McAfee Labs
Informe sobre amenazas

Noviembre de 2014

intel Security

Acerca de McAfee Labs

McAfee Labs es uno de los líderes mundiales en investigación e información sobre amenazas, e innovación en ciberseguridad. Gracias a la información de millones de sensores sobre los principales vectores de amenazas: archivos, la Web, la mensajería y las redes, McAfee Labs proporciona información sobre amenazas en tiempo real, análisis críticos y opiniones de expertos para mejorar la protección y reducir los riesgos. McAfee forma parte ahora de Intel Security.

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

Siga a McAfee Labs

Introducción

Las vacaciones de Navidad están a la vuelta de la esquina y ya hay más de uno dispuesto a arruinarlas con sus malas artes. McAfee ha publicado hace poco el documento ***Los 12 timos de las Navidades***, una lista en la que se recogen algunas de estas artimañas. Es un texto de lectura muy amena y muy recomendable. También hemos empezado a desvelar nuestras predicciones para 2015; desde el rumbo que va a tomar la economía global hasta cuáles serán las estrellas de Hollywood más populares.

McAfee Labs lleva ya varios años dando a conocer sus predicciones en nuestra área de especialidad. En el **informe de predicciones sobre amenazas del año pasado**, fuimos muy certeros. Por ejemplo, predijimos con acierto que el ransomware aumentaría, incluso en plataformas móviles, que los ataques de tintes políticos serían más frecuentes y que las empresas apostarían fuertemente por los servicios de inteligencia sobre amenazas y las herramientas analíticas para identificar amenazas cada vez más furtivas. Pero, obviamente, no somos perfectos y algunas de nuestras predicciones no fueron del todo acertadas. Suele ocurrir cuando se intentan prever tendencias de esta naturaleza.

Este año, hemos decidido adelantar nuestras predicciones de amenazas para 2015 e incluirlas en este informe. Con ello pretendemos que nuestros clientes tengan más tiempo para reflexionar sobre qué les espera en 2015 y prepararse para las amenazas más importantes. Por supuesto, continuaremos incluyendo los temas principales y las estadísticas sobre amenazas, como siempre, en nuestros informes trimestrales.

Este trimestre proponemos como tema principal BERserk, una vulnerabilidad del software de verificación de firmas RSA que los ciberdelincuentes podrían aprovechar para lanzar sus ataques de muy diversas formas. Cuando McAfee dio a conocer BERserk, la difusión pública de **Shellshock** logró más trascendencia y alarma, pero el daño potencial de esta vulnerabilidad es igualmente destacable. Encontrará más información sobre BERserk **aquí**. En un artículo relacionado, discutimos cómo los ciberdelincuentes se aprovechan de la confianza de los usuarios. Nos recuerda que estar informados y concienciados es crucial para combatir este tipo de amenazas.

Al leer este informe advertirá que hemos añadido nuevos gráficos y cambiado otros en la sección de estadísticas sobre amenazas. En sus comentarios, los lectores nos sugerían añadir estadísticas que consideraban importantes. Además, estamos empezando a aprovechar mejor los informes de nuestros propios sistemas para obtener gráficos más precisos. Esperamos que estos cambios y novedades sean de su agrado.

Quisiéramos agradecer a todos los que participaron en nuestra encuesta para los lectores del ***informe sobre amenazas de agosto***. Nos tomamos muy en serio sus opiniones, buena prueba de ello son todas estas mejoras que hemos introducido. Si desea decirnos qué piensa de este informe, haga clic **aquí** para completar una encuesta de apenas cinco minutos sobre el último *informe sobre amenazas.*

Le deseamos que pase unas Felices Fiestas junto a sus seres queridos.

—Vincent Weafer, Vicepresidente primero, McAfee Labs

Índice

Informe sobre amenazas de McAfee Labs
Noviembre de 2014

En la investigación y redacción de este informe han participado:

Cedric Cochin
Benjamin Cruz
Michelle Dennedy
Aditya Kapoor
Dan Larson
Haifei Li
Chris Miller
Igor Muttik
François Paget
Eric Peterson
Mary Salvaggio
Craig Schmugar
Ryan Sherstobitoff
Rick Simon
Dan Sommer
Bing Sun
Vinoo Thomas
Ramnath Venugopalan
James Walter
Adam Wosotowsky
Stanley Zhu

Resumen ejecutivo

Predicciones sobre amenazas para 2015 - McAfee Labs

Este *informe sobre amenazas* comienza con las predicciones que hemos realizado para 2015. Dichas predicciones abarcan temas muy variados e incluyen opiniones sobre el Internet de las cosas, el ciberespionaje, los dispositivos móviles, la privacidad y el ransomware, entre otros.

BERserk: golpe directo a la fiabilidad de las conexiones

BERserk aprovecha un fallo del software de verificación de firmas RSA para dejar el paso libre a los ciberdelincuentes, que pueden lanzar ataques de intermediario sin que los usuarios lo adviertan.

En septiembre, **Intel Security reveló detalles** sobre una grave vulnerabilidad denominada BERserk, que confirmaban el código subyacente que la origina. En el momento de elaborar este informe, aún se desconoce la verdadera trascendencia de BERserk, pero restarle importancia sería un gran error. BERserk aprovecha un fallo del software de verificación de firmas RSA para dejar el paso libre a los ciberdelincuentes, que pueden lanzar ataques de intermediario sin que los usuarios lo adviertan. Sabemos que accedemos a un sitio web de confianza cuando vemos "https" al inicio de una URL y el familiar icono de candado para blindar la transacción. BERserk pone en riesgo la conexión y permite a los delincuentes observar y hacer lo que les apetezca con la información intercambiada entre el usuario y el sitio web.

Abuso de confianza: ataque al eslabón más débil de la seguridad online

McAfee Labs cree que la confianza en muchas de las formas de interacción online terminará por parecerse al correo electrónico, que despierta recelos sobre su autenticidad.

Los usuarios son los eslabones más débiles en la mayoría de las configuraciones de seguridad. Guardamos gran parte de nuestra información en nuestros dispositivos y confiamos en ellos para obtener datos concretos de una forma segura. Pero los delincuentes a menudo se aprovechan de esta confianza que depositamos en nuestros dispositivos y la usan para robarnos información. Este tema principal aborda el abuso de la confianza y explica mediante ejemplos recientes las numerosas formas que tienen los ciberdelincuentes para aprovecharse de nuestra tendencia a ser confiados. McAfee Labs cree que la confianza en muchas de las formas de interacción online terminará por parecerse al correo electrónico, cuya autenticidad despierta no pocos recelos.

Comparta este informe

Predicciones sobre amenazas para 2015 - McAfee Labs

Compartir opinión

Ciberespionaje

Los ataques de ciberespionaje serán cada vez más frecuentes. Los delincuentes establecidos se convertirán en avezados cazadores furtivos de la información y los que empiecen a delinquir buscarán formas de robar dinero y fastidiar a sus adversarios.

Los países pequeños y los grupos terroristas internacionales combatirán en auténticas guerras en el ciberespacio. Sus ataques se basarán en devastadoras tácticas de denegación de servicio o en el uso de malware que borra los registros de arranque maestro para destruir las redes de sus enemigos. En paralelo, los delincuentes expertos en el ciberespionaje implementarán mejores métodos para permanecer ocultos en la red de una víctima, como tecnologías de camuflaje más sofisticadas y otros medios para infiltrarse en capas inferiores al sistema operativo sin ser vistos.

En concreto, McAfee Labs observa ahora cómo los sofisticados ciberdelincuentes de Europa del Este dejarán los ataques rápidos y directos dirigidos a las credenciales de los clientes de instituciones financieras (que facilitan robos financieros) para pasar a estrategias más evolucionadas de amenazas persistentes avanzadas (APT), con las que obtendrán datos que podrán vender o usar cuando lo consideren. De esta forma, se configura un sofisticado escenario criminal típico del ciberespionaje entre países, en el que los delincuentes se apostan hasta esperar el momento oportuno para hacerse con la información confidencial.

En el sector comercial, se está empezando a ver una situación similar. Muchos comerciantes recopilan perfiles detallados de sus clientes, en los que se incluyen datos de contacto, hábitos de compra, intereses, historial de crédito y ubicación, etc. Además, los planes financieros, operacionales y estratégicos que les han servido a estos comerciantes pueden resultar muy valiosos para la competencia. Algunos ciberdelincuentes parecen estar usando una táctica de ciberespionaje basada en APT para infiltrarse en los sistemas de los comercios, de donde obtienen subrepticiamente otros datos, aparte de los de tarjetas de crédito, que posteriormente venden al mejor postor.

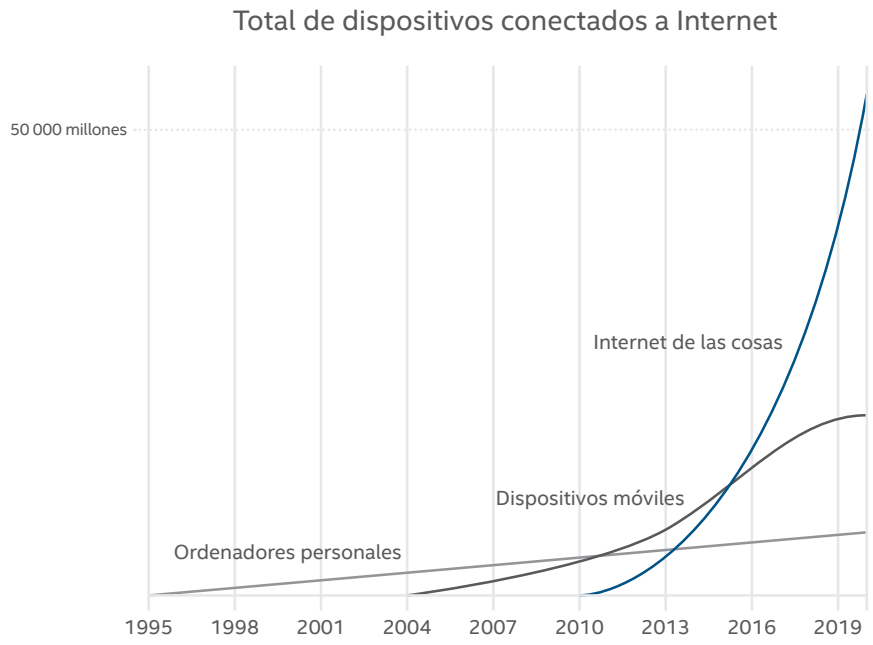
—Ryan Sherstobitoff

Internet de las cosas

Los ataques a los dispositivos conectados, lo que se conoce como el "Internet de las cosas" (o, del inglés, IoT), proliferarán rápidamente debido al gran aumento de objetos conectados, las pésimas prácticas de seguridad y el alto valor de los datos almacenados en estos dispositivos.

En el contexto del "Internet de las cosas", el número y la diversidad de objetos conectados están creciendo de forma exponencial. Dentro del ámbito de los consumidores, los electrodomésticos, los automóviles, la domótica e incluso las bombillas forman parte de estos objetos conectados. Por lo que respecta a las empresas, estos dispositivos están indicados en numerosas aplicaciones orientadas a sectores tan diversos como agricultura, fabricación y atención sanitaria. Los dispositivos IoT integran cada vez más componentes de software y hardware, lo que supone una complejidad añadida y el consiguiente detrimento de la seguridad.

Estos componentes, y por ende los propios dispositivos, no suelen desarrollarse con la seguridad como prioridad básica. La combinación de la arrolladora irrupción de los dispositivos IoT y la fragilidad de la seguridad representa una amenaza creciente para la privacidad y seguridad de los individuos y las empresas.



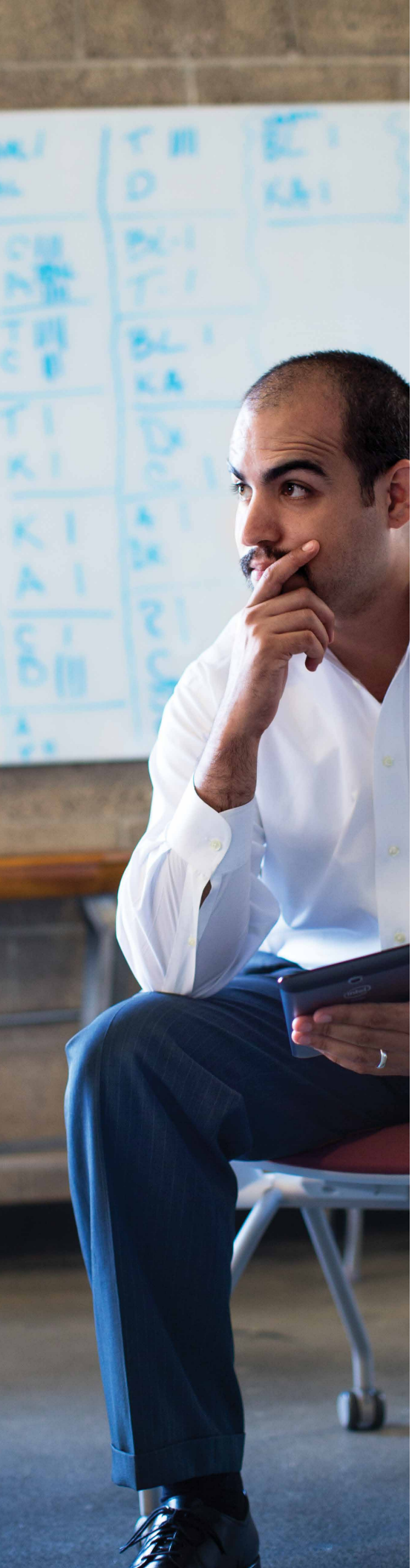
Fuentes: McAfee, basado en estudio de BI Intelligence, IDC e Intel.

