ENJOY SAFER TECHNOLOGY™

GUÍA DE SEGURIDAD PARA

Dispositivos Móviles

Introducción

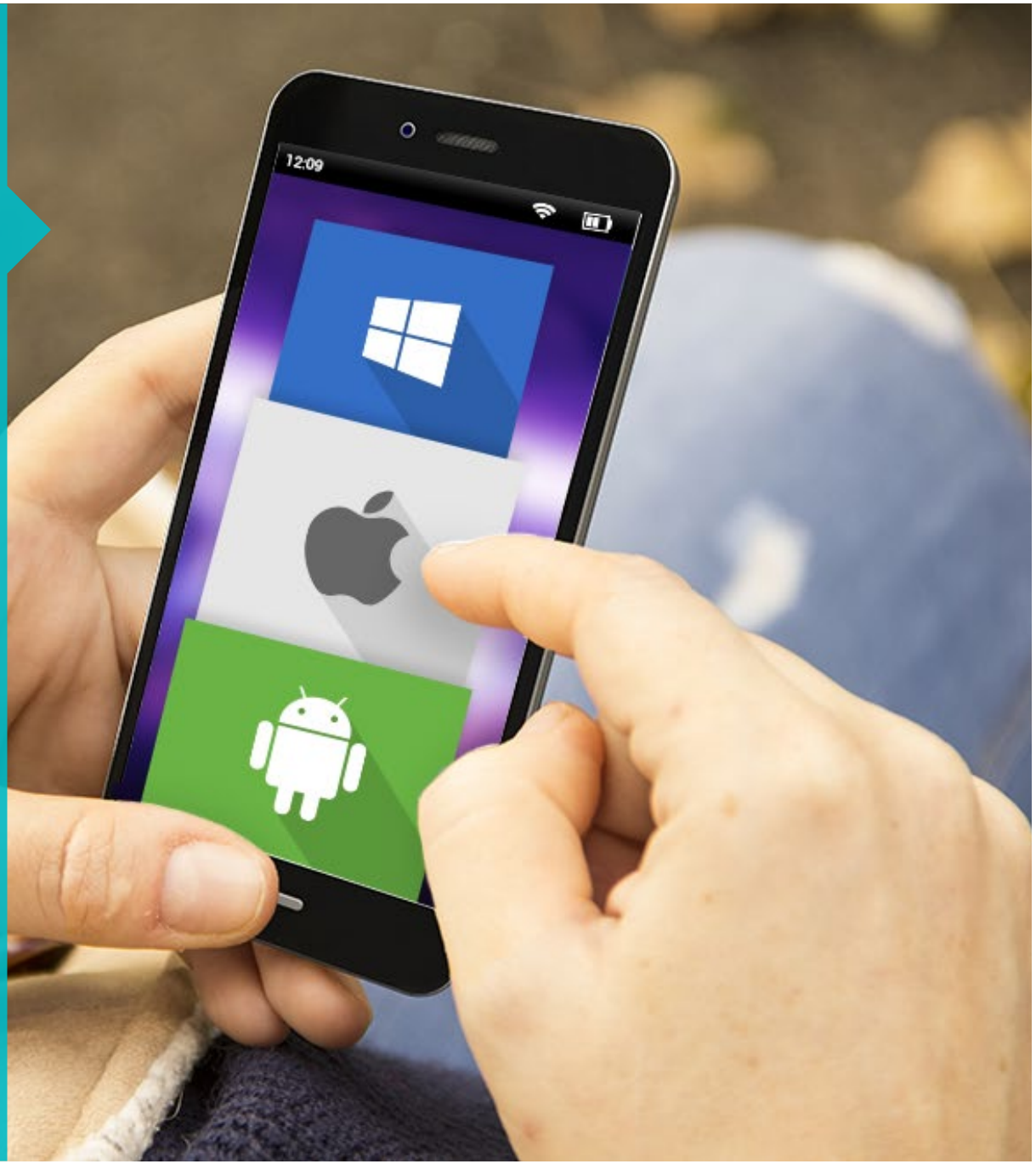
Con el pasar de los años, los teléfonos móviles han experimentado una intensa evolución e incorporado nuevas capacidades y servicios. En ellos, los usuarios almacenan cada vez más información personal y sensible que, además de estar expuesta al hurto o extravío del dispositivo, puede resultar valiosa para los ciberdelincuentes que buscan obtener ganancias ilícitas utilizando códigos maliciosos u otras amenazas.

