Informe de Amenazas Móviles

Qué hay en el horizonte para el 2016

intel Security

Este Informe de Amenazas fue escrito por:

Bruce Snell, Director de Ciberseguridad y Privacidad de Intel Security

Contenido

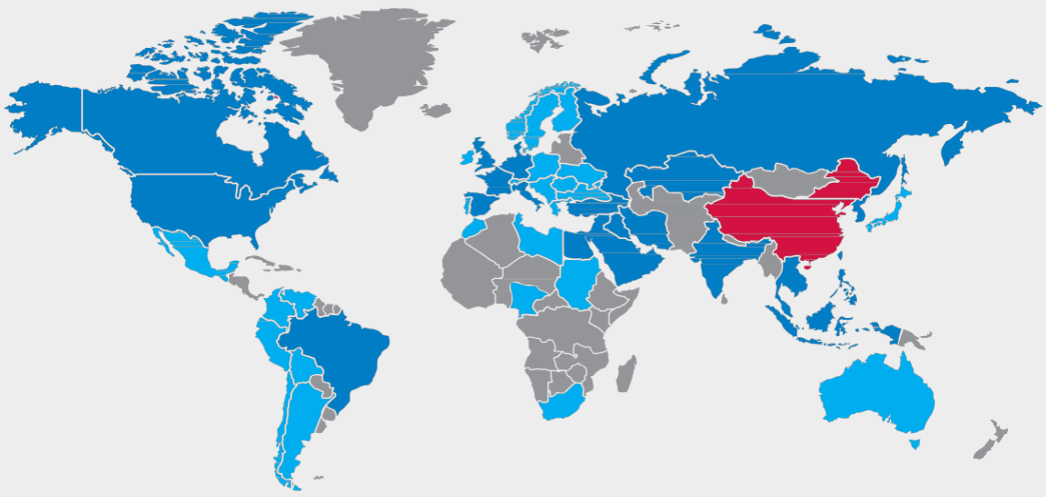
Descubrimos que el panorama de las amenazas móviles continúa creciendo y evolucionando con varios factores que contribuyen a ello. El aumento de la velocidad, potencia y espacio de almacenamiento en los dispositivos móviles ha hecho que más personas utilicen sus dispositivos en más lugares para compras online, administrar sus finanzas y pagar sus cuentas. Esto hace que la movilidad se convierta en un blanco mucho más valioso para los ciberdelincuentes. El año pasado observamos cómo las principales vulnerabilidades en el sistema operativo Android cambió la manera en que Google considera a las actualizaciones de seguridad. También observamos un agresivo espionaje de adware hacia sus hábitos de televisión y radio. Además observamos un incremento en malware más avanzado que trae las amenazas con las que ha estado lidiando por años en las PCs hacia el mundo móvil. El ransomware, los fraudes bancarios y las herramientas de acceso remoto (RATs), han incrementado su presencia en los dispositivos móviles.

Regla de las tres principales amenazas que enfrentan los usuarios móviles:

1. Android ha iniciado actualizaciones de seguridad mensuales, pero cada fabricante es responsable de implementar las actualizaciones, lo que frecuentemente genera retrasos
2. El malware sigue escabulléndose en las app stores
3. Los ciberdelincuentes están expandiendo sus esfuerzos en el espacio móvil

¿Cómo afectarán estas nuevas amenazas a sus dispositivos móviles? En nuestro último informe, detallamos las maneras en que las aplicaciones comparten en exceso su información; ahora observaremos los grandes números de aplicaciones infectadas que logran evadir el proceso de filtrado y aparecen en las app stores confiables. Ahondemos en algunos de los mayores problemas del 2015 que están causando impacto al ámbito móvil en el 2016 y más allá.

Malware Móvil 2016 ¿Qué Pasa en 1 Hora?



Intel Security: Malware detectado de más de 190 países por hora.

> 6000 | 100 – 1000 | 10 – 100

Fuente: McAfee Labs 2016

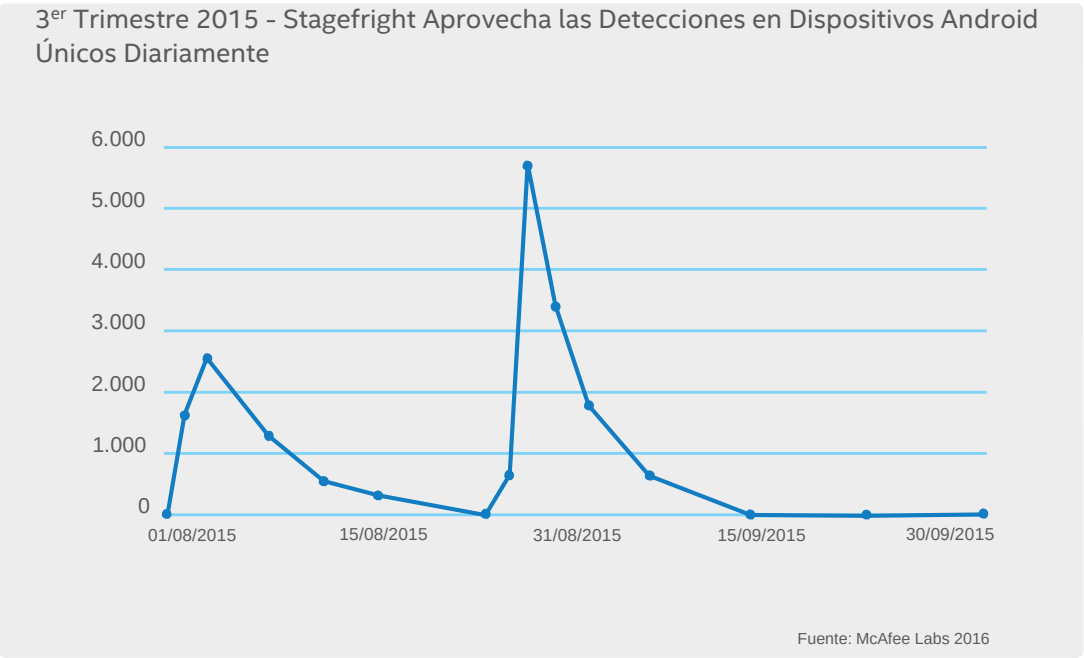
Stagefright: Preparando el Camino para Mayor Seguridad