Los ataques a los dispositivos IoT ya son una práctica común, desde cámaras IP con controles de seguridad insuficientes a medidores inteligentes con defectos de cifrado básicos, pasando por los dispositivos SCADA que alimentan infraestructuras críticas en todo el mundo. En España, por ejemplo, los contadores eléctricos conectados en red e instalados en millones de hogares tienen vulnerabilidades que los delincuentes pueden aprovechar para generar facturas falsas o incluso causar apagones. El año pasado, en una conferencia para hackers de "sombrero blanco", los investigadores demostraron cómo algunas cámaras de seguridad conectadas a Internet pueden manipularse fácilmente, de modo que es posible tanto robar el vídeo de las cámaras como acceder a la red a las que están conectadas.

Hay un tipo de amenaza especialmente alarmante: con la creciente aparición de dispositivos sanitarios IoT conectados y su uso en hospitales, la pérdida de la información almacenada en estos dispositivos es cada vez más probable. Los datos médicos son aún más valiosos que los de una tarjeta de crédito, porque solo una de estas credenciales puede venderse por 10 dólares, unas 10 o 20 veces más que el valor que puede alcanzar el número de una tarjeta de crédito en EE. UU., **según Reuters**.

Lo que antes se circunscribía a países y organizaciones de ciberdelincuencia empresarial, ahora despierta el interés de cualquier delincuente con aspiraciones. Prevemos que en 2015 se producirá un ataque importante directamente relacionado con las vulnerabilidades de los dispositivos IoT.

—Chris Miller y Ramnath Venugopalan



Privacidad

La privacidad de los datos seguirá en el punto de mira hasta que los gobiernos y las empresas no acoten bien el concepto de acceso justo y autorizado en la definición, hasta ahora imperfecta, de "información personal".

Nosotros definimos la privacidad de los datos como el procesamiento justo y autorizado de la información que identifica personalmente a los individuos. Aunque en esta sencilla frase podrían quedar reflejados el problema y la práctica de la privacidad, la complejidad y el riesgo asociados están aumentando y así continuará de forma exponencial en 2015.

Si analizamos la definición, el concepto "justo" se presta a una interpretación subjetiva por parte de los usuarios de los sistemas, los clientes, los empleados de una empresa o los ciudadanos de un país. Lo justo puede delimitarse aún más por un grupo de principios de prácticas honestas para la manipulación de la información (FIPP) con refrendo internacional desde los años 60. Algunos de estos principios son: transparencia, notificación, selección, recopilación proporcionada, manipulación y uso compartido de datos entre fronteras, seguridad, acceso limitado y eliminación.

El concepto "autorizado" es otro factor definitorio de la privacidad de los datos. ¿Quién soy y hasta qué punto puedo gestionar activos de datos? ¿Quién es usted como cliente, empleado o ciudadano en una economía global independiente y cada vez más digital? En 2015, seguiremos viendo cómo los anticuados sistemas basados en funciones y los esquemas de contraseñas fracasan y acaban bajo el control de sujetos malintencionados o con hábitos poco ortodoxos. La identificación biométrica y los identificadores contextualizados son probablemente los mejores indicadores de presencia e intención, y constituyen un área inmensa de innovación. Responder a interrogantes como quién, cuándo y dónde se encuentra continuará impulsando sobremanera la innovación y los riesgos de ataques.

El último concepto de la definición de privacidad es "información que identifique personalmente". En 2015, continuará la falta de precisión y el debate sobre qué es exactamente información "personal" y hasta qué punto es razonable que esté disponible para agentes privados o públicos. En numerosos lugares, la información personal se define legalmente como datos que identifican de forma directa a un individuo concreto o como datos que, junto con otros datos, podrían identificar a una persona específica. Aunque los expertos en estadística y economía siempre han usado grandes conjuntos de parámetros para crear "datos", a otros profesionales más modernos y tecnológicos les gusta hablar de macrodatos o "Big Data" cuando se trata de manejar grandes volúmenes de información. Cuanto mayores son los volúmenes de macrodatos, más difícil es para nosotros permanecer absolutamente en el anonimato. Por tanto, la tendencia para 2015 y años posteriores serán normativas más restrictivas sobre la privacidad de los datos, con especificaciones de seguridad y requisitos de fugas de datos, donde antes campaban sin control los conjuntos de datos anónimos.

Para finales de 2015, la Unión Europea actualizará su **directiva de protección de datos de 1995** con una normativa de protección de datos de 2016, que será de aplicación en todos los estados miembros de la UE y comprenderá a todas las organizaciones internacionales. Esta respuesta de la UE es quizá la más contundente entre los organismos rectores de políticas públicas, pero países de Latinoamérica, y Australia, Japón, Corea del Sur y Canadá, entre otros, adoptarán normativas y leyes de privacidad de datos más agresivas y delimitadas en lo territorial.

—Michelle Dennedy

Ransomware

En cuanto al ransomware, prevemos una evolución de sus métodos de propagación, cifrado y los objetivos a los que apunta. Más dispositivos móviles sufrirán ataques.

Creemos que las variantes de ransomware que consigan burlar el software de seguridad instalado en los sistemas apuntarán específicamente a los endpoints que se suscriben a la nube, por ejemplo, soluciones de almacenamiento como Dropbox, Google Drive y OneDrive. Con estos endpoints infectados, el ransomware intentará atacar las credenciales de acceso a la nube de los usuarios conectados para infectar también los datos guardados en la nube.

Cuando estos usuarios descubran que los datos de sus endpoints se han cifrado, sufrirán un verdadero shock traumático al intentar acceder a la nube para restaurar todo y finalmente darse cuenta de que el ransomware también ha cifrado sus copias de seguridad.

Aunque los archivos cifrados por el ransomware no pueden propagarse ni infectar a otros dispositivos por sí solos, nos aventuramos a creer que finalmente se logrará que cada archivo cifrado sea portador del ransomware y pueda convertir el archivo de destino en un ejecutable con el archivo de datos originales almacenado en el propio malware. Esta técnica ha sido utilizada por virus que infectan archivos para dañar ejecutables originales y convertirlos en portadores. Los autores de ransomware podrían repetir este modelo para el cifrado de los archivos.

Al igual que el año pasado, prevemos de nuevo un aumento en el ransomware dirigido a los dispositivos móviles. Los teléfonos y las tablets almacenan valiosas imágenes y datos personales, por lo que son un objetivo muy apetecible para los autores de malware. Dicho lo cual, prevemos que la técnica del ransomware dirigido a los datos almacenados en la nube se repetirá en la esfera móvil. Las plataformas móviles admiten todo tipo de métodos de pago sin regular, y los delincuentes sabrán por dónde colarse para cifrar información y chantajear a sus víctimas a cambio de devolverles sus datos en estado íntegro.

—Vinoo Thomas

Móviles

Los ataques a móviles continuarán aumentando rápidamente con la expansión de las nuevas tecnologías móviles y no hay mucho que se haya hecho para detener los abusos en las tiendas de aplicaciones.

El malware para PC aumentó al hilo de destacados acontecimientos, como la aparición de los kits de generación de malware (con los que cualquiera sin nociones de programación puede crear amenazas), la publicación de código abierto de malware (que permite modificar amenazas con apenas una experiencia mínima en programación), y el uso masivo de funciones, aplicaciones o motores de cifrado populares. En 2015 observaremos un impacto similar en el panorama del malware móvil. Aumenta el desarrollo de código fuente de malware móvil comercial y abierto, y no tardaremos mucho en ver las consecuencias. La proliferación de los kits de generación de malware para móviles es solo cuestión de tiempo y con ella se franquearía el paso a nuevos delincuentes.

El iPhone 6 de Apple, con su chip de comunicación de campo cercano (NFC) y su monedero digital integrado, legitimará el uso de NFC para los pagos digitales. Otros proveedores de dispositivos móviles adoptarán rápidamente estas tecnologías en 2015, y los usuarios empezarán a hacer transacciones de forma racional gracias a ellas. Ya que estas son transacciones de terminales punto de venta y a los ciberladrones les apasiona este medio, estos procesos estarán en el punto de mira de los delincuentes. En 2015, los investigadores probablemente descubran vulnerabilidades en el hardware de NFC y el software de monedero digital, y los ciberladrones, obviamente, intentarán aprovecharse.

El método de instalación del malware para móviles no se modificará. Las tiendas de aplicaciones de confianza, como App Store de Apple y Google Play, consiguen con bastante éxito mantener a raya las aplicaciones cargadas de malware, sin embargo, alguna que otra consigue colarse. Por otra parte, hay muchas tiendas de aplicaciones poco fiables y sitios web de descarga directa cuyas aplicaciones suelen contener malware. Los usuarios llegan a estos sitios y tiendas de aplicaciones de dudosas intenciones atraídos por publicidad engañosa, que ha proliferado rápidamente en las plataformas móviles. En 2015, esta publicidad experimentará un rápido aumento en el sector móvil, para perpetuar así el crecimiento del malware móvil.

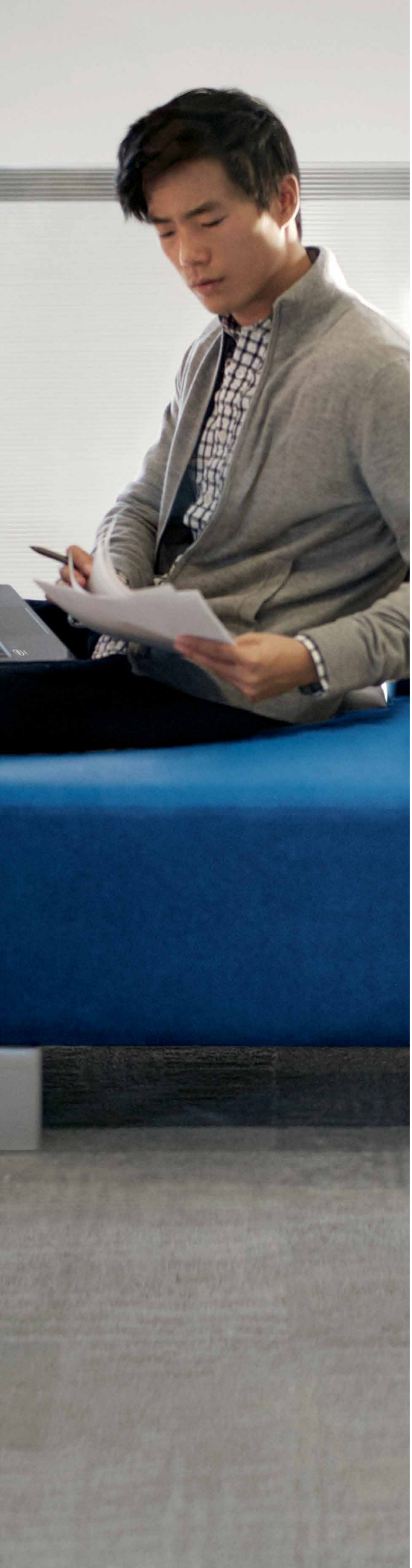
También prevemos un crecimiento en el ransomware para móviles, ya que los delincuentes pretenden trasladar a este medio los métodos de extorsión efectivos usados en el mundo del PC. Cuando esté perfeccionado en las plataformas móviles, el ransomware será aún más lucrativo para los ciberladrones que en el entorno del PC, ya que los usuarios móviles tienen una enorme dependencia de sus dispositivos para obtener acceso inmediato a información importante, como contactos, agendas y direcciones. Con tantos activos almacenados en el dispositivo móvil, los usuarios no escatimarán esfuerzos para conseguir de nuevo acceso a sus datos, incluido el pago de rescates.

—Craig Schmugar y Bing Sun

Puntos de venta

Los ataques en puntos de venta seguirán siendo lucrativos, y la creciente adopción de sistemas de pago digital en los dispositivos móviles de los consumidores abrirá nuevas líneas de ataque para los ciberdelicuentes.

En 2013, según un **artículo de Forbes**, se movieron 15 billones de dólares en transacciones comerciales. No es de extrañar entonces que los sistemas de pago para estas transacciones hagan las delicias de cualquier ciberdelincuente. En 2014, se registró un importante repunte en los ataques a estos sistemas, con una masiva fuga de datos en Home Depot. Entre tanto, los clonadores de tarjetas de crédito continuaban asediando a los consumidores. Estos delincuentes también han tenido mayor presencia este año y han operado en casi cualquier lugar, desde terminales de tarjetas en restaurantes, hasta cajeros automáticos y surtidores de combustible. Los ataques en los puntos de venta son tan comunes que se han convertido en una rutina diaria para los que trabajan en el sector. Sin embargo, no se ha hecho mucho para mejorar su seguridad, por lo que estimamos que en 2015 continuarán aumentando. Pese a lo anterior, en Estados Unidos la situación podría mejorar a finales de 2015, cuando los comerciantes empiecen a implementar lectores de tarjetas y tarjetas con chip y pin.



El próximo año se registrará un importante aumento en el uso de los sistemas de pago digital. Apple ha actualizado su iPhone para que incluya tecnología NFC. De esta forma, se habilita su nueva función iWallet, que lee y transmite la información de la tarjeta de crédito a los sistemas de pago sin que el cliente tenga que pasar la banda magnética de las tarjetas. Varios dispositivos Android también admiten NFC y usan el proceso llamado Host Card Emulation (Emular tarjeta) para facilitar los pagos desde móviles. Tanto Visa como MasterCard han adoptado esta tecnología y ya ofrecen aplicaciones de pago móviles compatibles con dispositivos NFC. Ahora que existe la infraestructura, solo cabe esperar una adopción más extendida entre los consumidores. Pero también veremos la otra cara de la moneda: los ataques a estos sistemas.

Los sistemas de pago digital pueden suponer el final de los clonadores de tarjetas de crédito, sin embargo, no estarán exentos de nuevos riesgos. Los principales serán las vulnerabilidades propias de la tecnología NFC. Algunas de estas vulnerabilidades se pusieron de manifiesto en la convención de hackers DEF CON 2013 y siguen analizándose en el proyecto **NFC Awareness Project**. El problema fundamental es que la información confidencial se envía ahora por medios inalámbricos, y los delincuentes pueden colarse a través de esta conexión. Hay un historial conocido de ataques de esta naturaleza, como la interceptación de comunicaciones Bluetooth de 2005 y la clonación remota de pasaportes con identificación por radio frecuencia (RFID) en 2009. La probabilidad de ataques similares a dispositivos NFC es real porque ya hay **vulnerabilidades documentadas**. Los consumidores envían ahora información de pago por un protocolo con vulnerabilidades conocidas, por tanto no es de extrañar que en 2015 se produzcan ataques a esta infraestructura.