Pese a que no todos los sistemas operativos del mercado móvil son igual de atacados por códigos maliciosos, existen recomendaciones generales que aplican a todo tipo de casos, dispositivos -smartphones, tablets o similares- y usuarios.

¿Cuáles son las principales amenazas que afectan a los dispositivos móviles? ¿Qué medidas se pueden adoptar para mitigar el impacto de estos ataques? A través de las respuestas a estos interrogantes, los usuarios podrán hacer un uso seguro y consciente de sus dispositivos móviles.

Índice

Sistemas operativos móviles



Sistemas operativos móviles

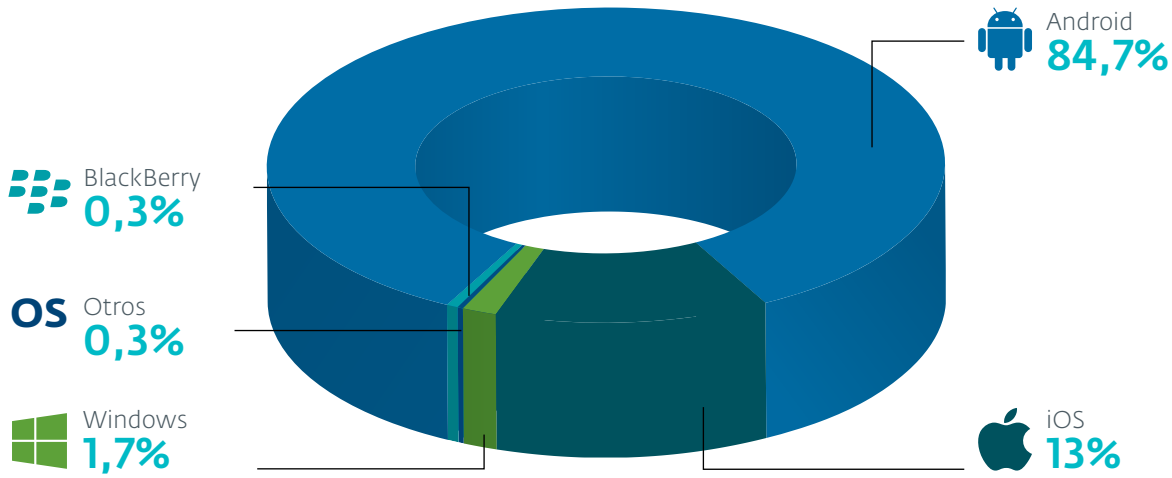
Al igual que con las computadoras en donde existen varios sistemas operativos, los teléfonos inteligentes también necesitan de uno para funcionar. Actualmente, existen diversas opciones dentro del mercado: Android, iOS, Windows Phone, Symbian, BlackBerry, entre otros.

