McAfee
Together is power.

Informe de McAfee Labs sobre amenazas

Junio de 2018

CAMPAÑAS PRINCIPALES

Gold Dragon amplía el alcance de los ataques a los Juegos Olímpicos

Lazarus resucita de nuevo y ataca a usuarios de criptomonedas

Los implantes de robo de datos avanzados GhostSecret y Bankshot tienen alcance y consecuencias globales

El malware de minería de monedas total contabilizado por McAfee Labs ascendió un 629 % en el primer trimestre, hasta los más de 2,9 millones de muestras.

En la investigación y redacción de este informe han participado:

- Christiaan Beek
- Taylor Dunton
- Steve Grobman
- Mary Karlton
- Niamh Minihane
- Chris Palm
- Eric Peterson
- Raj Samani
- Craig Schmugar
- ReseAnne Sims
- Dan Sommer
- Bing Sun

Introducción

Bienvenido al Informe de *McAfee® Labs sobre amenazas, junio de 2018.* En este número, destacamos el importante estudio de investigación y estadísticas de tendencias de amenazas recabadas por los equipos de McAfee Advanced Threat Research y McAfee Labs durante el primer trimestre de 2018.

Durante este primer trimestre salieron a la luz nuevas revelaciones sobre complejas campañas de amenazas financiadas por países dirigidas a usuarios y sistemas de empresas de todo el mundo. Estas campañas tenían muchas motivaciones, desde la ciberdelincuencia con fines económicos y la subversión política, a la vigilancia y el espionaje. Desde nuestro análisis del criptojacking del número anterior, hemos observado un continuo crecimiento de esta actividad delictiva durante este trimestre. El objetivo de los responsables es rentabilizar su actividad criminal con el mínimo esfuerzo, empleando el menor número de intermediarios posible y ejecutando sus delitos con la mayor rapidez y con el mínimo riesgo de ser descubiertos. También hemos observado que los ciberdelincuentes están demostrando un notable nivel de agilidad e innovación técnica. Muchas de las tramas de ataque que surgieron hacia finales de 2017 han sido mejoradas de forma creativa y compleja, para evitar la detección y la mitigación.

Campañas principales

Gold Dragon y los Juegos Olímpicos de Invierno

A principios del primer trimestre, McAfee Advanced Threat Research informó de un ataque dirigido contra empresas que participaban en los Juegos Olímpicos de Invierno de Pyeongchang en Corea del Sur. El ataque fue ejecutado a través de un archivo adjunto de Microsoft Word malicioso que contenía un script con un implante de PowerShell. El script estaba incrustado en un archivo de imagen y se ejecutó desde un servidor remoto.

Nuestro equipo de analistas también ha observado varios implantes secundarios que ampliaban la persistencia del implante sin archivo inicial para permitir el acceso y la filtración de datos continua. Entre los identificados había un implante en coreano, apodado Gold Dragon, que servía como carga útil secundaria y aparecía el primer día del ataque. Gold Dragon tenía dos funciones principales: actuaba de herramienta de reconocimiento y descargaba y ejecutaba cargas útiles posteriores en la cadena de ataque. Además, cifraba los datos incautados por otros implantes y los enviaba al servidor de control. Gold Dragon es una instancia de malware sin archivos particularmente escurridiza porque está diseñada para ser evasiva, ya que comprueba los procesos relacionados con soluciones antimalware.

Lazarus y las campañas de criptomonedas

El grupo de ciberdelincuentes Lazarus ha vuelto a aparecer, y lo ha hecho demostrando una alto grado de sofisticación con una nueva campaña de phishing de robo de bitcoins—HaoBao—, dirigida contra organizaciones financieras y usuarios de Bitcoin en todo el mundo. Cuando los destinatarios abren los adjuntos maliciosos, un implante analiza la actividad de Bitcoin y establece un implante para la recopilación de datos persistente. Estas técnicas guardan un gran parecido a otros ataques que se cree que han sido perpetrados por Lazarus.

A principios de 2017, Lazarus fue responsable de una campaña de correo electrónico de phishing en coreano y en inglés, en la que los ciberdelincuentes se hacían pasar por responsables de contratación. Los principales objetivos fueron contratistas de defensa e instituciones financieras, y el objeto de las campañas era obtener información militar sensible o robar dinero. Un componente clave de la campaña, que parece que terminó en octubre de 2017, fue el uso de adjuntos maliciosos.

Las investigaciones de varios ataques que distribuían documentos a través de Dropbox revelaron el uso de dos implantes: el primero para la recopilación de datos y el segundo para establecer la persistencia. Normalmente, estos archivos estaban incrustados en versiones más antiguas de documentos Word que se iniciaban a través de una macro de Visual Basic. Una vez realizadas estas acciones, el malware enviaba los datos a un servidor de control.

Estas técnicas, tácticas y procedimientos guardan un enorme parecido con las campañas de 2017 contra contratistas de defensa de EE. UU., el sector energético estadounidense, organizaciones financieras y operadores de cambio de criptomonedas. No se pierda el desenlace de los ataques contra criptomonedas HaoBao.

GhostSecret/Bankshot

McAfee Advanced Threat Research descubrió otra campaña mundial dirigida contra una amplia variedad de sectores: la sanidad, los servicios financieros, el entretenimiento y las telecomunicaciones. Parece que la Operación GhostSecret, activa actualmente, está vinculada al grupo de ciberdelincuencia internacional conocido como Hidden Cobra. Se trata de una campaña extremadamente compleja, que emplea una serie de implantes para apropiarse de datos de los sistemas infectados, y que se caracteriza además por su capacidad para eludir la detección y desviar la atención de los investigadores forenses. Nuestro análisis también descubrió una infraestructura con servidores ubicados en India que forman parte de una red encubierta que recopila datos y que parece utilizarse para lanzar otros ataques.

En principio, esta campaña iba dirigida contra instituciones financieras turcas y se empleó el implante Bankshot, del que informó por primera vez el Departamento de Seguridad Nacional estadounidense en diciembre de 2017. Como la mayoría de amenazas de este tipo, se utilizaron mensajes de correo electrónico de phishing y adjuntos de Word maliciosos para lanzar el ataque. Esta nueva variante de Bankshot utiliza un exploit de Adobe Flash incrustado para permitir la ejecución de un implante.

La última variante de GhostSecret no solo utiliza las técnicas del implante Bankshot, sino que incorpora elementos del malware Destover, que se utilizó en el ataque contra Sony Pictures de 2014, y el implante Proxysvc, sin documentar previamente, que ha actuado sin ser detectado desde mediados de 2017.

La combinación de estos implantes de recopilación de datos indica que agresores como Hidden Cobra siguen perfeccionando sus herramientas y aumentando sus funciones. Es muy probable que GhostSecret siga atacando a empresas de todo el mundo.

Tendencias principales: los ciberdelincuentes se esfuerzan por mejorar

En el primer trimestre de 2018, McAfee Labs registró una media de cinco nuevas muestras de malware por segundo, frente a las ocho muestras nuevas por segundo del 4.º trimestre. A pesar del descenso del 31 % de un trimestre a otro, durante el primer trimestre se observaron importantes avances técnicos entre los ciberdelincuentes que buscan mejorar las últimas tecnologías y tácticas que funcionan con éxito, con el fin de vencer a las defensas de sus objetivos.

De PowerShell a LNK: en 2017 asistimos a un aumento en la explotación de tecnologías inofensivas para fines maliciosos, como PowerShell. En el primer trimestre de 2018, hemos visto a los ciberdelincuentes alejarse de los exploits de PowerShell, que descendieron un 77 %, en favor de las funciones de LNK. El nuevo malware basado en LNK aumentó un 59 % durante el primer trimestre.

ESTADÍSTICAS

McAfee Global Threat Intelligence

Cada trimestre, el panel en la nube de McAfee® Global Threat Intelligence (McAfee GTI) nos permite ver y analizar los patrones de ataque del mundo real, lo que posteriormente nos facilita la mejora de la protección de los clientes. Dicha información nos ayuda a conocer con precisión los volúmenes de ataques que sufren nuestros clientes. Cada día McAfee GTI ha analizado una media de 2 400 000 URL y 700 000 archivos.

Durante el primer trimestre, estos fueron los volúmenes registrados:

- Una media de 51 000 millones de consultas recibidas al día.
- Las protecciones contra archivos maliciosos aumentaron hasta los 79 millones al día en el primer trimestre, desde los 45 millones del 4.º trimestre.
- Las protecciones contra URL de riesgo alto aumentaron hasta los 49 millones al día en el primer trimestre, desde los 37 millones del 4.º trimestre.
- Las protecciones contra direcciones IP de riesgo alto aumentaron hasta los 35 millones al día en el primer trimestre, desde los 26 millones del 4.º trimestre.

De Locky a Gandcrab: la actividad del ransomware Gandcrab también demostró agilidad técnica. Aunque el crecimiento general de nuevo ransomware se ralentizó un 32 % en el primer trimestre, Gandcrab infectó 50 000 sistemas durante las tres primeras semanas del trimestre, sustituyendo a las variantes del ransomware Locky como líder del trimestre en esta categoría. Gandcrab utiliza nuevos métodos delictivos, como realizar el pago de rescates a través de la criptomoneda Dash, en lugar de mediante bitcoins.

Criptojacking —infectar y recaudar: las criptomonedas también siguieron dibujando el panorama de ciberamenazas durante el primer trimestre, ya que los ciberdelincuentes ampliaron su actividad al criptojacking, la infección de los sistemas de los usuarios con el fin de secuestrarlos y utilizarlos para minería de criptomonedas.

El malware minero de monedas aumentó un impresionante 629 % hasta los más de 2,9 millones de muestras conocidas en el primer trimestre, desde las casi 400 000 muestras del 4.º trimestre. Esto sugiere que los ciberdelincuentes se están preparando ante la perspectiva de convertir en dinero las infecciones de los sistemas de los usuarios, sin pedir a las víctimas que realicen pagos, como en el caso de conocidos ataques de ransomware. Comparado con otras actividades de ciberdelincuencia bien consolidadas, como el robo de datos y el ransomware, el criptjacking es más simple, más directo y menos arriesgado. Lo único que tienen que hacer los ciberdelincuentes es infectar millones de sistemas y empezar a rentabilizar el ataque mediante la minería de criptomonedas en los sistemas de la víctimas. Sin intermediarios, sin tramas fraudulentas, sin víctimas a las que pedir un rescate y que podrían hacer una copia de seguridad de sus sistemas de antemano y negarse a pagar.

