McAfee
Together is power.

Informe de McAfee Labs sobre amenazas

Marzo de 2018

ESTADÍSTICAS SOBRE AMENAZAS

Malware

Incidentes

Amenazas en la Web y la red

Máximo histórico de malware nuevo contabilizado por McAfee Labs en el 4.º trimestre: 63,4 millones de muestras.

En la investigación y redacción de este informe han participado:

- Alex Bassett
- Christiaan Beek
- Niamh Minihane
- Eric Peterson
- Raj Samani
- Craig Schmugar
- ReseAnne Sims
- Dan Sommer
- Bing Sun

Introducción

Bienvenido al *Informe de McAfee Labs sobre amenazas, de marzo de 2018*. En este número ofrecemos las noticias y estadísticas recopiladas durante el 4.º trimestre de 2017 por los equipos de McAfee Advanced Threat Research y McAfee Labs. Hemos asistido a un fin de año increíble, no solo por las estadísticas sobre amenazas que presentamos en este informe, sino también por los hallazgos de algunas de nuestras últimas investigaciones.

Una de las mayores novedades observadas en el mundo de la ciberdelincuencia durante el pasado trimestre ha sido el aumento de casos de secuestro de criptomonedas, que ha coincidido con el creciente interés del mercado en las monedas digitales. El repunte experimentado en el valor de los bitcoins en el 4.º trimestre, que alcanzó su precio máximo en diciembre con 19 000 dólares por unidad, animó a muchos ciberdelicuentes a incluir en sus actividades el secuestro de monederos de bitcoins y Monero. Este cambio confirma la idea de que los ciberdelincuentes intentan siempre conseguir una combinación de máximos beneficios en el menor espacio de tiempo y con el mínimo riesgo. Los investigadores de seguridad también han descubierto recientemente aplicaciones para Adroid utilizadas para llevar a cabo acciones de minería de criptomonedas. Hemos observado que en algunos foros clandestinos se recomienda cambiar de bitcoins a Litecoins, ya que este modelo es más seguro y entraña menos riesgos.

Algunos ciberdelincuentes siguen desarrollando redes de bots que atacan el Internet de las cosas, y que toman prestado y desarrollan nuevo código. Por el momento, estas redes de bots se utilizan principalmente en ataques de denegación de servicio. El reto para el sector de la seguridad será ofrecer una protección adecuada contra estos ataques a medida que aumentan su capacidad y frecuencia.

Tendencias principales: los ciberdelincuentes dan un giro y adoptan nuevas estrategias y tácticas

En el 4.º trimestre de 2017, McAfee Labs registró una media de ocho nuevas muestras de malware por segundo, frente a las cuatro muestras nuevas por segundo del 3.er trimestre. En general, el trimestre se ha caracterizado por la aparición de nuevas herramientas y estratagemas, como el malware basado en PowerShell y la minería de criptomonedas, que han experimentado un aumento en sintonía con el valor del bitcoin.

PowerShell: en 2017, McAfee Labs observó un incremento del malware PowerShell del 267 % durante el 4.º trimestre, y del 432 % interanual, ya que esta categoría de amenazas se convirtió en herramienta de referencia para los ciberdelincuentes. El lenguaje de scripting tuvo gran relevancia, ya los ciberdelincuentes lo emplearon en archivos de Microsoft Office para ejecutar la primera etapa de los ataques.

En diciembre se destapó Operation Gold Dragon, una campaña de malware dirigida contra los Juegos Olímpicos de Invierno 2018. La campaña es una implementación ejemplar del malware PowerShell en un ataque.

Minería de criptomonedas: la moneda online sirve de estímulo para una buena parte de las actividades ciberdelictivas, incluidas las compras de malware y los pagos de ransomware. Los ciberdelincuentes prefieren recurrir a capacidad de computación externa, en lugar de utilizar sus propios equipos, ya que el precio de una máquina de minería dedicada supera los 5000 dólares. En el 4.º trimestre, el equipo de analistas de McAfee Advanced Threat Research informó sobre esta pujante industria, y explicó cómo a menudo los ciberdelincuentes intentan introducir de manera maliciosa malware destinado a aprovechar la capacidad computacional del usuario y extraer monedas, o directamente a localizar y robarles su criptomoneda.

Ransomware: en 2017, McAfee Labs observó un incremento interanual del ransomware del 59 %, con un aumento del 35 % solo en el 4.º trimestre. Esta actividad incluía el empleo de nuevas y creativas tácticas por los ciberdelincuentes, que desplazaron las motivaciones habituales de esta categoría de amenazas, es decir, extorsionar para conseguir dinero, para incluir el sabotaje de las redes corporativas. Los ciberdelincuentes diseñaron estrategias para crear una "cortina de humo" con la intención de alejar a los defensores de los ataques reales, como ocurrió en el caso del seudoransomware detectado en NotPetya y en un robo a un banco taiwanés.

A pesar del continuo crecimiento del ransomware, durante el 4.º trimestre las fuerzas de seguridad consiguieron desmantelar varias redes de ciberdelincuentes, con la detención de los ciberdelincuentes supuestamente responsables de la propagación del ransomware CTB Locker.

El sector sanitario como objetivo: en 2017, el sector de los servicios sanitarios experimentó un aumento de incidentes de seguridad comunicados del 210 %, en comparación con el año 2016, si bien los incidentes disminuyeron un 78 % en el 4.º trimestre. Al analizar los ataques, los expertos de McAfee Advanced Threat Research concluyeron que muchos de los incidentes se produjeron por incumplimiento de las mejores prácticas de seguridad o por vulnerabilidades del software médico.

Necurs y Gamut: en el 4.º trimestre, el 97 % del tráfico de redes de bots de spam fue generado por tan solo dos redes de bots que permitían a los ciberdelincuentes el acceso por alquiler. Necurs, un reciente proveedor de spam de tipo "lonely girl" (chica solitaria), spam de manipulación bursátil y downloaders del ransomware Locky, superó a Gamut, remitente de mensajes de phishing con ofertas de trabajo y de captación de intermediarios para transferir dinero, como red de bots de envío de spam más importante.

ESTADÍSTICAS

McAfee Global Threat Intelligence

Cada trimestre, el panel en la nube de McAfee Global Threat Intelligence 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. De media, McAfee GTI analizó 400 000 URL y 800 000 archivos al día. Durante el 4.º trimestre, los volúmenes de ataques que experimentaron nuestros clientes fueron los siguientes:

- McAfee GTI recibió de media 48 000 millones de consultas al día.
- Las protecciones de McAfee GTI contra archivos maliciosos aumentaron hasta los 45 millones al día en el 4.º trimestre, desde los 40 millones del 3.er trimestre.
- Las protecciones de McAfee GTI contra URL de riesgo descendieron hasta los 57 millones al día en el 4.º trimestre, desde los 99 millones del 3.er trimestre, a pesar del marcado incremento que se observó en las URL de alto riesgo tras el 19 de diciembre.
- Las protecciones de McAfee GTI contra direcciones IP de riesgo aumentaron hasta los 84 millones al día en el 4.º trimestre, desde los 48 millones del 3.er trimestre.