Este pasado verano en los días previos a la conferencia anual de seguridad Black Hat en Las Vegas, diversas vulnerabilidades fueron encontradas en los sistemas operativos Android. Esta colección de errores se denomina "Stagefright" en referencia a las bibliotecas stagefright (código subyacente en el sistema operativo que se comparte por muchas aplicaciones) contenidas en el sistema operativo Android. Estas vulnerabilidades son especialmente desagradables debido al hecho de que permiten a un atacante ejecutar código de forma remota en el teléfono de alguien enviado un mensaje MMS especialmente diseñado. Normalmente, un ciberdelincuente intenta engañar al usuario para que haga clic en un enlace Web malicioso o instalando una aplicación infectada. Ninguno de estos pasos es necesario con Stagefright. Si alguien sabe el número de teléfono del blanco previsto, eso es todo lo que necesita para lanzar un ataque. Más temible aún, debido a la naturaleza de los errores, sería posible que un atacante piratee un teléfono, implante una herramienta de acceso remoto, y cubrir cualquier rastro que el ataque ocurrió; todo ello mientras el teléfono se estaba cargando durante toda la noche en la mesa de noche de la víctima.

Pasos para reducir vulnerabilidades Stagefright:

1. Desactivar mensajes MMS
2. Actualice el software de su teléfono
3. No abra mensajes de desconocidos
4. Use software de seguridad completo

Observando los resultados de nuestro equipo móvil de McAfee Labs, podemos ver el número de dispositivos que informan de un ataque Stagefright, llegando a un poco más de 5000 dispositivos individuales atacados hacia finales de agosto, lo cual sucedió aproximadamente dos semanas después de que una vulnerabilidad adicional Stagefright fue descubierta.



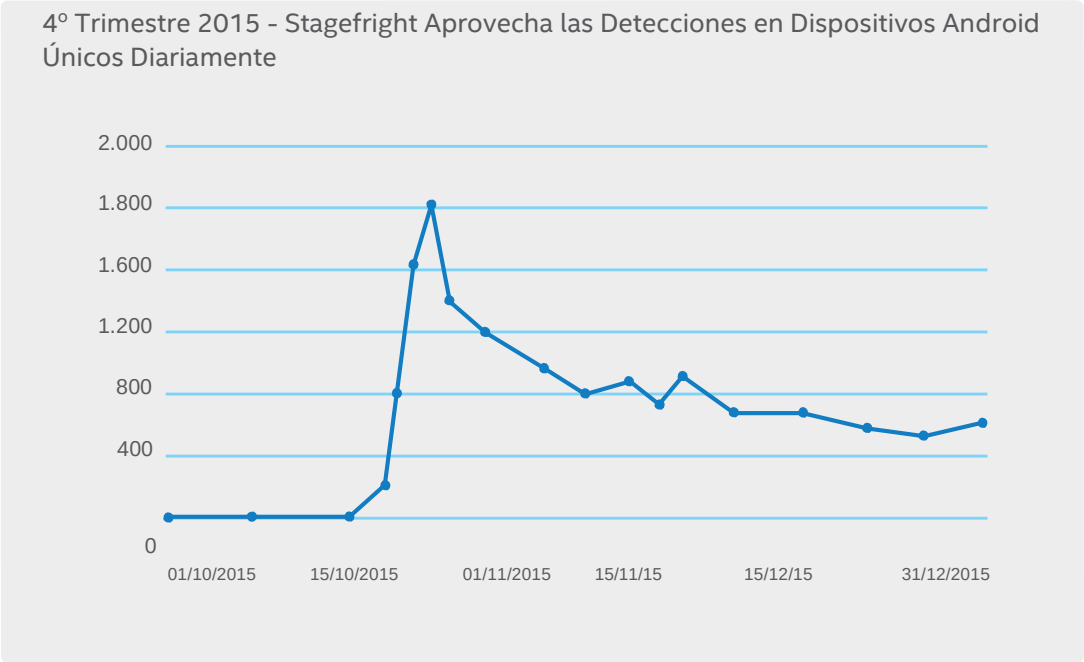
Las detecciones de la primera versión de Stagefright se dispararon poco después de que el código de prueba de concepto fue lanzado en la conferencia de seguridad Black Hat.