Para mantenerse informado sobre nuestras investigaciones, consulte nuestro canal de redes sociales —Twitter @McAfee_Labs— en el que ofrecemos análisis de nuevas campañas, así como una descripción de nuevas herramientas que puede utilizar para mejorar la protección de su entorno.

—Steven Grobman, Director de tecnología (CTO)

—Raj Samani, Científico jefe y McAfee Fellow, Advanced Threat Research

Twitter @Raj_Samani

Seguir

Compartir

Índice

Gold Dragon amplía el alcance de los ataques a los Juegos Olímpicos

El implante Gold Dragon, descubierto por primera vez por analistas de McAfee Advanced Threat Research como parte de un ataque de malware sin archivos contra empresas que participaban en los Juegos Olímpicos de Invierno de Pyeongchang, es indicativo de una nueva hornada de herramientas y técnicas que ganan terrero entre los ciberdelincuentes. Muchas campañas de malware sin archivos aprovechan PowerShell para lanzar un ataque en memoria destinado a crear una puerta trasera en un sistema. Gold Dragon destaca porque se personalizó para el ataque contra los Juegos Olímpicos,

persistía en los sistemas infectados y ha aparecido en ataques posteriores, concretamente en servidores en Chile poco después de una semana del incidente en los Juegos Olímpicos. Gold Dragon es una instancia de malware sin archivos particularmente escurridiza porque está diseñada para ser evasiva, ya que comprueba los procesos relacionados con soluciones antimalware.

Como en la mayoría de los ataques, el punto de entrada es el usuario. Se enviaron mensajes de correo electrónico con técnicas de ingeniería social, que incluían un adjunto de Word malicioso que contenía un script de implante de PowerShell oculto. Cuando los destinatarios hacían clic en el adjunto, se les pedía que activaran un proceso que les permitía ver el contenido en su versión de Word. El malware lanzaba una macro de Visual Basic que ejecutaba el script de PowerShell desde un servidor remoto. El script descargaba entonces un archivo de imagen y otros scripts de PowerShell incrustados en los píxeles de la imagen. Otras técnicas añaden otra capa de ocultación, lo que convierte a Gold Dragon en extremadamente difícil de detectar, en particular una vez que se abre camino hasta una línea de comandos y establece conexión con el servidor de control del agresor, recopilando datos a nivel de sistema que describen a las máquinas atacadas.

La versión en coreano de Gold Dragon es un implante secundario que ampliaba la persistencia del implante sin archivo inicial con el fin de permitir el acceso y la filtración de datos de forma continua. Existen muchas similitudes con implantes como Ghost419 y Brave Prince, que hemos observado desde mediados de 2017.

Gold Dragon desempeñaba varias funciones en el ataque a los Juegos Olímpicos:

- Se cree que fue una carga útil de segunda fase en el ataque a los Juegos Olímpicos.
- Actuó como herramienta de reconocimiento y como downloader de otras cargas útiles.
- Describía el dispositivo atacado, recogiendo información como los directorios del equipo de sobremesa, los archivos a los que se había accedido recientemente y la carpeta de archivos de programa; la clave del registro e información para la clave de ejecución del usuario, etc.
- Cifraba estos datos y los enviaba al servidor remoto.
- Para evitar la detección, buscaba y terminaba procesos relacionados con soluciones antimalware o antivirus.
- También era capaz de descargar y ejecutar otros componentes del ataque desde el servidor remoto.

Gold Dragon es simplemente uno de los muchos implantes utilizados en ataques de malware sin archivos que presenta ventajas inconfundibles, como la capacidad de establecer la persistencia y filtrar datos de manera continua.

Seguir

Compartir

Lazarus resucita de nuevo y ataca a usuarios de criptomonedas

Inactivo durante un corto período durante la última parte de 2017, el grupo internacional de ciberdelincuentes conocido como Lazarus ha resurgido en el primer trimestre de 2018. Esta vez con una compleja trama de criptomonedas conocida como HaoBao. En el número anterior del Informe de McAfee Labs sobre amenazas, comentamos cómo, animados por el aumento del valor de los bitcoins, los ciberdelincuentes han ampliado sus actividades más allá de la demanda de pago del ransomware con criptomoneda para incluir el criptojacking o la minería de criptomonedas.

Antes de la campaña de HaoBao, los investigadores de McAfee descubrieron una campaña de phishing selectivo asociada a Lazarus que iba dirigida contra empleados que trabajaban para contratistas de defensa o en instituciones financieras. El objetivo de la campaña era apropiarse de datos confidenciales o robar fondos. Esta campaña parecía haber llegado a su fin en octubre de 2017.

En el primer trimestre de 2018, los analistas de McAfee Advanced Threat Research descubrieron una nueva campaña, que supuestamente ofrecía un puesto de ejecutivo de desarrollo empresarial en un importante banco multinacional ubicado en Hong Kong.

El mensaje de correo electrónico incitaba a los destinatarios a descargarse de Dropbox documentos Word infectados. Al igual que ocurría en el ataque Gold Dragon descrito en la sección anterior, los documentos estaban incrustados en versiones antiguas de documentos Word lanzados a través

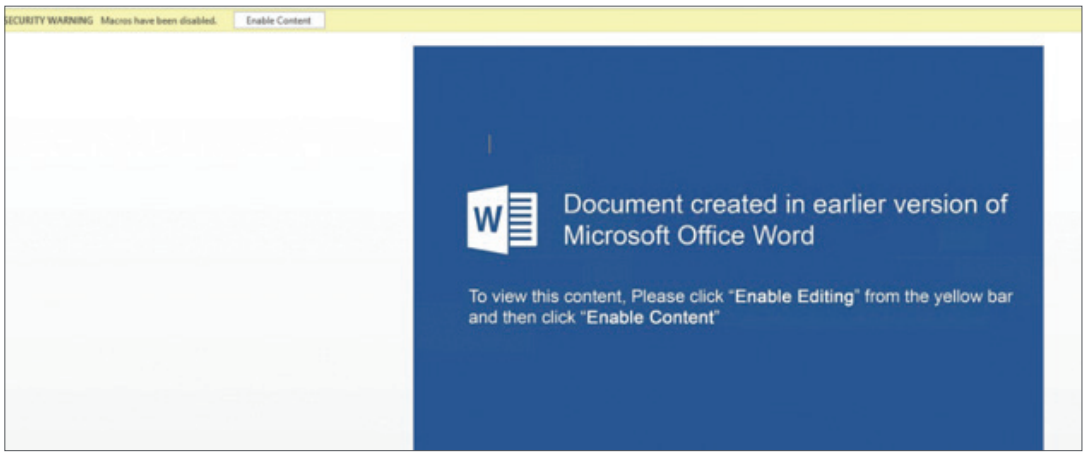


Figura 1. Ejemplo de señuelo de ataque: un documento de Microsoft Word que parece ser de una versión antigua.

Seguir
Compartir

de una macro de Visual Basic, que presumiblemente permitía al usuario ver el documento en la versión actual de Word. Una vez que el usuario había realizado estas acciones, el malware filtraba datos del sistema y los enviaba a un servidor de control.

Este tipo de implante no se había detectado antes. Esta campaña utilizaba un implante de recopilación de datos de uso único que dependía de la descarga de un implante de segunda fase para conseguir la persistencia. Los implantes contenían la palabra codificada *haobao*, que provocaba la ejecución del mecanismo de filtración de datos mediante

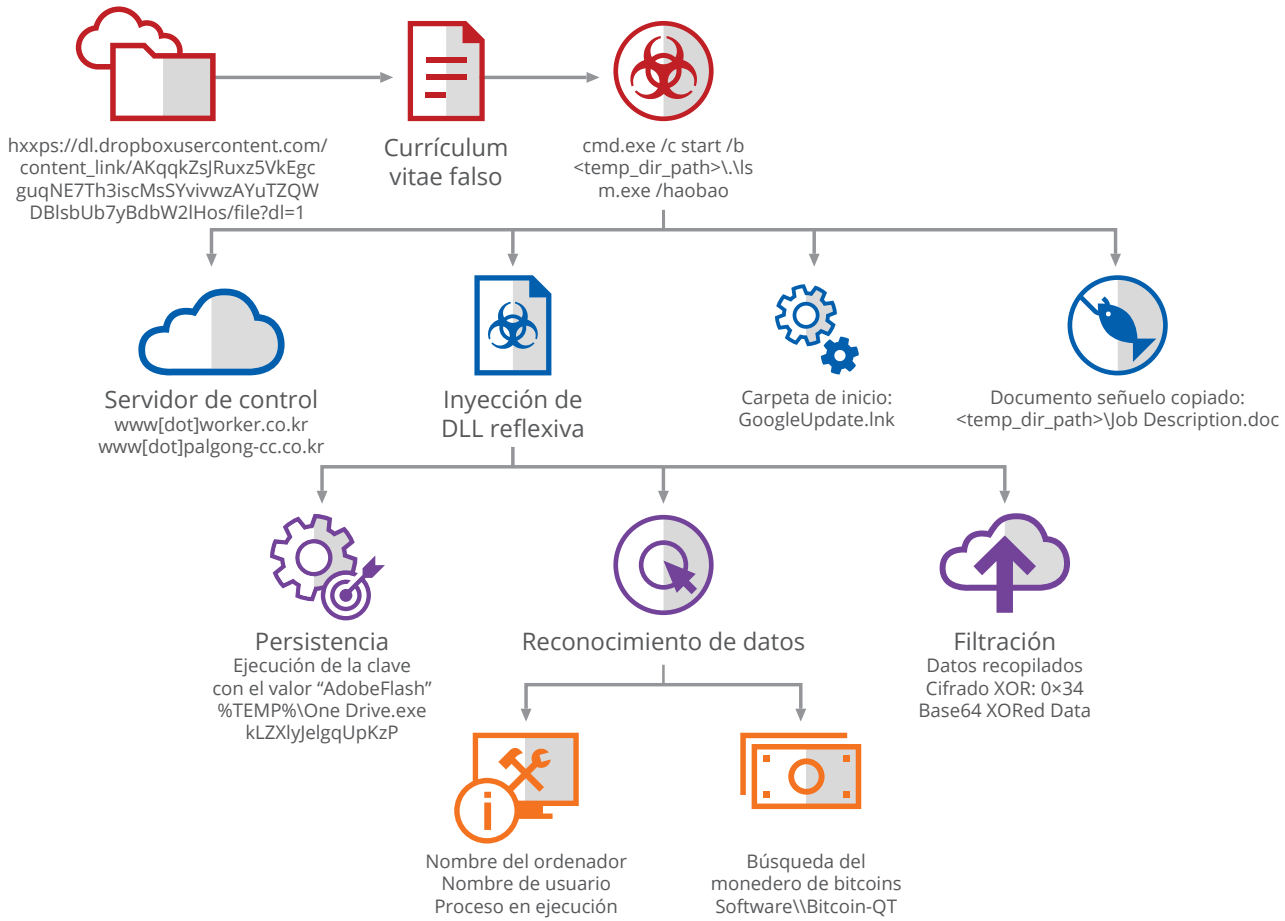


Figura 2. Trayectoria del implante HaoBao.