Porcentaje mundial de uso de cada sistema operativo móvil

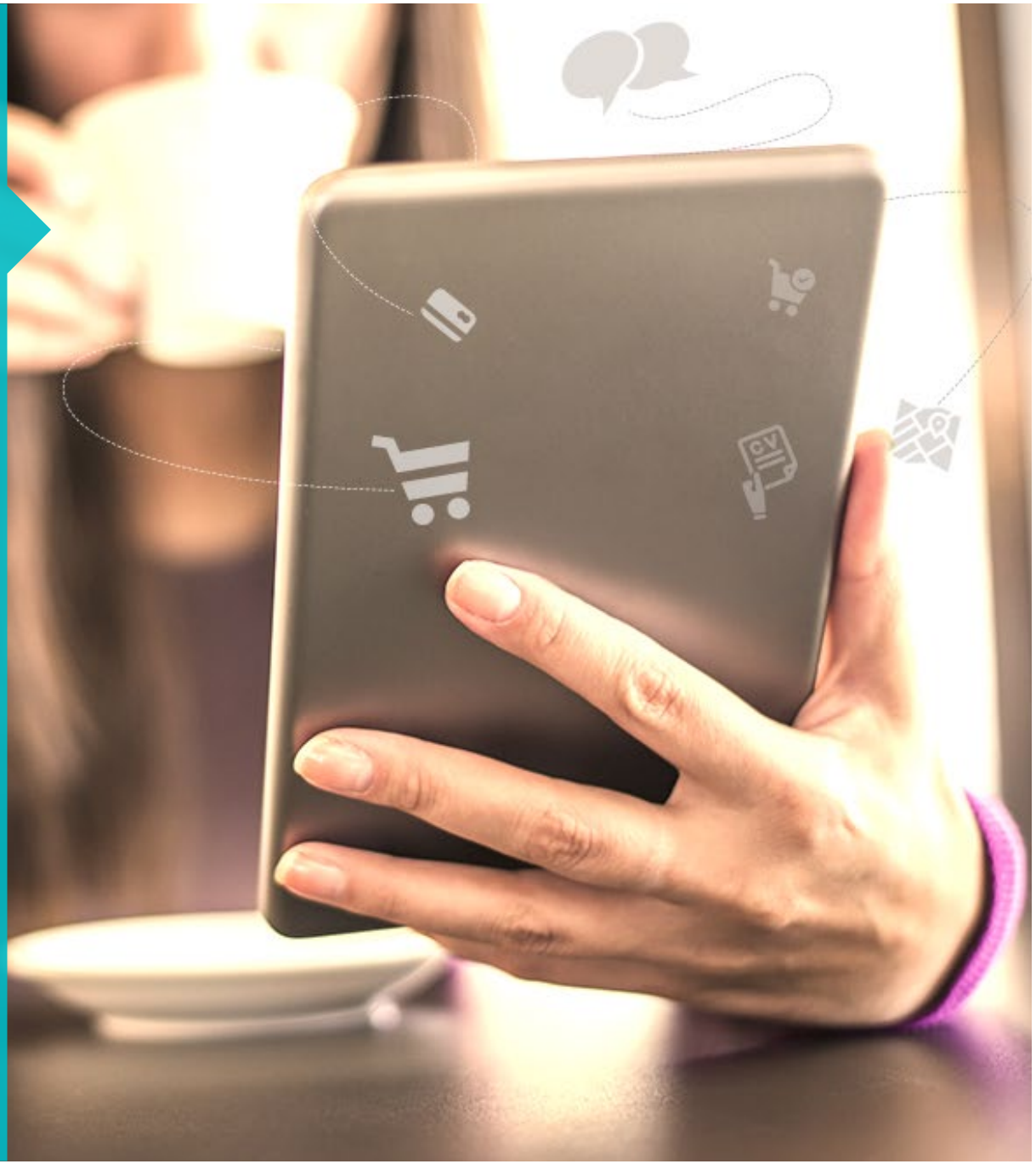
Existen muchas amenazas latentes en el mundo móvil. En particular, la mayor parte del mercado es abarcado por dos únicos gigantes: Android y iOS. Como es de imaginar, los cibercriminales tienen esto en mente cuando deciden generar campañas de propagación de códigos maliciosos. Es por ello que estas dos plataformas son blancos exclusivos para la gran variedad de amenazas móviles.

Según la consultora **Gartner**, el sistema operativo móvil con mayor tasa de participación del mercado es Android. Debido a la masividad y apertura del mismo, es posible observar que la mayoría de los códigos maliciosos mobile que se desarrollan en la actualidad están destinados a esta plataforma y sus usuarios.