En octubre, en otra ronda de vulnerabilidades Stagefright fue liberada (apodada Stagefright 2), esta vez especialmente diseñada utilizando archivos mp3 y mp4 para aprovechar una vulnerabilidad en una biblioteca central de Android (libutils) que ha existido desde que se lanzó la primera versión de Android. Esto implica que los dispositivos que ejecutan Android 1.5 a 5.1 son vulnerables a este ataque, que son cercanos a 1 mil millones de dispositivos.

Debido a su amplia gama de dispositivos vulnerables, esta nueva versión generó otro repunte de

malware basado en Stagefright que continuó ininterrumpidamente hasta finales de 2015.

Ramificaciones de Stagefright: Google cambió a actualizaciones de seguridad mensuales.



Fuente: McAfee Labs 2016

Poco después del anuncio de "Stagefright 2.0" el 01/10/15, el número de dispositivos únicos Android que detectaban aprovechamiento de vulnerabilidades basadas Stagefright ha permanecido estable.

¿Qué Significa Esto para el Consumidor?

Stagefright provocó un cambio radical en la forma en que Google maneja los parches de seguridad. Históricamente, no había una programación establecida para las actualizaciones, pero tras los eventos del verano de 2015, Google se ha comprometido a implementar actualizaciones mensualmente. Sin embargo, es importante señalar que estos parches de seguridad se distribuyen hacia otros fabricantes y operadores inalámbricos, y depende de empresas el proporcionar estas actualizaciones a sus clientes. El lado positivo es que ahora hay actualizaciones mensuales, pero el aspecto negativo consiste en que las actualizaciones pueden tardar algún tiempo en llegar a todos los dispositivos Android. Como se puede ver en el gráfico anterior, los ataques de stagefright han continuado ininterrumpidamente desde el lanzamiento de la vulnerabilidad. Si aún no se ha aplicado el parche en su dispositivo para estas vulnerabilidades, puede seguir estos pasos para reducir el peligro de infección:

- **Desactivar recuperación automática de MMS.** Esto no es necesariamente conveniente, pero usted debe desactivar la capacidad de su teléfono de recuperar automáticamente mensajes MMS (Servicio de Mensajes Multimedia) mientras Stagefright siga representando una amenaza. Toque en el icono "mensaje" en la pantalla de inicio de Android. A continuación toque los tres puntos (o líneas) en la esquina superior derecha y desplácese hasta configuración. Desplácese hasta que vea "MMS" y cambie ese conmutador a la posición "off". También puede ir a determinadas aplicaciones para ajustar la configuración que pueda cargar automáticamente archivos adjuntos de MMS.
- **Actualice su teléfono periódicamente.** Muchas actualizaciones contienen parches de seguridad para vulnerabilidades previamente desconocidas en sus dispositivos. Cuando usted sepa de una nueva actualización de software, o reciba un aviso de actualización, actualice su dispositivo. Implementar actualizaciones a medida que estén disponibles es una de las mejores maneras de proteger su dispositivo de ataques como el de Stagefright.
- **No abra mensajes de desconocidos.** No abra ni acepte mensajes de texto de gente que no conoce. Los textos de números desconocidos pueden ser un intento de infectar su dispositivo con Stagefright o con otra vulnerabilidad desconocida.

- **Use software de seguridad completo.** Independientemente de si está en un celular, laptop o dispositivo de sobremesa, necesitará protegerse de los ciberdelincuentes.

¿Su Teléfono Controla lo que Ve en la Televisión?

En nuestro informe anterior sobre amenazas, hablamos acerca de las aplicaciones que estaban agarrando los datos desde su teléfono sin su conocimiento. Ahora, una compañía de la India ha lanzado un kit de desarrollador de software de publicidad (SDK) llamado SilverPush que utiliza el micrófono de su teléfono para escuchar sonidos casi ultrasónicos colocados en televisión, radio y publicidad en la Web. Una vez SilverPush detecta la señal, recopila los datos de su dispositivo y envía información acerca de su dispositivo al anunciante. Aunque esto no es malware propiamente dicho, es una enorme preocupación desde una perspectiva de privacidad. Recopila información personal de su dispositivo, incluyendo, pero sin limitarse a:

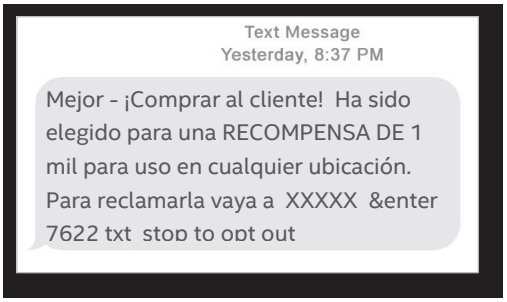
El problema de SilverPush
Su teléfono podría estar monitoreando lo que ve en la televisión sin su conocimiento o permiso.

- Número IMEI (un número único que identifica su teléfono).
- Versión del sistema operativo
- Ubicación
- Potencialmente la identidad del propietario
- El comportamiento en televisión, radio y web del usuario

SilverPush no es una aplicación autónoma, sino que está incorporada como parte de otra aplicación y normalmente se ejecuta sin el consentimiento del usuario. Si una aplicación en su dispositivo móvil es detectada como de contener SilverPush, la mejor solución es eliminar esa aplicación desde su dispositivo.

SMiShing Continúa Evolucionando

El SMiShing (phishing de SMS) ha continuado creciendo en popularidad como una herramienta de ingeniería social para los ciberdelincuentes. El objetivo de SMiShing es engañar al usuario para que haga clic en un enlace en un mensaje de texto; ese enlace va hacia una página que le pedirá que ingresar sus datos personales. El objetivo es obtener acceso a información confidencial como nombres de usuario y contraseñas. Además, muchos mensajes SMiShing incluirán enlaces con malware esperando en el otro lado a cualquiera que haga clic en ellos.