Campañas principales: la desigualdad en la ciberguerra sigue creciendo

A principios de 2017, los analistas de McAfee predecían los difíciles retos a los que se iba a enfrentar el sector de la ciberseguridad durante el año, y se referían a la asimetría de la información como uno de los principales obstáculos. En pocas palabras, los ciberdelincuentes tienen el privilegio de acceder a las investigaciones realizadas por la comunidad técnica y pueden descargar y utilizar herramientas de código abierto para sus campañas; por el contrario, el conocimiento que tienen los responsables de la seguridad acerca de las actividades de los ciberdelincuentes es considerablemente más limitado y, con frecuencia, la identificación de las nuevas tácticas solo es posible una vez que se han iniciado las campañas maliciosas. Los principales ataques del 4.º trimestre son la constatación de que la desigualdad en la ciberguerra no ha hecho sino aumentar.

Noviembre de 2017: APT28, conocido también como Fancy Bear, aprovechó una técnica de intercambio dinámico de datos (Dynamic Data Exchange) de Microsoft Office, que se había hecho pública solo unas semanas antes, para lanzar una campaña de mensajes de phishing en los que se mencionaban los ataques terroristas de Nueva York.

Diciembre de 2017: los ataques dirigidos contra organizaciones que participaban en los Juegos Olímpicos de Invierno de Pyeongchang emplearon esteganografía y una nueva herramienta publicada unos días antes del ataque, Invoke-PSImage. La campaña Operation Gold Dragon consiguió implantar el malware en los sistemas de las víctimas, dando a los ciberdelincuentes carta blanca para buscar y acceder a los datos almacenados en el dispositivo o en las cuentas en la nube conectadas.

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.

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

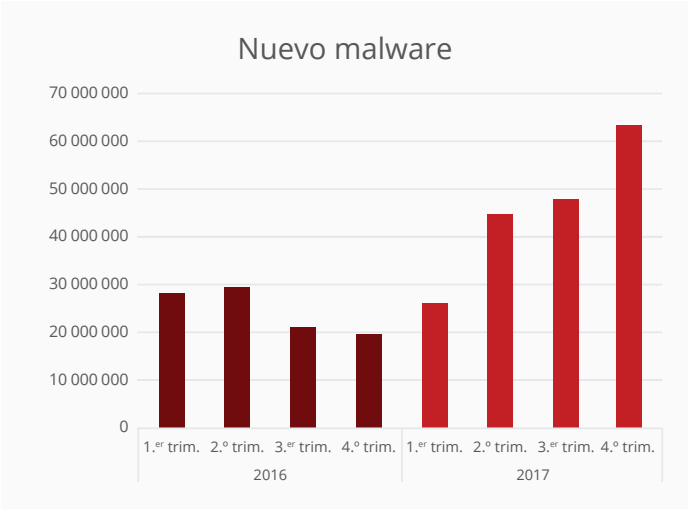
Twitter @Raj_Samani

Seguir

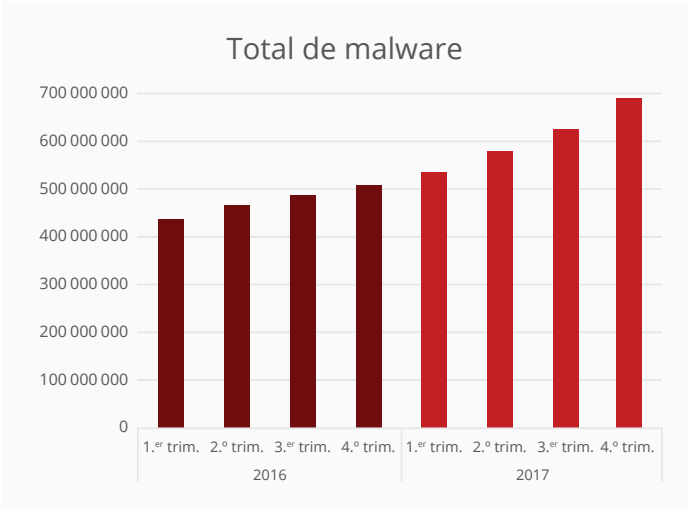
Compartir

Estadísticas sobre amenazas

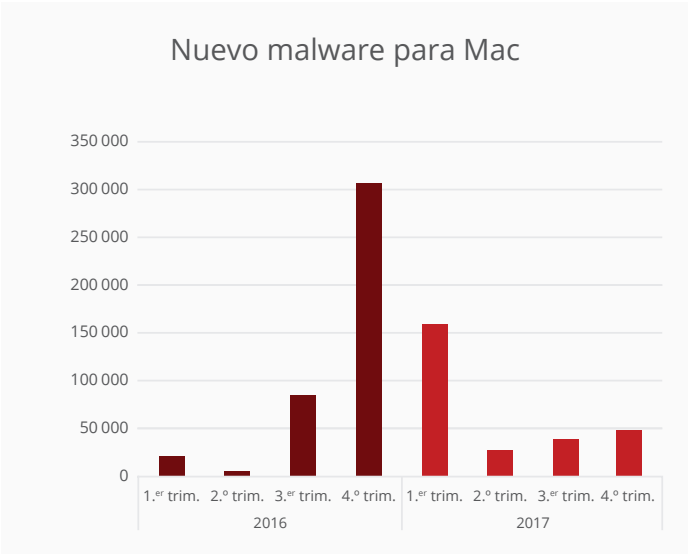
Malware



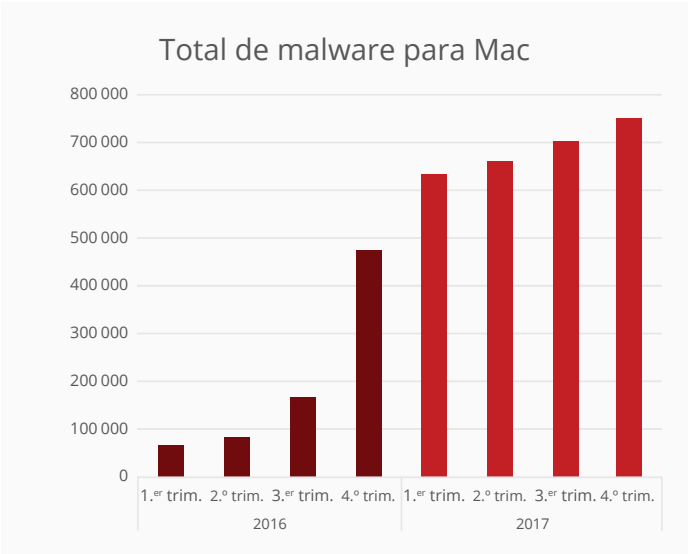
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



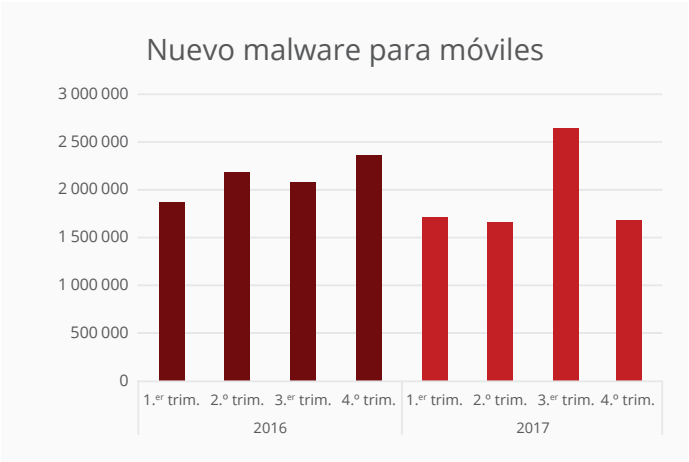
Fuente: McAfee Labs, 2018.