En el Laboratorio de Análisis de Malware ESET Latinoamérica se han detectado códigos maliciosos para Android capaces de sustraer información sensible de la víctima, rastrear a la misma a través del GPS, convertir el dispositivo móvil en parte de una **botnet**, infectar el terminal con **ransomware**, entre otras acciones maliciosas.



Riesgos asociados al uso de estos dispositivos



Riesgos asociados al uso de estos dispositivos

Mientras que los teléfonos celulares concentran más y más servicios encargados de procesar información sensible, los datos que manejan incrementan su valor a los ojos de los cibercriminales. En la actualidad, existen diversos tipos de ataques y/o riesgos que pueden afectar a los usuarios de smartphones, a saber: malware, explotación de vulnerabilidades, phishing, fraudes y robo o pérdida del dispositivo. Cada uno de estos riesgos puede perjudicar al usuario de diferentes maneras.

Los teléfonos móviles son equipos muy personales. A través de ellos, se manipulan datos privados, como información crediticia, compras, datos de contactos cercanos, videos y fotografías, itinerarios, geolocalización, archivos y sus metadatos, historiales de sitios web visitados, conexiones Wi-Fi realizadas, claves de acceso a servicios de correo electrónico y otros servicios en la nube, mensajes de texto y conversaciones en múltiples redes sociales, entre muchas otras cosas.

Todos estos datos almacenados pueden ser útiles para que un cibercriminal orqueste un ataque con técnicas de Ingeniería Social contra el dueño del terminal. El hecho de que esta información caiga en las manos erróneas puede derivar, incluso, en casos de extorsión y fraude bajo la amenaza de exponer estos datos.

No es menos preocupante la posibilidad de que extraños puedan acceder a las cuentas de aplicaciones personales activas en el dispositivo, como las redes sociales, plataformas de compra en línea o servicios bancarios. Por ello, es fundamental adoptar medidas preventivas para protegerse ante estos riesgos.

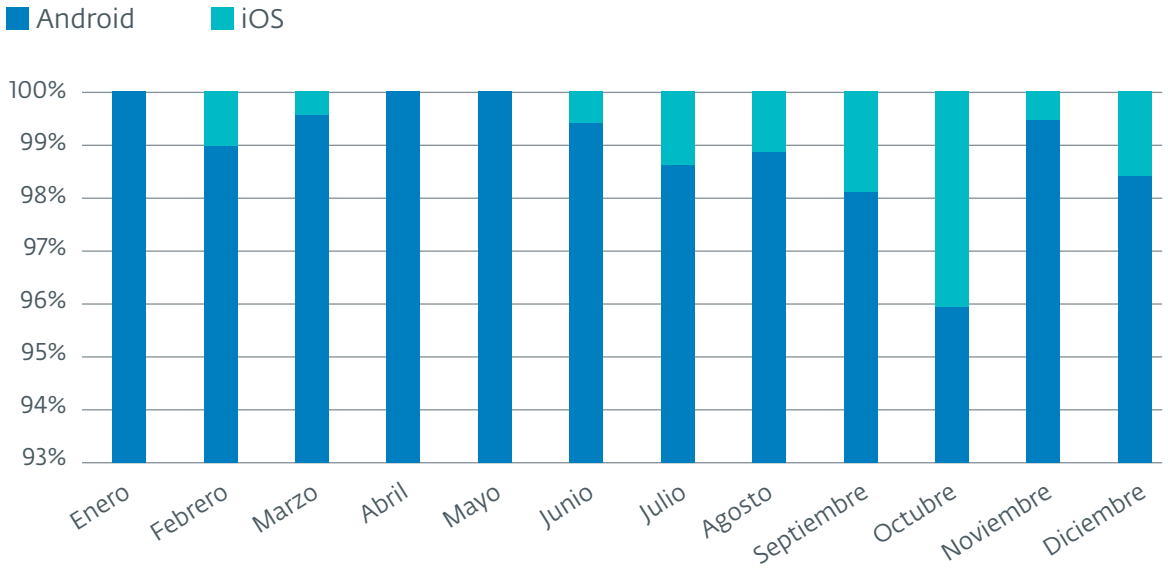
Malware e Ingeniería Social para smartphones

Malware e Ingeniería Social para smartphones

Aunque hace algunos años la problemática de los códigos maliciosos afectaba predominantemente a las computadoras, en la actualidad también representa un riesgo para los usuarios de smartphones. Así, la mayoría de las familias de códigos maliciosos móviles tienen como objetivo la suscripción a servicios SMS Premium, el robo de información, el secuestro del terminal o sus datos, la instalación de otras amenazas en el sistema o el control remoto del equipo.

