McAfee
Together is power.

Informe de McAfee Labs sobre amenazas

Septiembre de 2018

PRINCIPALES HISTORIAS DEL TRIMESTRE

¿Quiere piratear un dispositivo Windows 10 bloqueado? Pregúntele a Cortana (CVE-2018-8140)

Informe de amenazas: No participe en la revolución del blockchain sin garantía de protección

La banda AsiaHitGroup consigue introducir de nuevo en Google Play aplicaciones de fraude en la facturación

McAfee Global Threat Intelligence analizó, de media 1 800 000 URL, 800 000 archivos y otros 200 000 archivos en entorno aislado, cada día del 2.º trimestre.

Introducción

Bienvenido al Informe de McAfee® Labs sobre amenazas de septiembre de 2018. En este número, destacamos la importante investigación y las estadísticas sobre tendencias de amenazas recabadas por los equipos de McAfee Advanced Threat Research y McAfee Labs durante el segundo trimestre de 2018.

Los ciberdelincuentes siguen yendo donde está el dinero. Aunque esto no es nada nuevo, nuestro último informe sobre amenazas muestra claramente cómo algunos ataques más antiguos se trasladan a nuevos vectores de amenazas que ofrecen ahora mayor rentabilidad. Al igual que en el 1.er trimestre, observamos que la popularidad de la minería de criptomonedas sigue al alza.

En este informe detallamos hallazgos recientes de tres análisis de McAfee Labs que aparecieron en el 2.º trimestre. Puede leer los resúmenes de cada uno de ellos en las páginas 5-7. Una de las áreas de investigación de nuestros equipos se centra en los asistentes digitales. En el 2.º trimestre analizamos una vulnerabilidad de Cortana de Microsoft. Este defecto permitía a un agresor iniciar una sesión en un dispositivo Windows bloqueado y ejecutar código. De acuerdo con nuestra política de divulgación de vulnerabilidades, comunicamos nuestros hallazgos a Microsoft; el análisis dio lugar a la publicación de CVE-2018-8140. También examinamos el mundo de los ataques relacionados con criptomonedas, con una visión detallada de la tecnología blockchain. Nuestro informe describía muchas de las vulnerabilidades que aprovechan los ciberdelincuentes que buscan una rentabilidad rápida de su inversión.

En la investigación y redacción de este informe han participado:

- Christiaan Beek
- Carlos Castillo
- Cedric Cochin
- Ashley Dolezal
- Steve Grobman
- Charles McFarland
- Niamh Minihane
- Chris Palm
- Eric Peterson
- Steve Povolny
- Raj Samani
- Craig Schmugar
- ReseAnne Sims
- Dan Sommer
- Bing Sun

En cuanto al malware, en nuestro informe tratamos un área de la ciberdelincuencia que suele recibir poca atención, si se compara con la gran repercusión mediática de los ataques de ransomware de gran escala detectados en los últimos 18 meses. Durante algún tiempo el fraude en la facturación ha sido el modus operandi de varios grupos de ciberdelincuentes. Examinamos una campaña de AsiaHitGroup que ha intentado cobrar dinero a 20 000 víctimas, utilizando apps de tiendas oficiales, como Google Play.

En el segundo trimestre, McAfee Global Threat Intelligence recibió una media de 49 000 millones de consultas al día. Mientras tanto, la cantidad de nuevo malware desciende por segundo trimestre consecutivo; sin embargo, es posible que esto no sea significativo, ya que observamos un repunte en el 4.º trimestre de 2017, y no han surgido muchas nuevas muestras durante cuatro de los últimos cinco trimestres. Las muestras nuevas de malware para móviles aumentaron un 27 % en el 2.º trimestre, y es el segundo trimestre consecutivo de crecimiento. El malware de minería de monedas sigue muy activo; el total de muestras aumentó un 86 % en el 2.º trimestre, con más de 2,5 millones de archivos nuevos añadidos a la base de datos de malware.

Nos complace anunciar que todas nuestras investigaciones están ahora disponibles en la plataforma McAfee ePolicy Orchestrator® (McAfee ePO™), desde la versión 5.10.0. Esta nueva iniciativa se suma a nuestros canales sociales habituales, que se detallan a continuación, además de a las páginas McAfee Labs y McAfee Advanced Threat Research.

Protéjase. Infórmese.

—Steven Grobman, Director de tecnología (CTO)

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

Twitter

@SteveGrobman

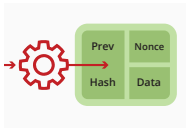
@Raj_Samani

Seguir

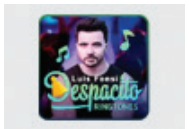
Compartir

Índice

5 ¿Quiere piratear un dispositivo Windows 10 bloqueado? Pregúntele a Cortana (CVE-2018-8140)



6 Informe de amenazas: No participe en la revolución del blockchain sin garantía de protección



7 La banda AsiaHitGroup consigue introducir de nuevo en Google Play aplicaciones de estafas en facturas

9 Estadísticas sobre amenazas

Principales historias del trimestre

¿Quiere piratear un dispositivo Windows 10 bloqueado? Pregúntele a Cortana (CVE-2018-8140)

McAfee Labs y el equipo de McAfee Advanced Threat Research descubrieron una vulnerabilidad en el asistente de voz Cortana en Microsoft Windows 10. El problema, corregido por Microsoft en junio, puede permitir la ejecución no autorizada de código. Nosotros explicamos cómo se puede utilizar esta vulnerabilidad para ejecutar código desde la pantalla bloqueada de una máquina Windows 10 con todos los parches aplicados (RS3 y RS4 antes del parche de junio). En este análisis, abordamos tres vectores de investigación que han sido combinados por Microsoft y que juntos representan CVE-2018-8140. El primero es una fuga de información; terminamos con una demostración de la ejecución completa del código ¡para iniciar una sesión en un dispositivo Windows bloqueado! Enviamos la vulnerabilidad a Microsoft en abril como parte de la política de divulgación responsable del equipo de McAfee Advanced Threat Research.
El responsable del envío de esta vulnerabilidad es Cedric Cochin, Arquitecto de ciberseguridad e Ingeniero jefe.

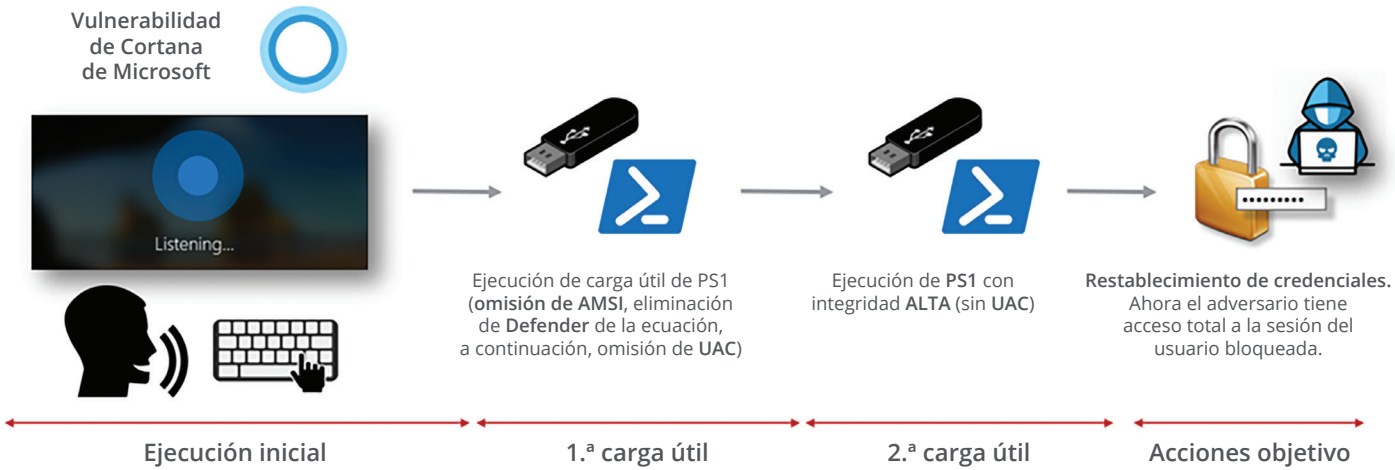


Figura 1. Con cuatro pasos básicos, un agresor puede aprovechar una vulnerabilidad de Cortana para conseguir el control total de un sistema Windows 10.