Frecuentemente un intento de SMiShing es fácil de localizar, con afirmaciones de que han ganado un concurso en el que nunca participó o un "reembolso no reclamado" esperando por usted. Muchas de las mismas técnicas que se utilizan en correos electrónicos de phishing han llegado al mundo de SMiShing. Aunque la mayoría de los intentos de SMiShing aparecerán como un número desconocido, haciéndolos parecer sospechosos para los usuarios atentos, los usuarios de banca móvil en China recientemente han comenzado a recibir textos de SMiShing que parecen provenir desde el número de teléfono oficial de su banco. Los teléfonos móviles están diseñados para saltar de una red a otra con el fin de mantener la conexión mientras se viaja. Los ciberdelincuentes pueden utilizar este diseño para configurar una estación base falsa con una herramienta de envío masivo de mensajes SMS para enviar mensajes de texto que parezcan ser completamente legítimos. Si la estación base falsa produzca una señal más fuerte que la estación base real y, cualquier persona que viaje a través del área recibirán el texto. El hardware necesario para esta configuración es relativamente barato y puede ser operado desde la parte trasera de un vehículo. Entonces es una simple cuestión de conducir a través un área poblada, enviando algunos textos en masa y, a continuación, pasar a la siguiente área.

Una reciente campaña en China envió mensajes diciendo que la cuenta bancaria del cliente pronto estaría indisponible, con instrucciones para iniciar sesión y validar la información de su cuenta. El hacer clic en el enlace llevaría al usuario a un sitio móvil que imitaba al sitio Web oficial del banco y solicitaba al usuario ingresar su cuenta bancaria, contraseña y su número de celular. Observando las siguientes imágenes, usted puede ver qué tan bien la interfaz falsa de la izquierda coincide con la interfaz legítima de la derecha.

¿Qué puede hacer para permanecer seguro?

La mejor defensa contra el SMiShing es aprender a reconocer mensajes de texto sospechosos. Si usted no hace clic en el enlace, el peligro de SMiShing disminuye dramáticamente. En nuestro blog de consumidor, mostramos algunos ejemplos de cosas que se deben buscar para detectar correos electrónicos de phishing y la mayoría de las reglas de detección de correos electrónicos de phishing aplican a SMiShing.

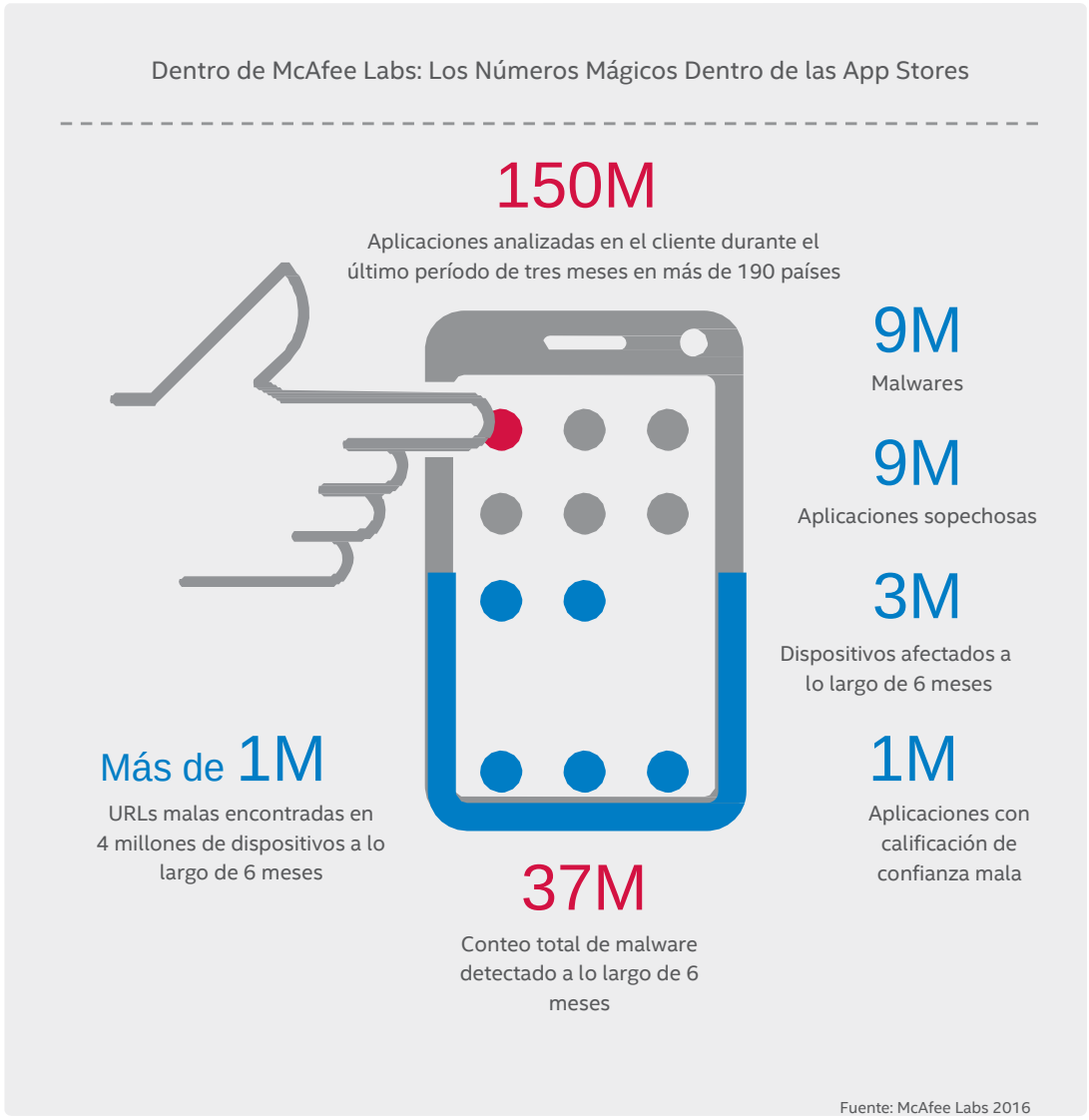
Obtenga la primicia aquí.

