen siendo legítimos o benignos, aunque muchos permanecen aparcados y no tienen ningún contenido, lo que indica que el solicitante podría estar esperando para incrementar su "antigüedad" y mejorar así su reputación en futuras comprobaciones.

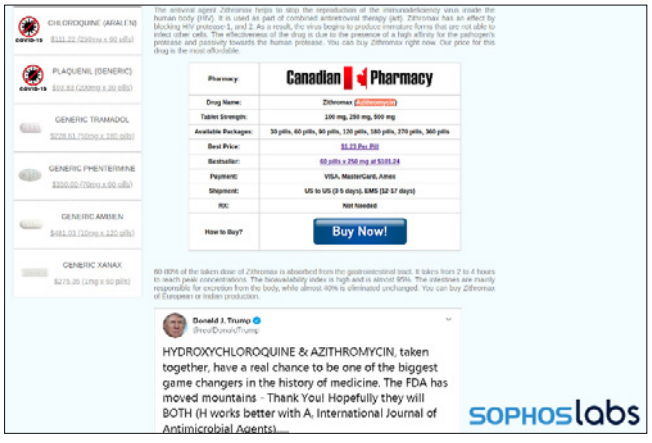


Fig. 19. Tampoco los infames distribuidores ilícitos de fármacos dudaron en aprovecharse de cualquier cura milagrosa que apareciera en Twitter, e incluso publicaron tweets en los anuncios.
Fuente: SophosLabs.

Se ha identificado un pequeño porcentaje (menos del uno por ciento) asociado con el phishing o el malware. Muchos son efímeros, con nombres de host que ya no se pueden resolver después de tan solo un día.

El teletrabajo incrementa la importancia de la informática en la nube segura

Cuando en marzo de 2020 empezaron los confinamientos por la COVID-19, las personas y los lugares de trabajo iniciaron una rápida transición sin precedentes que continúa a día de hoy. Es posible que la forma en que trabajamos, vamos a la escuela, asistimos a eventos y conferencias y nos divertimos haya cambiado para siempre, y la informática en la nube es una parte fundamental de esta veloz evolución, pero presenta un gran número de desafíos.

Unos permisos de acceso excesivos, una visibilidad limitada de los activos y los recursos en la nube y la falta de auditorías pueden contribuir a crear unos entornos en la nube más vulnerables a las ciberamenazas, y el malware es tan perjudicial en la nube como en cualquier otra ubicación. Por ejemplo, el criptojacking es un problema cada vez más presente en la nube. Los procesos de criptominería que utilizan muchos ciclos informáticos son muy perjudiciales cuando se ejecutan en equipos físicos, porque disparan los costes energéticos, y aún tienen una consecuencia indirecta más dañina cuando se ejecutan en instancias en la nube: el proveedor de la nube cobra a la víctima los ciclos de CPU consumidos por sus estaciones de trabajo virtuales, que realizan las complejas operaciones matemáticas necesarias para producir unos pocos centavos de criptomonedas.

Además, muchas plantillas que teletrabajan desde múltiples ubicaciones han sufrido ataques de ransomware, en que los delincuentes bloquearon la infraestructura en la nube de la misma forma que atacaban los equipos físicos. A fin de cuentas, el ransomware puede cifrar un disco duro o un almacén de objetos virtual con la misma facilidad que un almacén físico. Las empresas cuya infraestructura en la nube sufre un ataque de ransomware pueden enfrentarse no solo a la factura de los ciclos consumidos por el cifrado de datos, sino también al pago del rescate.

Empresas que han sufrido incidentes de seguridad en el último año

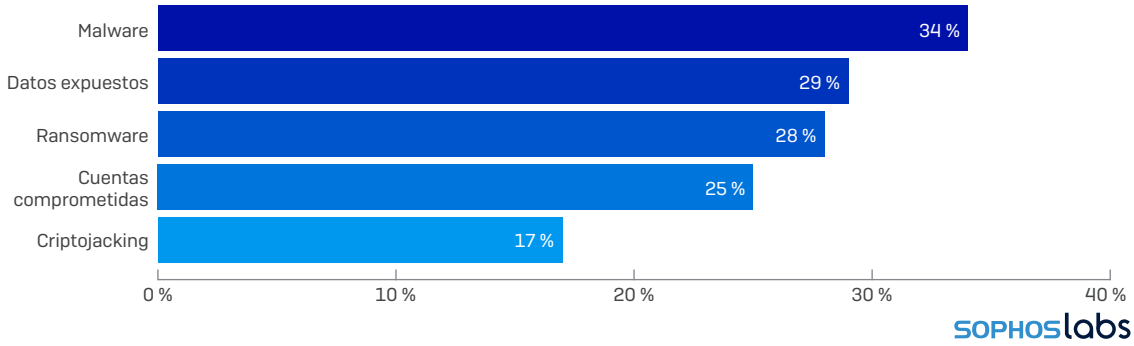


Fig. 20. En su informe sobre la seguridad en la nube en 2020, Sophos encuestó a más de 3500 profesionales de TI sobre su experiencia con el uso de la nube, y concluyó que muchos de los problemas de seguridad que afectaban a las redes físicas se han trasladado a las virtuales. Fuente: SophosLabs.