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. Una de las principales amenazas este trimestre fue Waboot.

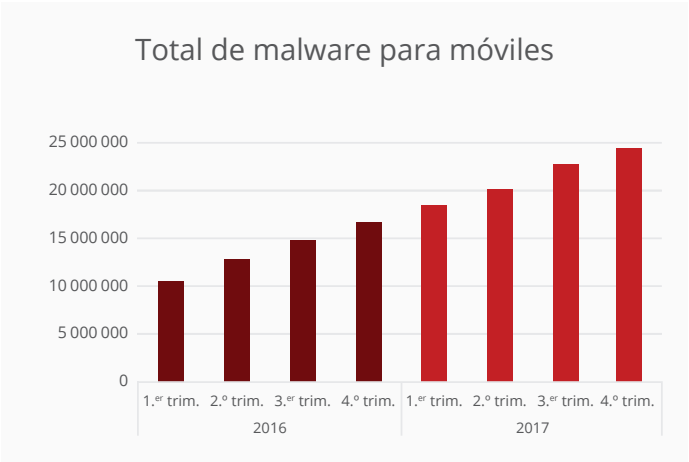
Dos casos de malware para Mac muy frecuentes este trimestre fueron Flashback, que se apodera de contraseñas y otros datos a través de los navegadores, y Longage, capaz de proporcionar al hacker el control de un sistema.

Seguir

Compartir

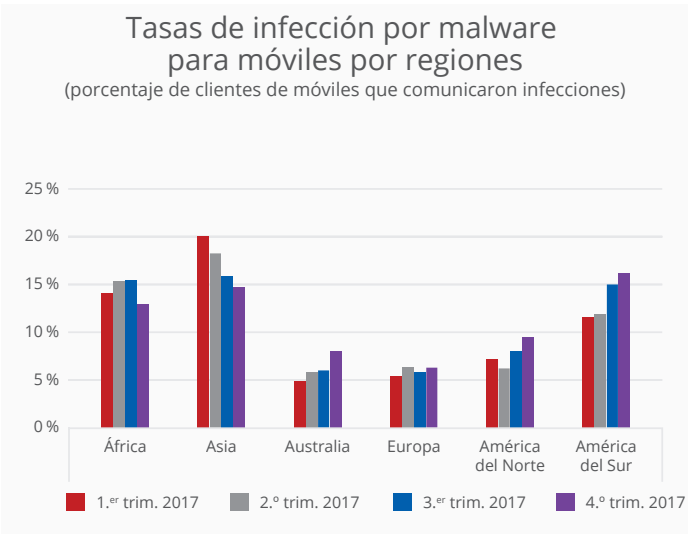


Fuente: McAfee Labs, 2018.

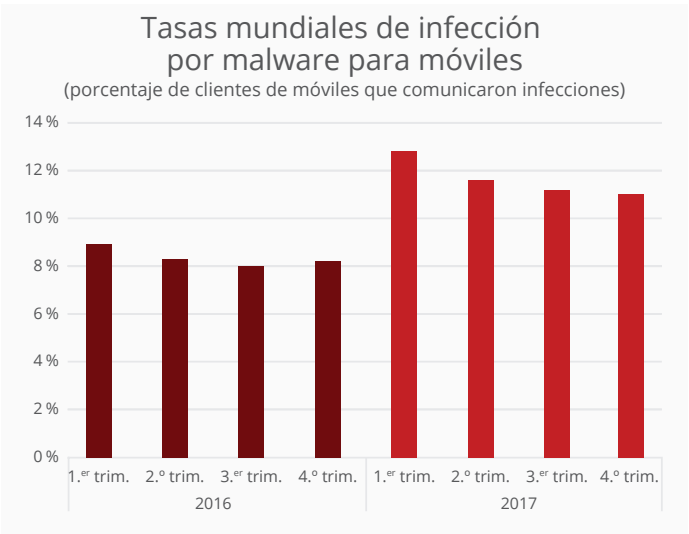


Fuente: McAfee Labs, 2018.

El aumento del ransomware de bloqueo de pantalla para Android descendió considerablemente este trimestre. (Véanse las gráficas de la página 9). La actividad del troyano dropper Piom también disminuyó notablemente.



Fuente: McAfee Labs, 2018.

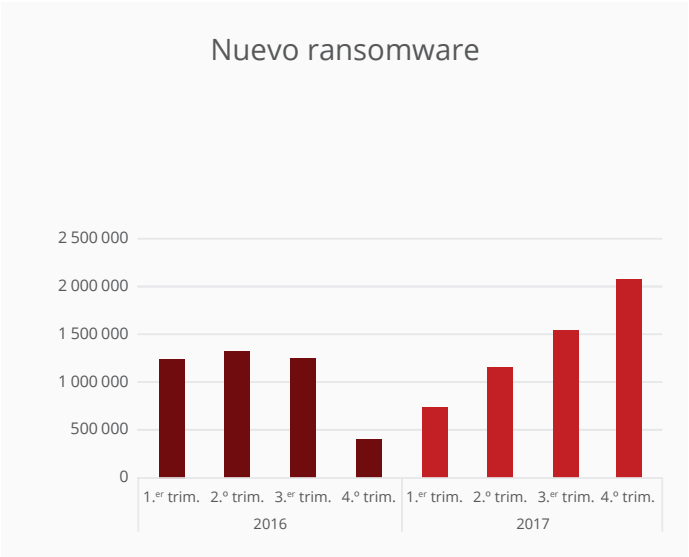


Fuente: McAfee Labs, 2018.

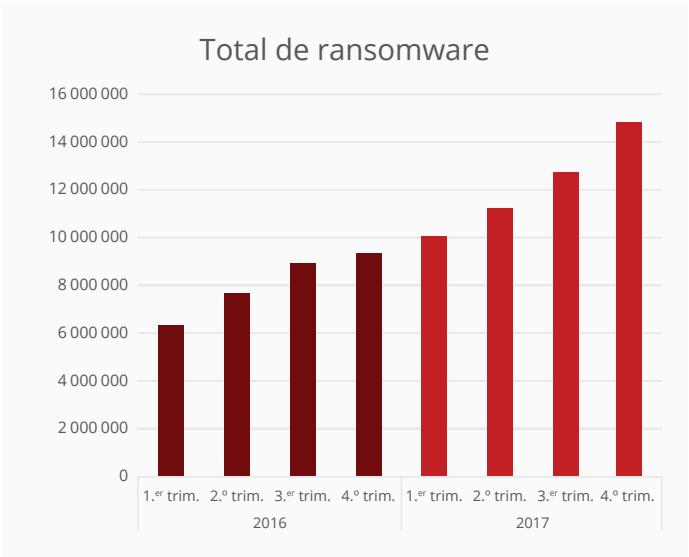
Las tasas de infección mundiales han descendido ligeramente durante los tres últimos trimestres, si bien los porcentajes han aumentado en Australia y América.