Seguir
Compartir

Informe de amenazas: No participe en la revolución del blockchain sin garantía de protección

Con la creciente popularidad de las criptomonedas, la revolución del blockchain está en pleno apogeo. Además, los ciberdelincuentes han encontrado nuevas vertientes, como el robo y la minería ilegal de monedas con fines lucrativos. El equipo de McAfee Advanced Threat Research publicó en junio un informe sobre amenazas contra blockchain para explicar las amenazas actuales contra los usuarios e implementadores de tecnologías blockchain.

Aunque no esté familiarizado con la tecnología blockchain, seguro que ha oído hablar de las criptomonedas y, en particular, de Bitcoin, la implementación más conocida. Las criptomonedas se basan en la tecnología blockchain, que registra las transacciones de forma no centralizada y facilita una especie de "libro de contabilidad" de confianza entre participantes que no son de confianza. Cada bloque del libro de contabilidad está vinculado con el siguiente, lo crea una cadena, de ahí el nombre en inglés. Gracias a esta cadena, cualquiera puede validar todas las transacciones, sin tener que recurrir a una fuente externa. Esto hace posible las monedas descentralizadas, como Bitcoin. En este informe, analizamos los principales vectores de ataque: phishing, malware, vulnerabilidades de implementación y tecnología.

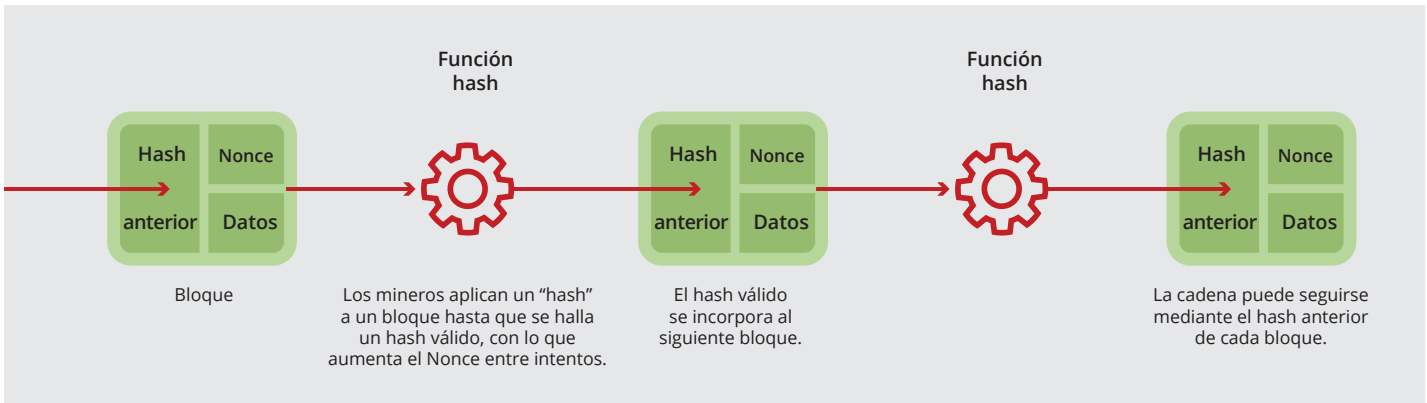


Figura 2. Un blockchain de prueba de trabajo, que se basa en cada hash anterior. Fuente: https://bitcoin.org/bitcoin.pdf

Seguir

Compartir

La banda AsiaHitGroup consigue introducir de nuevo en Google Play aplicaciones de estafas en facturas

El equipo de McAfee Mobile Research descubrió una nueva campaña de fraudes en la facturación con al menos 15 aplicaciones publicadas en 2018 en Google Play. El fraude telefónico (que incluye el fraude en la facturación) es una categoría destacada de aplicaciones potencialmente dañinas en Google Play, según el informe "Android Security 2017 Year in Review" (Seguridad de Android. Revisión del año 2017). Esta nueva campaña demuestra que los ciberdelincuentes siguen encontrando nuevas formas de robar dinero a sus víctimas mediante el empleo de apps en tiendas oficiales, como Google Play. Los responsables de esta campaña, AsiaHitGroup, llevan en activo como mínimo desde finales de 2016 con la distribución del instalador falso de aplicaciones Sonvpay.A, que intentó cobrar al menos a 20 000 víctimas, principalmente de Tailandia y Malasia, por la descarga de copias de aplicaciones populares. Un año más tarde, en noviembre de 2017, se descubrió una nueva campaña en Google Play, Sonvpay.B, que utilizaba la geolocalización de direcciones IP para confirmar el país de la víctima y añadía víctimas rusas al fraude de facturación a fin de incrementar sus posibilidades de robar dinero a usuarios desprevenidos. Nuestra investigación explica cómo funciona el malware en estas campañas.

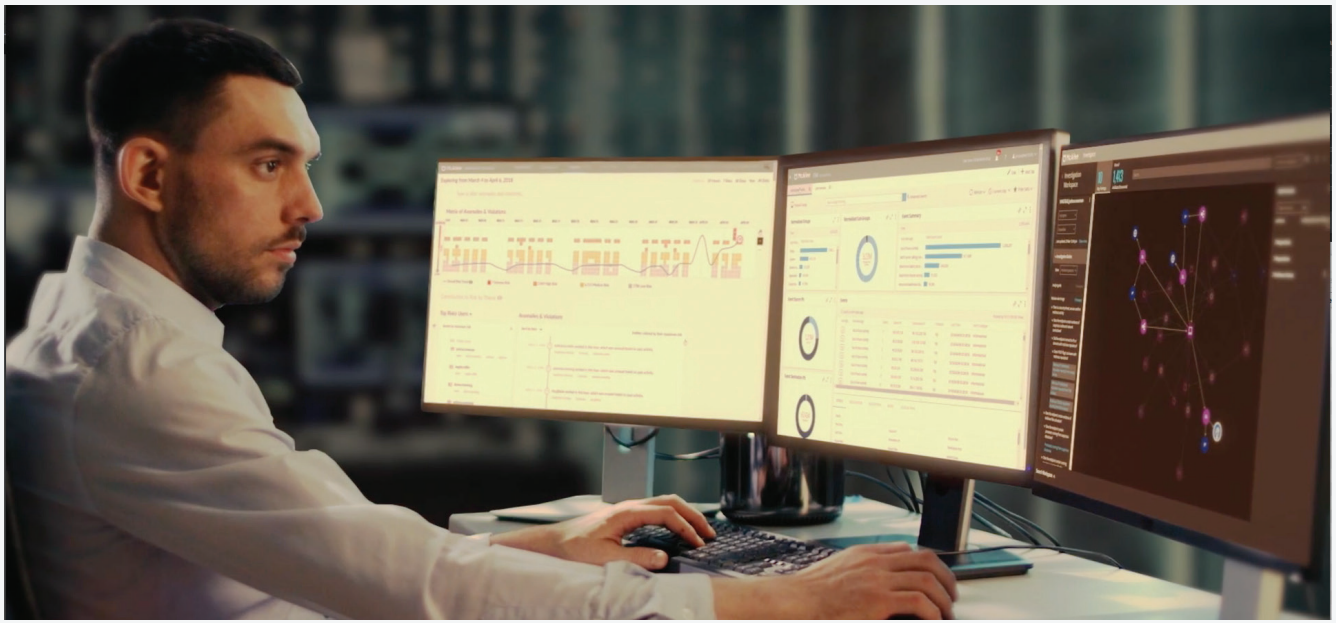
Figura 3. Apps maliciosas de AsiaHitGroup que se encontraban antes en Google Play.

Seguir

Compartir

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 recibió, de media, 49 000 millones de consultas y 13 000 millones de líneas de telemetría, mientras analizaba 1 800 000 URL y 800 000 archivos, además de otros 200 000 archivos en un entorno aislado.

- Las protecciones de McAfee GTI contra archivos maliciosos comunicaron que, de los 86 millones de archivos que se comprobaron en el 2.º trimestre, 86 000 (el 0,1 %) resultaron ser peligrosos.
- Las protecciones de McAfee GTI frente a URL maliciosas comunicaron que de los 73 millones de URL comprobadas en el 2.º trimestre, 365 000 (el 0,5 %) resultaron ser peligrosas.
- Las protecciones de McAfee GTI frente a direcciones IP maliciosas comunicaron que de los 67 millones que se comprobaron en el 2.º trimestre, 268 000 (el 0,4 %) resultaron ser peligrosas.