Durante el confinamiento, los departamentos de TI necesitaban encontrar la forma de prestar un servicio de asistencia técnica virtual igual que lo hacían desde un centro físico antes de que muchos lugares de trabajo cerraran. Los grandes cambios que requería la COVID-19 llegaron en tres oleadas.

Durante las primeras semanas después del inicio de los confinamientos, la primera oleada (la oleada del acceso) empezó a cobrar forma. De repente, millones de trabajadores no podían acudir a su lugar de trabajo y necesitaban acceder a los recursos locales de su empresa, y el rápido crecimiento de la demanda de redes privadas virtuales (VPN) y otros tipos de acceso con métodos de confianza cero arrasó los recursos existentes. Además de las VPN, las empresas tuvieron que añadir nuevos firewalls y otros dispositivos de seguridad, despliegues de sistemas de gestión unificada de amenazas modernos que complementaban los rudimentarios firewalls de capa 3 proporcionados por los proveedores de la nube.

En el mundo previo a la COVID-19, el uso de las VPN era moderado, ya que el número de empleados en el lugar de trabajo superaba con creces el de trabajadores móviles y remotos. Al transcurrir marzo y abril, luego mayo y finalmente junio, para estos empleados, la VPN se convirtió en un servicio esencial (por no decir el servicio esencial) para mantener las empresas operativas.

Pero estas empresas también se percataron pronto de que los empleados no debían utilizar dispositivos personales desde casa para acceder a la VPN, y el suministro cada vez más limitado de portátiles nuevos supuso un nuevo desafío para las empresas que ya tenían dificultades para satisfacer las necesidades de TI de sus plantillas distribuidas. Sin suficientes dispositivos físicos, las empresas optaron, provisionalmente, por el recurso en apariencia ilimitado que constituían los equipos virtuales, a fin de cubrir la necesidad de un espacio de trabajo informático seguro. Y así empezó la segunda oleada: la oleada de los escritorios virtuales.

A medida que los empleados se pasaban al uso de un escritorio corporativo virtual, el traslado de estos escritorios al alojamiento en la nube cobraba sentido desde un punto de vista práctico y financiero, pero seguían necesitando protección.

De repente, los departamentos de TI debían prestar soporte a cientos o miles de equipos virtuales de empleados y, de pronto, necesitaban herramientas que ofrecieran visibilidad para poder inventariar y configurar de forma segura la creciente infraestructura en la nube de servidores virtuales, escritorios virtuales y otros servicios en la nube, y así devino la oleada de la gestión de la nube.

Línea temporal del ataque

Fig. 21. Un ataque de criptojacking que investigamos empezó cuando un desarrollador incrustó sin percatarse sus credenciales en la nube en el código de un repositorio público.
El atacante lo descubrió y utilizó esas credenciales para atacar, usando las API nativas del proveedor de la nube y poniendo en marcha cientos de instancias de equipos virtuales para extraer bitcoins. Al mismo tiempo, el ciberdelincuente automatizó funciones en esas instancias para hacer que fuera más difícil detenerlas. Posteriormente, revocó el acceso a otros usuarios legítimos.
Fuente: SophosLabs.

La era de la COVID-19 ha estado marcada por una gran transformación en todos los aspectos de la vida humana, incluyendo cuántos de ellos funcionan. Según un estudio reciente de Reuters, el 97 % de los directores ejecutivos y tecnológicos encuestados afirmaron que los confinamientos aceleraron su transición hacia nuevas tecnologías. Pero en tiempos de presupuestos ajustados e incertidumbre, casi uno de cada tres de estos directores técnicos afirmó que su cometido era el de implementar estos cambios de la forma más rentable posible.

En el informe de seguridad en la nube más reciente de Sophos, descubrimos que la mayoría de los incidentes de seguridad que implicaban la informática en la nube se debían a dos causas raíz principales: credenciales robadas o conseguidas mediante phishing, o bien errores de configuración que se tradujeron en infracciones de seguridad. Siete de cada diez de los más de 3700 profesionales de TI encuestados para el informe mencionaron que la infraestructura en la nube a su cargo había sufrido una infracción en los 12 meses anteriores a la encuesta.