Por lo general, el éxito en la propagación de cualquier tipo de amenaza informática -exceptuando la pérdida o robo del teléfono- radica principalmente en las estrategias de Ingeniería Social que el cibercriminal utilice. Usualmente, las víctimas son engañadas con promesas de juegos móviles, nuevas versiones de apps para redes sociales o mensajería, programas para el rooting o jailbreaking del teléfono o repositorios de descargas no oficiales.

Nuevas variantes de malware 2015



Códigos maliciosos en Android

En lo que a Android respecta, la tasa de detección de nuevas muestras maliciosas promedia las dos centenas mensuales. Dentro de las familias que mayor crecimiento han tenido, el malware dedicado al envío de mensajes SMS a números Premium, el spyware y el **ransomware móvil** son las que ocupan los primeros lugares de la lista.

Esta tendencia es preocupante, puesto que se trata de códigos que tienen consecuencias sumamente perjudiciales para los dueños de los terminales: pérdida de información sensible, inutilización de los dispositivos y verdaderos gastos económicos.

A lo largo de 2015 se observaron nuevas muestras que causaron estragos a nivel global. Una de ellas fue **Android/Lockerpin**: un agresivo **ransomware para Android capaz de cambiar el código PIN del equipo e inutilizarlo**.

Tal vez lo más curioso del año fue el descubrimiento de malware en plataformas oficiales para la distribución de aplicaciones. **Variantes de scareware disponibles en la Play Store**, enmascaradas de trucos para el popular juego Minecraft con más de 600 mil usuarios infectados; **phishing orientado a robar credenciales de Facebook** instalado más de 500 mil veces; o una cincuentena de **troyanos clicker de sitios pornográficos**.

Códigos maliciosos en iOS

El debate acerca de las diferencias que los esquemas de seguridad de iOS y Android, sus ventajas y desventajas, parece que nunca tendrá un final. No obstante, es cierto que muchos usuarios de iOS descuidan su seguridad por asegurar que no existen códigos maliciosos dirigidos a este sistema operativo.

Aunque la cantidad de malware conocido para iOS continúa representando porcentajes menores cuando es contrastada con la enorme diversidad de malware para Android, la incidencia de códigos maliciosos en esta plataforma es innegable.

En este sentido, es posible recordar a **XCodeGhost**, uno de los contratiempos que sufrió Apple en materia de seguridad móvil, y que los llevó a remover más de 300 aplicaciones infectadas con malware de su App Store, luego de que se confirmara un incidente en su seguridad.

Poco después del hecho, investigadores encontraron otras **256 aplicaciones que violaban la política de privacidad de la App Store**, la cual prohíbe la recolección de direcciones de correo electrónico, aplicaciones instaladas, números de serie y demás información de identificación personal que se pueda utilizar para rastrear usuarios. Estas aplicaciones representaron una invasión a la privacidad de los usuarios que las descargaron, estimados en un millón.

Aunque hace algunos años la problemática de los códigos maliciosos afectaba predominantemente a las computadoras, en la actualidad también representa un riesgo para los usuarios de smartphones.

Por último, no se debe olvidar a **YiSpecter**, un código malicioso para iOS que se aprovecha de API privadas en el sistema operativo para implementar funcionalidades maliciosas. Lo alarmante del caso es que afecta a dispositivos iPhone que tengan hecho el jailbreak o no. Este malware puede descargar, instalar y poner en marcha aplicaciones para iOS arbitrarias, incluso sustituyendo las verídicas ya instaladas en el dispositivo.