Seguir

Compartir

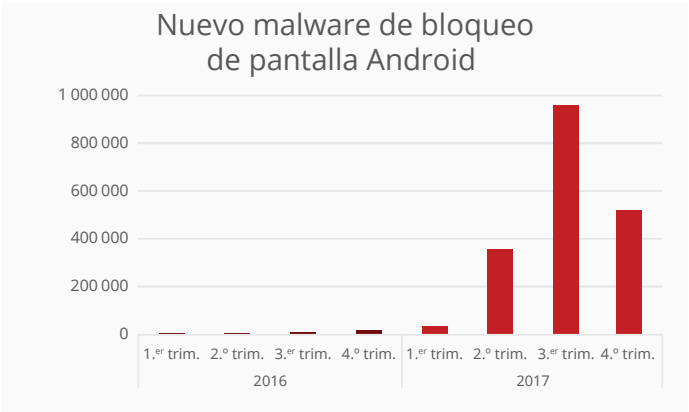


Fuente: McAfee Labs, 2018.

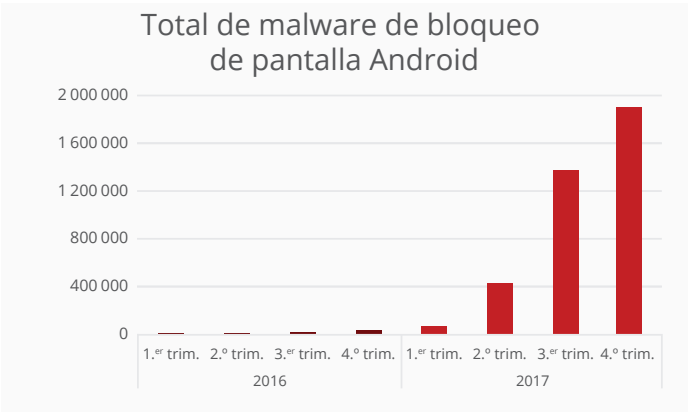


Fuente: McAfee Labs, 2018.

Ransom:Win32/Genasom ha contribuido de manera importante al aumento del ransomware.



Fuente: McAfee Labs, 2018.

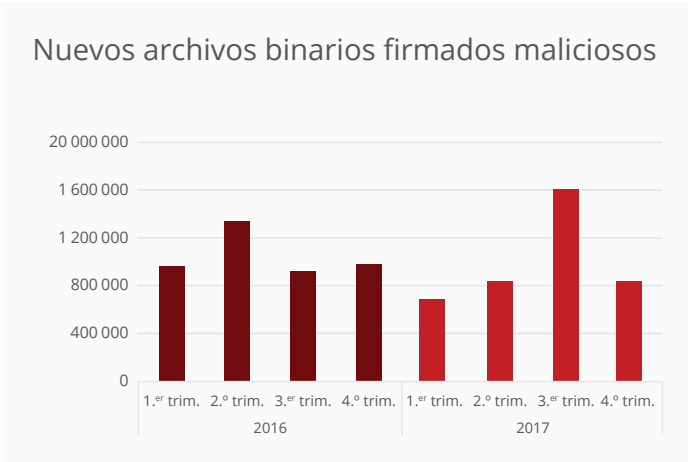


Fuente: McAfee Labs, 2018.

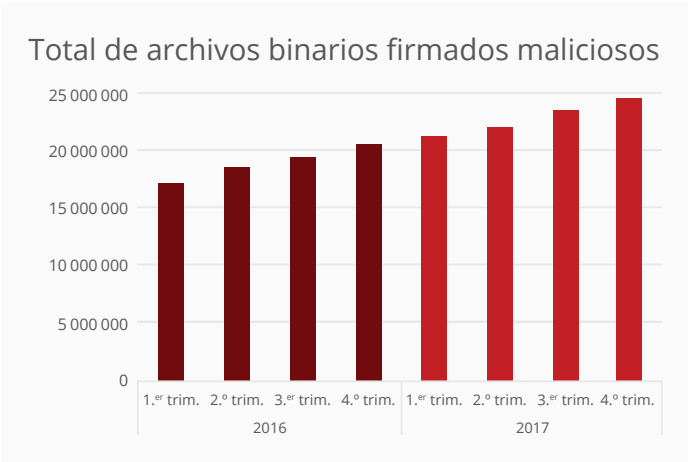
Este tipo de ransomware inició su actividad lentamente en 2016, pero alcanzó una enorme importancia el año pasado.

Seguir

Compartir

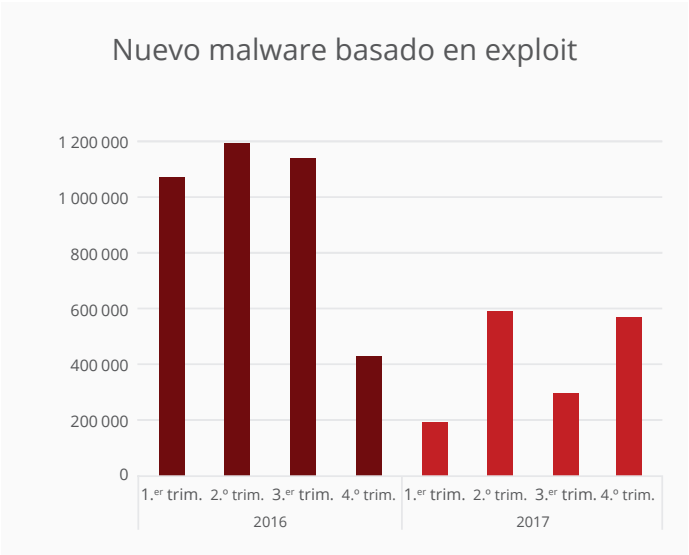


Fuente: McAfee Labs, 2018.

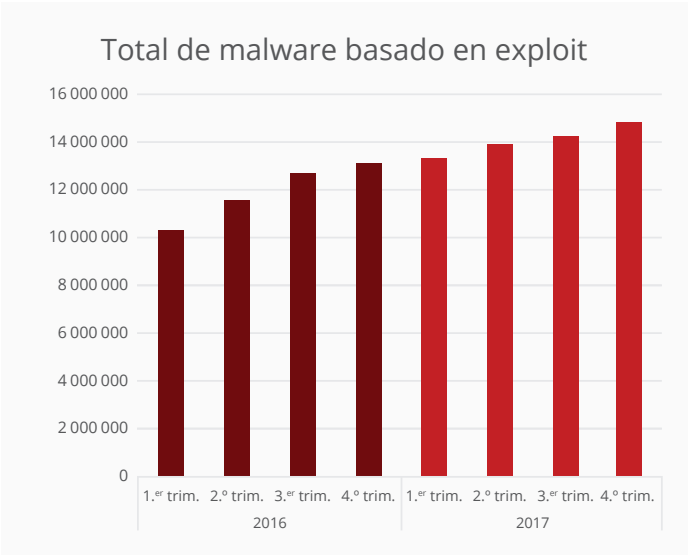


Fuente: McAfee Labs, 2018.