Seguir

Compartir

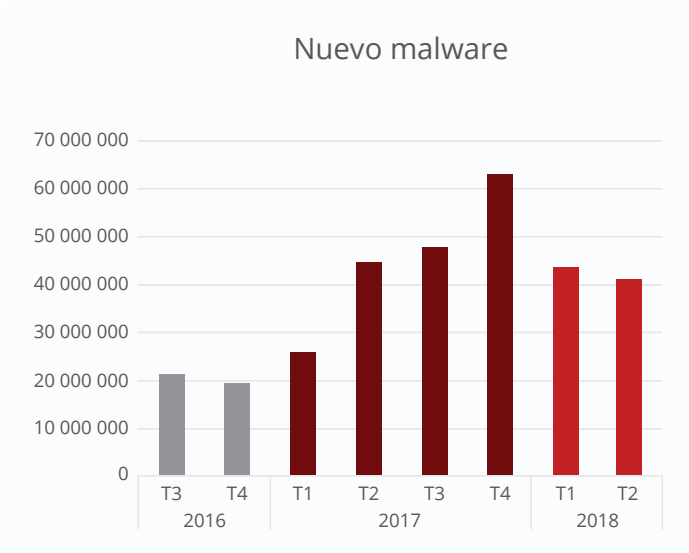
Estadísticas sobre amenazas

10 Malware

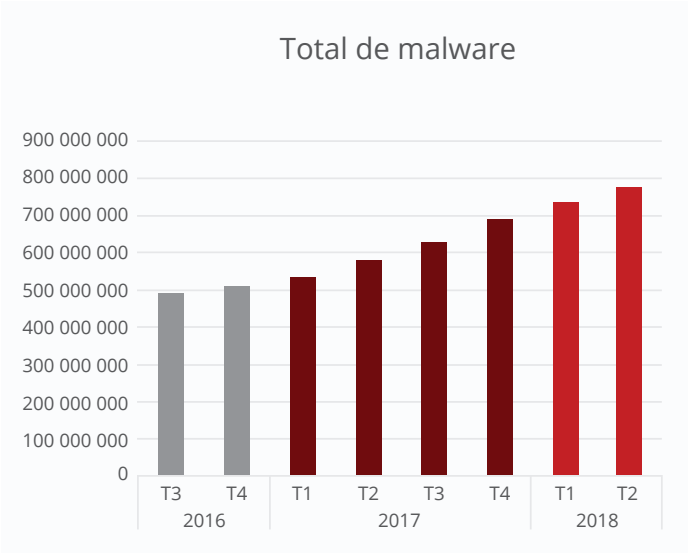
17 Incidentes

19 Amenazas en la Web y la red

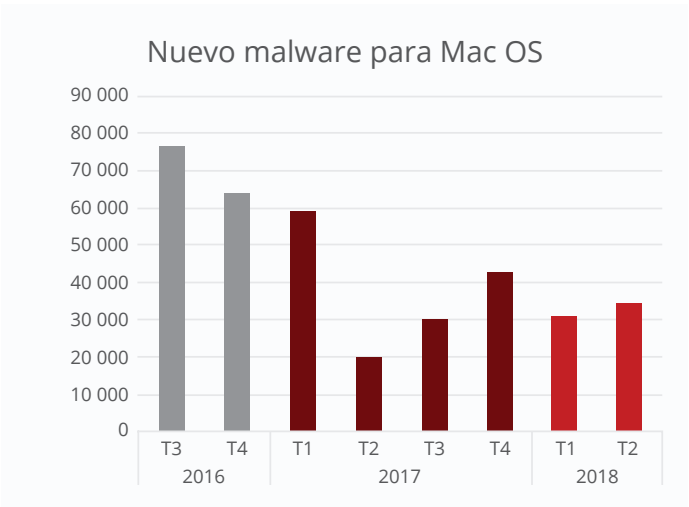
Malware



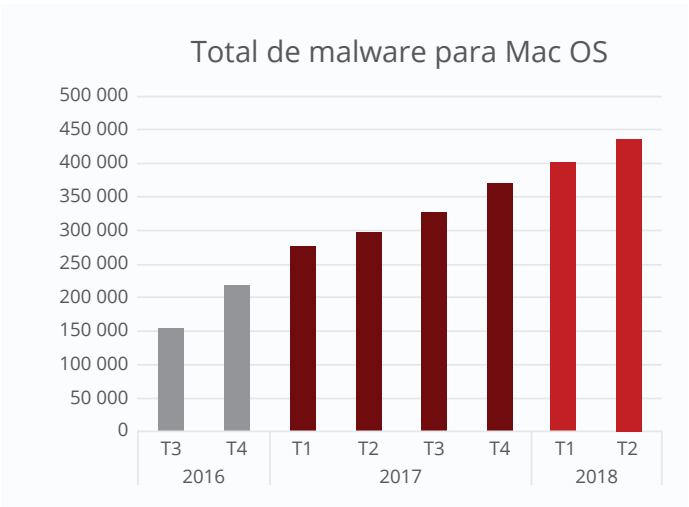
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.

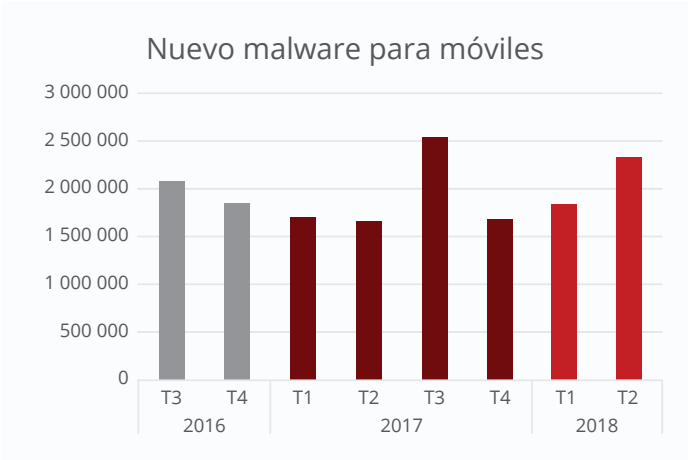


Fuente: McAfee Labs, 2018.

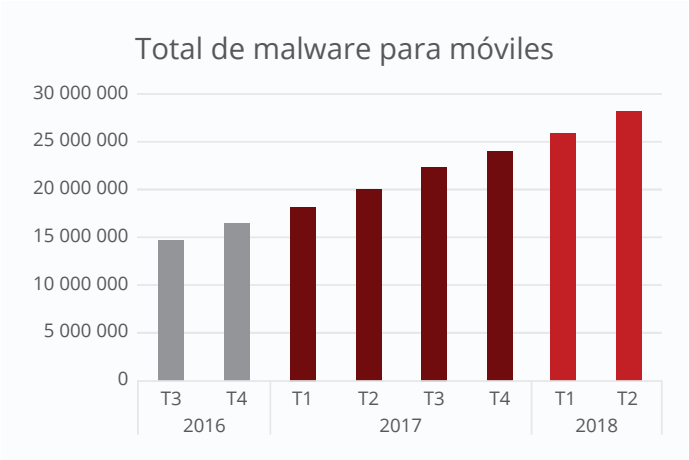
Los datos del malware proceden de la base de datos de muestras de McAfee, McAfee Sample Database, que incluye archivos maliciosos obtenidos de trampas para spam (*spam traps*) de McAfee, rastreadores de la Web (*crawlers*) o envíos de clientes, así como de otras fuentes del sector.

Seguir

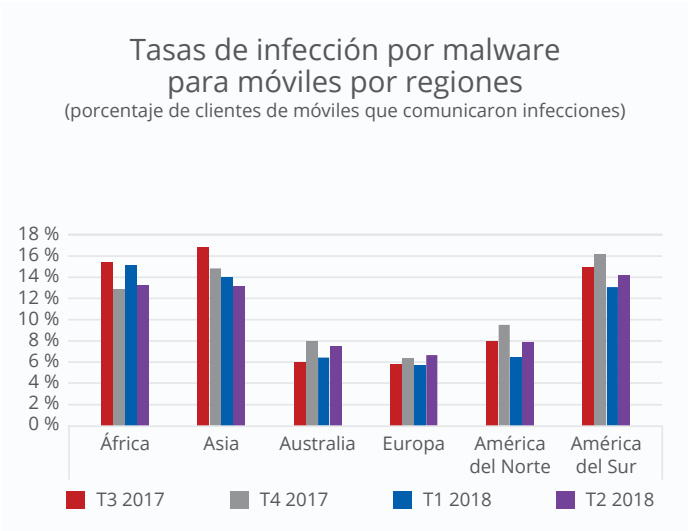
Compartir



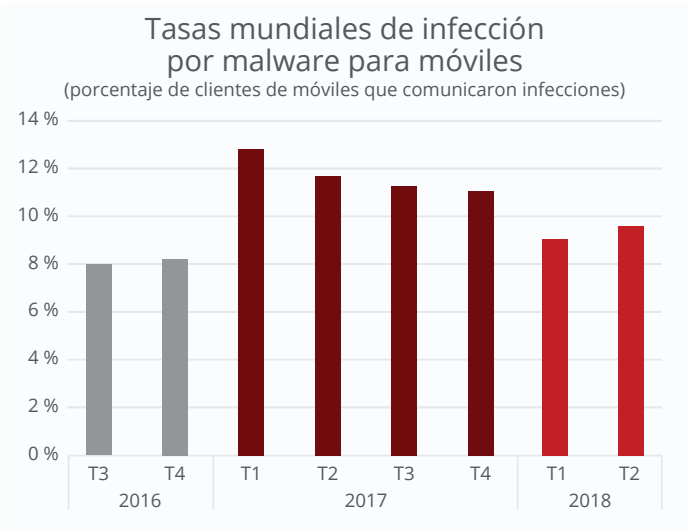
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