—Dan Larson

El malware traspasa las fronteras de Windows

Los ataques de malware que no se dirijan a sistemas Windows aumentarán, aprovechando la vulnerabilidad Shellshock.

Durante la segunda mitad de 2014, nos hemos topado con la **vulnerabilidad Shellshock**: una brecha en bash, un shell de comandos de máquinas Unix, Linux y OS X. Gracias a esta brecha, un delincuente puede ejecutar comandos arbitrarios en la máquina de la víctima, lo que la sitúa como el tipo de vulnerabilidad más peligrosa, con los 10 puntos máximos de gravedad que otorga la base de datos **National Vulnerability Database de los Estados Unidos**.

Los efectos de esta vulnerabilidad recién descubierta se apreciarán durante los próximos años. Son muchos los dispositivos que ejecutan alguna forma de Unix o Linux, desde routers a televisores, controladores industriales, sistemas de vuelo e infraestructuras críticas. Por el momento, solo estamos empezando a ser conscientes de la envergadura de esta vulnerabilidad.

Este vector de ataque será el punto de entrada a infraestructuras de todo tipo, desde electrodomésticos, hasta empresas que dependen mucho de sistemas no Windows. Por tanto, esperamos ver un aumento importante de malware no Windows durante 2015, ya que los delincuentes desplegarán sus fuerzas para filtrar datos, retener sistemas en cautiverio, integrar bots de spam y realizar otras artimañas nefastas. Shellshock estará en boca de todos cuando los delincuentes ataquen nuevos (y viejos) dispositivos vulnerables para sus viles propósitos.

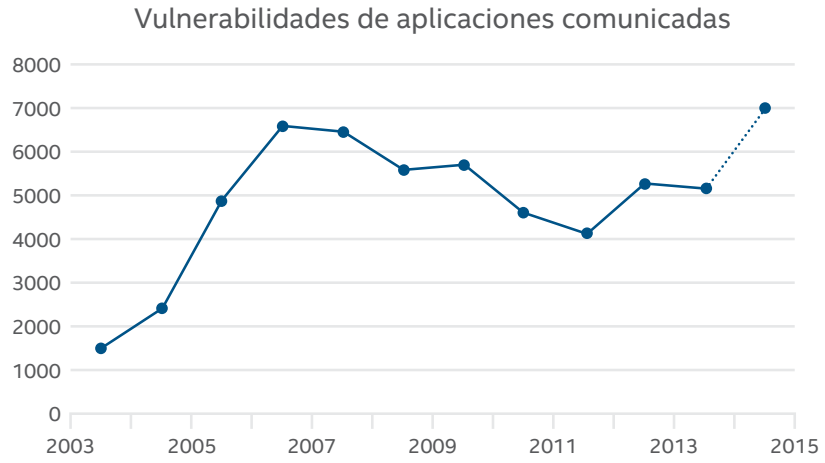
—Craig Schmugar

Vulnerabilidades

Las vulnerabilidades aumentarán, ya que el número de fallos en el software popular continuará creciendo.

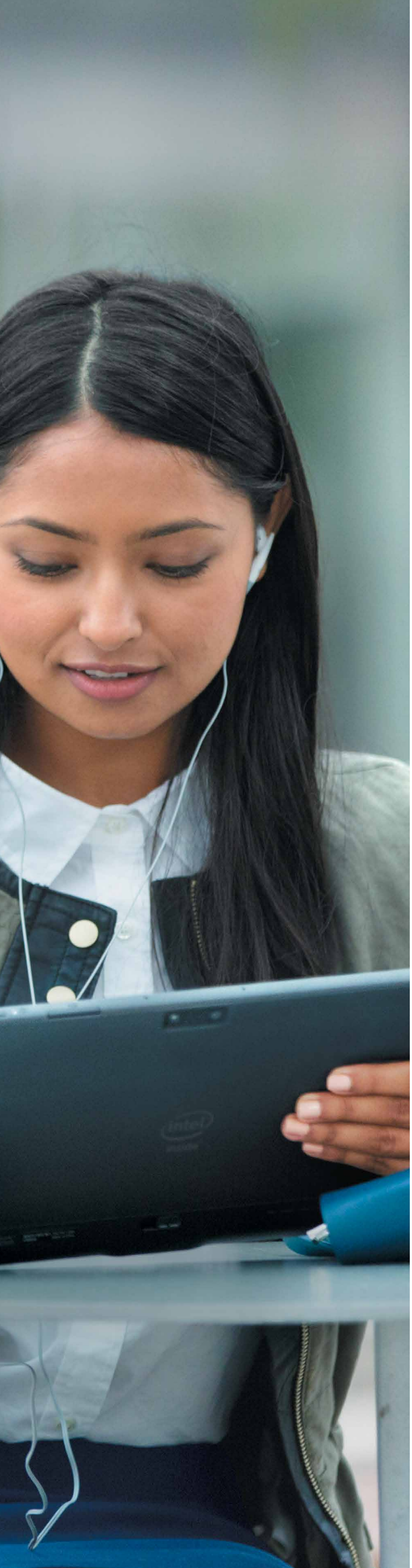
Los datos obtenidos de la National Vulnerability Database del gobierno estadounidense confirman que estos tres últimos años el número de vulnerabilidades ha aumentado. Según las 5200 entradas registradas a día 30 de septiembre, el número total para 2014 superará el registro de 2006.

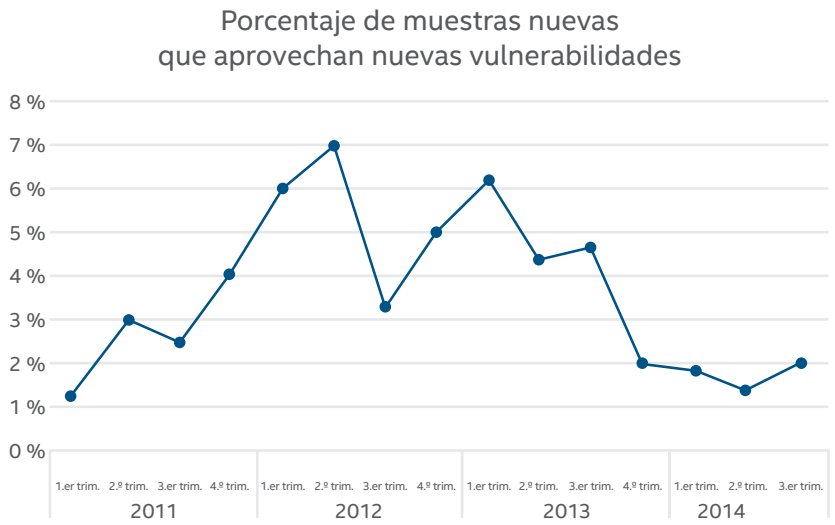
El número de vulnerabilidades no es indicativo directo del riesgo, ya que también influyen muchos otros factores interrelacionados: la velocidad y cobertura de los parches, la gravedad de cada vulnerabilidad, el nivel de exposición, etc. No obstante, estas estadísticas nos dan una perspectiva del estado general del ecosistema.



Fuente: National Institute of Standards and Technology—National Vulnerability Database.

Entre 2006 y 2011, se apreció un descenso en el número de vulnerabilidades, pero la situación ha cambiado. Esta caída podría deberse al empleo de técnicas como la comprobación de la pila en los compiladores, la prevención de ejecución de datos y el diseño aleatorio del espacio de direcciones en el software de 64 bits. La tendencia actual de aumento de los ataques probablemente es reflejo de las nuevas técnicas de ataque empleadas, como la identificación de pila y la programación con instrucciones return y jump, además de que los hackers, ya sean de "sombrero blanco" o de "sombrero negro", conocen mejor el software de 64 bits.





Fuente: McAfee Labs.

McAfee Labs ha analizado nuestro zoológico de malware para determinar con qué frecuencia el malware se dirige a vulnerabilidades conocidas. Según el trimestre, entre el 1 % y el 6 % de todas las muestras nuevas de malware aprovechan una vulnerabilidad conocida. En este periodo, la cifra era de aproximadamente el 2 %, es decir 821 000 muestras nuevas de malware atacaron una vulnerabilidad conocida. Dado que crece el número total de muestras que usan técnicas de exploits, el volumen de malware aumenta también; por lo tanto, la proporción de muestras "asociadas a exploits" permanece relativamente estable.

En 2015, estimamos que no habrá cambios importantes en las soluciones a las vulnerabilidades disponibles para los desarrolladores de sistemas operativos o aplicaciones. Igualmente, es poco probable que aumente el índice de adopción de prácticas recomendadas nuevas y actuales. En definitiva, el número de vulnerabilidades nuevas seguirá incrementándose y con él el volumen de malware que las aprovechará.

—Igor Muttik y François Paget

Huida del entorno aislado

Las huidas del entorno aislado serán un área de contención importante para los sistemas de seguridad de TI.

Muchas aplicaciones importantes y de uso común, como Microsoft Internet Explorer, Adobe Reader y Google Chrome, han implementado sus propias tecnologías de entorno aislado para confinar comportamientos maliciosos. Aislar las aplicaciones es un método eficaz para detener muchos tipos de ataques, por eso, los autores de malware han estado ingeniándoselas para sortear este mecanismo de seguridad.

Fijémonos, por ejemplo, en Internet Explorer. El malware que no pueda sortear su entorno aislado no supone ningún peligro para los usuarios, porque el ataque no puede causar un daño persistente en el sistema. Sin embargo, hay dos versiones de tecnología de entorno aislado en Internet Explorer: el modo protegido (PM) y el modo protegido mejorado (EPM). Actualmente, el modo predeterminado para Internet Explorer 10 y 11 es PM, y nuestro estudio ha concluido que este modo protegido se sortea con relativa facilidad. Aunque no hemos visto ningún ataque que se salte los controles de PM o EPM, la realidad es que podría darse, así que en 2015 probablemente se registren casos de huidas del entorno aislado de Internet Explorer y, por tanto, ataques de tipo zero-day.

Se han descubierto y revelado vulnerabilidades que pueden propiciar la huida de un entorno aislado de aplicaciones en muchas aplicaciones cliente importantes. Se han detectado vulnerabilidades documentadas en Adobe Reader y Flash, Chrome, Apple Safari, Oracle Java e Internet Explorer. Todo esto ha provocado que tanto investigadores como delincuentes sigan estudiando la situación. Por ejemplo, en BlackHat 2014, los investigadores describieron cuatro técnicas que se sirvieron para sortear un entorno aislado de aplicaciones en la competición de hackers Pwn2Own de este año. De hecho, en la convocatoria de este año, casi todos los ganadores incluían huidas del entorno aislado en la fase final del ataque.

Ya hemos visto técnicas que aprovechan vulnerabilidades y huyen de los entornos aislados de aplicaciones. Es solo cuestión de tiempo hasta que estas técnicas lleguen a manos de los ciberdelincuentes a través del mercado negro. Creemos que será en 2015.

Otra predicción más: hasta la fecha, los ciberdelincuentes se han centrado principalmente en escapar de los entornos aislados de aplicaciones. Sin embargo, los sistemas de entorno aislado autónomos ofrecidos por proveedores de software de seguridad, cada vez más populares, suponen un nuevo obstáculo para los ciberladrones. Como respuesta, los ciberdelincuentes han empezado a buscar formas para que su malware pueda sortear estos sistemas de entorno aislado. Actualmente, un número significativo de familias de malware identifican y evaden la detección basada en entornos aislados. Sin embargo, hasta ahora no tenemos noticias de ningún malware en circulación que haya conseguido aprovechar vulnerabilidades del hipervisor para escaparse de un entorno aislado. Aunque esperamos que esto ocurra en 2015.

—Haifei Li, Rick Simon, Bing Sun, y Stanley Zhu

Temas principales

BERserk: golpe directo a la fiabilidad de las conexiones

Abuso de la confianza: ataque al eslabón más débil de la seguridad online

Compartir opinión

BERserk: golpe directo a la fiabilidad de las conexiones

—James Walter

En el tema principal **"Abuso de la confianza: ataque al eslabón más débil de la seguridad online"**, describimos los retos asociados a la fiabilidad de los sitios web. En este tema principal, nos detenemos en una vulnerabilidad específica que merma considerablemente la confianza.

El equipo de investigación de amenazas avanzadas de Intel Security centra sus estudios en áreas clave que afectan a la seguridad de las transacciones online y al tráfico de información. Una de estas áreas es la seguridad de referencia en las comunicaciones, y se incluye un análisis detallado de amenazas y exposición a riesgos en los protocolos SSL/TLS, TPM 2.0, canales criptográficos y otras áreas a las que solemos otorgar plena confianza asumiendo que el modelo existente es "sólido".

En septiembre, el equipo de investigación de amenazas avanzadas de Intel Security desveló detalles de la vulnerabilidad BERserk. Su nombre se refiere a la brecha que abre el análisis de secuencias codificadas específicas que siguen reglas de codificación básicas (BER) en la implementación de la verificación de firmas RSA. Tanto Intel Security como el investigador de seguridad Antoine Delignat-Lavaud informaron de esta vulnerabilidad a Mozilla, y aconsejaron a la empresa que publicara actualizaciones para varios productos, incluidos Firefox, Thunderbird, SeaMonkey y NSS. Google también actualizó su navegador Chrome y OS porque la biblioteca criptográfica NSS se usa en estos productos.