Lo que significa la CCTC para una respuesta rápida a amenazas a gran escala

Fig. 22. Fuente: Sophos.

Aproximadamente una semana después del inicio del confinamiento por la COVID-19, el científico jefe de Sophos, Joshua Saxe, hizo un llamamiento de voluntarios a escala global. Esta brigada de voluntarios se convirtió rápidamente en la COVID-19 Cyber Threat Coalition (CCTC), una organización con más de 4000 miembros en servicio con un objetivo: dedicar un esfuerzo especial a combatir cualquier tipo de amenaza o ingeniería social que intentara aprovecharse del miedo de las personas a la COVID-19, ya fuera por mención directa o indirecta.

"No soy bombero, de modo que no sé cómo sofocar un incendio en un edificio, pero puedo ayudar al equipo que va a reforzar las defensas de una infraestructura crítica, como los hospitales", explica Nick Espinosa, miembro de la CCTC y analista de seguridad y podcaster de Chicago.

Este proyecto era muy necesario. Desde el primer momento del período de confinamiento, los atacantes propagaron spam, malware y diversas amenazas de otros tipos que hacían referencia, de una forma u otra, a la nueva y aterradora jerga pandémica. Como se menciona en el informe principal, en un determinado momento, se estaban registrando miles de nuevos dominios con las palabras COVID-19, corona o CoV en sus nombres, todos los días. Sophos rastreó dominios relacionados con certificados TLS con estas mismas cadenas de texto en los datos del certificado y encontró otros miles.

Crecimiento del número de miembros de la CCTC

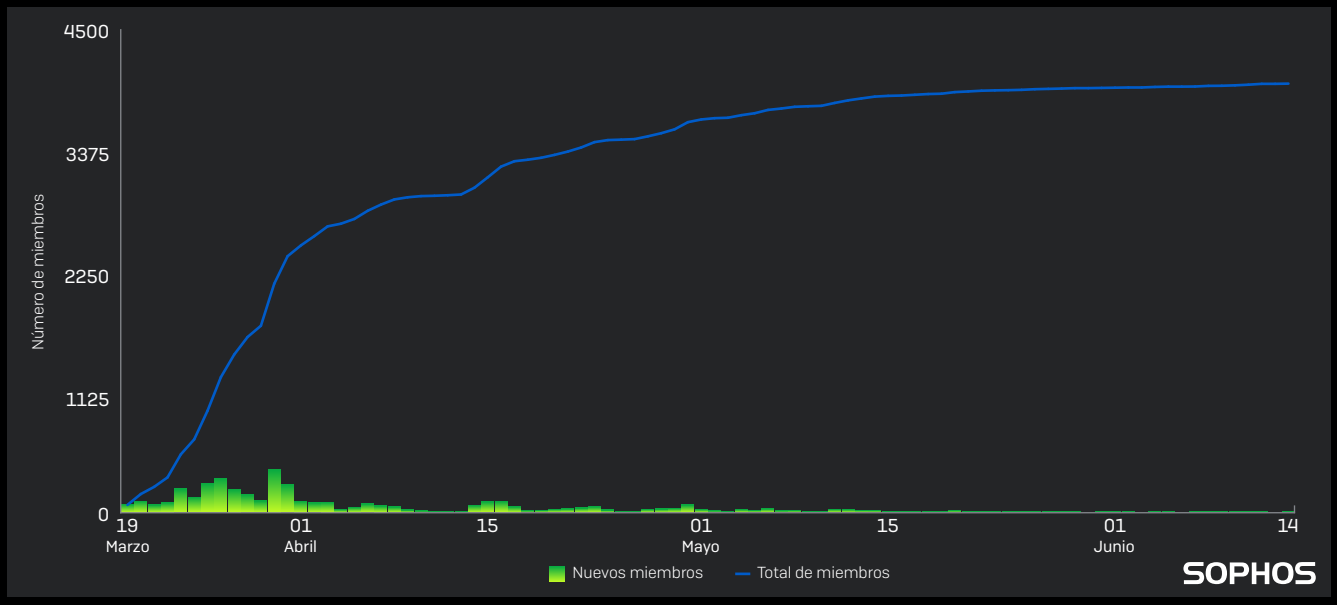


Fig. 23. Fuente: Sophos.