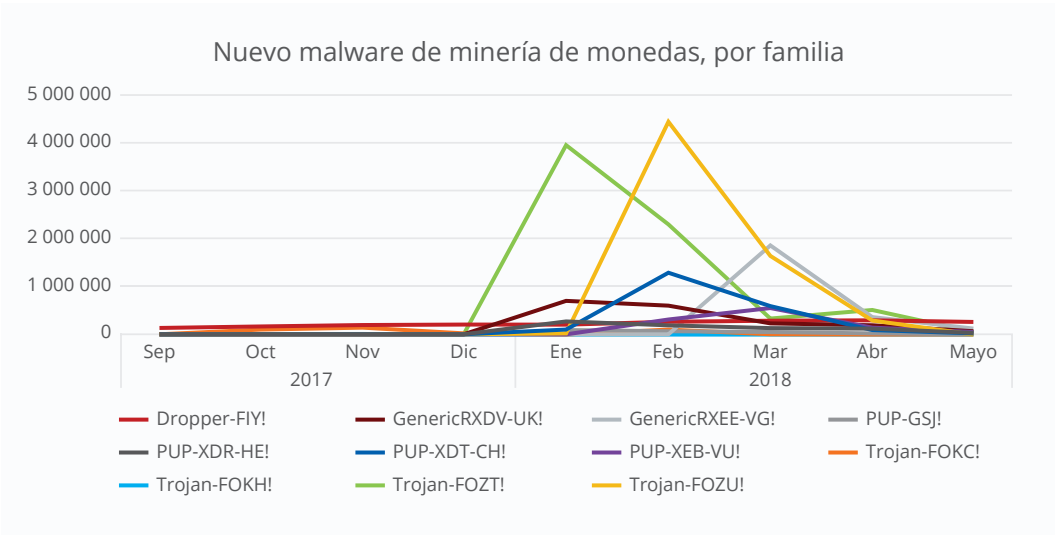
la macro de Visual Basic. El propósito de los datos recopilados era identificar objetivos para futuros ataques, concretamente los que ejecutaban software relacionado con Bitcoin a través de determinados análisis del sistema.

Los analistas de McAfee establecieron una conexión con Lazarus basándose en técnicas que son similares a las de campañas de 2017 contra el Departamento de Defensa y el Departamento de Energía de EE. UU., instituciones financieras y operadores de cambio de criptomonedas. Llegaron a esta conclusión con un alto grado de confianza a través de estas observaciones:

- Los ciberdelincuentes contactan con una dirección IP o un dominio utilizado para albergar un documento malicioso de una campaña de Lazarus anterior en 2017.
- El mismo autor que aparece en estos documentos maliciosos recientes también aparecía en las campañas de Lazarus de 2017.
- HaoBao utiliza la misma estructura de documentos maliciosos y anuncios de contratación laboral que campañas de Lazarus anteriores.
- Las técnicas están en sintonía con el interés del grupo Lazarus en el robo de criptomonedas.

Prevemos que las campañas de minería de criptomonedas tomen más fuerza o tal vez incluso que superen al ransomware. Para los ciberdelincuentes, las campañas como HaoBao son muy ventajosas, ya que son más rentables y más difíciles de detectar sin que aparentemente causen daño alguno.

Para conocer en más detalle el aumento de prevalencia de CoinMiner, una variante de malware que se hace con el control del ordenador de una víctima para la minería de nuevas monedas mediante la infección de ejecutables de usuarios, inyectando código JavaScript de Coinhive en archivos HTML, y bloqueando los productos de



seguridad para detener las actualizaciones de firmas, lea la publicación de McAfee Labs "Parasitic Coin Mining Creates Wealth, Destroys Systems" (La minería de monedas parásita genera riqueza y destruye sistemas).

Los implantes de robo de datos avanzados GhostSecret y Bankshot tienen alcance y consecuencias globales

El grupo de ciberdelincuencia internacional patrocinado por un estado, Hidden Cobra, ha lanzado recientemente campañas de reconocimiento a nivel mundial. Parece que ningún sector se ha librado de Operación GhostSecret. Hidden Cobra ha dirigido sus ataques a organizaciones de infraestructuras críticas, instituciones financieras, el sector sanitario, las telecomunicaciones y la industria del entretenimiento. Los nuevos implantes aprovechados en esta campaña guardan algún parecido con los empleados en otros ataques, como Bankshot y Proxysvc.

El conclusión principal es que los ciberdelincuentes siguen mejorando sus herramientas, aumentando la complejidad y la funcionalidad. Además de descubrir estas funciones, nuestra investigación reveló una infraestructura conectada a estas operaciones con servidores en India. El principal objetivo de Operación GhostSecret parece ser la recopilación de datos encubierta, en preparación para ataques futuros a gran escala.

La primera actividad detectable iba dirigida contra instituciones financieras y de comercio turcas. En este campaña, asistimos al retorno del implante Bankshot, que apareció por primera vez en 2017. El objetivo parece ser la recopilación de datos de instituciones financieras para posibles golpes futuros. Bankshot aprovecha una vulnerabilidad de tipo zero-day sin corregir en Adobe Flash. Los implantes se distribuyen desde un dominio que parece similar a la plataforma legítima de préstamo de criptomonedas Falcon Coin.

Iniciada mediante un mensaje de correo electrónico de phishing selectivo que utilizaba un documento Word, esta campaña introduce el implante Bankshot incrustado en un archivo Flash que se ejecuta cuando el destinatario abre el documento. Esta versión del implante Bankshot otorga a los agresores acceso remoto completo a los sistemas y les permite borrar archivos y contenido para eliminar las pistas de actividad destructiva o maliciosa.

```
                push    0
                push    edx
                push    eax
                mov     eax, zero_file_buffer
                push    eax
                push    ebx
                call    WriteFile

                push    edx
                push    ebx
                call    MoveFileW
                test    eax, eax
                jz      short move_failed_loc_40A318

move_failed_loc_40A318:                 ; CODE XREF: secure_delete_file_
                push    ebx
                call    DeleteFileW
```

Figura 3. Técnica de borrado de archivos utilizada en Operation GhostSecret.

Seguir

Compartir

Las funciones de reconocimiento van desde la generación de una lista de archivos en un directorio que se reenvía al servidor de control hasta la recopilación de nombres de dominio y cuentas para todos los procesos en ejecución. Además, Bankshot puede crear un proceso mediante la suplantación de un usuario conectado, sobrescribir archivos con ceros y marcarlos para su eliminación al reiniciar, o terminar completamente los procesos.

En Operation GhostSecret, Hidden Cobra ha llevado su nivel de actividad más allá del sector financiero con una nueva clase de implante que extrae algunas estructuras de codificación y funciones de implantes anteriores. El implante, descubierto recientemente y más avanzado, puede aceptar comandos extensos del servidor de control, lo que lo convierte en una plataforma robusta de reconocimiento y filtración de datos. Además de borrar y eliminar archivos, el implante puede ejecutar otros implantes, extraer datos de los archivos, etc.

Nuestras observaciones y análisis corroboran nuestro profundo convencimiento de que a medida que aumenta la sofisticación de las capacidades de los creadores de malware, campañas como Operation GhostSecret abrirán la puerta a ataques de mayor envergadura y más maliciosos contra varios sectores en un futuro cercano.

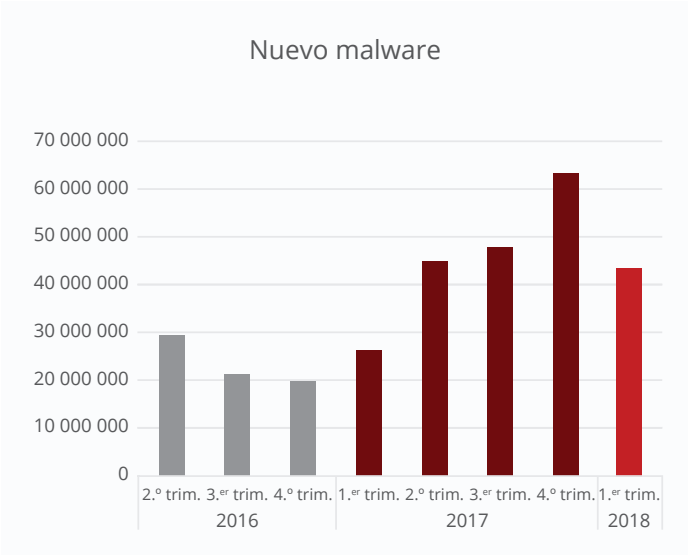
Trojan-Bankshot2: MITRE - Adversarial Tactics, Techniques, and Common Knowledge (Tácticas, técnicas y conocimiento del adversario)

- **Filtración a través del canal del servidor de control:** los datos se filtran a través del canal del servidor de control mediante un protocolo personalizado.
- **Puerto utilizado habitualmente:** los agresores utilizaron puertos comunes, como el 442, para las comunicaciones con el servidor de control.
- **Ejecución del servicio:** el implante se registró como servicio en la máquina de la víctima.
- **Recopilación automatizada:** el implante obtiene automáticamente datos de la víctima y los envía al servidor de control.
- **Datos del sistema local:** el malware descubre el sistema local y recopila datos.
- **Descubrimiento de procesos:** el implante puede identificar los procesos que se ejecutan en el sistema.
- **Descubrimiento de la hora del sistema:** como parte del método de reconocimiento de datos, se envía la hora del sistema al servidor de control.
- **Eliminación de archivos:** el malware puede eliminar los archivos indicados por el agresor.

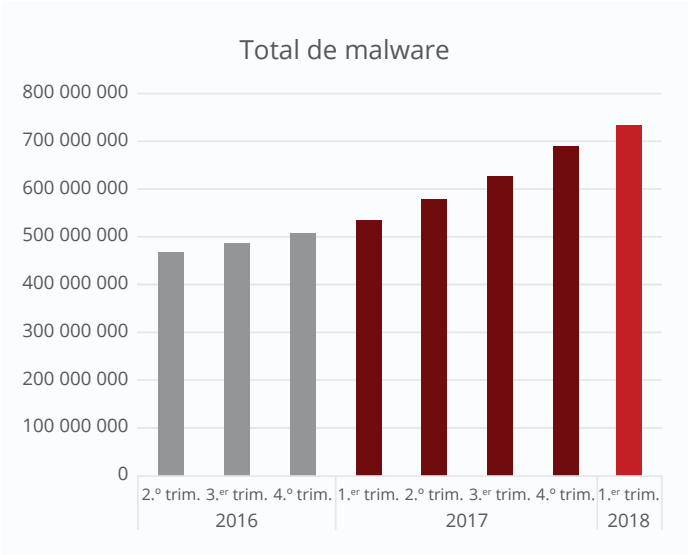
Figura 4. Indicadores de peligro del implante Bankshot.