Peligros de las App Stores

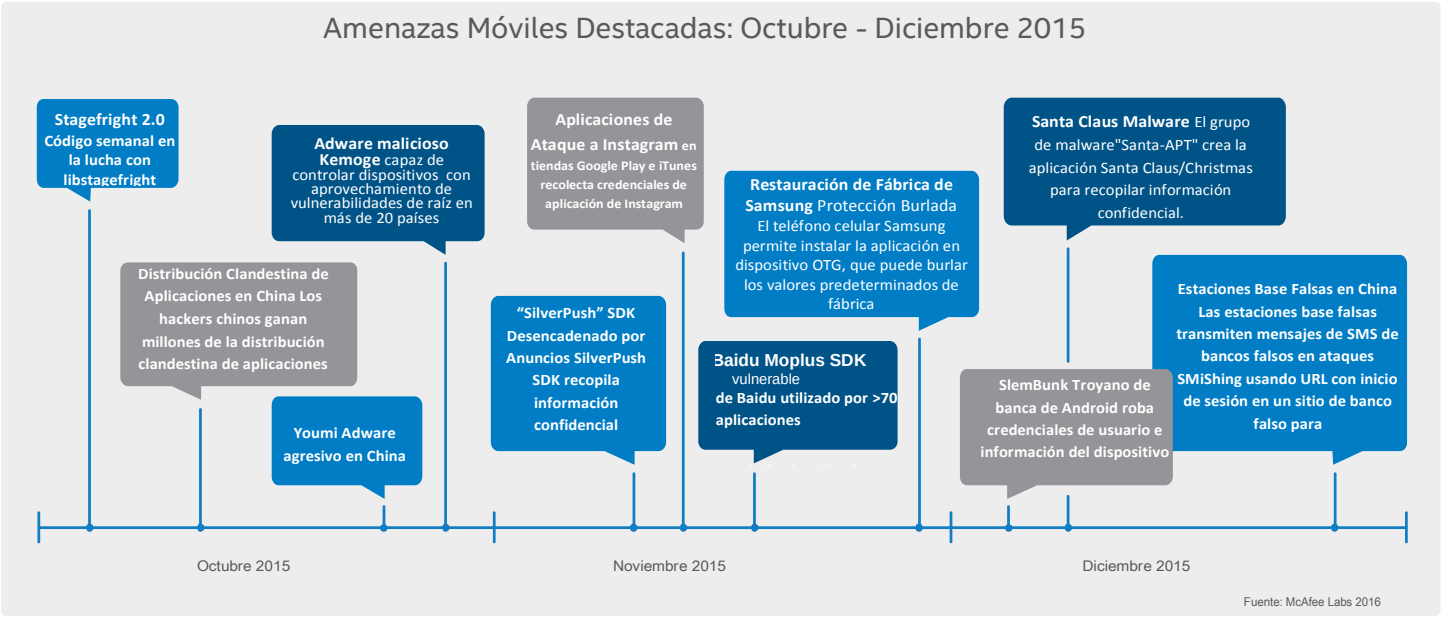
Durante el año pasado hubo cientos de aplicaciones removidas de Google Play y de Apple App Store debido a motivos de seguridad. Para los iOS, la mayor amenaza este año provino de aplicaciones con adware extremadamente agresivo, mientras que Google Play vi un número igual de importante de aplicaciones infectadas con malware. Tanto Google como Apple han removido rápidamente a las aplicaciones maliciosas de sus app stores asociadas, sin embargo es inevitable que algunas aplicaciones infectadas todavía se escabullan en el proceso de filtrado.

Durante los pasados seis meses, McAfee Labs ha explorado sigilosamente las app stores para detectar problemas de seguridad y obtuvo diversos resultados interesantes:

Siempre hay algo nuevo:
Durante la elaboración de este informe, se descubrió que más de 60 juegos de Android hospedados en Google Play estaban infectados con "Android. Xiny.19.origin" que oculta ejecutables Android (APKs) dentro de imágenes para evitar su detección.