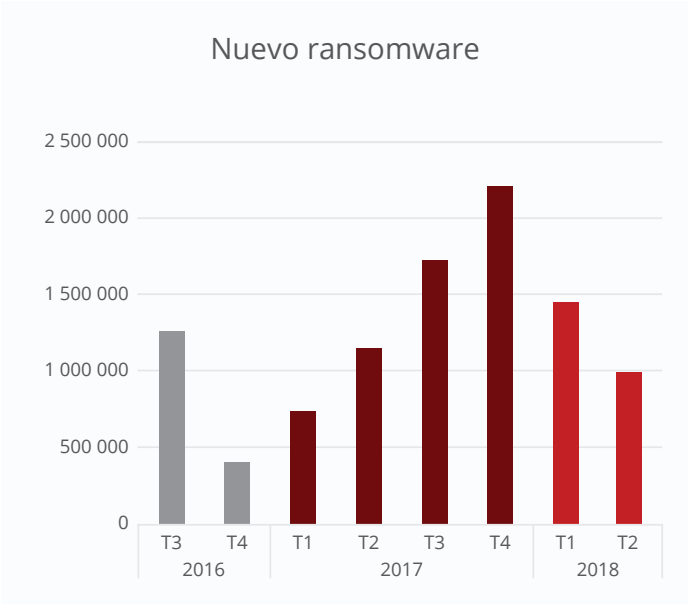
Fuente: McAfee Labs, 2018.



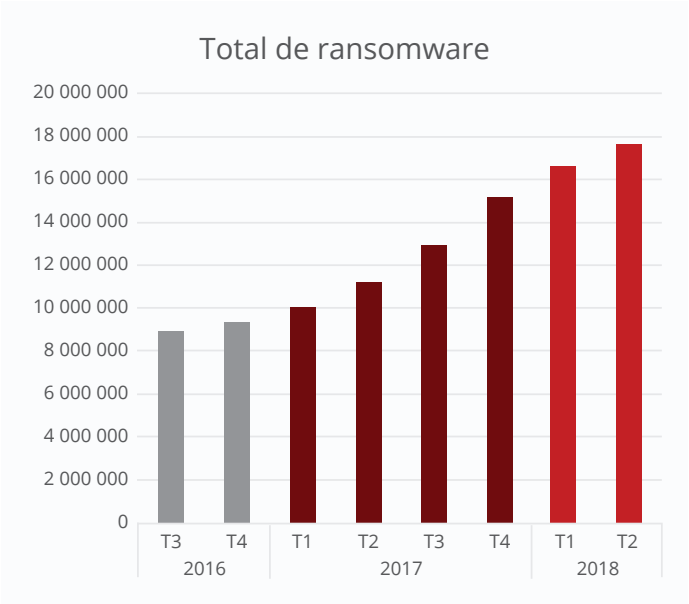
Fuente: McAfee Labs, 2018.

Seguir

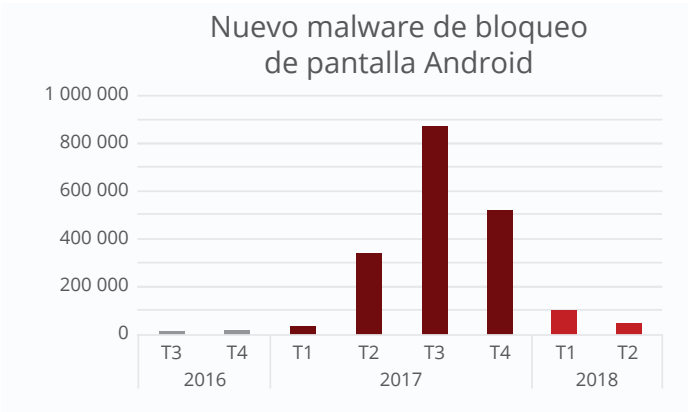
Compartir



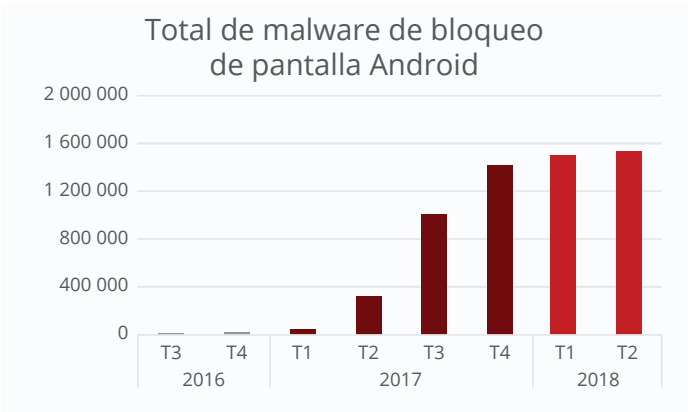
Fuente: McAfee Labs, 2018.



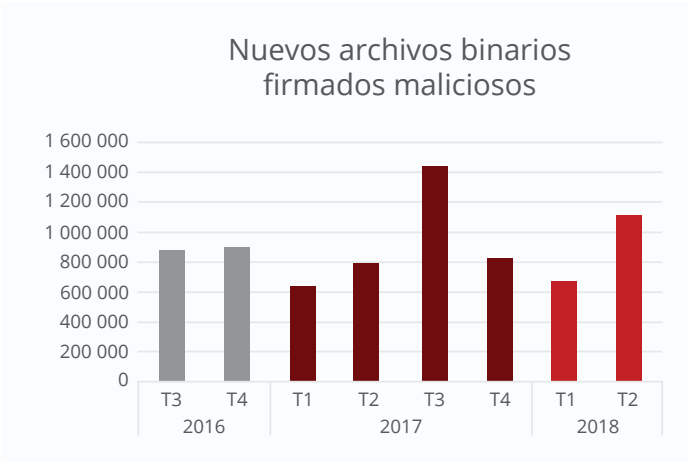
Fuente: McAfee Labs, 2018.



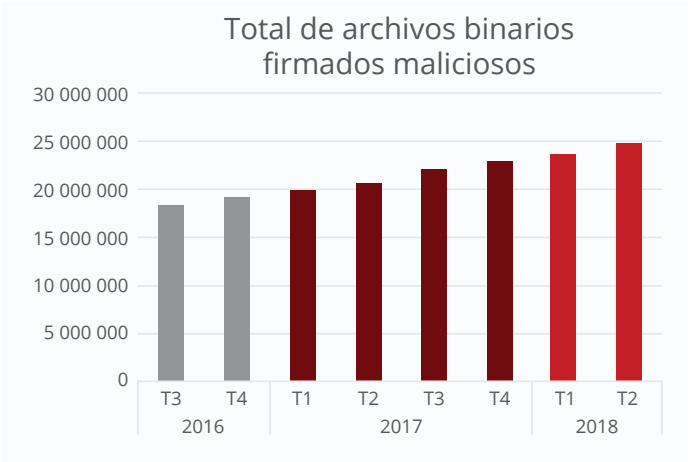
Fuente: McAfee Labs, 2018.



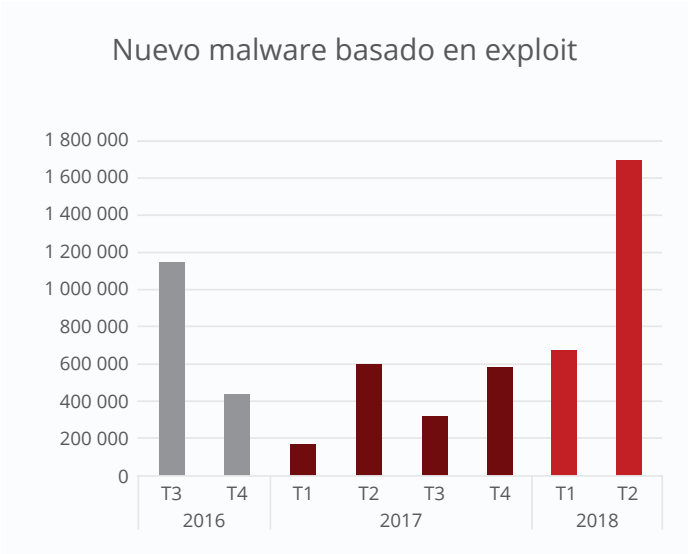
Fuente: McAfee Labs, 2018.