Debido al tipo de amenaza único que supone la COVID-19, el spam malicioso que se aprovecha de la crisis global es un fenómeno que resulta especialmente indignante y ofensivo. "Vimos una explosión de hacking delictivo que utilizaba la COVID-19 como señuelo", explica Espinosa. Proliferaron las campañas de spam, en que se enviaban mensajes que simulaban comunicados oficiales de la Organización Mundial de la Salud, el CDC de EE. UU., el NHS del Reino Unido, empresas farmacéuticas o autoridades sanitarias nacionales en países de fuera de EE. UU. y el Reino Unido.

Los analistas también observaron referencias a la COVID-19 en cadenas dentro de binarios y utilizadas como variables en los llamados LOLscripts.

Los integrantes de la CCTC compartieron ejemplos e información sobre todo tipo de incidentes a través de un canal de Slack creado apresuradamente. Aunque caótica al principio, la organización formó una estructura rudimentaria con rapidez. "Se juntaron muchísimas personas y se lanzaban muchísima información", comenta Espinosa.

El producto de la CCTC, el resultado colectivo, es una fuente de información que enumera los indicadores de peligro recién recopilados. Todo el mundo puede utilizar esta fuente, que es gratuita. Estos indicadores de peligro complementan las tecnologías de defensa ya existentes, con independencia de los proveedores. Cuando la CCTC se asoció con la Cyber Threat Alliance, los proveedores de seguridad que participaban en la CTA amplificaron el efecto protector de la información sobre amenazas de la CCTC al procesarla y proteger contra esas amenazas.

La rápida unión de profesionales de la seguridad compartiendo un objetivo común fue alentador", afirma Espinosa. "Seguramente éramos un enorme caos al principio", comenta, pero el grupo se organizó rápidamente. La finalización de la plataforma de información compartida de la CCTC significa que cualquiera que tenga que responder a una pandemia parecida a la COVID-19 en el futuro no tendrá que reinventar la rueda, y podrá responder de forma más inmediata a las amenazas; una metáfora y una analogía saludables del propio sistema inmunitario.

IMPOSIBLE BAJAR LA GUARDIA: AMENAZAS A TRAVÉS DE PLATAFORMAS NO TRADICIONALES

Vivimos en un mundo rodeados por dispositivos informáticos que no se parecen a un ordenador ni a un servidor: enrutadores, teléfonos móviles, firewalls, televisores inteligentes, reproductores de contenido multimedia, centralitas VoIP, cámaras y videoporteros, dispositivos de almacenamiento en red, determinados electrodomésticos, etc.

Pero que no se parezcan a ordenadores tradicionales no significa que no puedan usarse de forma incorrecta o maliciosa igualmente.

Crece el volumen del malware Joker para Android

Los usuarios de Android se encuentran en medio de una carrera armamentística entre Google (propietario de la plataforma Android y su principal Google Play Store) y los creadores de malware que quieren que su malware se incluya como descarga en Google Play Store. Google ha dedicado años a construir un sistema diseñado para inspeccionar el código fuente de las apps para Android enviadas para su inclusión en Google Play Store, en búsqueda de fragmentos de código que indiquen intenciones maliciosas o efectos no deseados para los usuarios de Android. Los desarrolladores de apps de malware han tenido que trabajar duro para eludir las comprobaciones de código de Google Play Store.

Joker, también conocido como Bread, es una app fraudulenta de facturación y SMS con tarifas especiales, uno de los ejemplos más exitosos de una familia de malware que ha evolucionado para esquivar estas comprobaciones de código. Google ha retirado miles de estas apps maliciosas modificadas por Joker de Google Play Store desde el año pasado, cuando fue descubierto por los investigadores. A pesar de todos los esfuerzos dedicados a deshacerse del malware, Joker sigue resurgiendo.

Joker puede adoptar la forma de una amplia gama de apps distintas, como utilidades y herramientas, fondos de pantalla, traductores, o servicios de mensajería, a modo de clon de numerosas apps populares. Recuerde que, de hecho, Joker puede estar incrustado en una app que parezca y funcione exactamente igual que la versión real de casi cualquier app que utiliza. Las apps de Joker simplemente incorporan un poco de código de malware adicional, profundamente integrado en una de las bibliotecas de terceros que los creadores de apps compilan rutinariamente en sus apps por diversos motivos legítimos.

Hay distintas razones por las que Joker consigue eludir con éxito las comprobaciones de seguridad del código de Google Play Store una y otra vez:

1. Las apps maliciosas se sirven de la ofuscación, desde la simple sustitución de cadenas hasta complejos empaquetadores comerciales, para ralentizar el análisis y engañar a Google Play Store.
2. Cuando el "desarrollador" de Joker publica la app, no contiene nada de código malicioso. Así se establece un historial que demuestra que la app que se incorpora en Google Play Store está limpia. El código malicioso aparece en la app solo posteriormente, después de una actualización.
3. La app descifra su carga en tiempo de ejecución, o bien la descarga dinámicamente después.