Estadísticas sobre amenazas

Malware

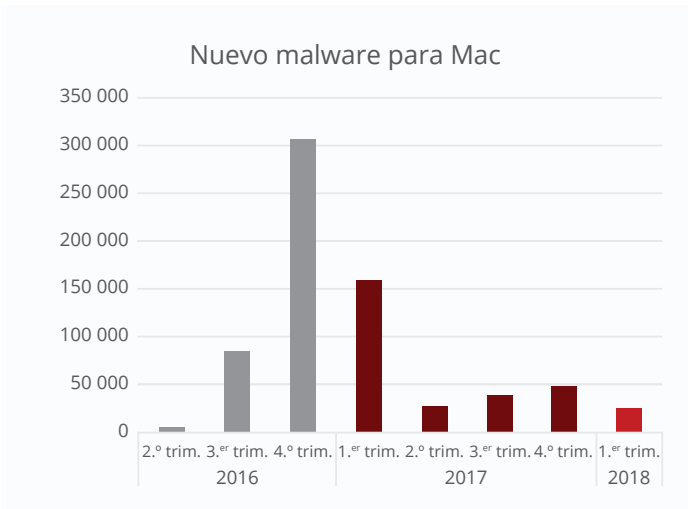


Fuente: McAfee Labs, 2018.

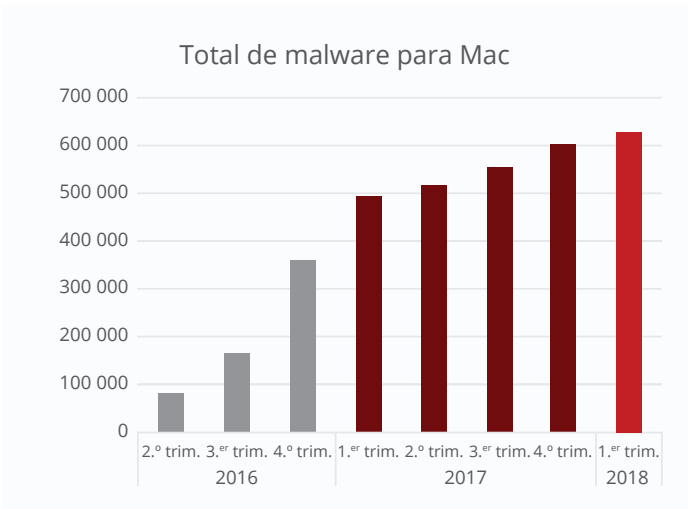


Fuente: McAfee Labs, 2018.

Los datos del malware proceden de la base de datos de muestras de McAfee, McAfee Sample Database, que incluye archivos maliciosos obtenidos de trampas para spam (*spam traps*) de McAfee, rastreadores de la Web (*crawlers*) o envíos de clientes, así como de otras fuentes del sector.



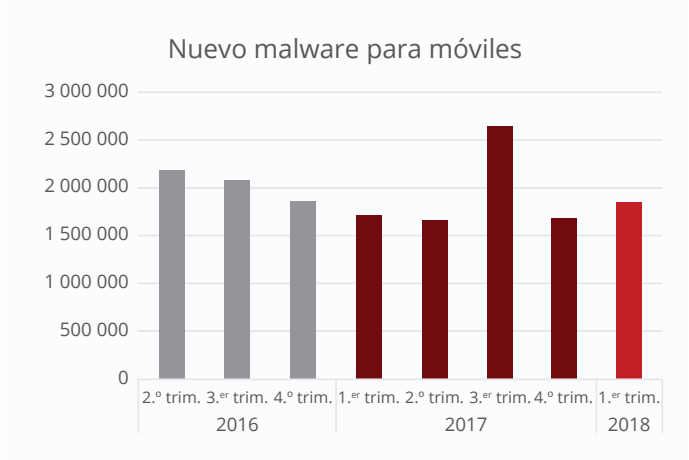
Fuente: McAfee Labs, 2018.



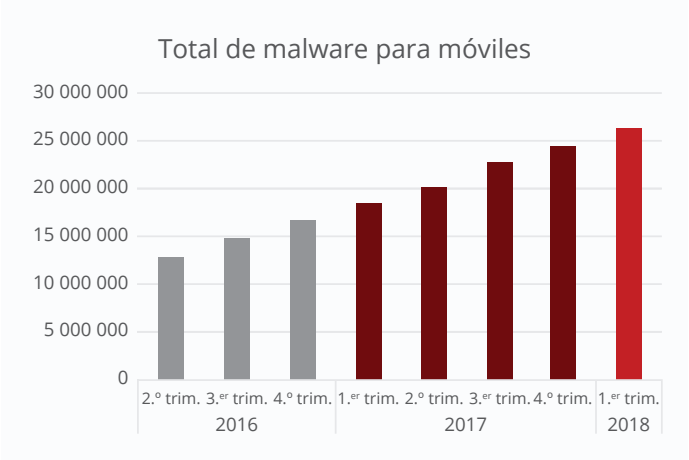
Fuente: McAfee Labs, 2018.

Seguir

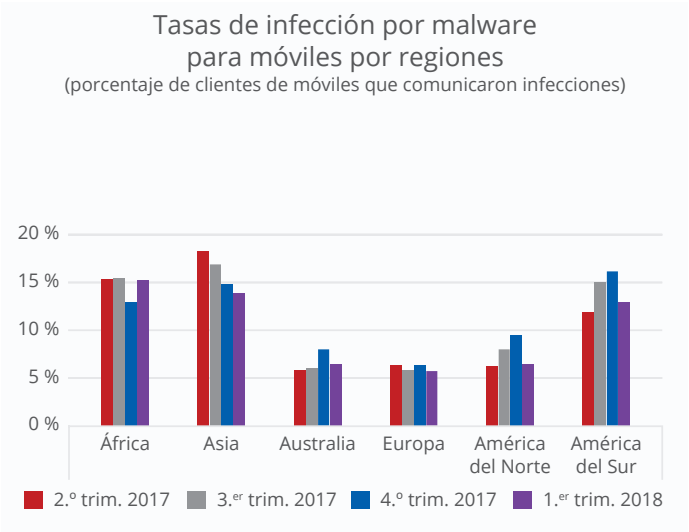
Compartir



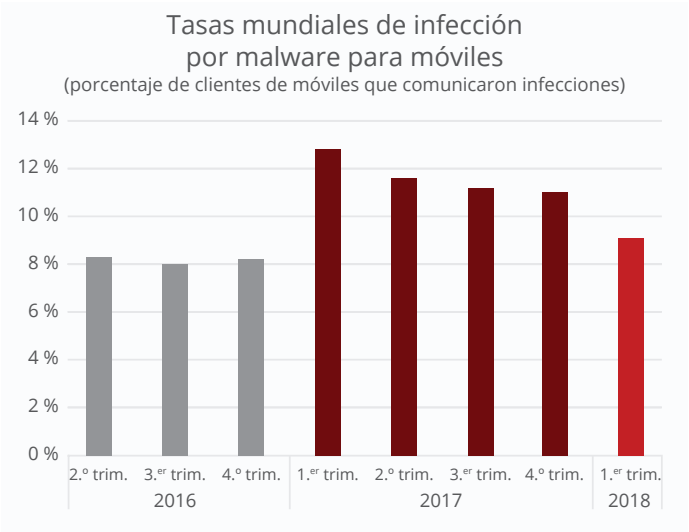
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



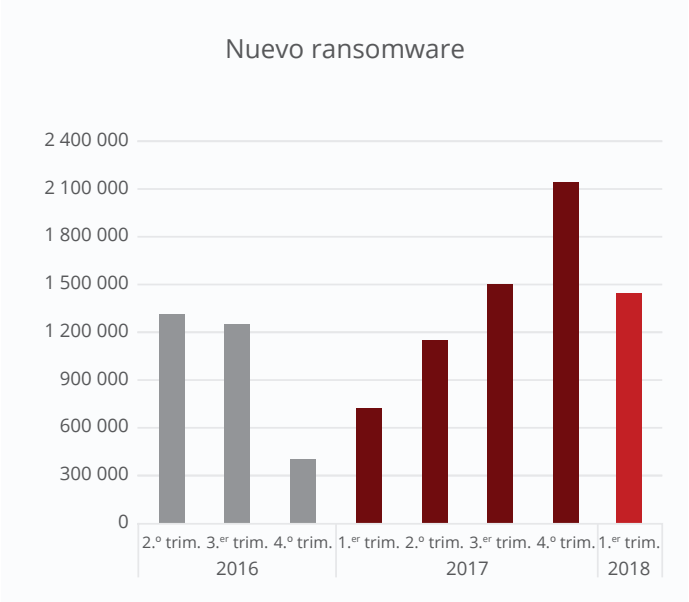
Fuente: McAfee Labs, 2018.



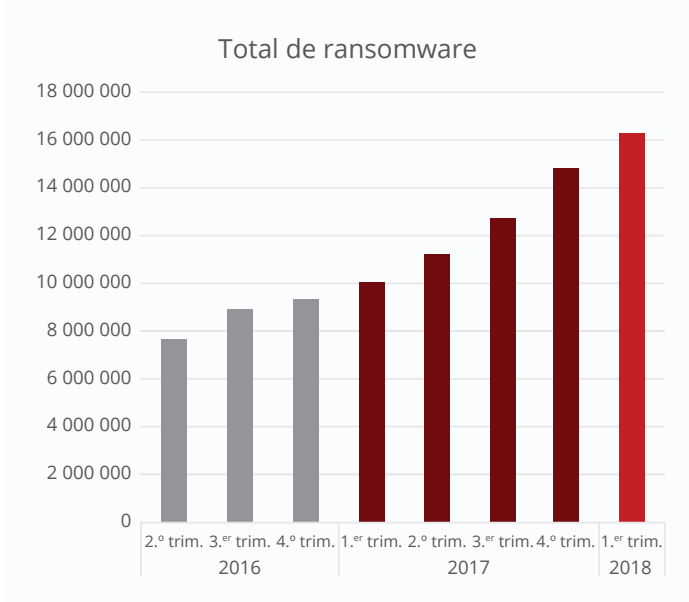
Fuente: McAfee Labs, 2018.