Las autoridades de certificación ofrecen certificados digitales que proporcionan información online una vez que una aplicación, o binario, es firmada o validada por el proveedor de servicios propietario del contenido. Sin embargo, este modelo de confianza no funciona cuando los ciberdelincuentes obtienen certificados para binarios firmados maliciosos, o aplicaciones maliciosas, que facilitan enormemente la ejecución de los ataques.



Fuente: McAfee Labs, 2018.

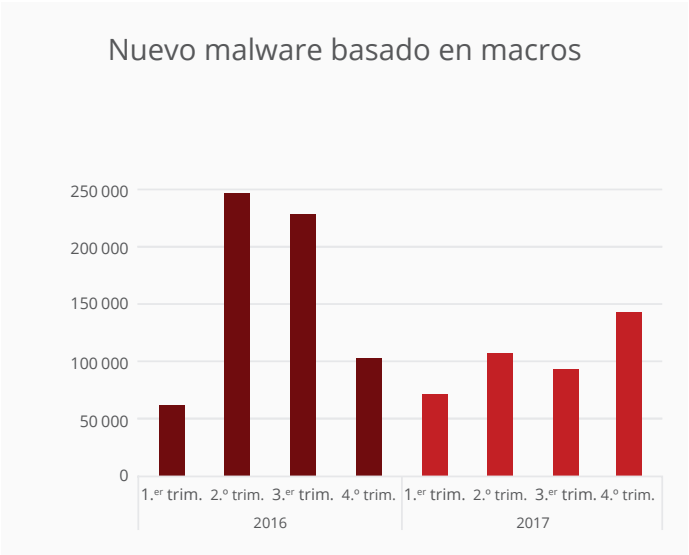


Fuente: McAfee Labs, 2018.

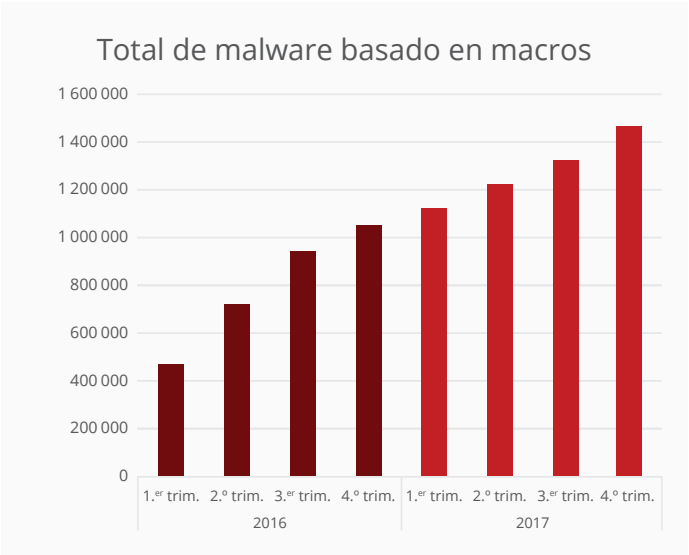
Los exploits aprovechan los errores y vulnerabilidades del software y el hardware. Los ataques de tipo zero-day son ejemplos de exploits que consiguen sus objetivos. Se incluye un ejemplo en el artículo de McAfee Labs "Analyzing Microsoft Office Zero-Day Exploit CVE-2017-11826: Memory Corruption Vulnerability"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

Seguir

Compartir

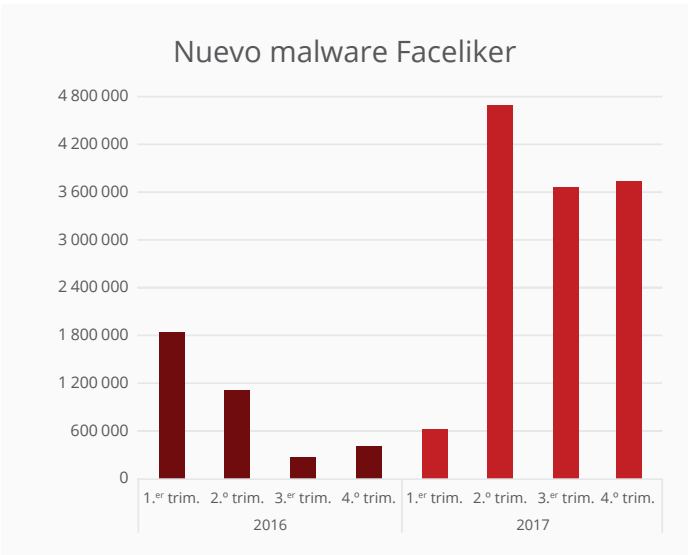


Fuente: McAfee Labs, 2018.

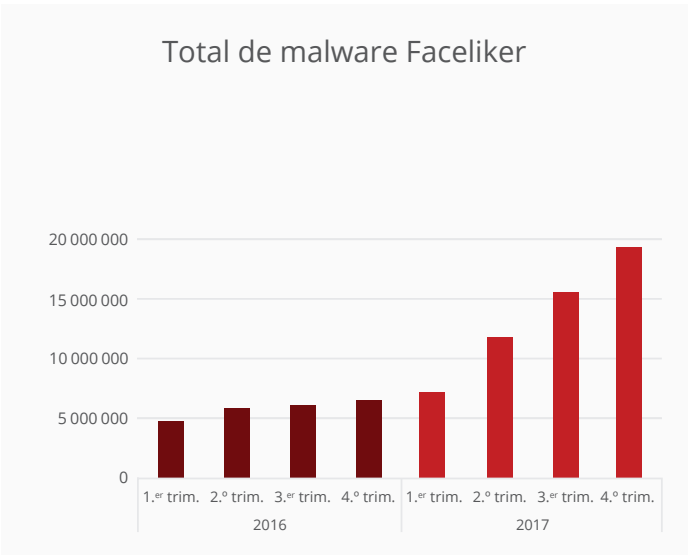


Fuente: McAfee Labs, 2018.

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.

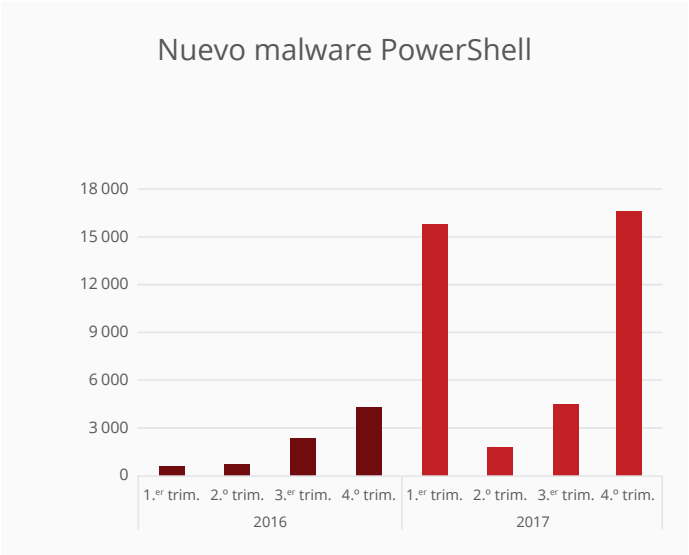


Fuente: McAfee Labs, 2018.