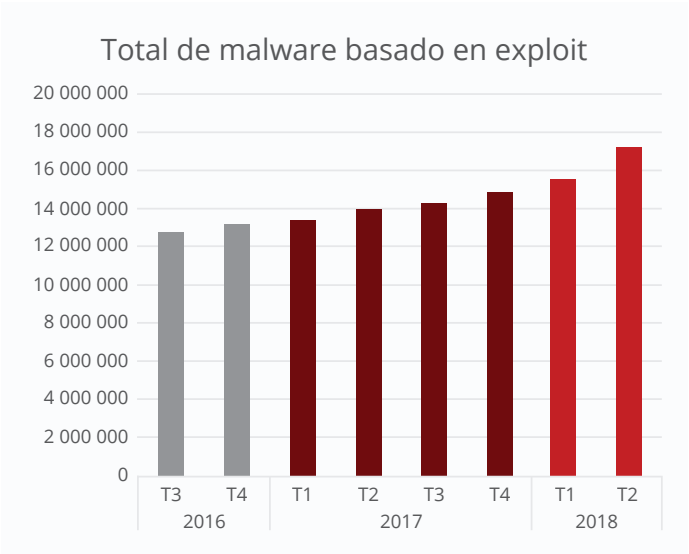
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



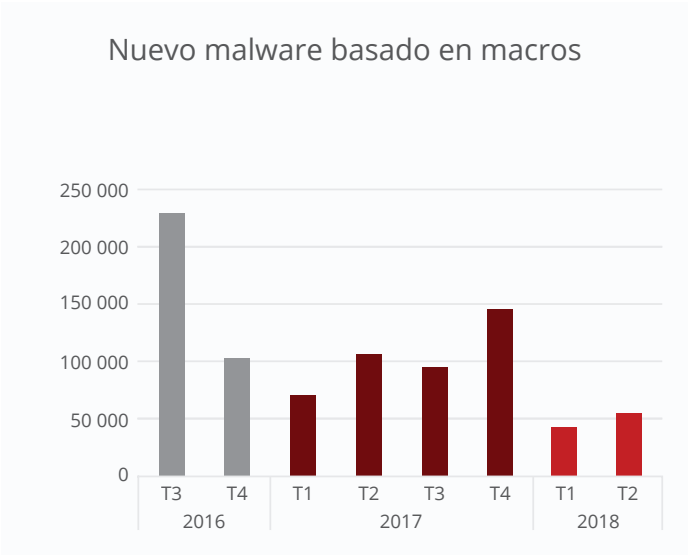
Fuente: McAfee Labs, 2018.

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.

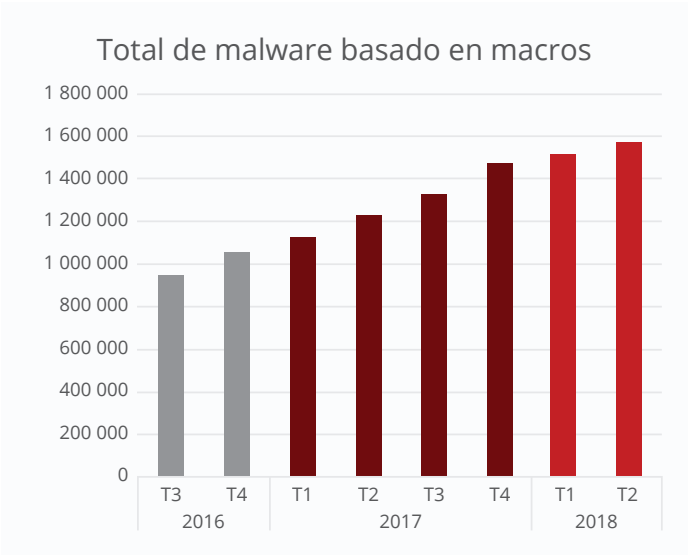
Los exploits aprovechan los errores y vulnerabilidades del software y el hardware. Los ataques de tipo zero-day son ejemplos de exploits que consiguen sus objetivos. Se incluye un ejemplo en el artículo de McAfee Labs "Analyzing Microsoft Office Zero-Day Exploit CVE-2017-11826: Memory Corruption Vulnerability"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

Seguir

Compartir

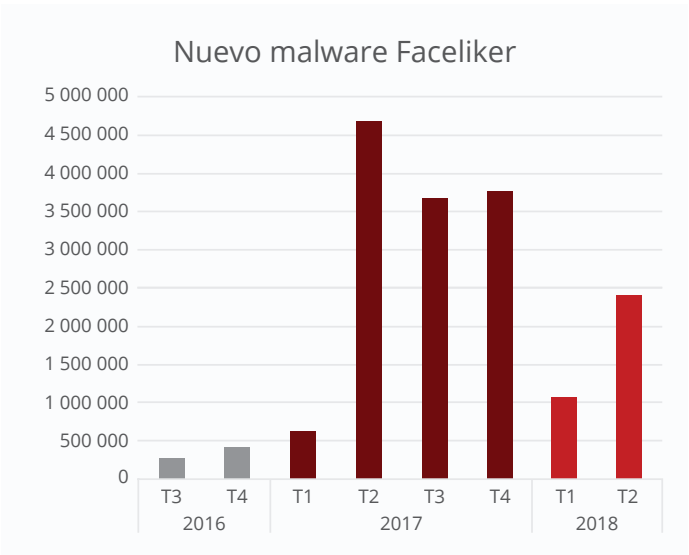


Fuente: McAfee Labs, 2018.

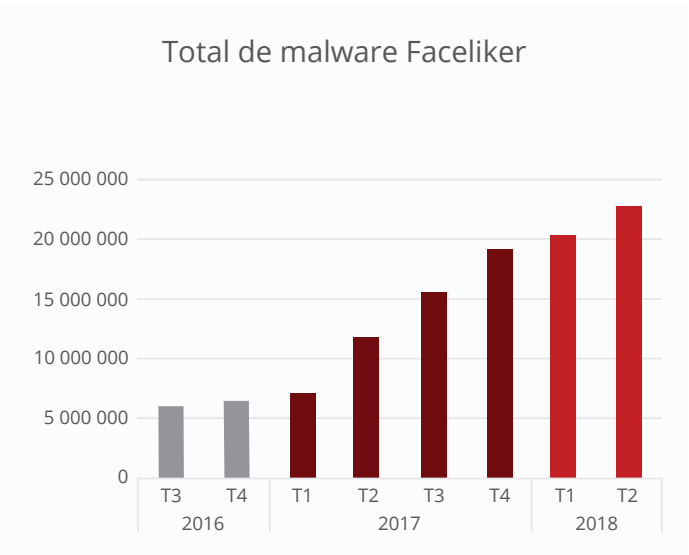


Fuente: McAfee Labs, 2018.

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.

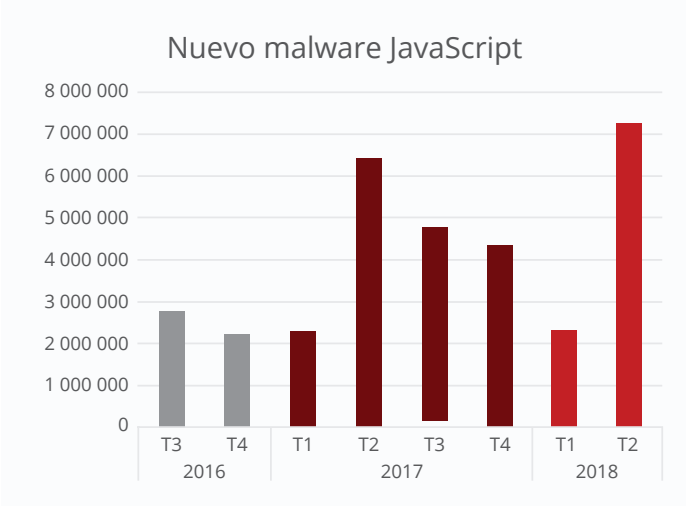


Fuente: McAfee Labs, 2018.