Seguir

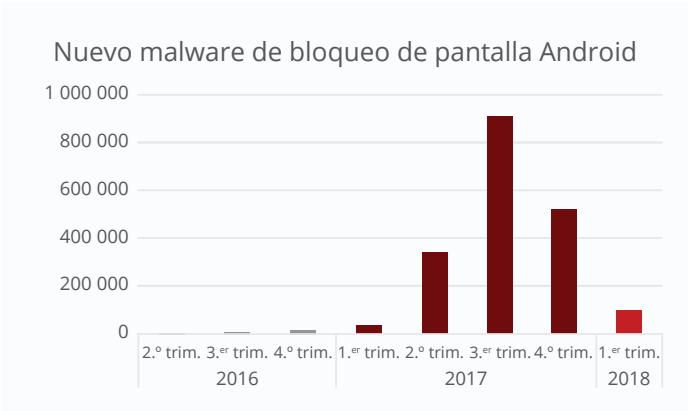
Compartir



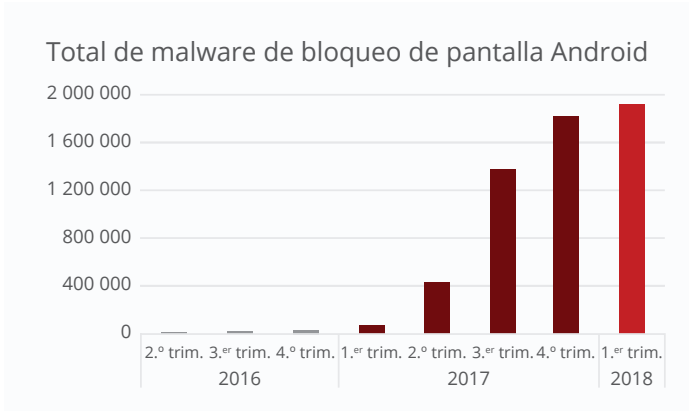
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.

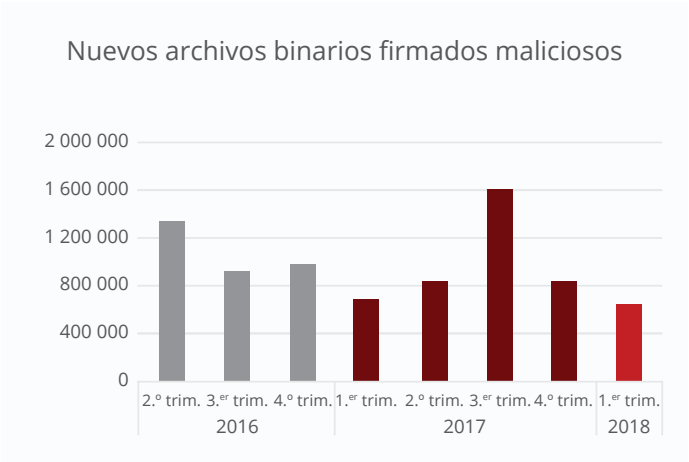


Fuente: McAfee Labs, 2018.

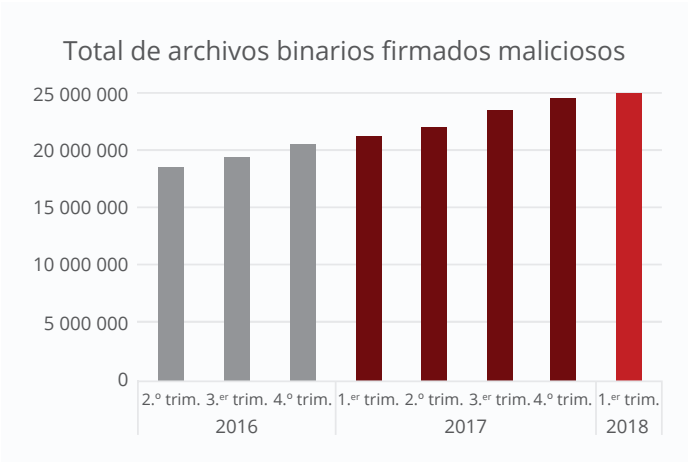
El descenso del 81 % de nuevo malware de bloqueo de pantalla Android contribuyó de manera importante a la caída de nuevo ransomware en el primer trimestre.

Seguir

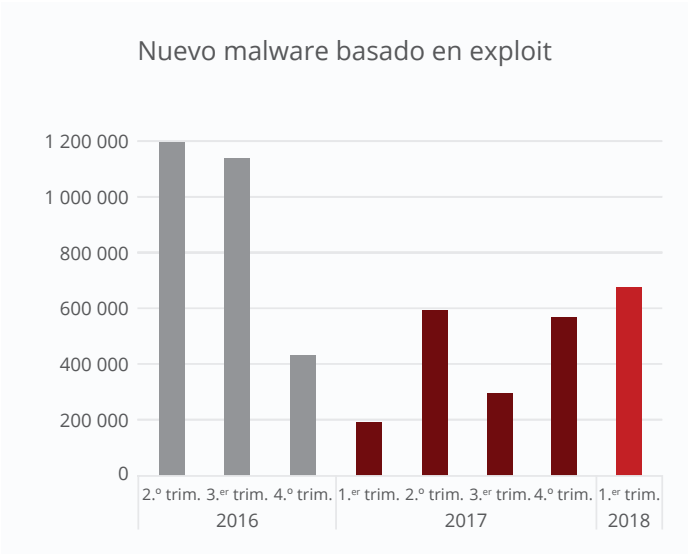
Compartir



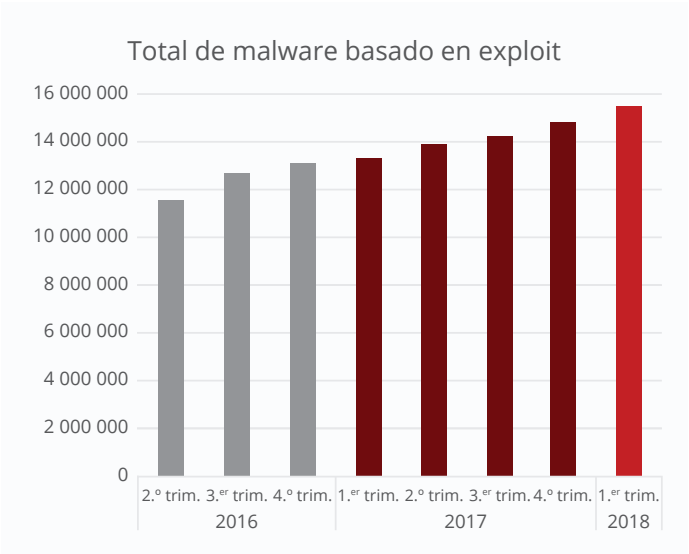
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



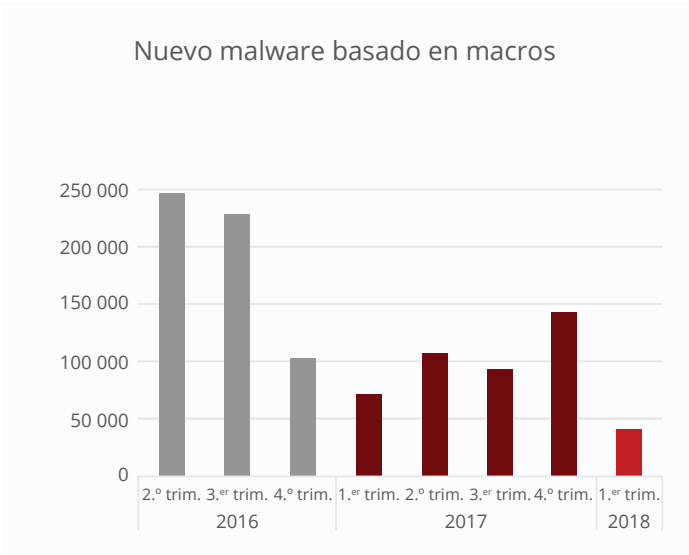
Fuente: McAfee Labs, 2018.

Las autoridades de certificación ofrecen certificados digitales que proporcionan información una vez que un binario (aplicación) es firmado o validado por el proveedor del contenido. Cuando los ciberdelincuentes obtienen certificados para binarios firmados maliciosos, se facilita enormemente la ejecución de los ataques.

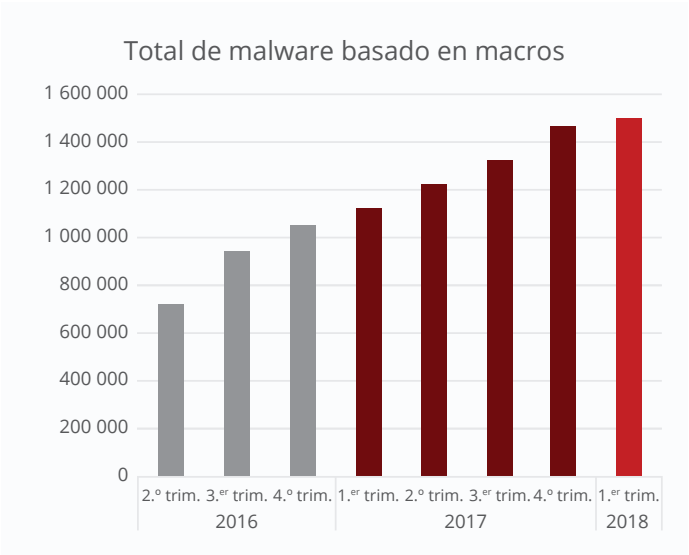
Los exploits aprovechan los errores y vulnerabilidades del software y el hardware. Los ataques de tipo zero-day son ejemplos de exploits que consiguen sus objetivos. Se incluye un ejemplo en el artículo de McAfee Labs "Analyzing Microsoft Office Zero-Day Exploit CVE-2017-11826: Memory Corruption Vulnerability" (Análisis del exploit de tipo zero-day de Microsoft Office CVE-2017-11826: vulnerabilidad de corrupción de memoria).