El malware Joker utiliza código nativo (JNI) en lugar de DEX, que es más común. El código nativo utiliza C para programar, lo que ralentiza el análisis del código malicioso. En comparación, DEX, que es una variación del código Java, es mucho más fácil de descompilar en un formato legible. El malware utiliza este código JNI para enviar mensajes SMS, para ganar dinero y como forma de contactar con su red de comando y control. El uso de JNI y señalización fuera de banda a través de la red telefónica en lugar de Internet podría ayudar a Joker a eludir los escáneres automatizados de DEX que no entienden JNI.

Está claro que Joker ha conseguido ventaja en la batalla contra la revisión automatizada de código de Google en las nuevas apps, y no vemos indicios de que Joker vaya a desacelerarse en 2021, e incluso puede que se le unan competidores más pronto que tarde.

Anuncios y apps no deseadas son cada vez más difíciles de distinguir del malware

Los anuncios maliciosos siguen siendo una de las principales fuentes de amenazas para diversos dispositivos. Recientemente ahondamos en dos tendencias actuales en las amenazas de la publicidad maliciosa que quedan fuera del ámbito de los ataques de malware: estafas de soporte técnico que utilizan páginas web de "bloqueo del navegador" y anuncios en dispositivos móviles con vínculos a apps fraudulentas o de fleeceware. Sophos los clasifica como ataques de "alertas falsas", anuncios maliciosos que intentan asustar a sus víctimas para que realicen acciones que enriquezcan a los estafadores que se ocultan tras ellos.

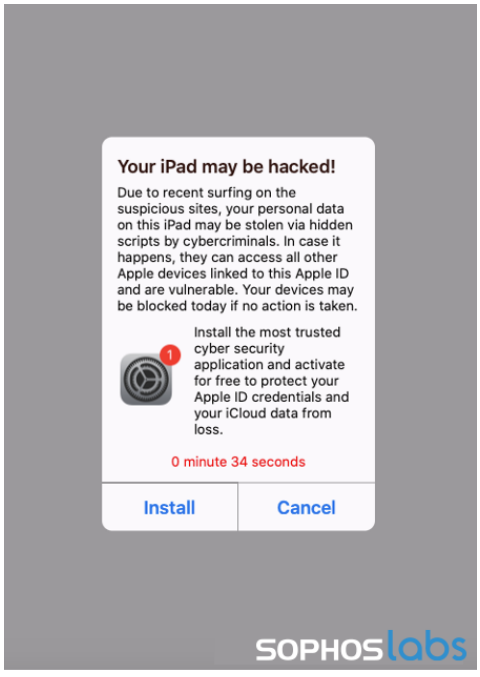


Fig. 24. Fuente: SophosLabs

Normalmente, las estafas de soporte técnico tratan de condicionar a las víctimas para que concedan acceso remoto a sus ordenadores, para después convencerlas de que compren un software de soporte técnico a un precio desorbitado, o bien obtener los datos de las tarjetas de crédito de los afectados con fines fraudulentos. Si bien en el pasado muchos de estos fraudes se realizaban por medio de llamadas de telemarketing directo, muchos estafadores se han pasado a un modelo de "persuasión", usando anuncios web maliciosos que intentan convencer al usuario de que su ordenador ha sido bloqueado por motivos de seguridad, e instándole a que llame él mismo a los estafadores.

Para conseguirlo, los estafadores despliegan kits de sitios web que contienen scripts diseñados para dificultar al usuario la salida de la página, incluyendo variaciones del "cursor maligno" (hacer que el puntero del ratón parezca que está en un lugar en el que no está o hacerlo invisible) y ataques de "descarga infinita" para sobrecargar el navegador, al tiempo que imitan el aspecto de una alerta de Microsoft o Apple. Algunos de los kits que hemos detectado explotaban un error que el equipo de seguridad ofensiva de SophosLabs descubrió en Firefox este año, mientras que otros ejecutaban ataques similares a otros navegadores, todos ellos propagados a través de anuncios web subyacentes maliciosos.