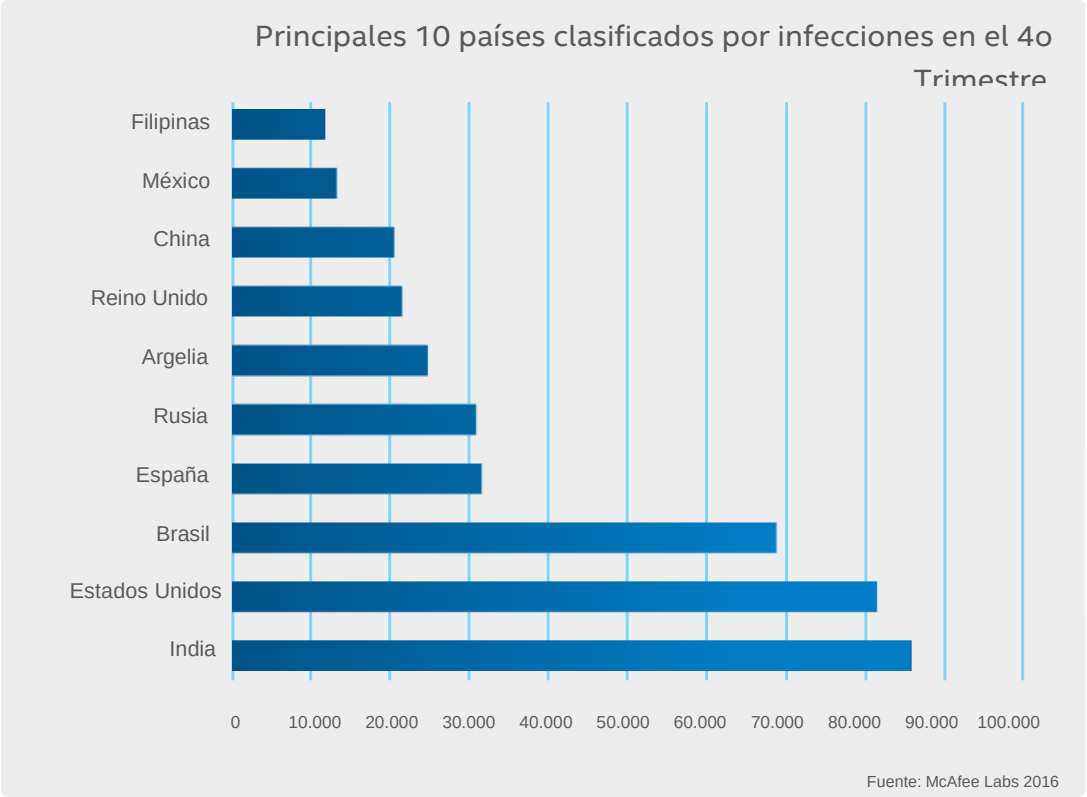


McAfee Labs analiza rutinariamente las principales app stores para detectar sistemas infectados, así como aplicaciones con un comportamiento sospechoso.



McAfee Labs

McAfee Labs es la división de investigación de amenazas de Intel® Security y una de las principales fuentes del mundo para investigación de amenazas, inteligencia de amenazas y liderazgo de opinión con respecto a la ciberseguridad. Los investigadores de amenazas de McAfee Labs correlacionan los datos del mundo real recolectados de millones de sensores a lo largo de vectores de amenazas claves -archivos, web, mensajes y red- y proporcionan inteligencia de amenazas en tiempo real para aumentar la protección y reducir el riesgo.



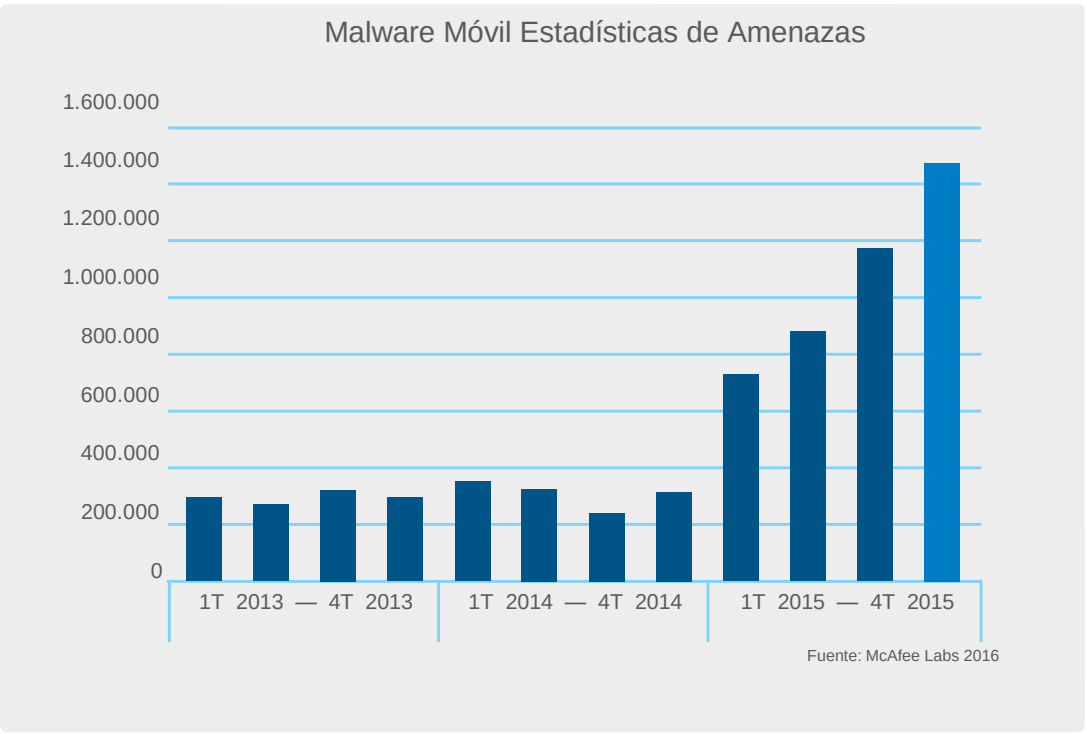
Estos números representan el total de infecciones únicas con infecciones repetitivas descartadas.