Seguir

Compartir

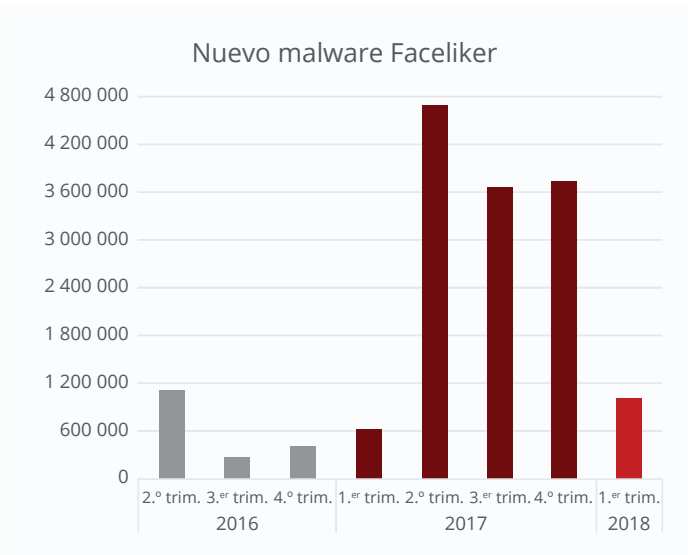


Fuente: McAfee Labs, 2018.

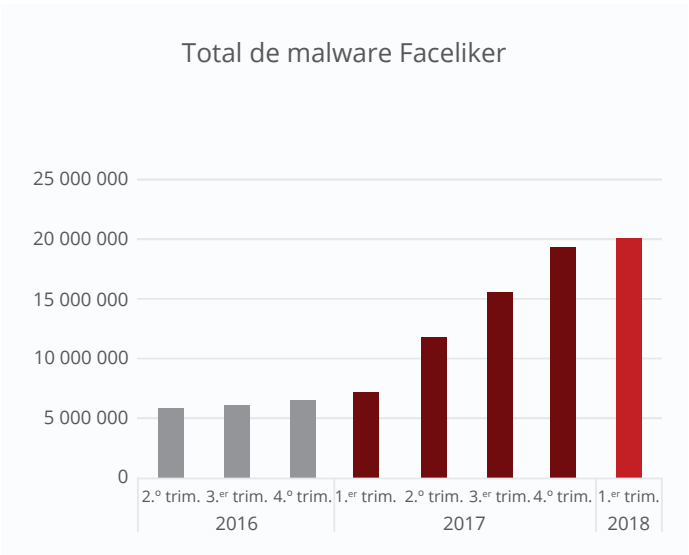


Fuente: McAfee Labs, 2018.

El malware basado en macros suele llegar como un documento Word o Excel en un mensaje de spam o un archivo adjunto comprimido. Se emplean nombres de archivo falsos, pero atractivos, con el fin de incitar a la víctima a abrir los documentos, lo que desencadena la infección si están activas las macros.



Fuente: McAfee Labs, 2018.

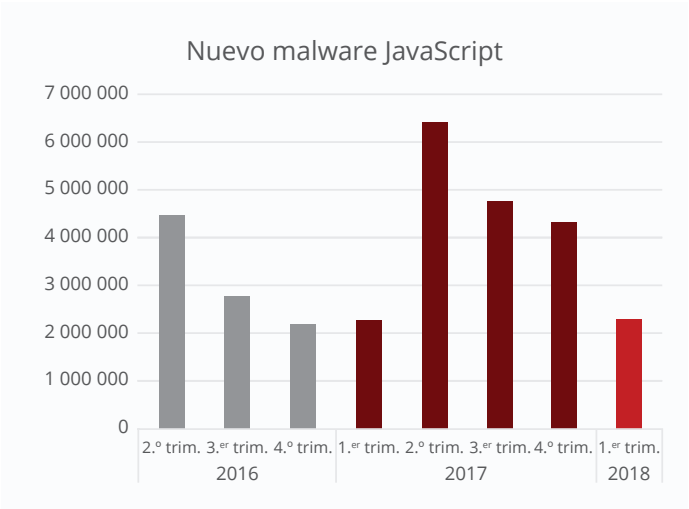


Fuente: McAfee Labs, 2018.

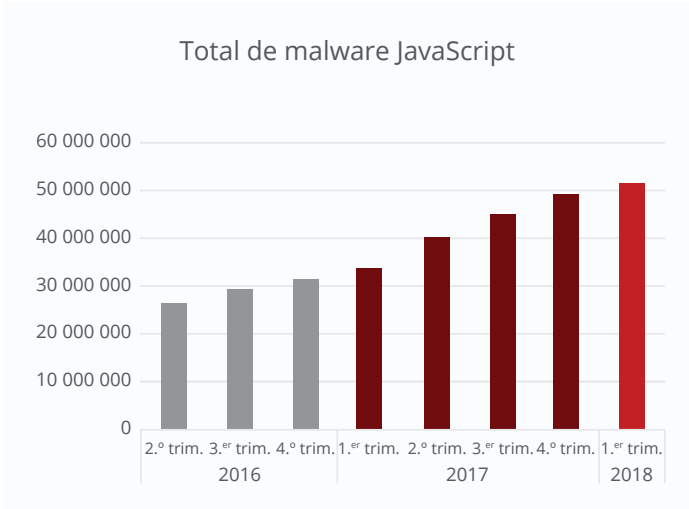
El troyano Faceliker manipula los clics que hacen los usuarios en Facebook, con el objetivo de aumentar artificialmente el número de "Me gusta" de determinado contenido. Para más información, lea este artículo de McAfee Labs.

Seguir

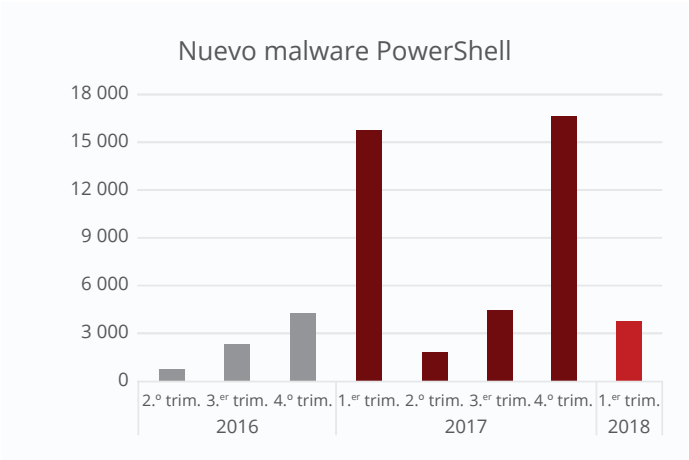
Compartir



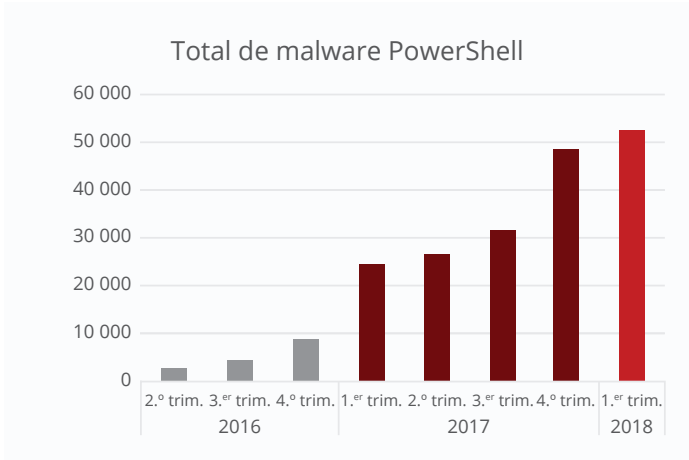
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.

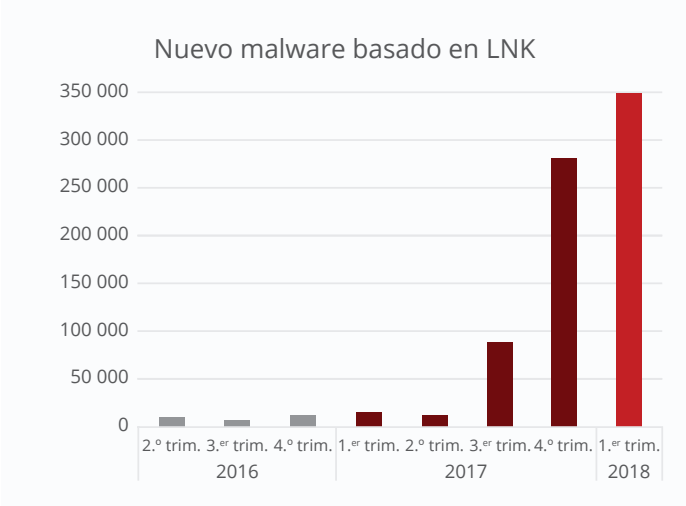


Fuente: McAfee Labs, 2018.

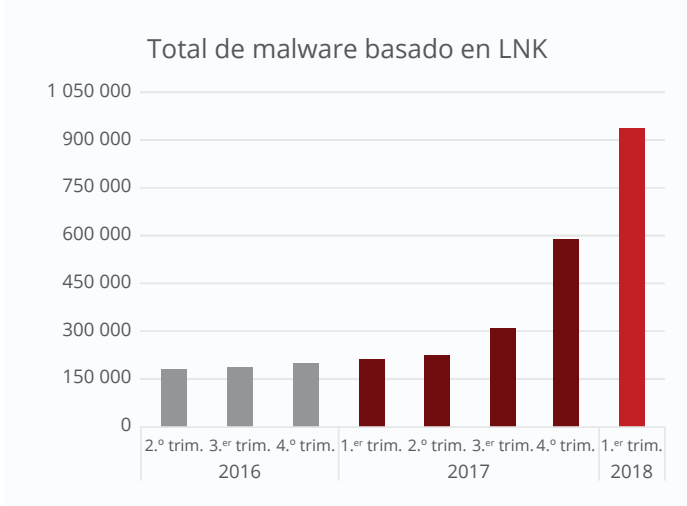
Para obtener más información sobre amenazas basadas en PowerShell y JavaScript, consulte el apartado "El auge del malware basado en scripts" de un *Informe de McAfee Labs sobre amenazas* anterior.

Seguir

Compartir

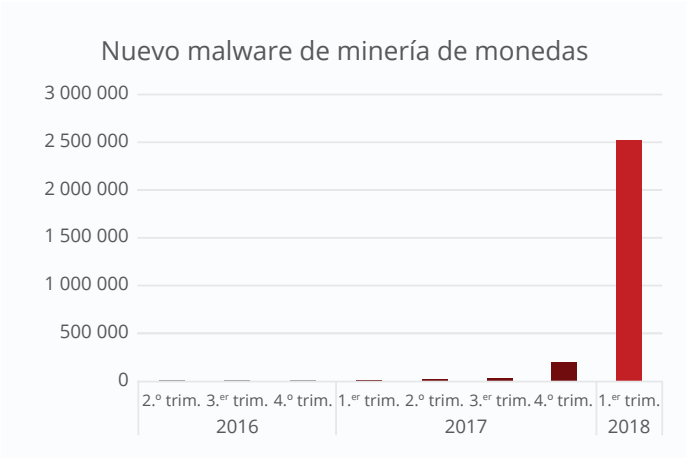


Fuente: McAfee Labs, 2018.