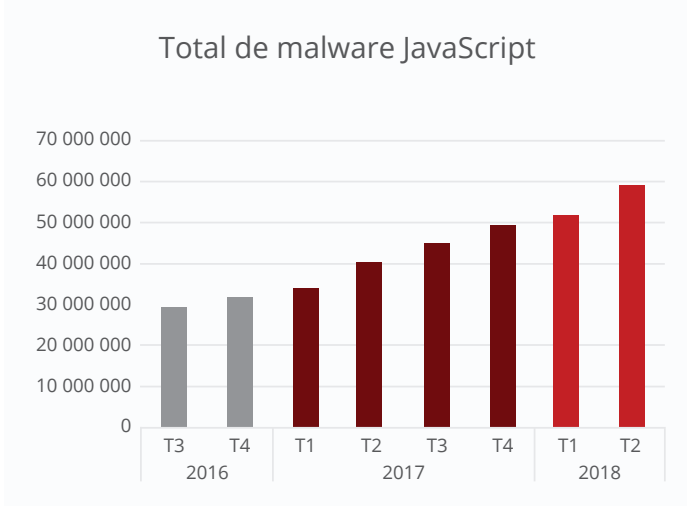
El troyano Faceliker manipula los clics que hacen los usuarios en Facebook, con el objetivo de aumentar artificialmente el número de "Me gusta" de determinado contenido. Para más información, lea este artículo de McAfee Labs.

Seguir

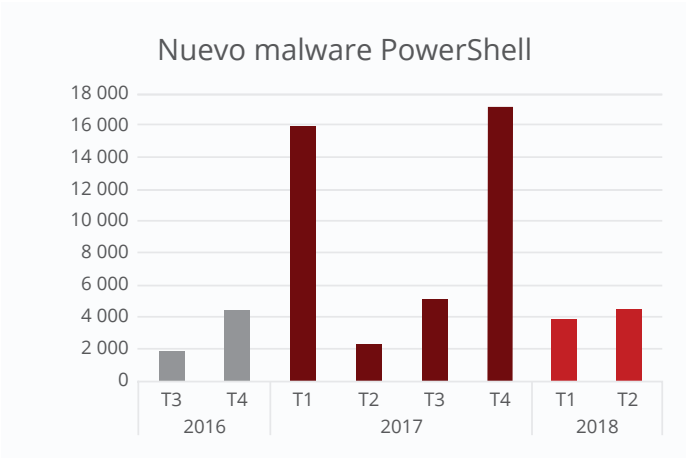
Compartir



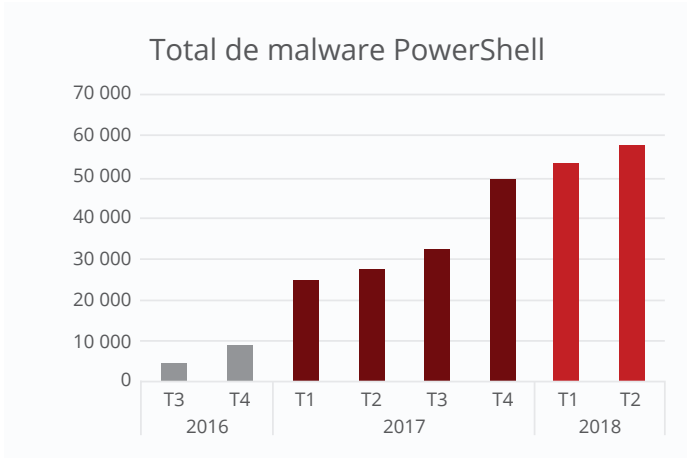
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.

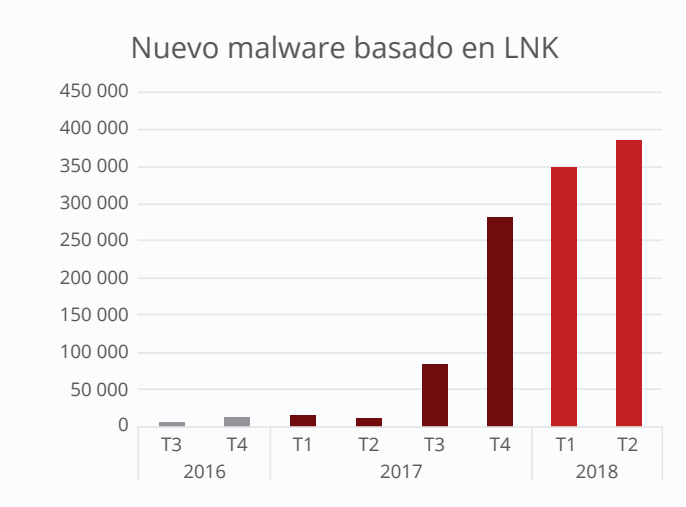


Fuente: McAfee Labs, 2018.

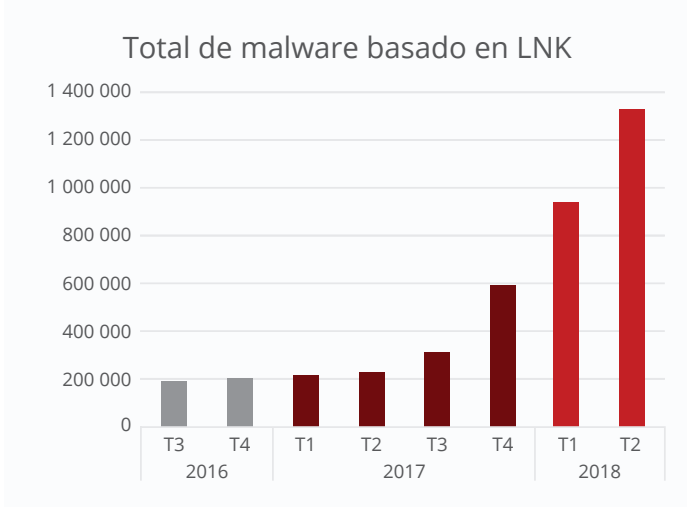
Para obtener más información sobre amenazas basadas en PowerShell y JavaScript, consulte el apartado "El auge del malware basado en scripts" de un *Informe de McAfee Labs sobre amenazas* anterior

Seguir

Compartir

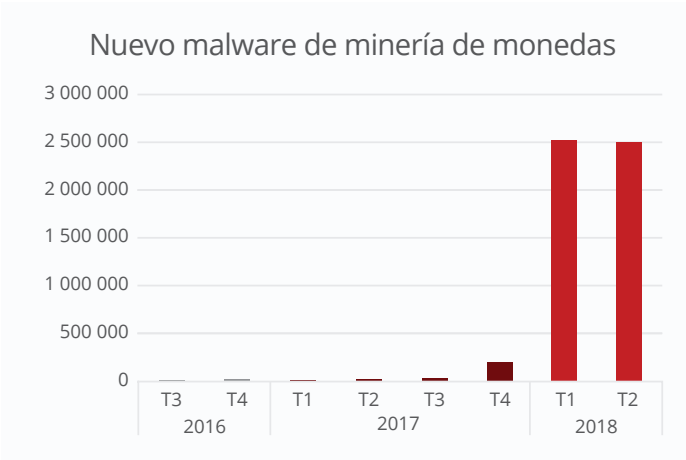


Fuente: McAfee Labs, 2018.

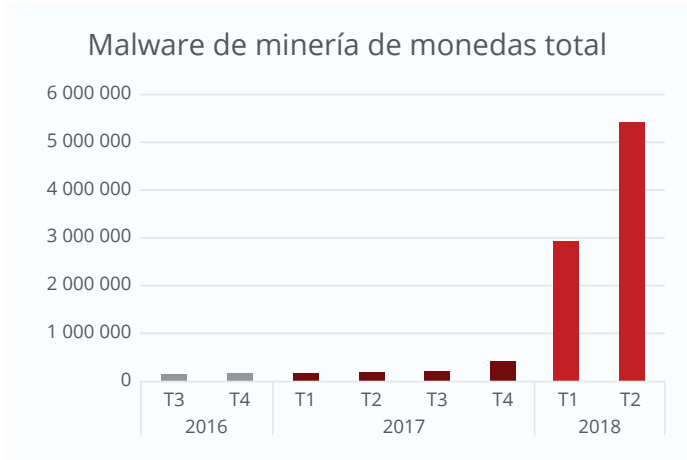


Fuente: McAfee Labs, 2018.

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.