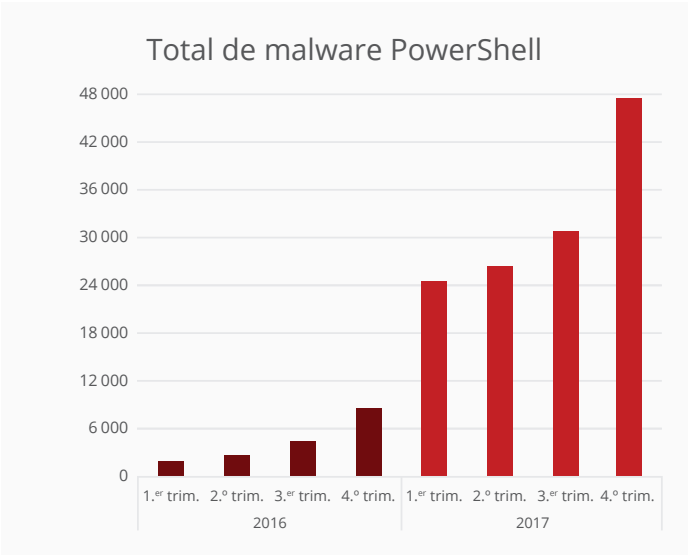
El troyano Faceliker manipula los clics que hacen los usuarios en Facebook, con el objetivo de aumentar artificialmente el número de "Me gusta" de determinado contenido. Para más información, lea este artículo de McAfee Labs.

Seguir

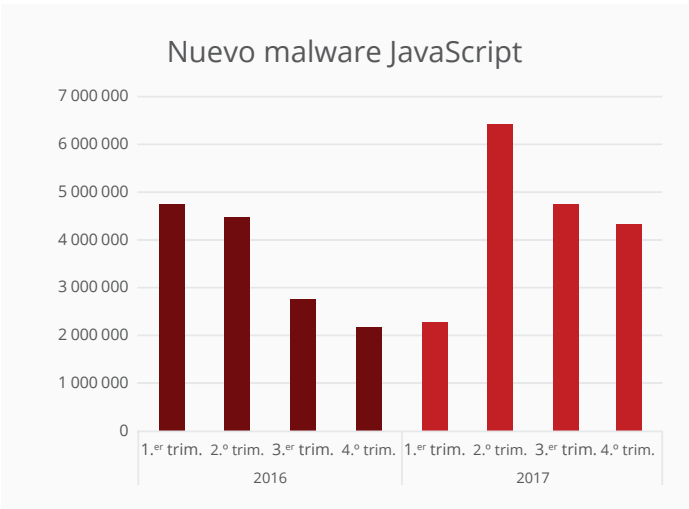
Compartir



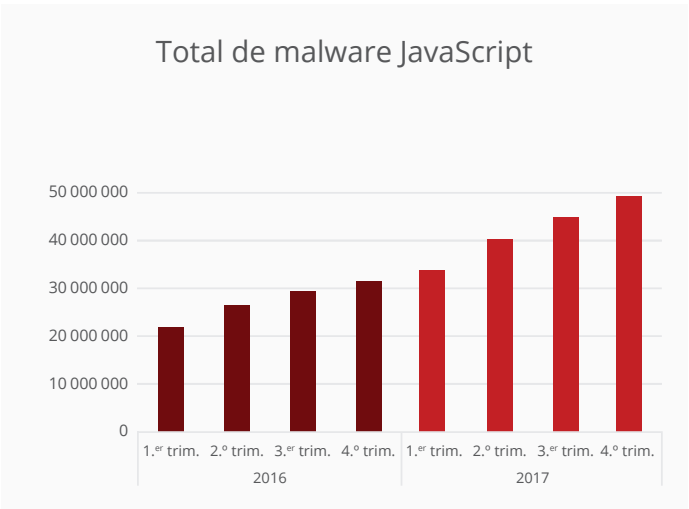
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



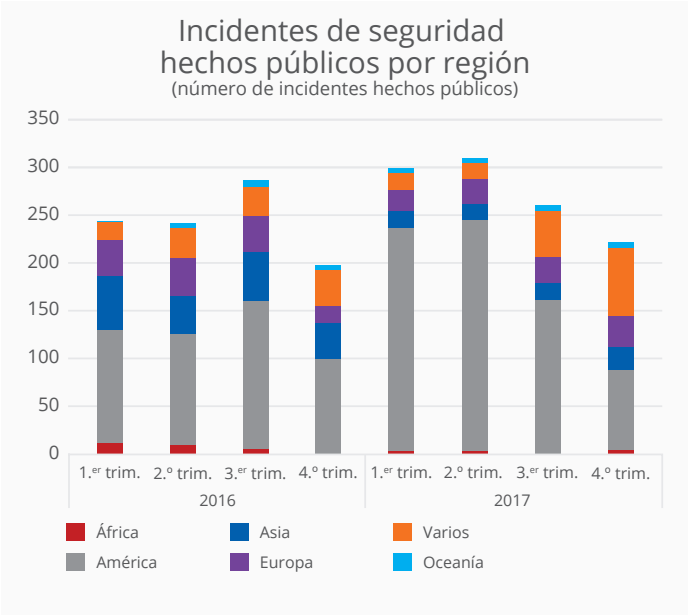
Fuente: McAfee Labs, 2018.

Las amenazas basadas en PowerShell han experimentado un fuerte incremento debido a una ola de downloaders durante el 4.º trimestre. Para obtener más información sobre amenazas basadas en PowerShell y JavaScript, consulte "El auge del malware basado en scripts" en el *Informe de McAfee Labs sobre amenazas, septiembre de 2017.*

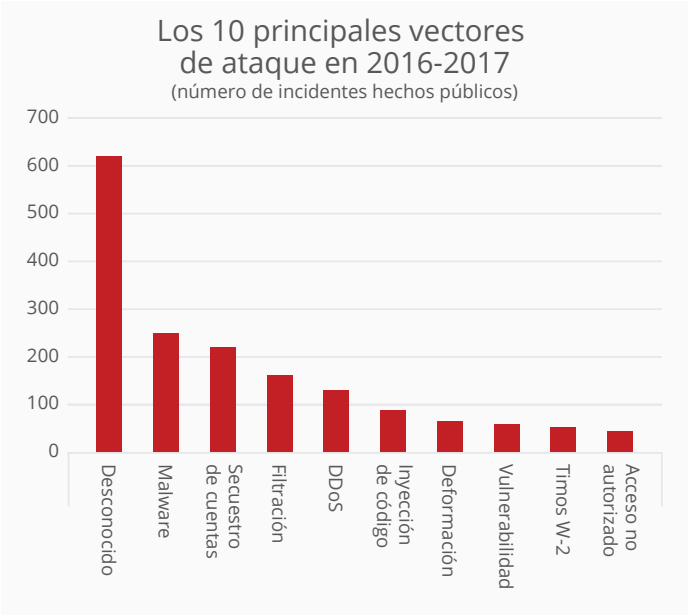
Seguir

Compartir

Incidentes



Fuente: McAfee Labs, 2018.