El fallo está en la verificación de firmas RSA, específicamente en el análisis incorrecto de secuencias codificadas con ASN.1 durante la verificación de secuencias. Esta vulnerabilidad es una variación de la vulnerabilidad de falsificación de firmas RSA PKCS#1 v1.5 de Bleichenbacher definida en **CVE-2006-4339**. Las implementaciones vulnerables buscan en el mensaje codificado bytes de relleno 0xFF hasta que se detecta el byte separador 0x00. El proceso continúa comparando DigestInfo y el resumen del mensaje con los valores previstos sin asegurarse de que DigestInfo y el resumen estén justificados a la derecha en el mensaje codificado, lo que significaría que no hay más bytes tras el resumen del mensaje. Sin esa comprobación, puede formularse un mensaje codificado para que incluya datos inservibles tras el resumen del mensaje, de modo que este mensaje codificado cumpliría la siguiente verificación de firmas:

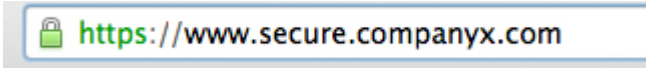
Mensaje codificado = 00 01 FF FF FF FF FF FF FF FF 00 DigestInfo MessageDigest Garbage

Los datos inservibles extras en el mensaje codificado permiten a un adversario generar firmas RSA que, tras estructurar en cubo el módulo de RSA, da como resultado este mensaje codificado:

EM' = (s')^3 mod N

Un adversario puede crear firmas RSA sin conocer la clave privada RSA {p,q,d} y así podrá falsificar firmas RSA.

El resultado permite a un delincuente falsificar certificados de RSA sin conocer la clave privada de RSA correspondiente. ¿Qué significa todo esto? ¿Cómo nos afecta?

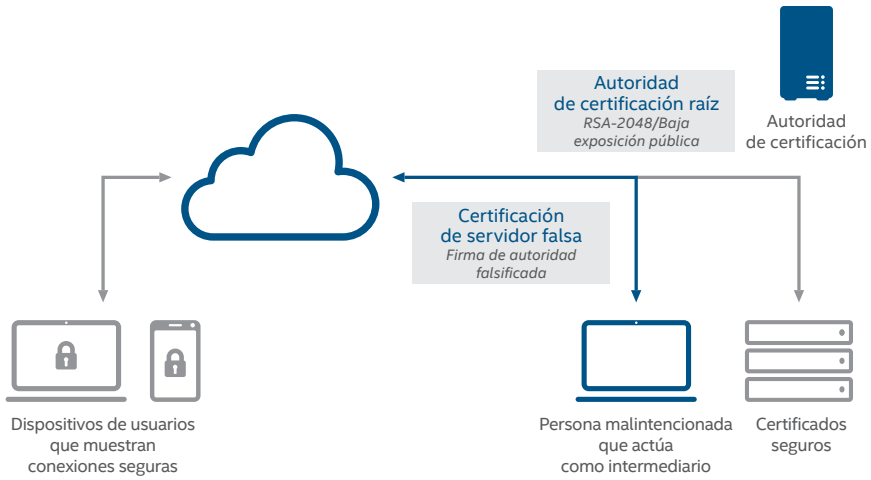


BERserk abre la puerta a los ciberdelincuentes para lanzar ataques de intermediario en sesiones de Internet sin que los usuarios lo adviertan. Su potencial de daño rivaliza con el de Shellshock.

La respuesta es sencilla. Como buenos ciudadanos y usuarios de Internet, nos hemos acostumbrado a un modelo de confianza concreto. Cuando realizamos una transacción online (financiera, médica u otra que requiera datos personales), sabemos cómo comprobar si la sesión es segura. Nos han enseñado a buscar "https" en la URL, además de los útiles iconos de candado. Estos indicativos nos ayudan a decidir si un sitio o una aplicación son seguros y no están exponiendo los datos a manos indeseables.

BERserk y las vulnerabilidades relacionadas ponen en duda todo esto y desafían nuestra percepción de confianza y seguridad de las sesiones por SSL/TLS. Con capacidad para falsificar firmas RSA perfectamente, un delincuente puede establecer sesiones de intermediario en muy distintos casos.

La vulnerabilidad BERserk
podría facilitar ataques de intermediario



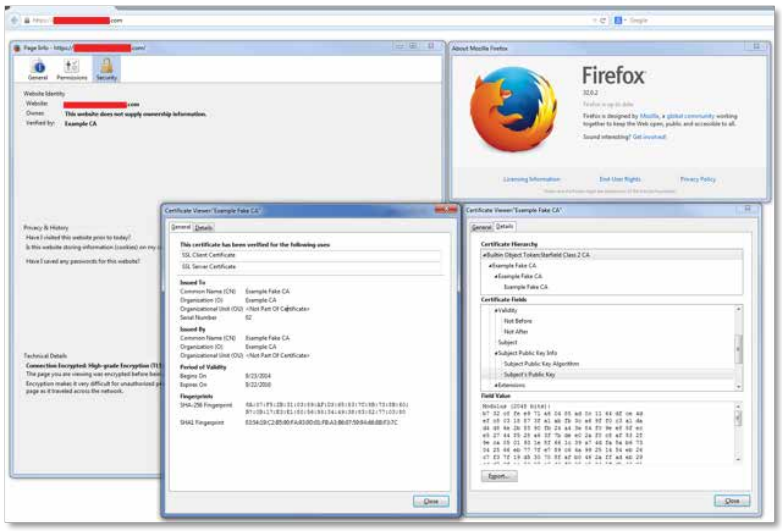
Por ejemplo, la confidencialidad e integridad de las sesiones entre los clientes y los sitios web de sus bancos pueden verse comprometidas. Con certificados falsos, los usuarios pueden visitar sitios e incluso ver certificados para confirmar su supuesta autenticidad. Todo parecerá válido, pero nada más lejos de la realidad. En otro ejemplo similar, los usuarios que introducen sus datos en el sitio web de su servicio médico para consultar unos resultados podrían acabar convirtiéndose en víctimas de este ataque. Lo mismo ocurre con la presentación de la declaración de la renta por Internet y muchos otros casos.

Aparte de las amenazas de software y de la Web, las bibliotecas criptográficas de los dispositivos de hardware, como los teléfonos, almacenan datos confidenciales a los que las aplicaciones acceden a demanda. Imagine que una tablet o un teléfono móvil contiene una memoria segura y el ejecutable para ofrecer funciones criptográficas al software del dispositivo. Habrá firmware en el dispositivo firmado digitalmente para evitar modificaciones no autorizadas por parte de algún malware o del usuario. Sin embargo, con la vulnerabilidad BERserk, es posible manipular el firmware, por lo que se ataca a la integridad y confidencialidad de los datos almacenados en el elemento de hardware seguro.

Descubra cómo McAfee puede protegerle frente a esta amenaza.

Un uso habitual de este modelo es el almacenamiento de los datos de cuentas financieras usados para los pagos en proveedores especializados o en terminales, como los sistemas de pago NFC, en los que todos los datos de las tarjetas se almacenan en el dispositivo. En este caso, los delincuentes podrían manipular las sesiones de muy diversas formas, por ejemplo, mediante el secuestro y la manipulación de la entrada y la salida, o simplemente a través de la obtención y el robo de datos confidenciales.

Para nuestra investigación, hemos podido falsificar certificados de RSA de hasta 1024 y 2048 bits. Esto supone ventajas para los delincuentes. En concreto con Mozilla NSS, los agresores pueden falsificar sus certificados, y Mozilla NSS confiará en la cadena de certificación.



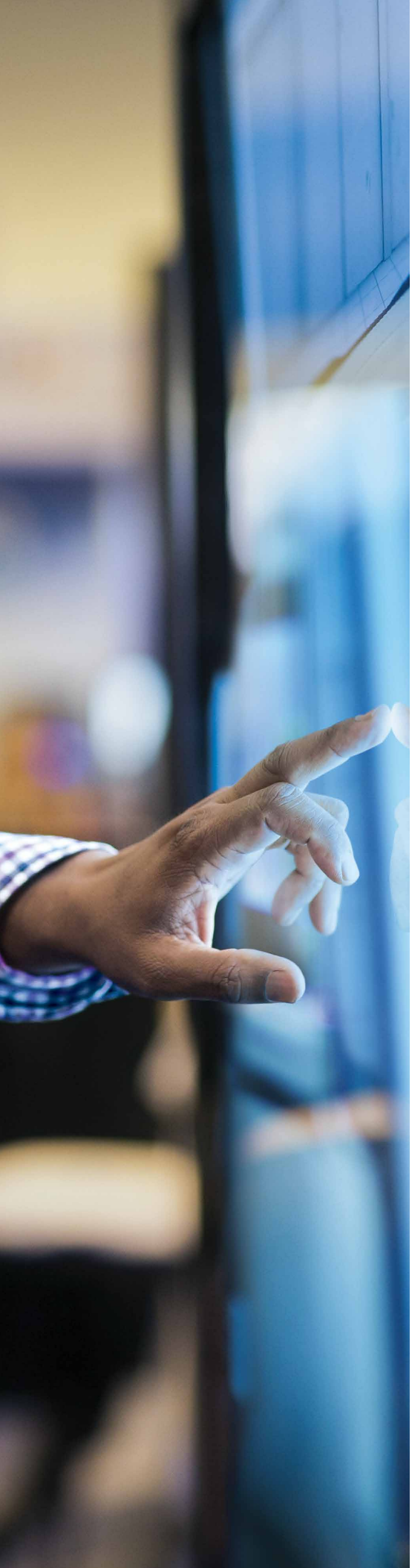
Un certificado falsificado, visto en Firefox.

El equipo de investigación de amenazas avanzadas de Intel Security continúa estudiando estos temas y sus efectos en otros casos, aparte del comportamiento del navegador. Nuestro equipo también está colaborando con CERT y los proveedores afectados para encontrar una solución a todo esto.

Los proveedores de las bibliotecas criptográficas afectadas siguen publicando actualizaciones y ayuda. Mozilla y Google han actualizado los productos. Los usuarios afectados deberían seguir los consejos de sus proveedores y mantener los sistemas actualizados.

Para obtener más información sobre BERserk:

- Vulnerabilidad BERserk: **Part 1: RSA signature forgery attack due to incorrect parsing of ASN.1 encoded DigestInfo in PKCS#1 v1.5** (Parte 1: Ataque de falsificación de firmas de RSA debido al análisis incorrecto de la codificación ASN.1 DigestInfo en PKCS#1 v1.5)
- Vulnerabilidad BERserk: **Part 2: Certificate forgery in Mozilla NSS** (Parte 2: Falsificación de certificados en Mozilla NSS)
- Intelsecurity.com: **BERserk**
- Equipos de respuesta a emergencias informáticas: **VU#772676**
- National Vulnerability Database: **CVE-2014-1568**



Abuso de la confianza: ataque al eslabón más débil de la seguridad online

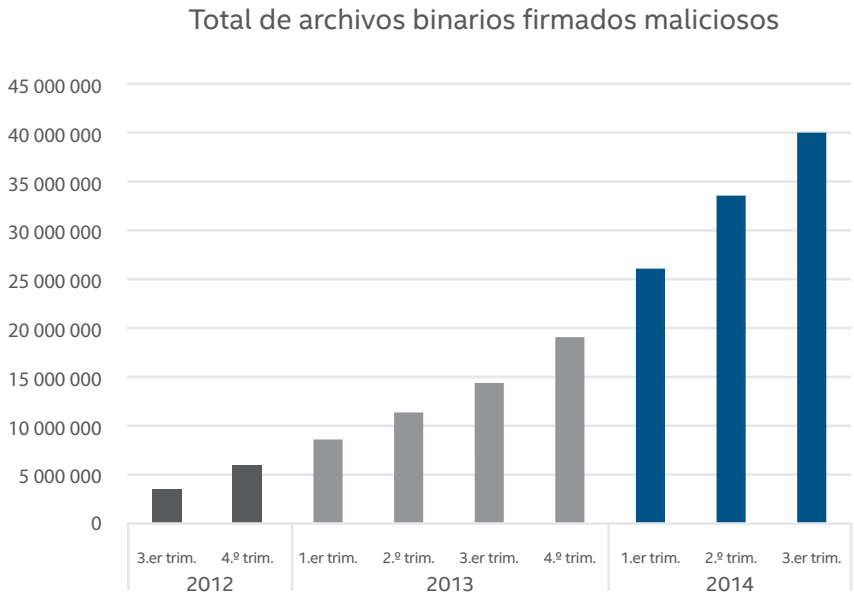
—Cedric Cochin y Craig Schmugar

A diario, gran parte de la población mundial usa un dispositivo electrónico, como un ordenador personal, un teléfono móvil, un televisor o incluso un automóvil. Hemos llegado a depender de estos artículos y la mayoría de las veces confiamos en que nos proporcionan información exacta.

Pero la confianza debe ganarse y mantenerse, un proceso que suele implicar tiempo y dinero. Las empresas gastan millones de euros al año para reforzar sus imágenes de marca, conscientes de que es una buena inversión que les reportará una rentabilidad muy superior. Saben que la decisión de compra de los consumidores está influida por el buen nombre del artículo.

Los delincuentes también son conscientes de todo esto, pero no suelen tener el tiempo, los recursos y la paciencia necesarios para establecer una relación de confianza con sus víctimas. Se dedican a buscar formas de aprovecharse de las inversiones y las relaciones que otros han establecido para generar confianza.

Los abusos de confianza se producen en numerosas ocasiones a lo largo del día, y la tendencia está yendo a peor. Por ejemplo, McAfee Labs supervisa binarios firmados maliciosos, que son una forma de abuso de confianza, ya que los delincuentes camuflan el malware haciéndolo pasar por un archivo certificado legítimo. Desde que empezamos a vigilarlos en 2007, el aumento de binarios firmados maliciosos es imparable.