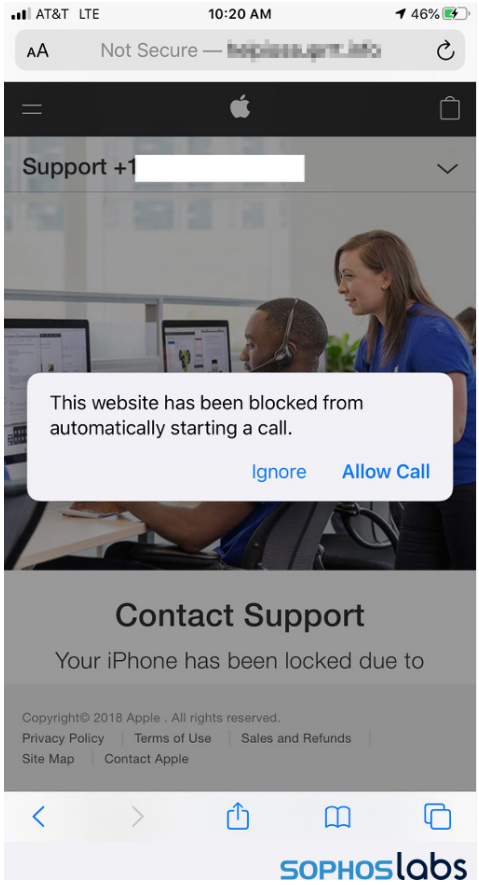


Fig. 25. Fuente: SophosLabs

La misma infraestructura de red de anuncios que respalda estos ataques en navegadores para PC y Mac también está detrás de las estafas de soporte técnico y las alertas falsas que dirigen a aplicaciones móviles potencialmente no deseadas, como apps que se presentan como servicios de red privada virtual y herramientas más "limpias" que se promocionan como limpiadores de malware, con cuotas de suscripción integradas (y, en algunos casos, malware para Android). Sophos detectó una serie de servidores de campañas de publicidad que publicaban estos anuncios, usando software comercial de un desarrollador ruso creado especialmente para ejecutar dichas campañas.

Uso de sus propias defensas contra usted: explotación delictiva de herramientas de seguridad

Algunos ataques no implican malware en absoluto (o esperan a liberar el malware en el último instante del ataque) y, en lugar de ello, simplemente utilizan las herramientas que ya están en los sistemas operativos que se ejecutan en ordenadores de toda la red. Otros delincuentes pueden explotar la potencia de una serie de herramientas usadas por dos grandes segmentos del sector de la seguridad de la información: los gestores de respuesta a incidentes y los técnicos de pruebas de penetración.

La comunidad de la seguridad de la información ha definido el estilo de los ataques que implican poco o nada de malware, pero que en cambio aprovechan los componentes existentes del sistema operativo o paquetes de software populares, como "vivir de la tierra" (técnica LOL, por sus siglas en inglés). Estos ataques suelen implicar uno o varios procesos de automatización en la forma de scripts nativos como PowerShell, archivos por lotes o scripts VBScript, que colectivamente se denominan LOLscripts. Los atacantes utilizan estos LOLscripts para ejecutar secuencias de comandos que usan binarios que "viven de la tierra" (aplicaciones), llamados coloquialmente LOLbins.

El software diseñado originalmente para el segmento de los equipos rojos del sector permite el método de autoataque. En este caso, los atacantes despliegan y utilizan herramientas de seguridad estándar que usan habitualmente los administradores de redes y los técnicos de pruebas de penetración. Entre ellas se cuentan herramientas como Cobalt Strike y elementos del marco Metasploit, diseñado para usarse en evaluaciones de seguridad y pruebas técnicas.

Conjunto de herramientas de un atacante de Netwalker en la matriz de ATT&CK

ACCESO INICIAL	EJECUCIÓN	AUMENTO DE PRIVILEGIOS	EVASIÓN DE DEFENSA	ACCESO A CREDENCIALES	DETECCIÓN	PROPAGACIÓN LATERAL	IMPACTO
Exploit de Tomcat	Scripts de PowerShell	CVE-2020-0796	Carga sin archivos	mimikatz	SoftPerfect Network Scanner	psexec	Ransomware Netwalker
Exploit de Weblogic	psexec	CVE-2019-1458	Eset AV Remover	Mimidogz	NLBrute	TeamViewer	Ransomware Zeppelin
Correo electrónico de phishing		CVE-2017-0213	Gordon's Eset Password Recovery	Mimikittenz		Anydesk	Ransomware Smaug
		CVE-2015-1701	Security Agent Uninstall Tool de Trend Micro	Editor de credenciales de Windows			Exfiltración de datos
			Desinstalación de Microsoft Security Client	pwdump			
				NLBrute			
				LaZagne			
				WinPwn			

SOPHOSlabs

Fig. 26. El conjunto de herramientas utilizado por un ciberdelincuente implicado en ataques con ransomware Netwalker incluyó numerosas utilidades de código abierto, freeware y comerciales en distintos puntos del ataque. Fuente: SophosLabs.