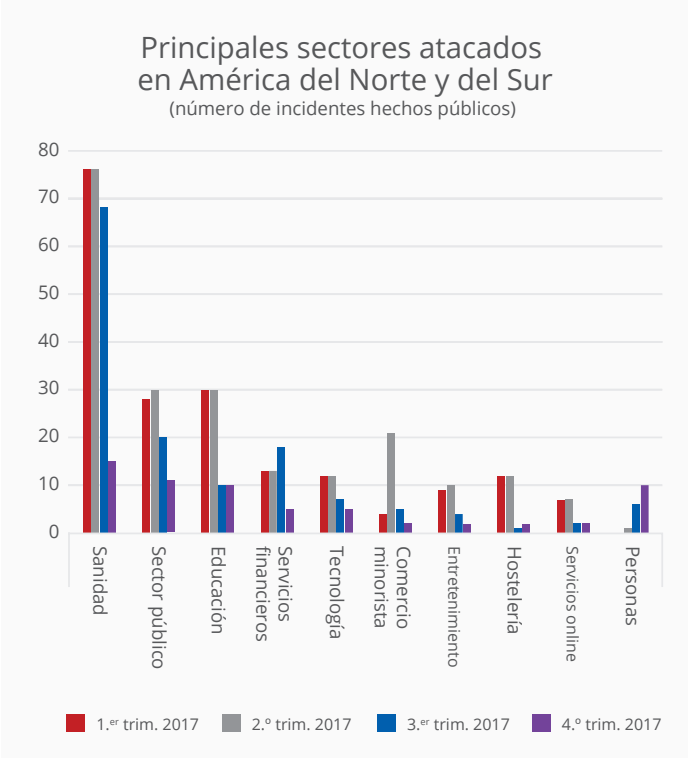
Fuente: McAfee Labs, 2018.

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

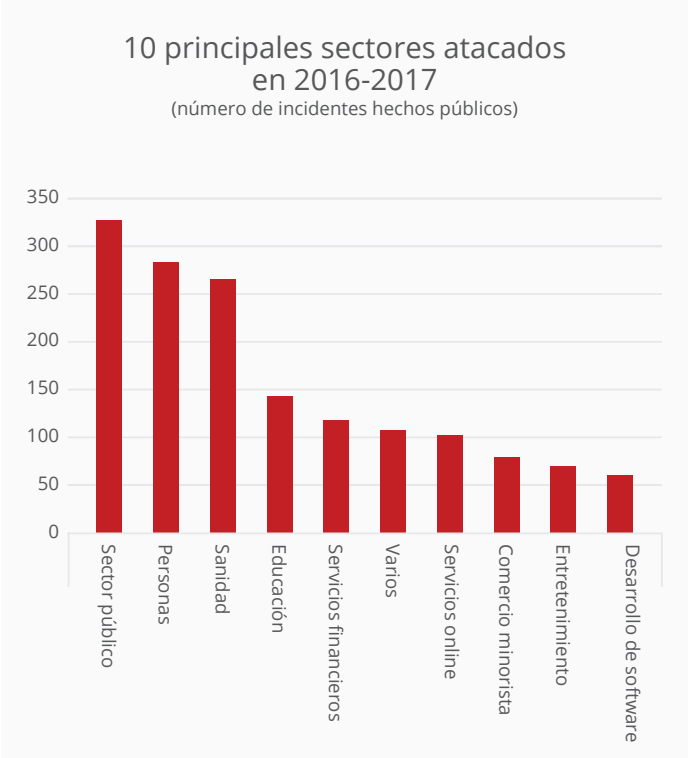
La mayoría de los vectores de ataque no se conocen o bien no se han hecho públicos.

Seguir

Compartir



Fuente: McAfee Labs, 2018.

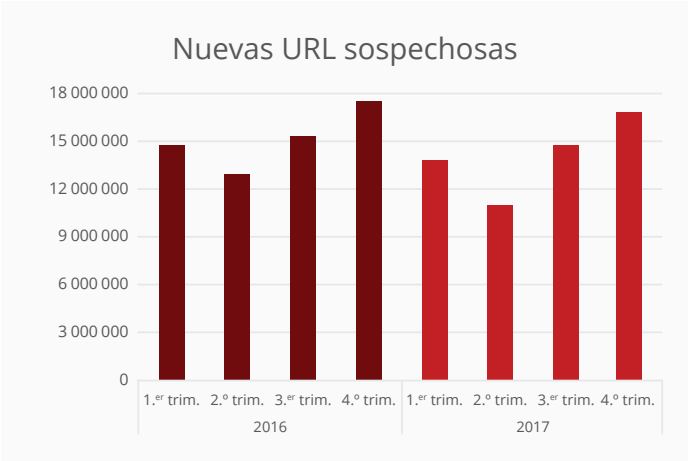


Fuente: McAfee Labs, 2018.

Seguir

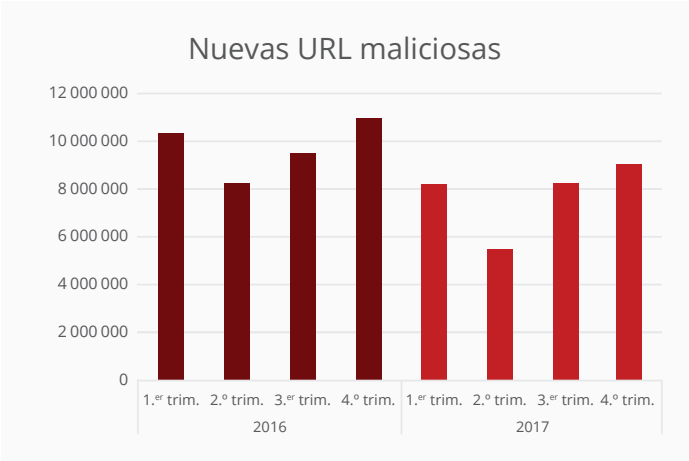
Compartir

Amenazas en la Web y la red



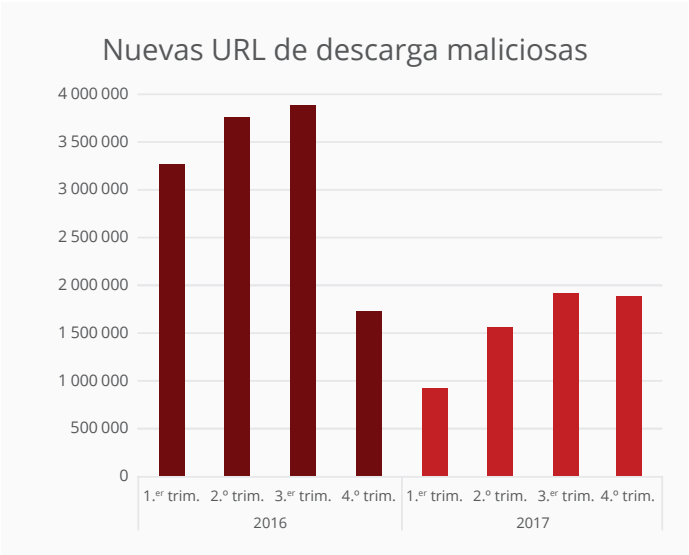
Fuente: McAfee Labs, 2018.