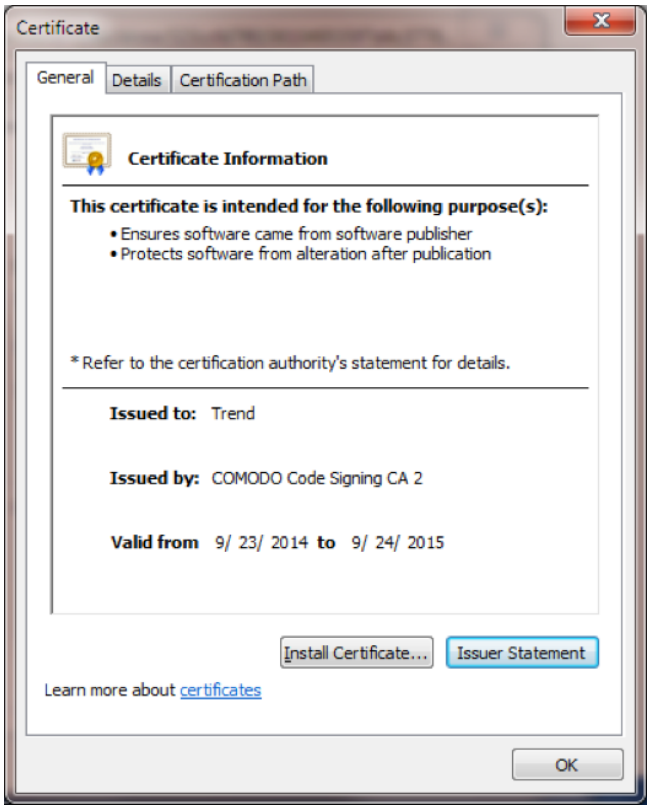


Los autores de malware firman digitalmente sus amenazas para abusar de la confianza de los usuarios, productos y sistemas operativos. Fuente: McAfee Labs.

La confianza heredada aprovecha el valor que los usuarios dan a un nombre de marca. Los sitios web a menudo enmascaran la relación entre las marcas de confianza y otras marcas que también aparecen en sus sitios.

Confianza heredada

Durante años, para depositar la confianza en una marca comercial durante una transacción bastaba con verificar la marca. Actualmente, los consumidores también deben averiguar si la marca de confianza a su vez confía en otras marcas representadas por la presencia online de la marca de confianza. En septiembre, la **red de publicidad maliciosa "Kyle y Stan"** quedó expuesta tras distribuir anuncios maliciosos en sitios web conocidos como Amazon.com, ads.yahoo.com y youtube.com, además de **importantes redes publicitarias como Double-Click y Zedo**. Una campaña maliciosa propagada por la red publicitaria Zedo **habría afectado a usuarios** de los sitios web más puntuados por Alexa con variantes del troyano CryptoWall firmadas. La firma digital empleada se había concedido a "Trend", con intención de copiar al proveedor de seguridad Trend Micro. Según la telemetría inicial, entre los usuarios más afectados se encontraban los de América del Norte. Lamentablemente, muchos consumidores pecan de inocentes otorgando una confianza que a menudo es inmerecida.



Certificado usado para firmar CryptoWall.

Esta relación de confianza entre un consumidor y una marca comercial suele ser objeto habitual de abuso. Un ejemplo es una aplicación falsificada en la que nos intentan convencer de que un virus o troyano es un programa legítimo y, normalmente, conocido. Durante el último trimestre, los falsificadores intentaron colarnos como auténtico un "FlashPlayer11" de Adobe. Según el recuento de descargas de Google Play y la telemetría de detección de McAfee Mobile Security, los falsificadores lograron engañar a algunos usuarios.

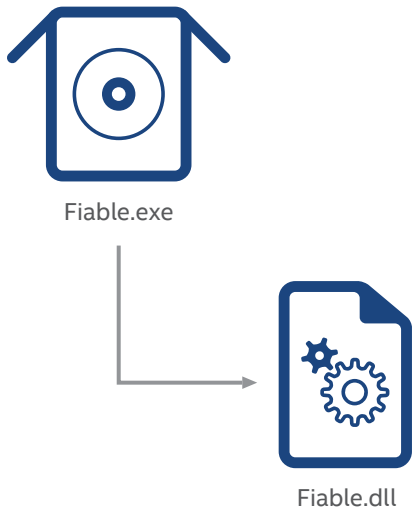
Una de las aplicaciones "FlashPlayer11" falsificadas en Google Play.

Detección realizada por McAfee Mobile Security del malware "FlasherPlayer11" (Android/Fladstep.B).

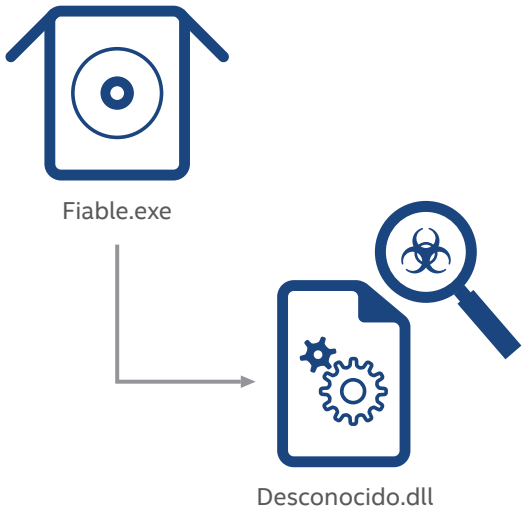
Los delincuentes abusan de la confianza en los sistemas operativos o productos mediante la carga en DLL, una técnica común usada para insertar código malicioso.

Confianza en el sistema operativo y en el producto

Los productos de seguridad actuales se suelen cimentar en la confianza. Para aumentar el rendimiento y disminuir los falsos positivos, un inventario del sistema determina las aplicaciones inocentes, cuyo comportamiento no se somete a análisis. Los delincuentes saben que si sus códigos maliciosos pueden subirse a una aplicación de confianza, la probabilidad de acertar con el ataque es grande. El malware ha aprovechado esta circunstancia durante años, usando una metodología conocida como carga en DLL. Esta técnica consiste en ejecutar una aplicación legítima que ejecute código de una biblioteca externa. Los delincuentes diseñan su carga útil para que asuma la función de la DLL objetivo, con lo que consiguen que la aplicación limpia ejecuta el código malicioso.

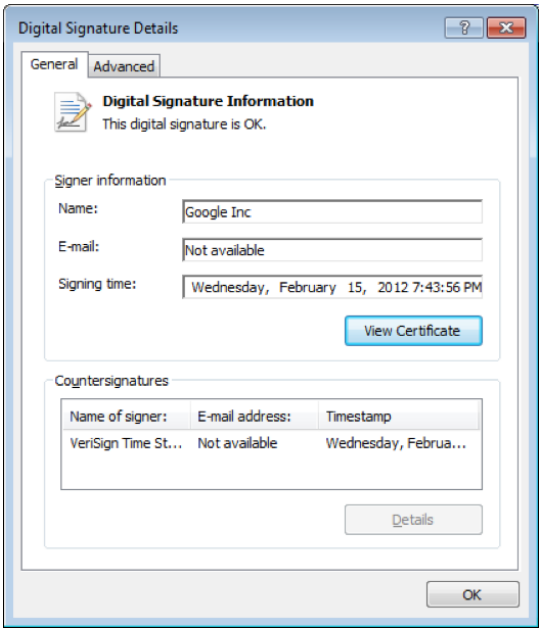


Caso típico: un ejecutable de confianza carga una biblioteca de confianza.

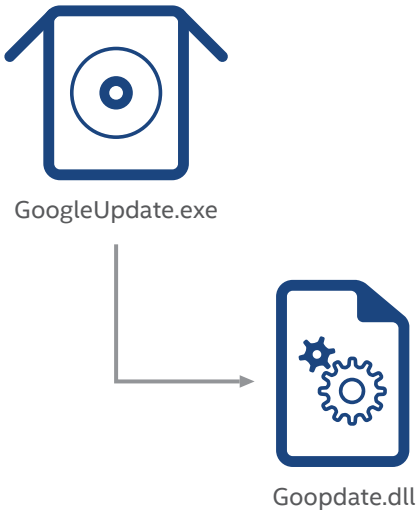


Caso malicioso: un ejecutable de confianza carga una biblioteca de malware desconocida.

Durante el tercer trimestre, McAfee Labs observó ataques con carga en DLL contra un objetivo relativamente nuevo: una aplicación Google Updater firmada. Las nuevas variantes de malware PlugX asumen la función de la DLL goopdate.dll importada, pero PlugX va más allá para ocultar sus acciones. El módulo goopdate.dll no es más que un intermediario que lee el contenido de un archivo de datos cifrado, goopdate.dll.mpa, lo descifra en la memoria y transfiere el control de ejecución a ese código. Esta estrategia tiene la ventaja de que enmascara la funcionalidad del archivo DLL intermediario. Los tres componentes participantes del ataque son benignos por sí solos, por lo que si se analizan los archivos por separado se podría llegar a una conclusión equivocada. Sin embargo, combinados, la intención maliciosa es bastante obvia. Con esta técnica, los delincuentes se aprovechan de los productos que confían en archivos firmados por un certificado legítimo de Google Inc.

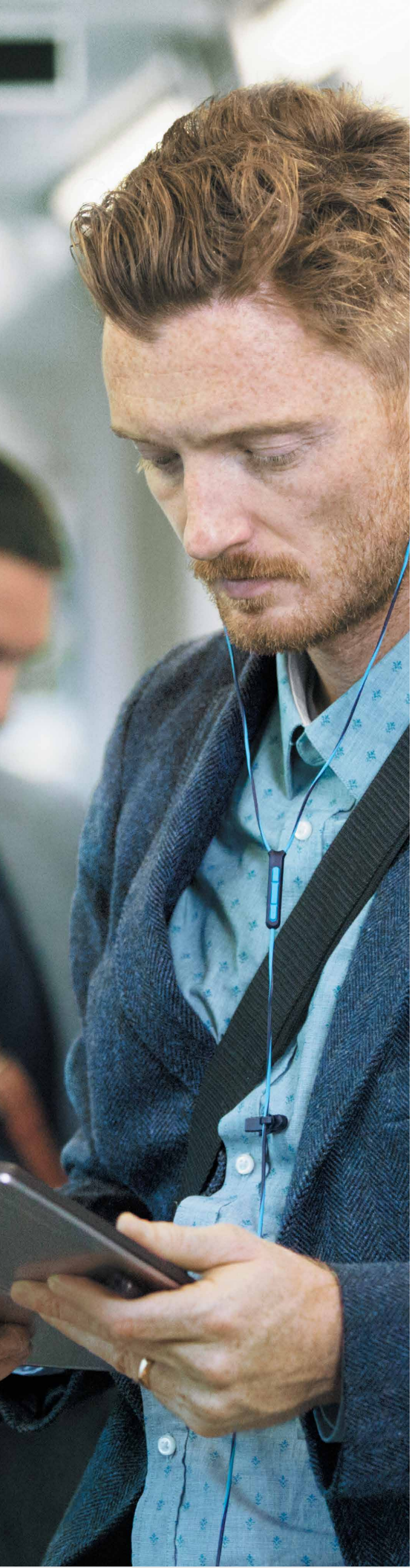


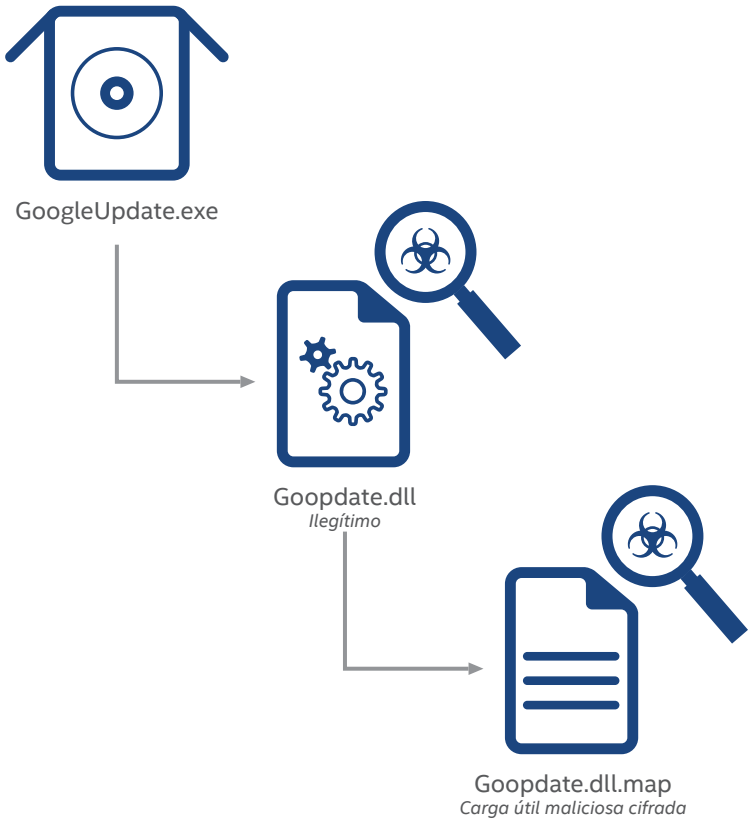
Aplicación Google Updater con firma legítima.



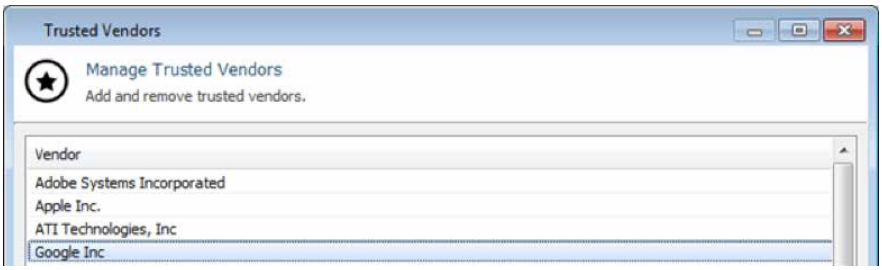
La aplicación Google Updater legítima carga una biblioteca de Google.

Comparta este informe

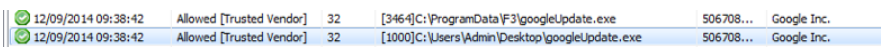




Un ejecutable de Google legítimo carga un módulo malicioso, que carga la carga útil. Google Updater carga una biblioteca de Google.



Esta aplicación de lista blanca confía implícitamente en las aplicaciones de Google válidas de forma predeterminada.