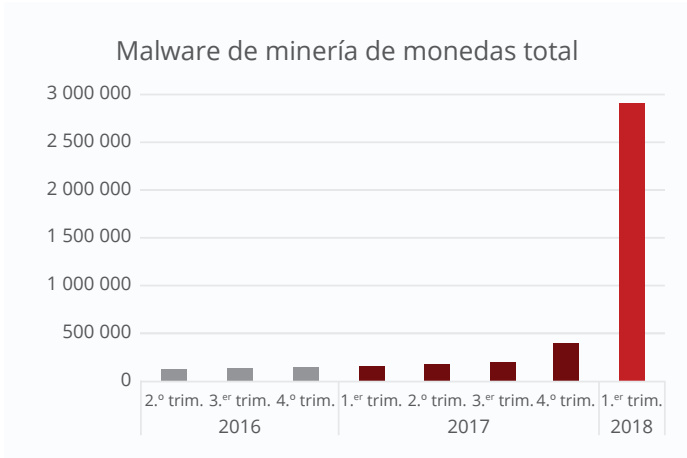


Fuente: McAfee Labs, 2018.

Los ciberdelincuentes utilizan cada vez más accesos directos .lnk para distribuir de manera encubierta scripts de PowerShell maliciosos y otros tipos de malware.



Fuente: McAfee Labs, 2018.



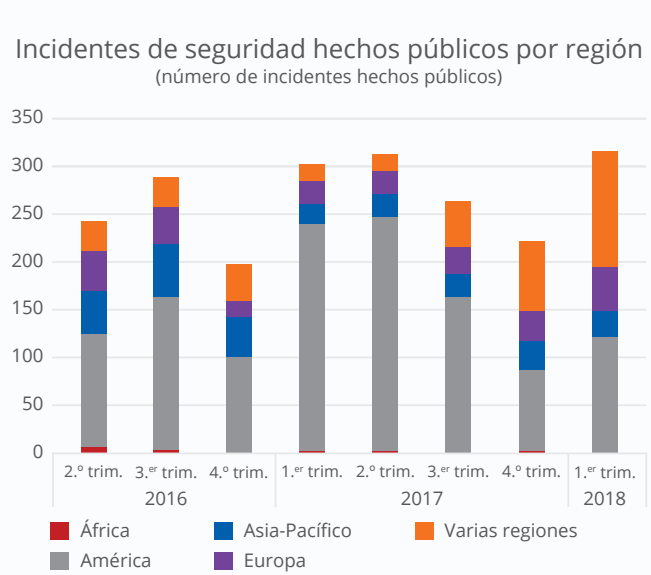
Fuente: McAfee Labs, 2018.

El malware de minería de monedas secuestra los sistemas para crear cibermonedas (lo que se denomina "minería"), sin el consentimiento ni el conocimiento de las víctimas. Las amenazas de minería de monedas se incrementaron un 1189 % en el primer trimestre.

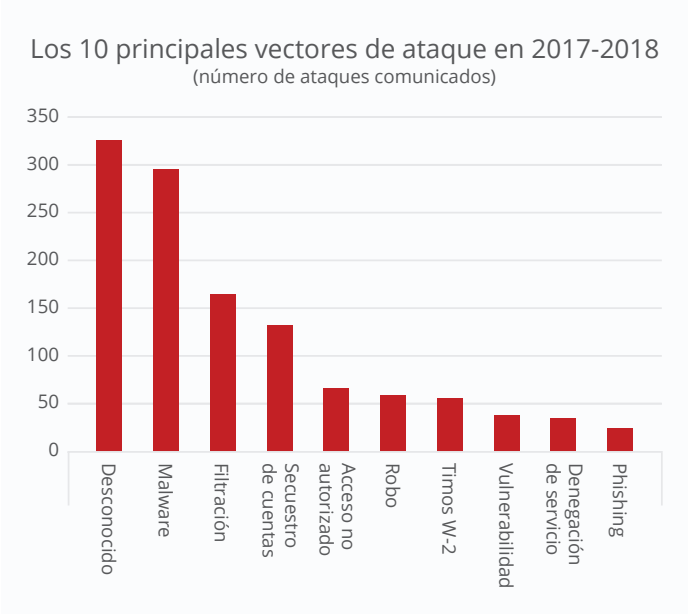
Seguir

Compartir

Incidentes



Fuente: McAfee Labs, 2018.



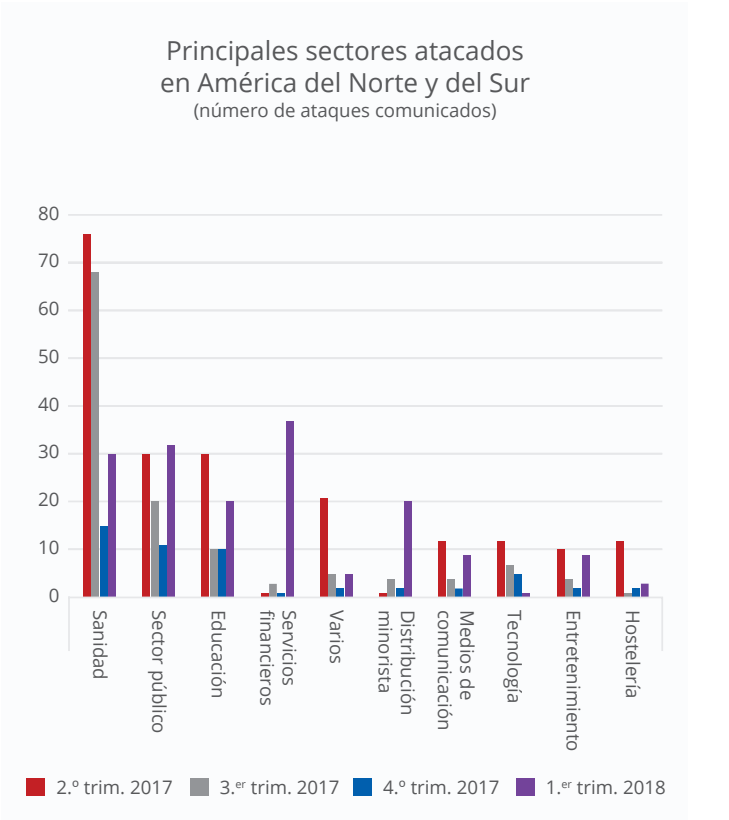
Fuente: McAfee Labs, 2018.

Los datos de los incidentes de seguridad se obtienen de varias fuentes, como hackmageddon.com, privacyrights.org/data-breaches, haveibeenpwned.com y databreaches.net.

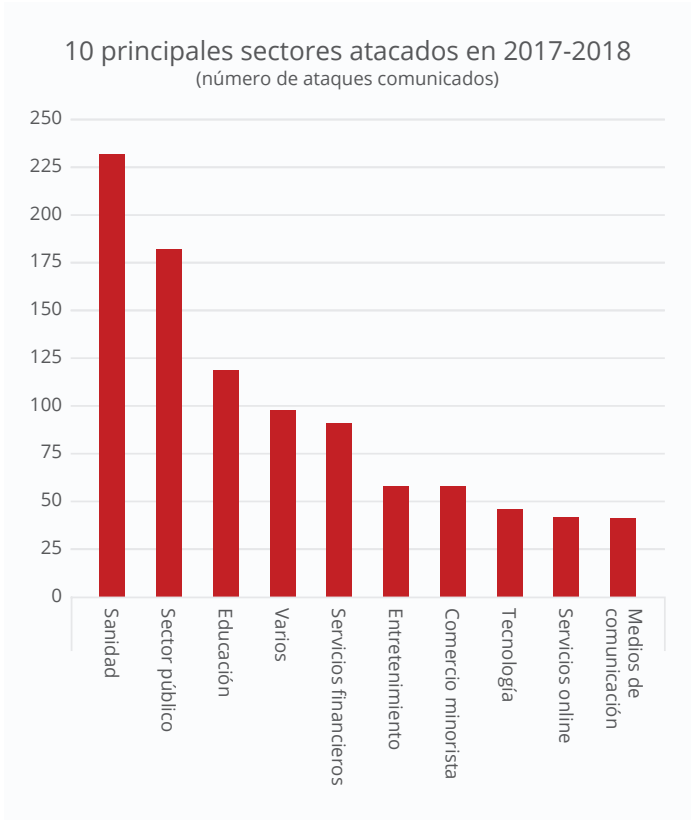
La mayoría de los vectores de ataque no se conocen o bien no se han hecho públicos.

Seguir

Compartir



Fuente: McAfee Labs, 2018.

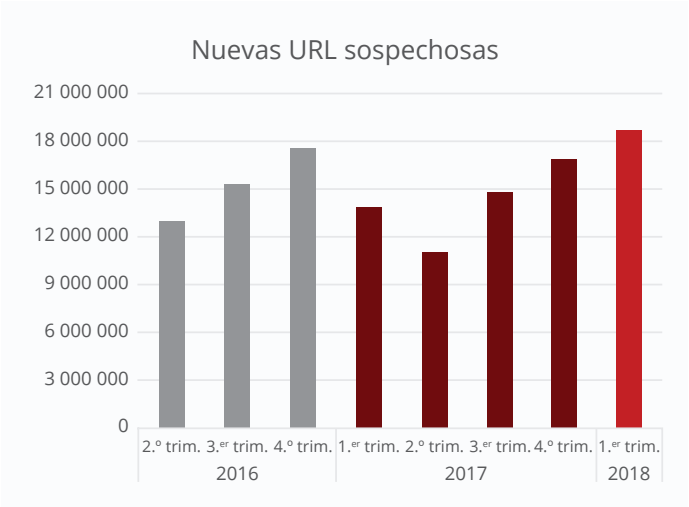


Fuente: McAfee Labs, 2018.