Estas herramientas son valiosas para los atacantes por diversas razones: puesto que suelen utilizarse de forma legítima (para auditar o mejorar la seguridad del sistema), también puede ser difícil para un antivirus u otras soluciones de seguridad detectar estas herramientas o actividad de forma clara. Por tanto, Sophos debe basarse más en el estudio del comportamiento de LOLscripts a la hora de identificar posible actividad maliciosa. Y, por supuesto, es más fácil utilizar algo que ya existe que crear herramientas propias desde cero.

Aunque el uso de LOLscripts y shells inversos no fue una novedad del pasado año, en 2020 se convirtieron en un elemento omnipresente en los ataques de irrupción con ransomware complejo operado manualmente. De hecho, tanto la cantidad como la variedad de herramientas de ataque que observamos durante los incidentes parecieron incrementarse.

Cadena de herramientas de ataque del RaaS Dharma

ACCESO INICIAL	EJECUCIÓN	AUMENTO DE PRIVILEGIOS	EVASIÓN DE DEFENSA	ACCESO A CREDENCIALES	DETECCIÓN	PROPAGACIÓN LATERAL	EXFILTRACIÓN	IMPACTO
Pulverización de credenciales RDP	PowerShell	CVE-2019-1388	Deshabilita protección antimalware	mimikatz	PCHunter	Objetos de política de grupo	Programa de envío de capturas de PowerShell	Ransomware Dharma
Credenciales RDP robadas	WMI	CVE-2018-8120	Revo Uninstaller	Remote Desktop Passview	Process Hacker	Escritorio remoto	TOR	
	AutoIT	CVE-2017-0213	IOBit Uninstaller	LaZagne	GMER	Administración remota WinRM	dropmefiles[.]com	
	Línea de comandos/ RDP			NLBrute	Advanced IP Scanner			
				Herramientas de Hash Suite	NS2.EXE			

SOPHOSlabs

Fig. 27. Fuente: SophosLabs.

La amplia gama de herramientas de ataque incluye desde aplicaciones disponibles comercialmente hasta repositorios de GitHub de código abierto, con funcionalidades como:

- Marcos de comando y control de tipo red de bots
- Generación y ofuscación de shellcode
- Evasión de antivirus y detección de espacios seguros
- Extracción de contraseñas o credenciales
- Kerberoasting (mantener la persistencia de privilegios de administrador de dominio)
- La capacidad de interceptar contraseñas por fuerza bruta utilizadas por diversos servicios
- Exfiltración de datos del sistema

Muchos de estos tipos de herramientas contienen cargas benignas o ninguna carga en absoluto en su estado inicial pero, en el pasado, hemos detectado que muchas de ellas se han visto implicadas en actividad maliciosa, basándonos en información contextual adquirida gracias a nuestras tecnologías de detección de comportamientos.

Según nuestra telemetría, las diez herramientas de ataque que hemos visto utilizar más habitualmente son (en orden de frecuencia de uso) Metasploit, BloodHound, mimikatz, PowerShell Empire, Cobalt Strike, Veil Evasion, Hydra THC, Enigma, Nishang, y Shellter. Metasploit es con diferencia la herramienta más comúnmente observada, ya que aparece en el doble de ocasiones que la siguiente herramienta de ataque más habitual, BloodHound.

Actualmente, Sophos rastrea el uso de 99 herramientas de ataque distintas, y no parece probable que los atacantes vayan a dejar de aprovecharse de estas herramientas bien diseñadas durante 2021.

Epidemiología digital

¿Qué porcentaje de dispositivos informáticos se infectan con malware no detectado? ¿Qué porcentaje de ejecuciones de línea de comandos son ejecutadas por adversarios no detectados? ¿Qué porcentaje de correos electrónicos de phishing dirigido no son detectados? ¿Cómo varían todos estos índices en función del sector, la geolocalización y la postura de red?

Plantear estas preguntas es como cuestionarse qué porcentaje de personas tienen la COVID-19 en un contexto en que, probablemente, mucha gente no se hará nunca la prueba del virus y en que las pruebas que sí se realizan tienen unos altos índices de falsos positivos y falsos negativos.

Dicho de otra forma, es difícil.

A pesar de estos desafíos, los epidemiólogos responden preguntas críticas sobre la COVID-19 a diario. Desafortunadamente, los investigadores de la ciberseguridad no consiguen hacer lo propio con los ciberataques. Vamos por detrás de los epidemiólogos con respecto a las herramientas, las técnicas y los procedimientos que hemos creado para razonar en la incertidumbre. No hay excusa, y es hora de que construyamos nuestras propias herramientas para entender la naturaleza de la amenaza a la que nos enfrentamos, que informemos de manera precisa sobre los riesgos a quienes defendemos, y que tomemos decisiones sobre hacia dónde dirigir nuestros esfuerzos.