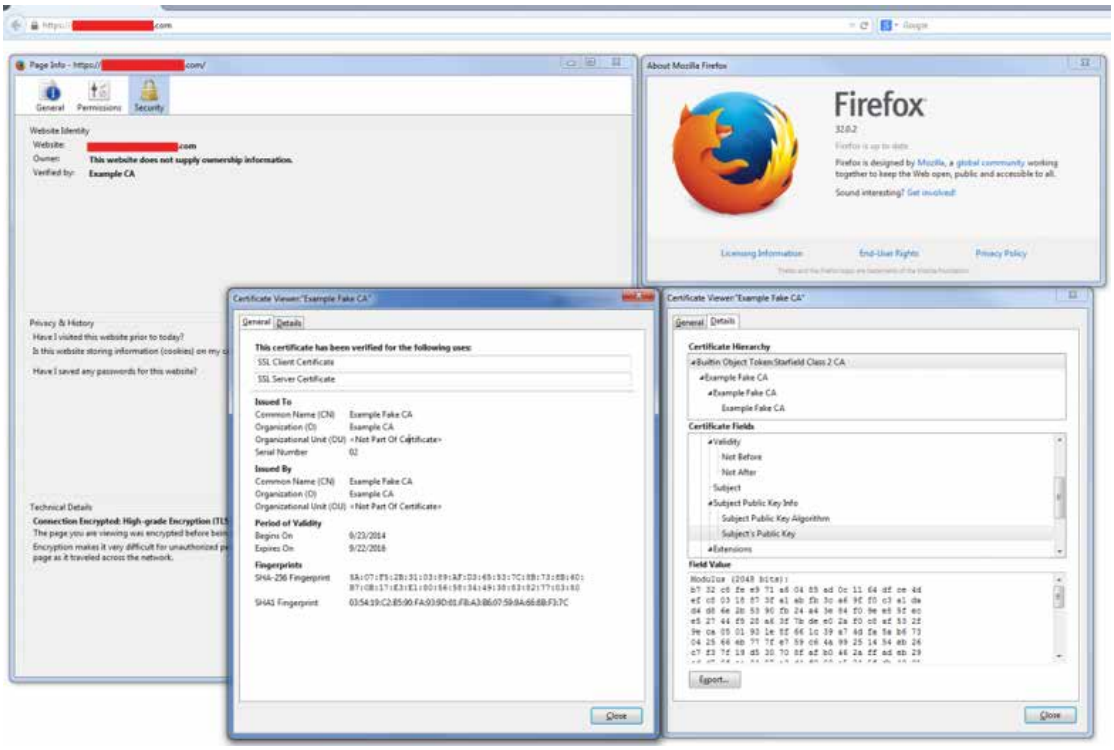


La aplicación del [proveedor de confianza] se permite de forma predeterminada.

Hemos visto un avance más importante en abusos de la confianza en los productos en una reciente **variante del kit de exploits Angler**. Este ataque permite la ejecución directa de una carga útil sin tener antes que copiarla en disco, lo que evita la posibilidad de que las aplicaciones de listas blancas puedan aceptar o rechazar el código recién entregado, y por extensión, ejecutado. Este paso también omite los análisis antivirus de los archivos porque no hay ningún archivo que analizar en este punto del ataque.

Otra forma de abuso de confianza afecta a la interacción entre el sistema operativo y los controles de direccionamiento de la red. Las aplicaciones confían en que el sistema operativo les brinde un método de comunicación seguro y fiable. Por ejemplo, las aplicaciones dan por hecho que su tráfico se dirigirá de forma segura y correcta al destinatario previsto. Un grupo muy conocido de malware son los cambiadores DNS. La única finalidad de este malware es modificar la configuración de DNS del sistema operativo, con el fin de dirigir todas las consultas DNS a un servidor DNS controlado por los delincuentes. Aunque el navegador actúa como si se comunicara con el sitio web de un banco de confianza, en realidad está intercambiando datos con un sitio falso o un proxy transparente malicioso que está captando los datos del usuario.

Averiguar si un usuario está interactuando con un sitio falso no es tan fácil como cabría pensar. La vulnerabilidad "BERserk" ASN.1, **de la que informó Intel el 24 de septiembre** y que se describe en el tema **"BERserk: golpe directo a la fiabilidad de las conexiones"** de este informe, es un ejemplo perfecto de cómo se pueden alterar los navegadores para dar la apariencia de que se están comunicando con sitios de confianza. Esta vulnerabilidad permite a los delincuentes falsificar firmas RSA, omitiendo por tanto la autenticación en los sitios web que usan SSL/TLS. Dado que se pueden falsificar certificados para cualquier dominio, este problema es muy preocupante, ya que pone en duda la integridad y confidencialidad de los sitios web que visitamos confiados de que son sitios seguros.



La vulnerabilidad "BERserk" ASN.1.

Descubra cómo McAfee puede protegerle frente a esta amenaza.

Los abusos relacionados con la resolución de nombres también afectan a los sistemas operativos. Los delincuentes han logrado desplegar malware dirigiendo el sistema a un servidor de actualización malicioso y usando un certificado de confianza para una finalidad que no es la prevista. Un ejemplo famoso es el **malware de espionaje Flame** descubierto en 2012. Flame contenía código para infectar los ordenadores elegidos como víctimas infiltrándose en el mecanismo de actualización de Microsoft Windows para distribuir parches de seguridad.

Ataques similares afectan a otros componentes de una red, como los routers, y permiten a los delincuentes capturar el tráfico desde los equipos de sobremesa y portátiles, así como desde televisores, consolas y otros dispositivos conectados. En agosto, durante un ataque de este tipo, los usuarios de dispositivos de almacenamiento conectados a la red Synology sufrieron la infección de SynoLocker, un troyano de tipo ransomware que retenía sus datos a cambio de un rescate.

La confianza es una oportunidad para los delincuentes, y los casos de abuso de confianza se multiplican. Los usuarios deben permanecer vigilantes. Es preciso que los productos de seguridad ayuden a los clientes a definir en qué pueden confiar y en qué no, y que ofrezcan controles flexibles que les permitan otorgar más permisos a los sitios de confianza limitando los de los demás. Si no se cumplen estas condiciones, podría cundir la desconfianza en muchas tecnologías usadas para acceder a Internet, y quizá incluso disminuir el uso general de la Web.

Protección frente al abuso de confianza

Abuso	Medida
Confianza heredada (publicidad maliciosa), confianza en los sistemas operativos y productos	Mantenga actualizados los sistemas operativos, las aplicaciones y el software de seguridad.
Exploits maliciosos (a través de descargas desapercibidas)	Mantenga los sistemas actualizados. Visite sitios web de reputación conocida. Pase el ratón por los hipervínculos para comprobar los destinos. No siga vínculos sospechosos que llegan en mensajes de correo electrónico o de las redes sociales.
Abuso de confianza en la marca (correo electrónico falsificado, aplicaciones falsificadas, dominios falsos)	Sospeche y confirme, introduzca manualmente las direcciones web, busque las aplicaciones en sitios fiables, elija las que tengan una reputación consolidada (muchas descargas, revisiones positivas), e inspeccione las solicitudes de permisos de las aplicaciones.
Abusos de confianza en los dispositivos	Mantenga los dispositivos actualizados con el último firmware.

Estadísticas sobre amenazas

Malware para móviles

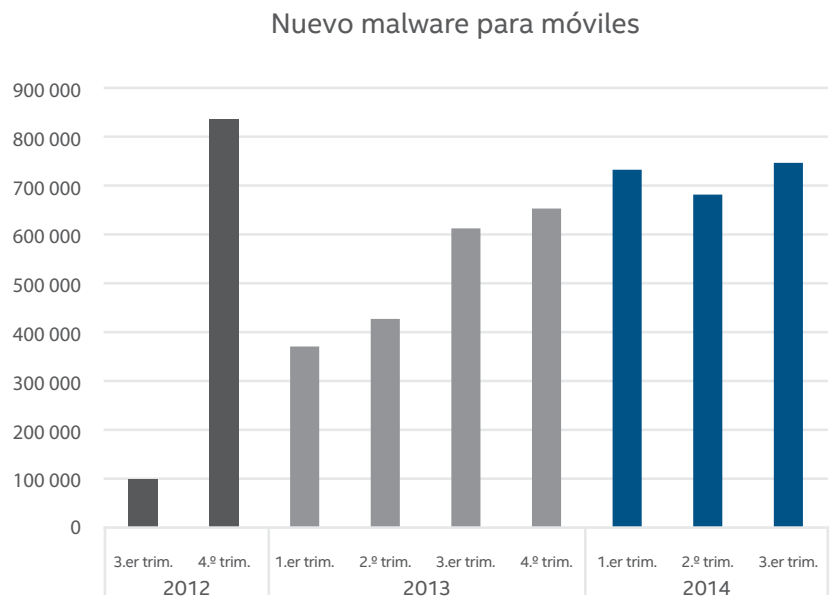
Malware

Amenazas a través de la Web

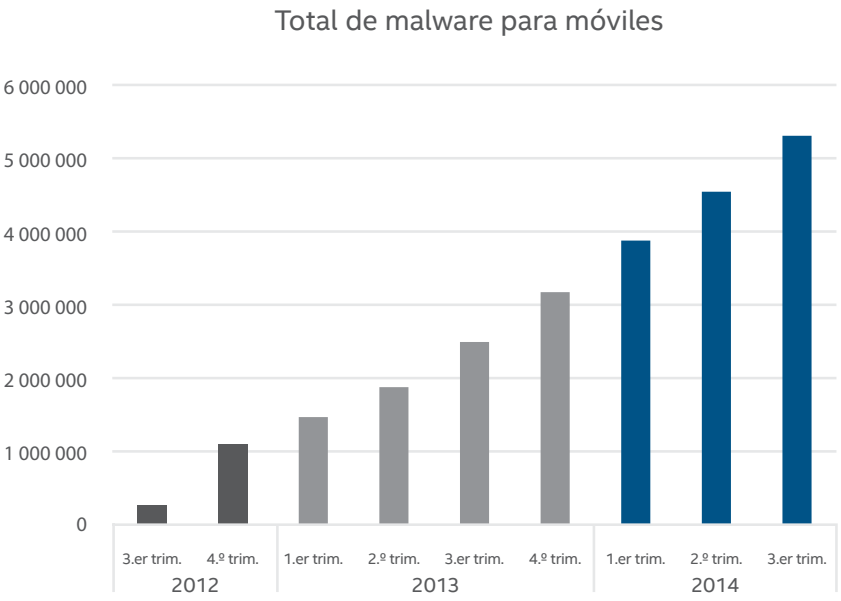
Amenazas a través de la red y propagadas por mensajería

Compartir opinión

Malware para móviles



Fuente: McAfee Labs.



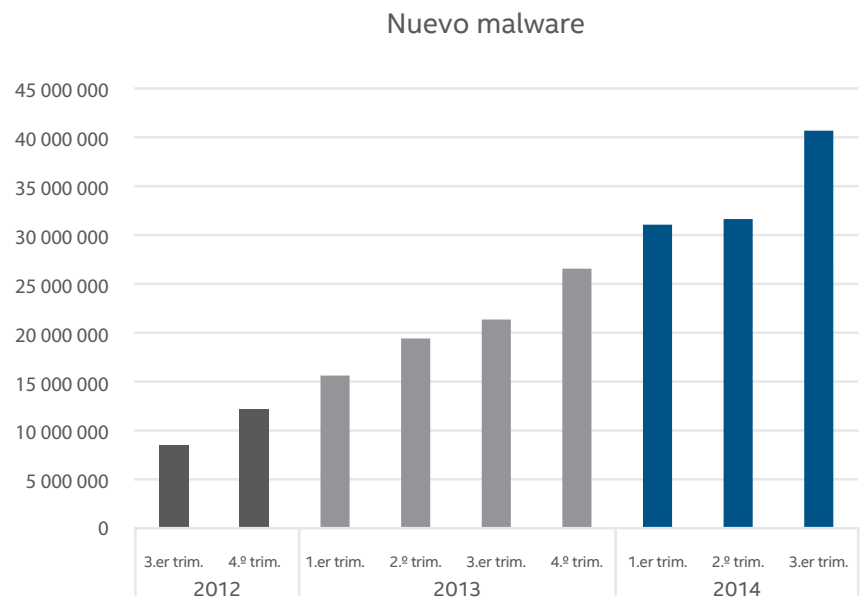
Fuente: McAfee Labs.

El número total de muestras de malware para móviles superó los 5 millones en el tercer trimestre de 2014, con un aumento del 16 % este trimestre y del 112 % respecto al año pasado.

Comparta este informe

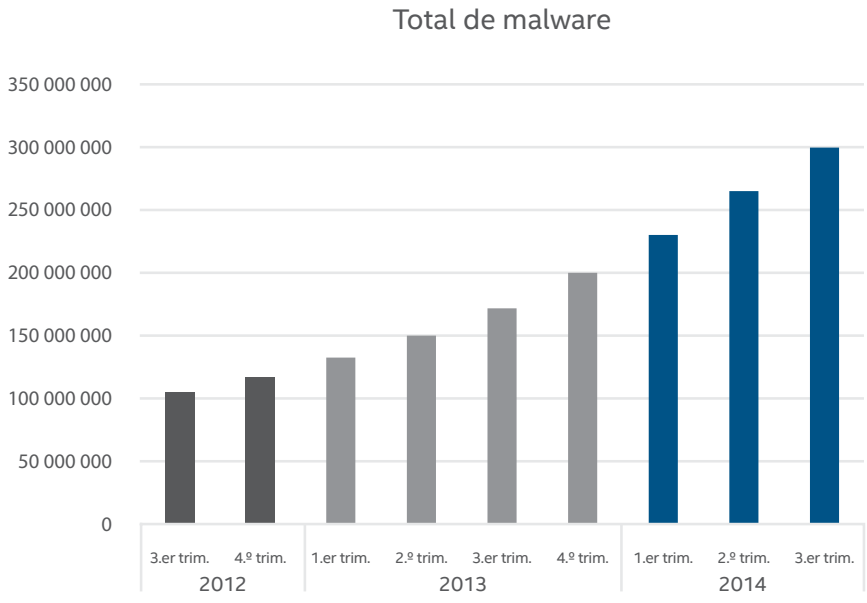
Malware

Hay más de 307 amenazas nuevas cada minuto, o más de 5 cada segundo.