El Malware Móvil Crece

Durante el año pasado observamos un dramático aumento en la cantidad de nuevo malware, pero también observamos un aumento en la sofisticación y complejidad. También hay en cierto grado un círculo vicioso con el malware. Los parches de seguridad son liberados, lo que hace que la mayoría del malware actual sea obsoleto. Posteriormente, los autores de malware buscan nuevas vulnerabilidades y liberan nuevo malware o variantes de malware antiguo para burlar las nuevas protecciones. Para agravar el problema, los autores del malware empacarán su malware como un kit para aprovechar vulnerabilidades para su venta a otros ciberdelincuentes. A continuación se emiten nuevos parches para corregir las vulnerabilidades recién descubiertas, y el ciclo comienza de nuevo.

McAfee Labs recolectó muestras de malware móvil únicas - aumento del 24% desde el 3er Trimestre

Históricamente, el malware móvil ha en cierta medida una idea adicional para los ciberdelincuentes, siendo que la mayoría de sus esfuerzos se enfocaron en las PCs. Sin embargo, durante el último año hemos observado un aumento dramático no sólo en el número de malware nuevo, sino también en la sofisticación y complejidad del malware móvil.

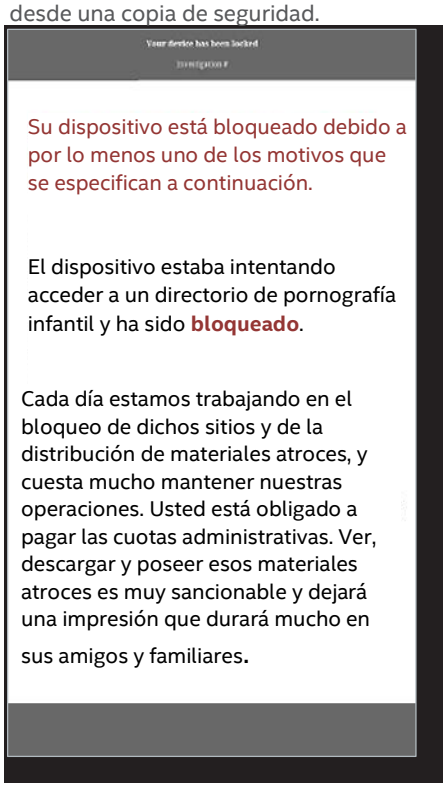


Un troyano llamado "SlemBunk" fue descubierto a mediados de diciembre que se comporta de forma muy parecida a una amenaza persistente avanzada (APT) que uno encontraría atacando a una PC. Se instala por mediante una descarga desapercibida (es decir, el usuario simplemente tiene que visitar un sitio infectado para infectarse), instala un downloader en segundo plano y se comunica con un servidor de comando y control de backend y extrae el último código de actualización para el malware. Esta configuración tiene todas las marcas distintivas de una sofisticada campaña de ciberdelincuencia y podría convertirse en un problema grave en 2016.

También hemos observado herramientas de acceso remoto (RAT) fácilmente disponibles en Internet para su venta. Una herramienta en concreto incluso tiene un sitio web bien elaborado que pone a la mayoría del software comercial en vergüenza con tutoriales, diversos modelos de precios y sistemas de pago fáciles de usar. Ahora, en lugar de sumergirse en la Dark Web, puede utilizar moneda electrónica común para comprar un paquete de cliente y servidor que le permitirá controlar los sistemas infectados (tanto para PCs como para celulares) desde su plataforma preferida.

¿Huelo a RAT?
La herramienta de acceso remoto, comúnmente conocida como RAT, es utilizada por los hackers para obtener el control completo de un sistema. Por lo general se utilizan por los ciberdelincuentes en un modelo de cliente/servidor en el que un gran número de sistemas infectados son controlados por un sistema para lanzar ataques contra otros sistemas, para enviar SPAM, o para cualquier tipo de cosas nefastas. En los últimos años, los RATs se han vuelto más robustos y elaborados con funcionalidades que rivalizan con las herramientas de gestión remota comerciales.

Junto las APTs y las RATs que ganan más tracción en la movilidad, también observamos un aumento de ransomware en Android. Mientras que el ramsonware en PC tiende a cifrar archivos y exigir un rescate para desbloquearlos, el ransomware de Android se enfoca más en el bloqueo del dispositivo de un usuario hasta que se pague una cuota. Debido a que se hacen copias de seguridad más frecuentemente en un dispositivo móvil que una PC, los autores ransomware suelen combinar una falsa amenaza legal junto con el bloqueo, asustando a la víctima para que pague en lugar de simplemente limpiar el sistema y restaurarlo desde una copia de seguridad.