Otros riesgos en el uso de smartphones

Otros riesgos en el uso de smartphones

Spam

Al envío masivo de correo electrónico basura por parte de terceros, ahora se suman otros canales de comunicación propios de los teléfonos móviles como los mensajes de texto (SMS) y multimedia (MMS) con el fin de distribuir publicidad o, en algunos casos, propagar códigos maliciosos.

Aunque el spam no necesariamente resulta peligroso para la integridad de la información, estadísticas indican que aproximadamente la mitad de los casos están relacionados al fraude, y en los otros representa una molestia o distracción para el usuario.

Robo o extravío físico del dispositivo

En este tipo de situaciones el mayor problema no es la pérdida del dispositivo en sí y el perjuicio económico que ello acompaña, sino la imposibilidad de recuperar la información no respaldada y el mal uso que se le pueda hacer a la misma. Por ello, es necesario que el usuario contacte de inmediato a la empresa prestadora de servicios de telefonía móvil que tenga contratada, como también que cuente con un software que permita la remoción de información de forma remota. Ambas acciones podrían ser de gran ayuda para proteger la privacidad y confidencialidad de la información.

Estafas multiplataforma

Desde hace tiempo, es posible observar un aumento en la cantidad y complejidad de campañas de fraudes difundidas a través de aplicaciones móviles para redes sociales y mensajería instantánea, como Facebook y WhatsApp. Algunas de ellas **afectaron a marcas de diversas tiendas muy populares** -Zara, Starbucks y McDonald's, entre otras- robando datos personales de las víctimas.

La Ingeniería Social es uno de los puntos fuertes en este tipo de fraudes, lo que nuevamente evidencia por qué la educación es la primera barrera de protección; en ese sentido, es necesario reflexionar y alertar sobre estas nuevas tendencias que aplican antiguas técnicas a nuevos canales de comunicación.

Phishing

Técnica que consiste en obtener información personal o financiera del usuario haciéndole creer que quien solicita esos datos es un ente de confianza, como un banco o una empresa reconocida. Generalmente, el phishing llega como un correo electrónico en el que se asusta a la víctima con amenazas falsas para que ingrese cierta información sensible y privada. En el mundo móvil esta amenaza también se puede propagar por mensaje de texto o incluso llamados telefónicos.

Explotación de vulnerabilidades

Los errores de código en la programación de un software son conocidos como vulnerabilidades. A través de ellas, los ciberdelincuentres pueden infiltrarse para comprometer un sistema y robar información. Esto se conoce como la explotación de vulnerabilidades, algo que se convirtió en un mecanismo cada vez más vigente entre los atacantes para ganar el control de los dispositivos.

Esto plantea nuevas presiones para la rápida actualización y parcheo de las plataformas, lo que puede devenir en una importante falencia para sistemas operativos como Android, donde existe tal cantidad de proveedores de equipos que las actualizaciones pueden tardar demasiado en ser desplegadas a los usuarios finales.

Particularmente en Android, **Stagefright** fue una de las fallas más conocidas, que alarmó a más de 950 millones de usuarios potencialmente afectados al permitir el robo de información a través de código ejecutado de manera remota con tan solo enviar un SMS preparado para tal fin. Pero también es posible recordar fallas en aplicaciones, como el importante **fallo de seguridad en SwiftKey, la aplicación de teclado de Samsung**.

Por su parte, iOS también se vio comprometido a través de numerosas falencias. Hacia mediados de 2015, un **artículo académico** reveló una serie de fallas que, combinadas, podrían explotar apps maliciosas para obtener acceso no autorizado a los datos almacenados por otras aplicaciones (contraseñas de iCloud, tokens de autenticación o credenciales web almacenadas en Google Chrome). Además, otra vulnerabilidad en **Airdrop de iOS** permitió instalar apps maliciosas aparentemente legítimas con gran sigilo.