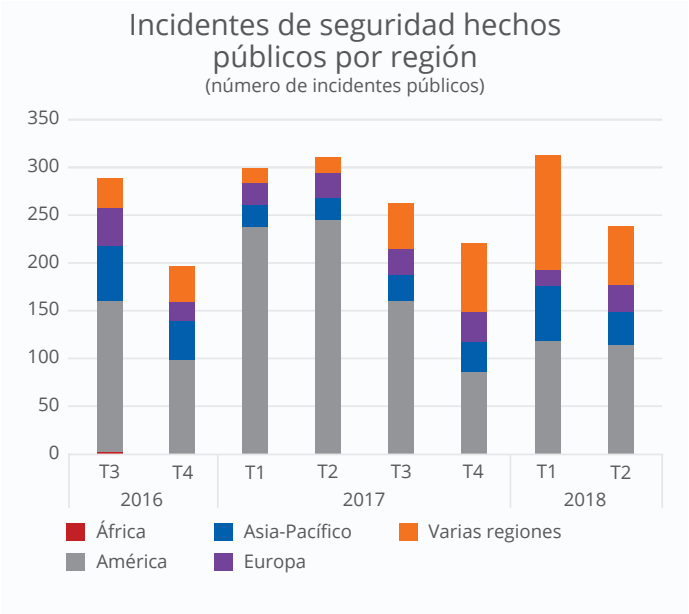
Fuente: McAfee Labs, 2018.

El malware de minería de monedas secuestra los sistemas para crear criptomonedas ("minar"), sin el consentimiento ni el conocimiento de las víctimas. Las amenazas de minería de monedas nuevas se dispararon a gran escala en 2018.

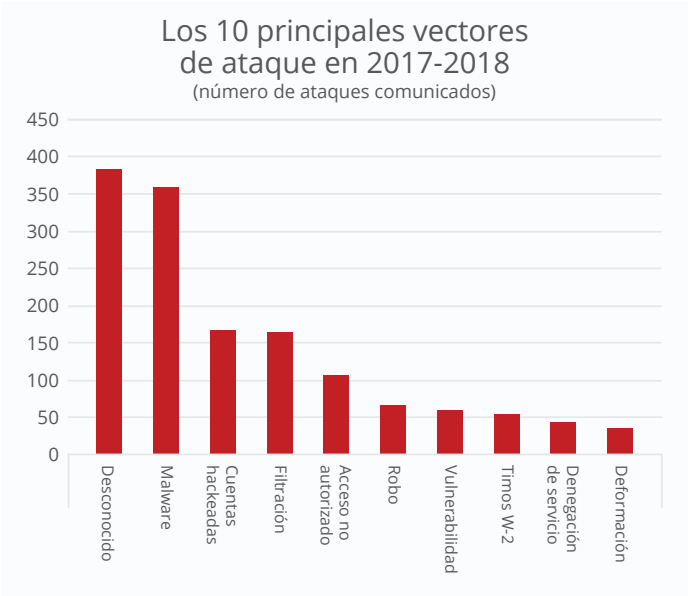
Seguir

Compartir

Incidentes



Fuente: McAfee Labs, 2018.



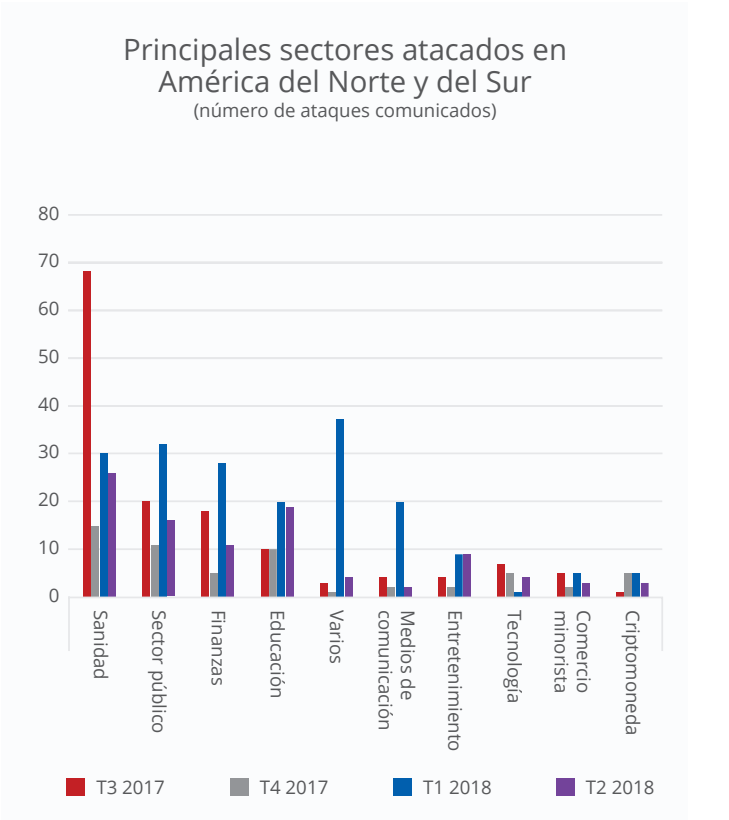
Fuente: McAfee Labs, 2018.

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

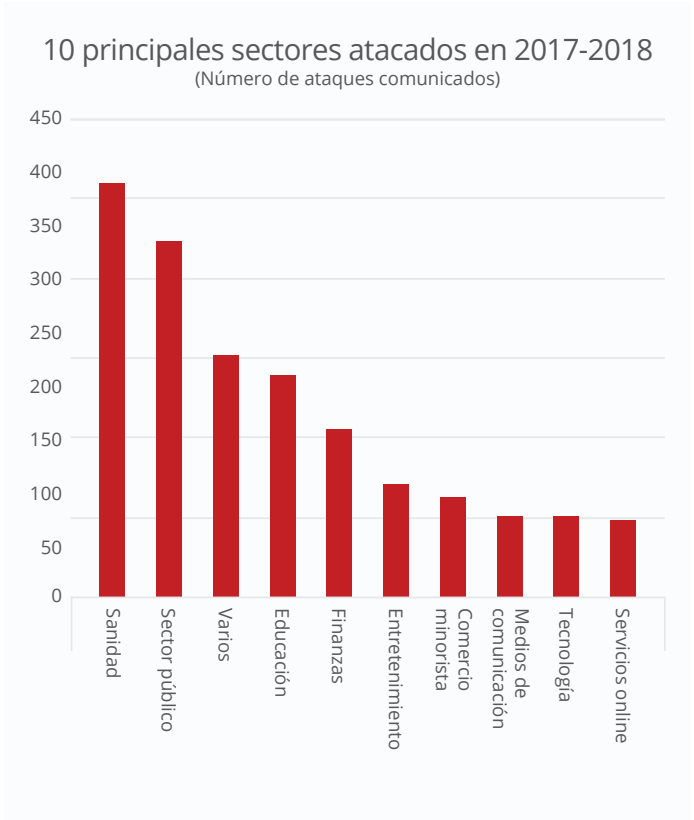
La mayoría de los vectores de ataque no se conocen o bien no se han hecho públicos.

Seguir

Compartir



Fuente: McAfee Labs, 2018.

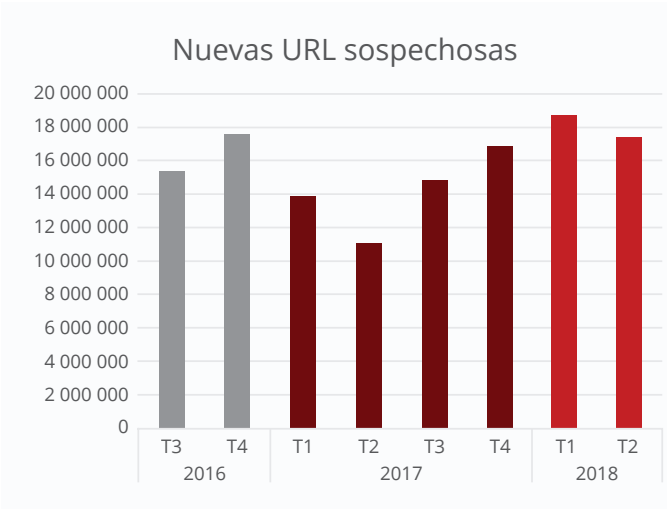


Fuente: McAfee Labs, 2018.