Fuente: McAfee Labs.

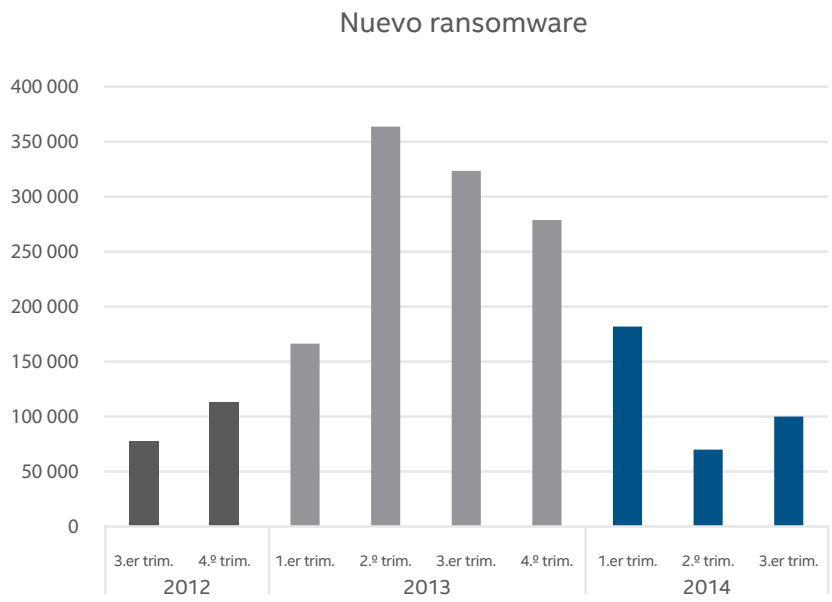
El "zoológico" de malware de McAfee Labs superó la barrera de los 300 millones de muestras en el tercer trimestre de 2014, con un aumento del 76 % respecto al año pasado.



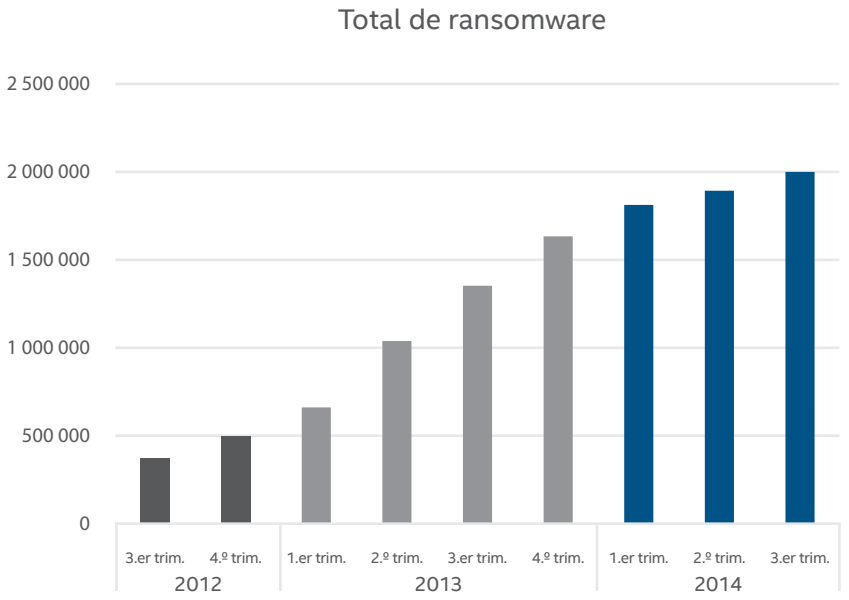
Fuente: McAfee Labs.

Comparta este informe

Tras cuatro trimestres, el número de muestras de ransomware nuevas ha dejado de disminuir. Nos sorprendimos con la caída, pero no nos extraña que la cifra vuelva a crecer.



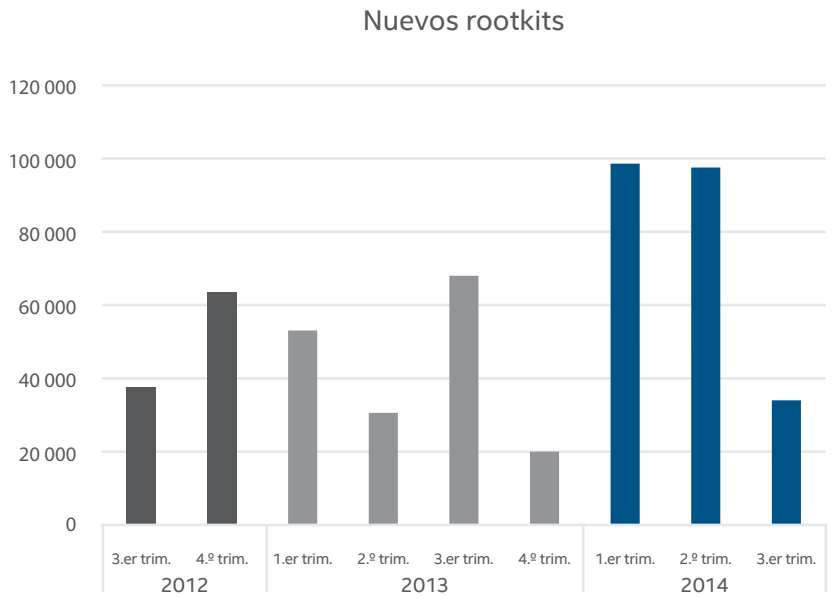
Fuente: McAfee Labs.



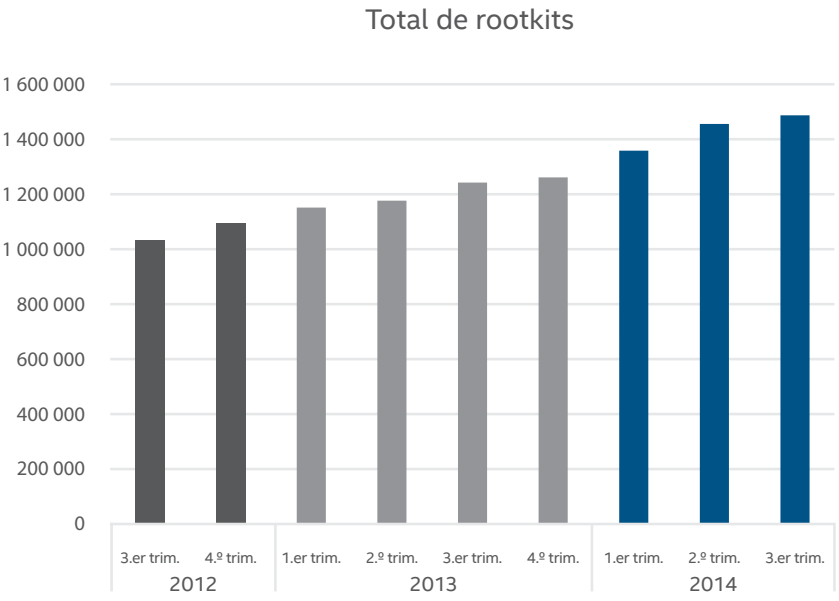
Fuente: McAfee Labs.

Comparta este informe

Los nuevos rootkits descendieron un 65 % en el tercer trimestre, reflejo de la volatilidad de esta forma de malware.



Fuente: McAfee Labs.

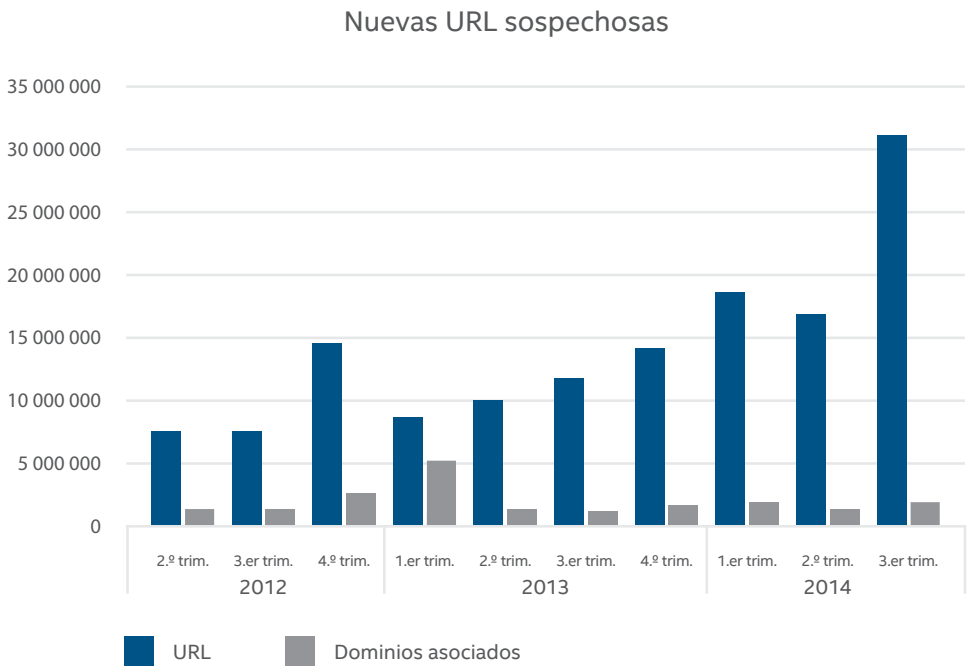


Fuente: McAfee Labs.

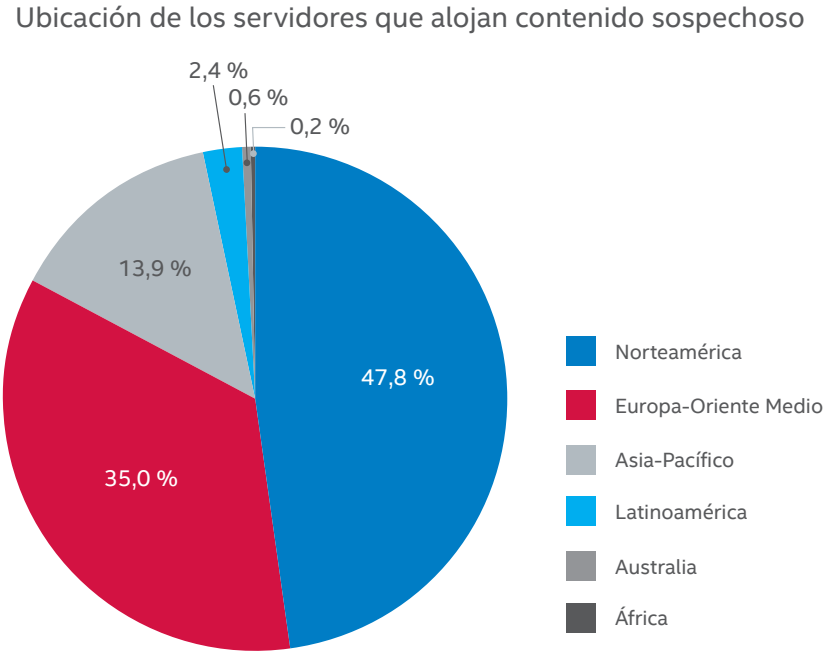
Comparta este informe

Amenazas a través de la Web

El número de nuevas URL sospechosas se ha disparado este trimestre. En parte este aumento puede atribuirse a una duplicación de nuevas URL abreviadas, que a menudo ocultan sitios web maliciosos, y a un acusado aumento en las URL de phishing.



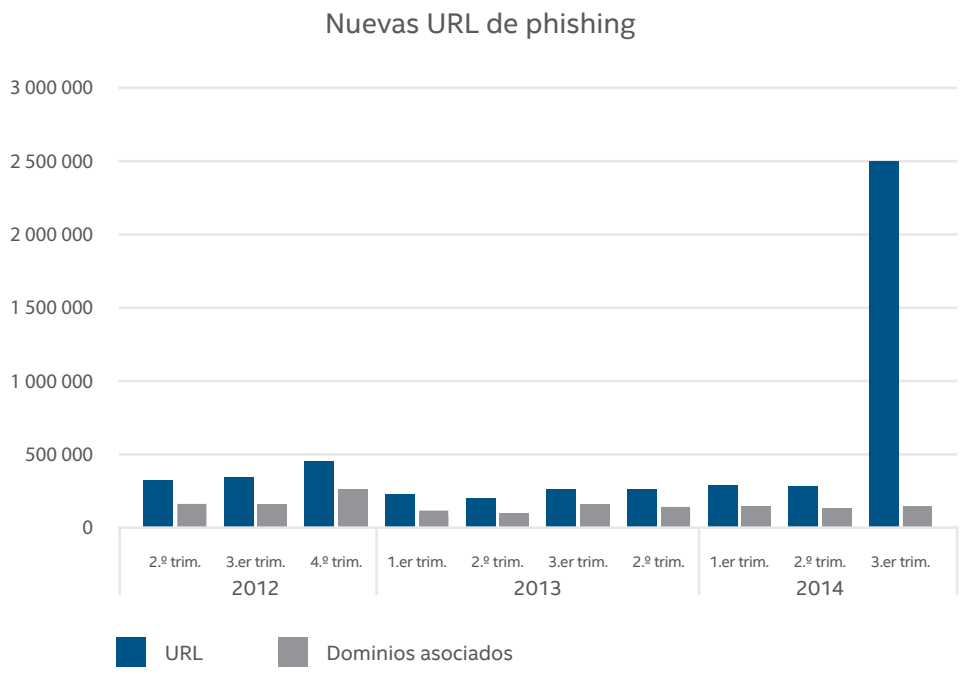
Fuente: McAfee Labs.