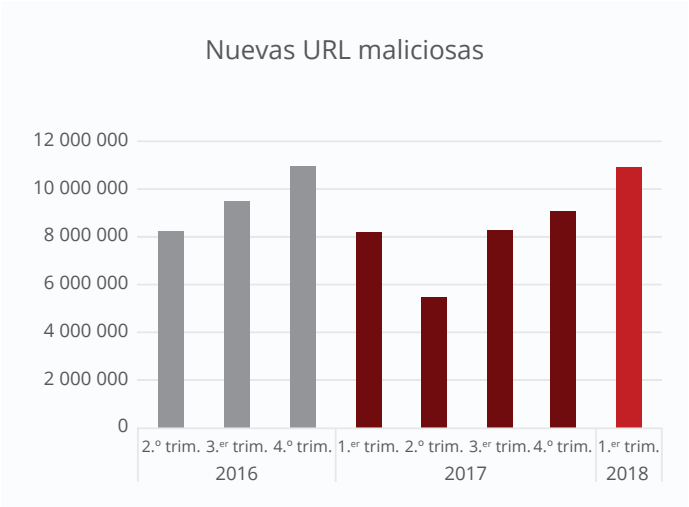
Seguir

Compartir

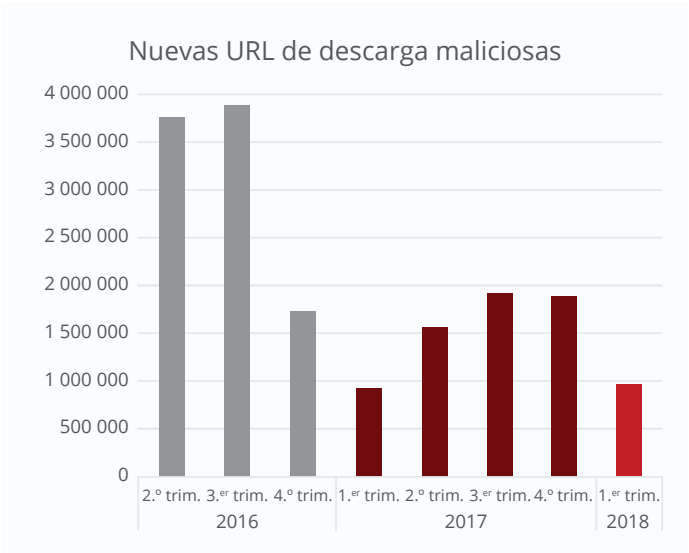
Amenazas en la Web y la red



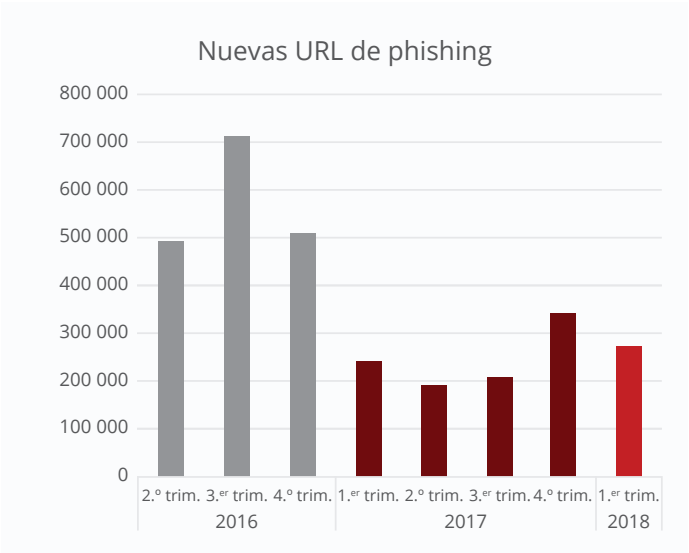
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.

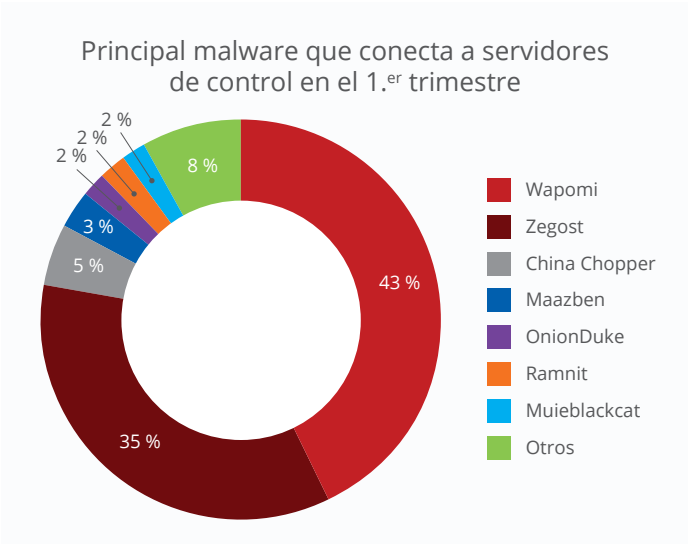


Fuente: McAfee Labs, 2018.

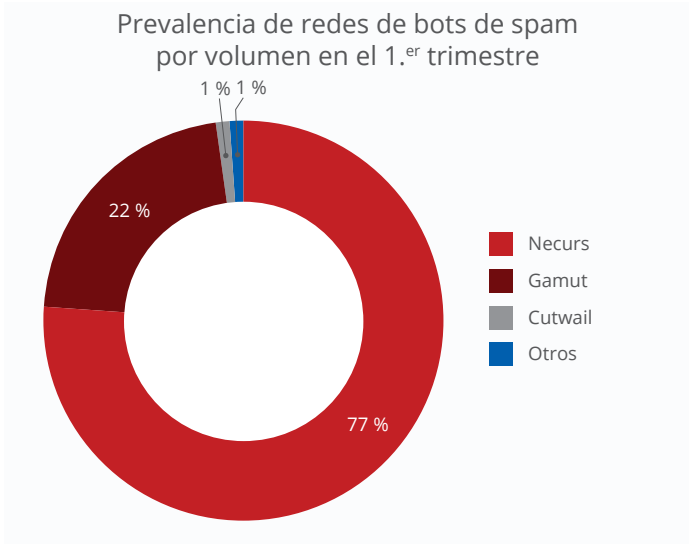
La base de datos de la Web de McAfee® TrustedSource™ contiene URL (páginas web) organizadas en categorías según su reputación web, con el fin de utilizarlas en directivas de filtrado para gestionar el acceso a la Web. Las URL sospechosas son el total de sitios con una calificación de riesgo alto o medio. Las URL maliciosas despliegan código, incluidos archivos ejecutables de descargas "desapercibidas" y troyanos, que tiene como objetivo secuestrar la configuración o la actividad de un ordenador. Las descargas maliciosas comienzan en sitios que permiten a un usuario, en ocasiones sin su conocimiento, descargar de manera inadvertida código dañino o molesto. Las URL de phishing son páginas web que suelen llegar en mensajes de correo electrónico falsos con el fin de robar información de cuentas del usuario.

Seguir

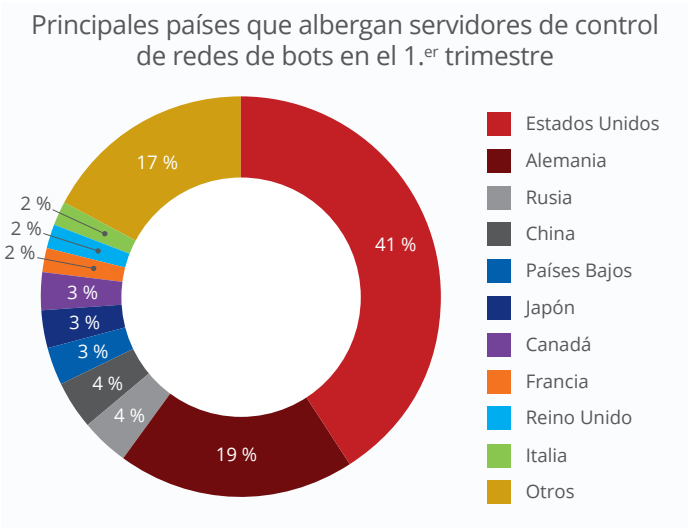
Compartir



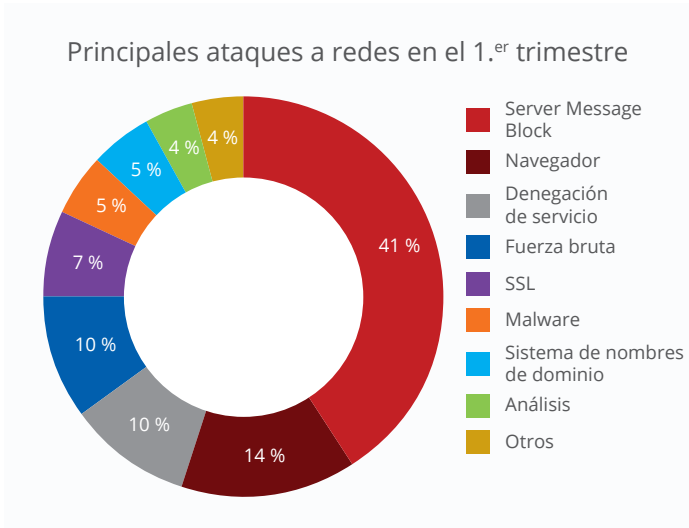
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.

Responsable de aproximadamente del 75 % del spam de redes de bots observado durante el primer trimestre, la red de bots Necurs vuelve a ocupar el primer puesto. Los timos de citas, el ransomware y los downloaders fueron amenazas muy populares. Gamut continúa en segundo lugar, a pesar del descenso de casi el 50 % en el volumen respecto al 4.º trimestre de 2017.

Seguir

Compartir

Acerca de McAfee

McAfee es una de las empresas de ciberseguridad independientes más importantes del mundo. Inspirándose en el poder de la colaboración, McAfee crea actividades y soluciones de consumo que hacen del mundo un lugar más seguro. Al diseñar soluciones compatibles con los productos de otras firmas, McAfee ayuda a las empresas a implementar entornos cibernéticos verdaderamente integrados en los que la protección, la detección y la corrección de amenazas tienen lugar de forma simultánea y en colaboración. Al proteger a los consumidores en todos sus dispositivos, McAfee protege su estilo de vida digital en casa y fuera de ella. Al trabajar con otras empresas de seguridad, McAfee lidera una iniciativa de unión frente a los ciberdelincuentes en beneficio de todos.

www.mcafee.com/es

Acerca de McAfee Labs y McAfee Advanced Threat Research

McAfee Labs, dirigido por el equipo de McAfee Advanced Threat Research, es una de las referencias mundiales en investigación e inteligencia sobre amenazas, y líder en innovación en ciberseguridad. Gracias a la información que reciben de millones de sensores situados en los principales vectores de amenazas —archivos, la Web, la mensajería y las redes—, McAfee Labs y McAfee Advanced Threat Research proporcionan inteligencia sobre amenazas en tiempo real, análisis críticos y opiniones de expertos que permiten mejorar la protección y reducir los riesgos.

www.mcafee.com/es/mcafee-labs.aspx

McAfee Together is power.

Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
www.mcafee.com/es