Para ayudar con esta misión, Sophos AI se ha embarcado en un proyecto para crear una serie de modelos estadísticos inspirados en la epidemiología para calcular la prevalencia de las infecciones de malware en total. Combinamos un proceso de recopilación de datos robusto que recoge datos de 100 millones de endpoints con una serie de métodos estadísticos bayesianos que nos permiten afrontar estas difíciles preguntas, a fin de generar una visión completa del rendimiento de nuestros modelos "sobre el terreno".

Por ejemplo, planteémonos esta pregunta: "¿cuánto malware está afectando realmente a nuestros clientes todas las semanas, y cuánto de este malware estamos detectando?".

Si ya supiéramos qué archivos son malware y cuáles son benignos en todos los casos, habríamos terminado. Por desgracia, tenemos dos problemas.

1. Realmente no conocemos la verdad fundamental tras ningún archivo: todos los productos para endpoints se perderán al menos una parte del malware, y el falso positivo ocasional (un archivo normal que se marca como malware) es inevitable.
2. La balanza entre los archivos benignos y los maliciosos se decanta indiscutiblemente hacia los benignos, por lo que es probable que no lo podamos averiguar con análisis manuales. Tendríamos que realizar un análisis en profundidad de miles de archivos que nuestro producto para endpoints hubiera etiquetado como benignos para poder encontrar un solo archivo malicioso.

Para abordar estos problemas, recurrimos a las estadísticas bayesianas. En términos sumamente simplificados, construimos un modelo "generativo" de datos: un programa matemático que puede tratar de adivinar parámetros ("¿Cuánto malware hay realmente?") y convertir esas conjeturas en simulaciones de cuántas detecciones de endpoints podríamos ver. Luego probamos varias conjeturas, vemos qué simulaciones coinciden con la realidad observada y trabajamos a la inversa para encontrar valores plausibles del parámetro que nos interesa.

Por ejemplo, imaginemos que tenemos 2000 detecciones de endpoints y una buena estimación de los índices de verdaderos y falsos positivos del modelo para una semana en particular. Podemos simular mundos con índices de malware del 0 %, el 2 %, el 5 % y así sucesivamente, y ver qué predice la simulación en términos de detecciones de endpoints; si vemos cerca de 2000 detecciones para algunos índices de malware, entonces ese es (quizás) un valor plausible.

Fig. 28. Proponer un índice de malware, probarlo, ver si la simulación coincide con la realidad observada, computar los índices que sí lo hagan y repetir. Fuente: SophosAI.

Se puede repetir este proceso millones de veces para crear una distribución de valores plausibles de índices de malware y, como utilizamos un enfoque bayesiano, las barras de error están "integradas" en la estimación. En nuestro ejemplo, el modelo piensa que el valor más probable para "¿Qué porcentaje de archivos son malware?" es algo más del 3 %, pero cualquier valor entre el 2,75 % y el 3,35 % aproximadamente es bastante plausible.

Y una vez que nos hacemos una buena idea de esta cifra (cuántos archivos de cada cien son probablemente malware en todos los endpoints del cliente), resulta bastante sencillo calcular las omisiones en la detección y los falsos positivos. Si miramos los datos de nuestro sistema de detección de malware basado en Deep Learning durante una semana en mayo (sin ninguna opción basada en firmas, comportamientos o heurística activada), podemos desarrollar una matriz completa de verdaderos y falsos positivos y negativos, y finalizar nuestra visión del rendimiento del modelo. En este caso, vemos que, si bien tenemos algunos falsos negativos, el número de falsos positivos es bajo y tiende a cero, y el número de verdaderos positivos es alto y tiende a 161 000 (el número total de resultados positivos en la muestra). Al observar la escala, podemos ver que las tres cantidades quedan eclipsadas por el número de verdaderos negativos, es decir, los archivos benignos que nuestro Machine Learning ha etiquetado como benignos.

Nuestra herramienta inspirada en la epidemiología nos ha permitido estimar, si no encontrar, las agujas en nuestro pajar de archivos PE.

Fig. 29. Análisis de verdaderos y falsos positivos del modelo de Machine Learning a principios de mayo de 2020. Fuente: SophosAI.

Ventas en España:
Tel.: (+34) 91 375 67 56
Email: comercialES@sophos.com

Ventas en América Latina:
Email: Latamsales@sophos.com

20-11-01 ES (DD)

SOPHOS