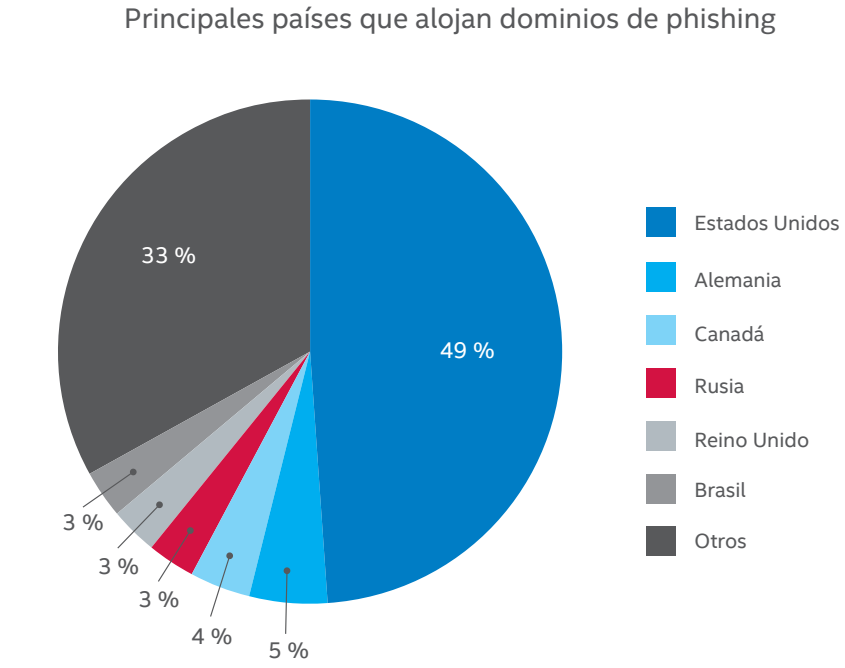
Fuente: McAfee Labs.

Comparta este informe

Atribuimos la gran diferencia de este trimestre a una campaña de phishing con spam de productos farmacéuticos rusos que crea un subdominio independiente para cada destinatario. En los datos recopilados se han incluido cada uno de estos subdominios.



Fuente: McAfee Labs.

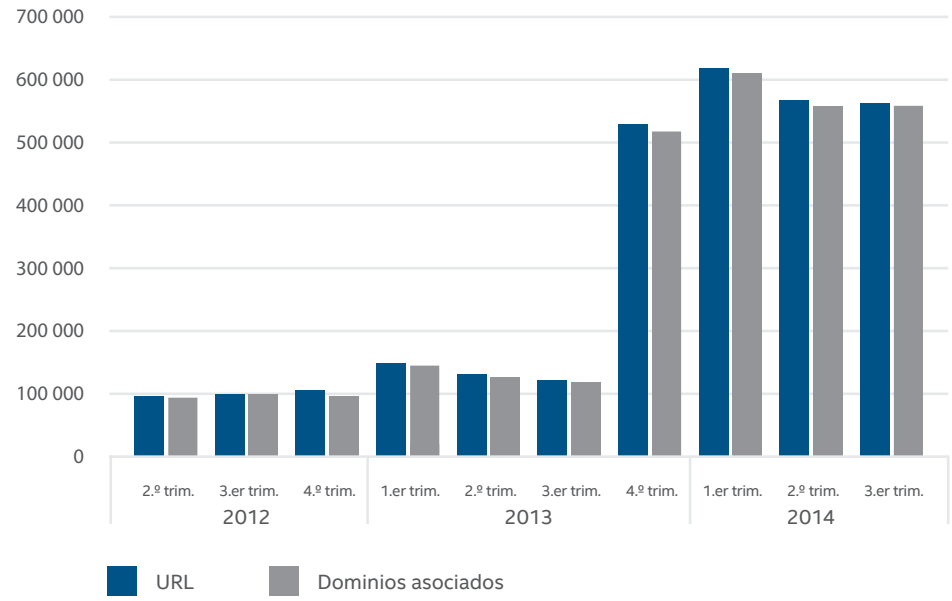


Fuente: McAfee Labs.

Comparta este informe

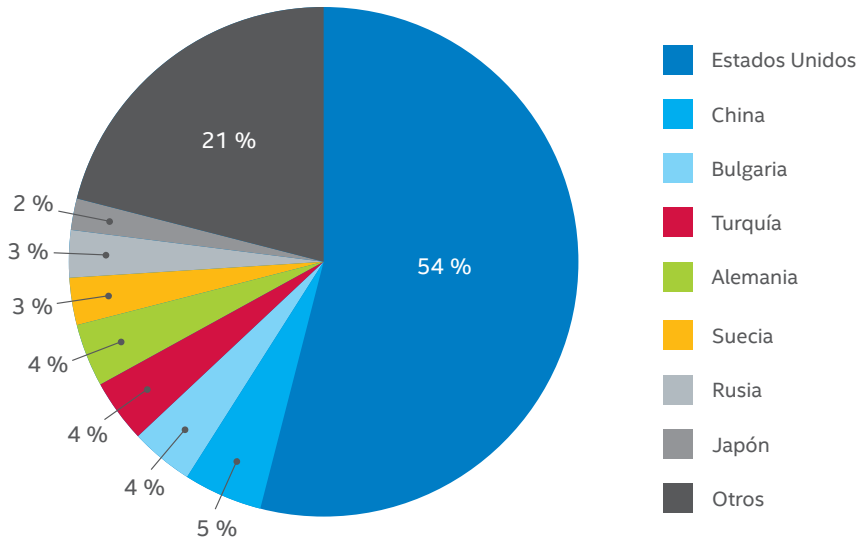
A partir de este trimestre, ofrecemos el total de nuevas URL de spam de todo el mundo. El número de URL nuevas en el tercer trimestre se redujo ligeramente en relación al segundo trimestre. La gran diferencia se produjo en el cuarto trimestre del año pasado, cuando mejoramos la recopilación de datos.

Nuevas URL de spam



Fuente: McAfee Labs.

Principales países que alojan dominios de spam

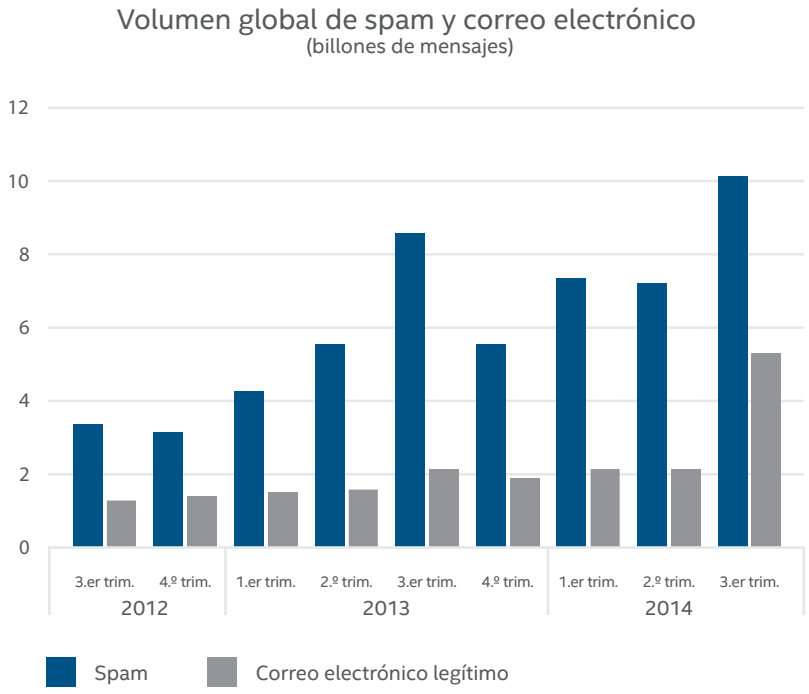


Fuente: McAfee Labs.

Comparta este informe

Amenazas a través de la red y propagadas por mensajería

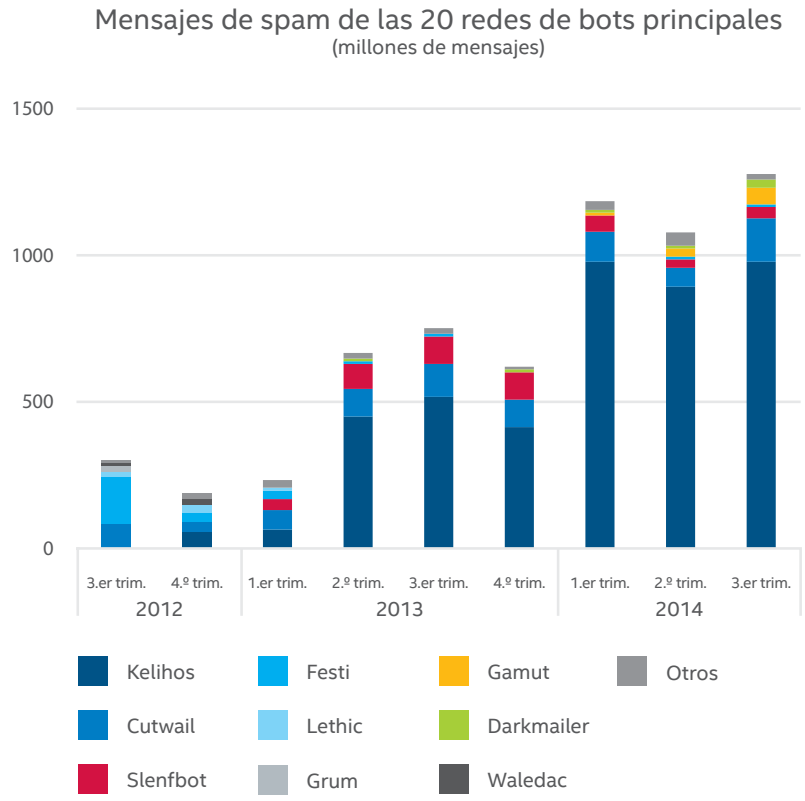
Este trimestre, el aumento del 148 % en el correo electrónico legítimo se debe a la mejora en nuestro método de recopilación de datos. La cifra no es directamente comparable con los trimestres anteriores, pero en el futuro tendremos una medida histórica más precisa del volumen de correo. Entre tanto, el volumen de spam ha aumentado un 40 %. En parte, lo atribuimos a nuestra técnica para recopilar datos, pero también a una mayor base de clientes, al aumento de la actividad de redes de bots y al incremento de spam de tipo "raqueta de nieve".



Fuente: McAfee Labs.

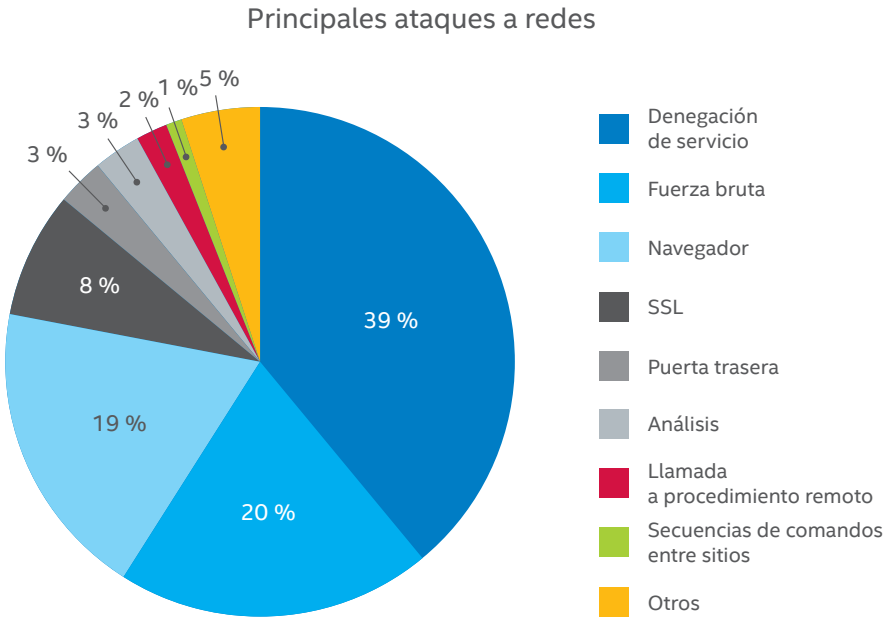
Comparta este informe

A partir de este trimestre, ofrecemos un nuevo desglose de las 20 primeras redes de bots de spam. Kelihos ha sido la red de bots más prolífica este año. En el tercer trimestre, los correos electrónicos de Kelihos contabilizaron el 76 % del spam generado por las 20 primeras redes de bots. Más recientemente, Kelihos se ha asociado con spam de mejora empresarial ("8 reglas sencillas reflejan la esencia de las ventas B2B"), spam de medicamentos ("Compre medicinas baratas. Ahorre hasta un 70 %") y spam para conseguir dinero rápido ("¿376 dólares en solo un día? ¿De verdad? Aquí tiene la prueba"). Kelihos está muy distribuido, con direcciones IP que envían spam procedentes de 226 países este año.



Fuente: McAfee Labs.

Este trimestre, los tres principales tipos de amenazas suman el 78 % de todas las amenazas. Los ataques de SSL pasaron a ser el 8 % en el tercer trimestre, desde el 5 % del segundo trimestre. Este aumento está posiblemente relacionado con el continuo ataque masivo de Heartbleed.



Fuente: McAfee Labs.

Comparta este informe

Comentarios. Para saber en qué dirección orientarnos, nos interesan sus opiniones. Si desea transmitirnos sus impresiones, **haga clic aquí** para completar un rápido cuestionario de solo cinco minutos sobre el informe de amenazas.

Siga a McAfee Labs

Acerca de Intel Security

McAfee ahora forma parte de Intel Security. Con su estrategia Security Connected, su innovador enfoque de seguridad reforzada por hardware y su exclusiva red Global Threat Intelligence, Intel Security trabaja sin descanso para desarrollar soluciones y servicios de seguridad proactivos que protejan los sistemas, las redes y los dispositivos móviles de uso personal y empresarial en todo el mundo. Intel Security combina la experiencia y los conocimientos de McAfee con la innovación y el rendimiento demostrado de Intel para hacer de la seguridad un ingrediente fundamental en todas las arquitecturas y plataformas informáticas. La misión de Intel Security es brindar a todos la tranquilidad para vivir y trabajar de forma segura en el mundo digital. www.intelsecurity.com.

www.intelsecurity.com

McAfee. Part of Intel Security.
Avenida de Bruselas n.º22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347
www.intelsecurity.com