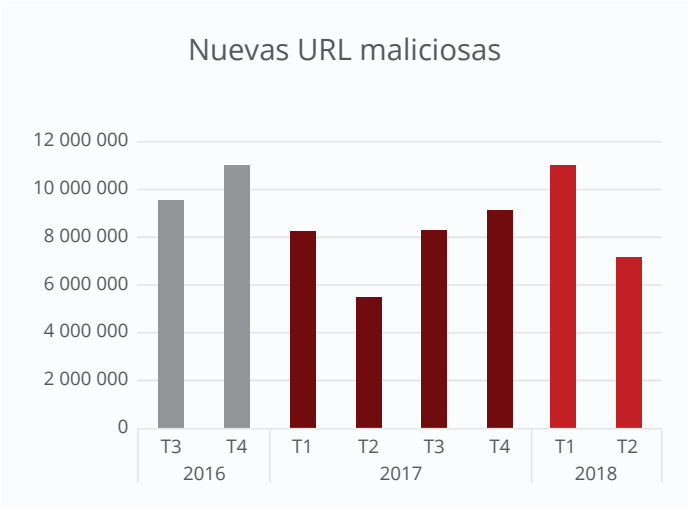
Seguir

Compartir

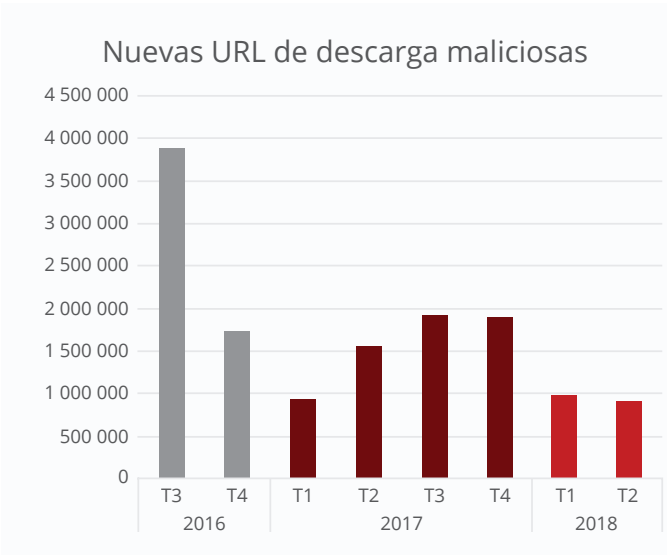
Amenazas en la Web y la red



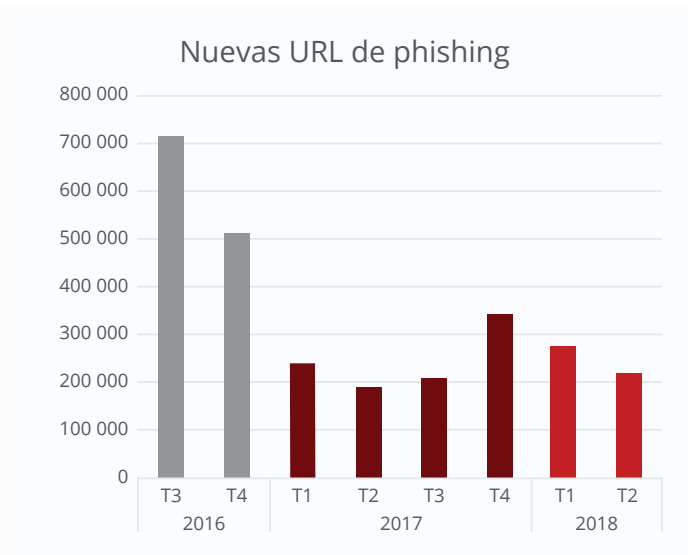
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.



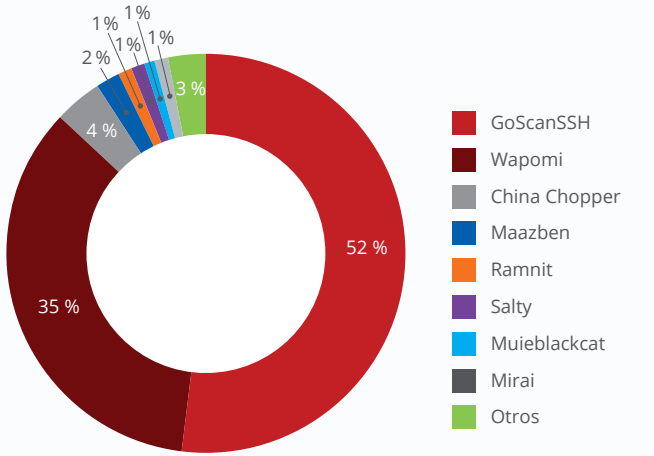
Fuente: McAfee Labs, 2018.



Fuente: McAfee Labs, 2018.

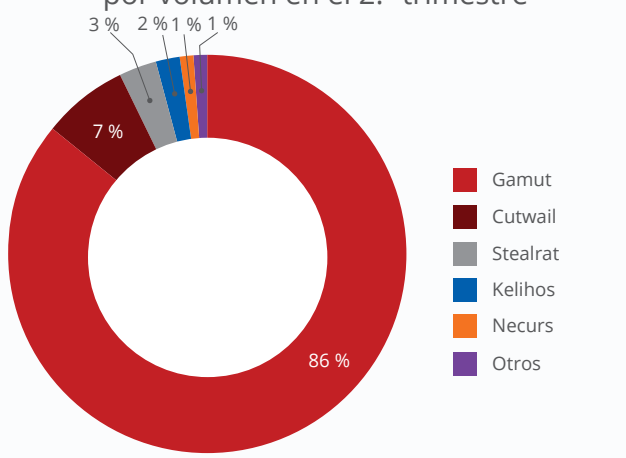
La base de datos de la Web de McAfee® TrustedSource™ contiene URL (páginas web) organizadas en categorías según su reputación web, con el fin de utilizarlas en directivas de filtrado para gestionar el acceso a la Web. Las URL sospechosas son el total de sitios con una calificación de riesgo alto o medio. 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.

Principal malware que se conectó a los servidores de control en el 2.º trimestre



Fuente: McAfee Labs, 2018.

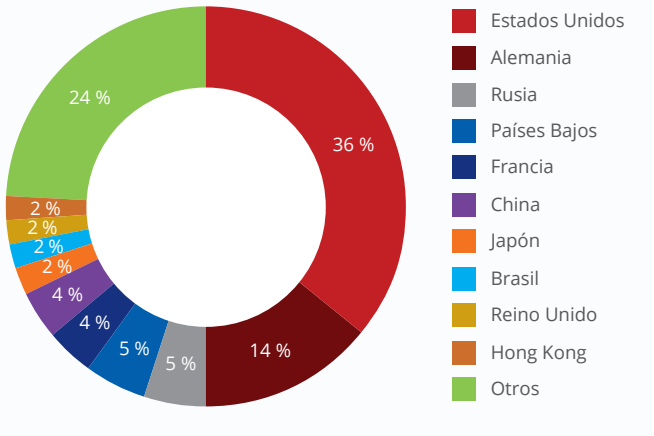
Prevalencia de redes de bots de spam por volumen en el 2.º trimestre



Fuente: McAfee Labs, 2018.

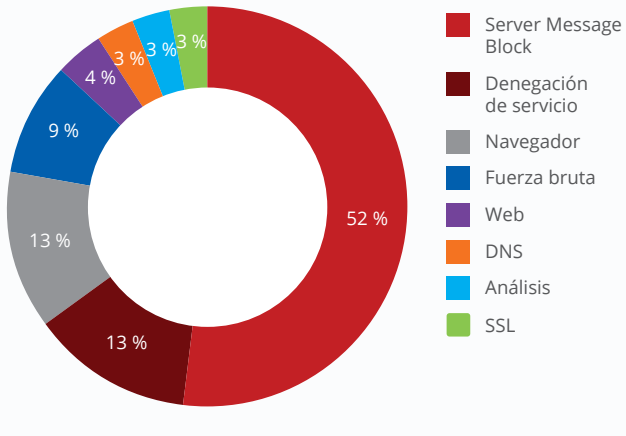
La red de bots de spam Gamut superó con creces a todas las demás durante el 2.º trimestre. Concretamente, incrementó notablemente el número de timos relacionados con la administración fiscal canadiense ("Canada Revenue Agency"). Hay campañas recientes relacionadas con ofertas de empleo falsas que se utilizan con frecuencia como una táctica de captación de intermediarios para transferir dinero.

Principales países que albergan servidores de control de redes de bots en el 2.º trimestre



Fuente: McAfee Labs, 2018.

Principales ataques a redes en el 2.º trimestre



Fuente: McAfee Labs, 2018.

Seguir

Compartir

Acerca de McAfee

McAfee es la empresa de ciberseguridad que ofrece protección total, desde los dispositivos a la nube. Inspirándose en el poder de la colaboración, McAfee crea soluciones para empresas y particulares 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 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