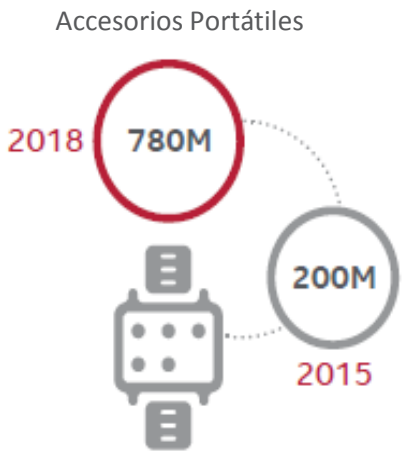


Por ejemplo, Svpeng dice al usuario que el sistema se bloqueó porque estaba tratando de acceder a un sitio web que contiene pornografía infantil y que para desbloquear su sistema debe pagar una "cuota administrativa". El ransomware también hará uso de la cámara del dispositivo para tomar una foto del usuario como una "táctica para asustar" adicional.

Mirando Hacia Adelante: IoT y Accesorios Portátiles

Las estimaciones actuales de la industria estiman que el número de accesorios portátiles conectados a Internet será de alrededor de 780 millones para 2018, lo que se traduce en un dispositivo portátil en una de cada 10 personas en la Tierra. Si consideramos menos dispositivos portátiles en los países en desarrollo, ese número está probablemente más cercano que una de cada cuatro o cinco personas en los países más ricos que tendrán algún tipo de accesorio portátil.

Desde la perspectiva de un hacker, las áreas densamente pobladas representan un ambiente rico en blancos para atacar a los accesorios portátiles. Aunque irrumpir en un dispositivo accesorio portátil no necesariamente proporciona valor inmediato al hacker, el valor real yace en la conexión de accesorio portátil a un smartphone.



La mayoría de estos dispositivos utilizan la tecnología Bluetooth LE (low energy), que ha sufrido una serie de fallas de seguridad muy bien documentadas y probablemente se producirán más con cada nueva versión. Esto hace que la conexión entre el accesorio portátil y el dispositivo móvil sea más fácil para que los hackers accedan a una gran cantidad de información personal y confidencial.

¿Seguridad inteligente desde un hogar inteligente?

Estamos observando un crecimiento enorme en el Internet de las Cosas (IOT, por sus siglas en inglés), incluyendo un gran empuje hacia dispositivos conectados a Internet, termostatos y más. Conforme el número de estos dispositivos crece, los ciberdelincuentes podrán comenzar a mirar hacia los ataques a IoT como una forma de afianzarse en su red doméstica.

Permanezca Seguro

Como hemos visto en este informe, las amenazas móviles siguen aumentando en frecuencia y complejidad. A medida en que nos hacemos más dependientes de nuestros dispositivos móviles, debemos pensar más acerca de la seguridad conforme realizamos nuestras actividades cotidianas. Aquí presentamos algunos consejos para ayudarle a mantener su vida digital segura.

1. **¡Actualice!**

Para mantener sus datos seguros y privados, tiene que prevenir que los ciberdelincuentes penetren en sus dispositivos. La mayoría de las infecciones de malware podrían prevenirse simplemente manteniendo su sistema actualizado con la última versión del sistema operativo y las actualizaciones de aplicaciones.

2. **Sólo Use App Stores Oficiales**

En la medida en que Intel Security analiza las app stores para detectar aplicaciones maliciosas, las app stores son alertadas cuando se encuentran nuevas aplicaciones maliciosas, así que incluso si algo es pasado por alto, usted estará más seguro yendo a una app store confiable que a una fuente no verificada.

3. **Revise las Puntuaciones de Reputación de Aplicación**

Hemos descubierto que hay muchas aplicaciones que aunque técnicamente no son maliciosas, revelan demasiada información personal sin tener un motivo legítimo. Debido a esto, es importante estar consciente de la reputación de seguridad y privacidad de una aplicación.

4. **¡Desconfíe!**

Los ciberdelincuentes intentarán todo tipo de métodos para obtener sus datos y uno de los más exitosos métodos es la ingeniería social. Sea siempre cauteloso al hacer clic en cualquier enlace de un mensaje de correo electrónico o SMS que no esperaba. Esto incluye mensajes de personas que conoce, ya que pueden haber sido infectados y no se dan cuenta de que están enviando malware.

5. **Use Software de Seguridad Completo**

Mantener su dispositivo móvil actualizado le ayudará a estar a salvo de virus antiguos, pero también debe instalar el software antivirus en sus dispositivos para protegerse contra nuevas o antiguas amenazas que aún no han sido arregladas por actualizaciones de sistema operativo o de aplicaciones. La mayoría tienen otros beneficios tales como la búsqueda de aplicaciones que puedan ser sospechosa en función de los permisos que están pidiendo, y notificarle cuando va a conectarse a

una Wi-Fi potencialmente insegura.

Resumen

Los smartphones y las tablets representan increíbles herramientas para mantenerse conectado con sus amigos y familiares, para actualizarse instantáneamente con relación al trabajo, para realizar compras, para pagar nuestras facturas y para gestionar nuestro tiempo libre. Los ciberdelincuentes observan una oportunidad de depredar a las víctimas atacando sus dispositivos móviles, impulsando un aumento en el número y sofisticación de las amenazas. Esperamos que esta tendencia continúe durante el próximo año, lo que requerirá mayor diligencia y concienciación tanto por parte de la industria de la seguridad, como por parte de los usuarios finales. Nos parece que esto será aún más complejo en la medida en que los consumidores llevan dispositivos conectados a sus hogares y utilicen más accesorios portátiles.

McAfee. Parte de Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com