La base de datos McAfee® TrustedSource™ Web Database 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.



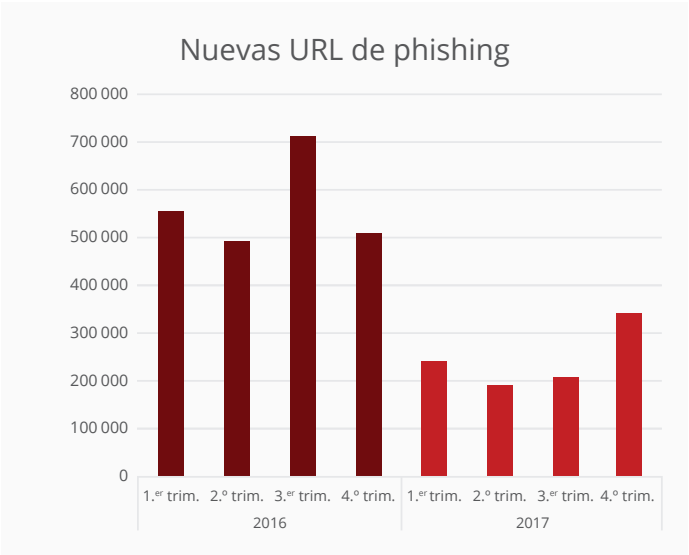
Fuente: McAfee Labs, 2018.

Los sitios maliciosos despliegan código que tiene como objetivo secuestrar la configuración o la actividad de un ordenador. Esta categoría incluye aplicaciones autoinstalables (archivos ejecutables de descargas "desapercibidas"), troyanos y otro malware que aprovecha vulnerabilidades de los navegadores y otras aplicaciones.



Fuente: McAfee Labs, 2018.

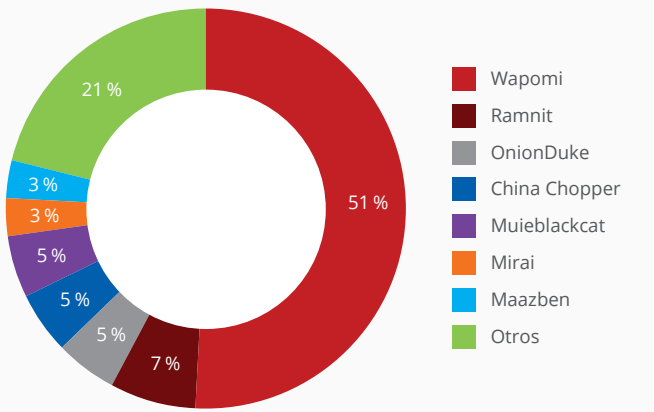
Las descargas maliciosas comienzan en sitios que permiten a un usuario descargar de manera inadvertida código dañino o molesto. Esta categoría incluye protectores de pantalla, barras de herramientas y programas para compartir archivos que contienen adware, spyware, virus y otro código malicioso. En ocasiones el malware se añade sin el conocimiento de los usuarios, como cuando hacen clic en "Sí" o en "Acepto" sin leer en su totalidad los términos y condiciones. Los efectos pueden incluir una ralentización del rendimiento, robo de contraseñas y la pérdida o daños de archivos personales.



Fuente: McAfee Labs, 2018.

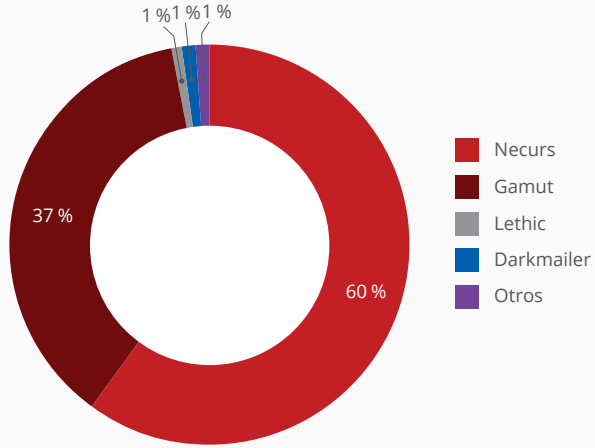
Las URL de phishing son páginas web que suelen llegar en mensajes de correo electrónico falsos con el fin de robar información de cuentas del usuario. Estos sitios simulan ser páginas web de empresas legítimas para engañar al usuario y conseguir sus datos con el fin de llevar a cabo actividades fraudulentas o robos.

Principal malware que conecta a servidores de control en el 4.º trimestre



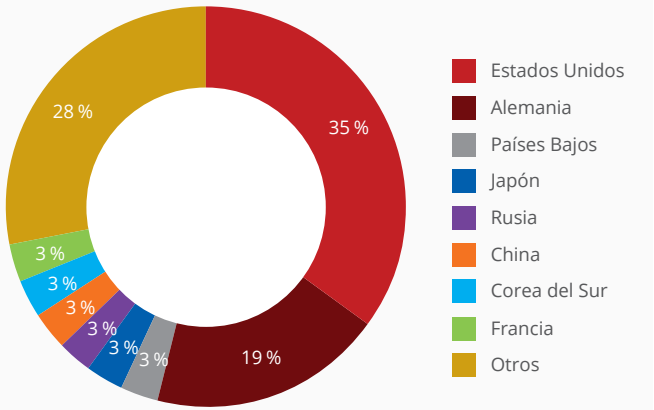
Fuente: McAfee Labs, 2018.

Prevalencia de redes de bots de spam por volumen en el 4.º trimestre



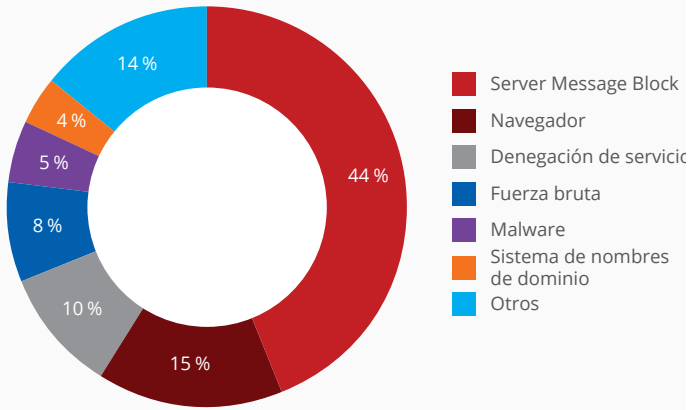
Fuente: McAfee Labs, 2018.

Principales países que albergan servidores de control de redes de bots en el 4.º trimestre



Fuente: McAfee Labs, 2018.

Principales ataques a redes en el 4.º trimestre



Fuente: McAfee Labs, 2018.

Necurs —un reciente proveedor de mensajes de spam con el tema "lonely girl" (chica solitaria), spam de manipulación bursátil y downloaders del ransomware Locky—, y Gamut, que envía mensajes de phishing con ofertas de trabajo (y de captación de intermediarios para transferir dinero), en inglés, alemán e italiano, fueron los responsables del 97 % del tráfico de redes de bots basadas en spam en el 4.º trimestre.

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 ciberdelicuentes en beneficio de todos.

www.mcafee.com/es

Acerca de McAfee Labs

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