La importancia de configurar y utilizar correctamente los servicios y aplicaciones móviles

La importancia de configurar y utilizar correctamente los servicios y aplicaciones móviles

Compras y pago de servicios desde un smartphone

Los smartphones y tablets, al igual que las computadoras, pueden ser utilizados para comprar productos, contratar servicios y realizar transacciones bancarias en línea. Aunque esta característica indudablemente facilita la vida cotidiana de las personas, también puede transformarse en un problema grave si no se adoptan las medidas de seguridad necesarias. En este sentido, ya se han reportado varios casos de códigos maliciosos móviles que roban información sensible de este tipo.

Por esto, es vital utilizar solo aplicaciones reconocidas, descargadas desde el sitio oficial del fabricante y que se utilicen en un dispositivo protegido ante códigos maliciosos, para minimizar la probabilidad de ataques o incidentes.

Redes inalámbricas y Bluetooth

Las tecnologías de conexión inalámbrica permiten que el usuario pueda conectarse desde casi cualquier lugar a Internet, como también compartir archivos con otras personas. Lo que a simple vista puede parecer algo muy útil también puede resultar bastante riesgoso en caso de no adoptar las medidas de seguridad pertinentes.

En todo momento se debe evitar utilizar conexiones inalámbricas (Wi-Fi) públicas sin protección o clave. En caso de ser imposible, la recomendación es no realizar transacciones bancarias ni utilizar servicios que requieran de información sensible por ese medio. Además, el Bluetooth debe permanecer apagado si no se está utilizando para evitar la propagación de gusanos y el desgaste innecesario de batería.

Redes Sociales

Las redes sociales permiten un nivel de interacción impensado antes de su invención, además han logrado un gran impacto y alcance en poco tiempo. De esta forma, sus características hacen que estos servicios sean muy atractivos para los usuarios. Sin embargo, lo mismo ocurre con los cibercriminales quienes invierten tiempo y recursos en crear códigos maliciosos que se propaguen por estas vías. Por otro lado, una incorrecta configuración de la cuenta de la red social puede exponer información del usuario a terceros, facilitando el robo y la suplantación de identidad.

Es recomendable analizar la configuración que ofrecen las redes sociales en estos dispositivos y, si la seguridad no es la óptima, evitar utilizarlas en redes Wi-Fi públicas donde la privacidad de los datos no esté garantizada.

Es vital utilizar aplicaciones reconocidas, descargadas desde el sitio oficial del fabricante.

Buenas prácticas y recomendaciones

1 Implementar una solución de seguridad integral

La misma debe detectar malware proactivamente, filtrar mensajes no solicitados, revisar la configuración del teléfono y ofrecer la posibilidad de borrar remotamente toda la información almacenada en caso de robo o extravío.

2 Instalar aplicaciones provenientes de repositorios o tiendas oficiales

Utilizar software legítimo proveniente de fuentes y repositorios oficiales ayuda a minimizar la posibilidad de convertirse en una víctima de códigos maliciosos. Asimismo, es importante controlar que los permisos que demanda esa app sean consecuentes con lo que dice hacer, al igual que evaluar la reputación del desarrollador.

3 Actualizar el sistema operativo y las aplicaciones

Al igual que con las computadoras, actualizar tanto el sistema operativo como los programas es necesario para obtener mejoras de seguridad y nuevas funcionalidades.

4 Establecer contraseña de bloqueo

Es recomendable que posea más de cuatro caracteres.

5 Cifrar el dispositivo

Algunos sistemas operativos proveen cifrado por defecto, mientras que otros como Android no. Activar el cifrado ayudará a proteger la confidencialidad de los datos si el equipo cae en las manos equivocadas.

6 Respaldar la información

Es recomendable realizar copias de seguridad periódicas de la información almacenada en el dispositivo. También se debe evitar escribir información sensible como contraseñas en forma de recordatorios o mensajes de texto.

7 Evitar el rooting o jailbreaking

Estos procesos rompen el esquema de seguridad que los sistemas operativos son capaces de brindar, lo que facilita la instalación de amenazas.

8 Desactivar opciones no utilizadas como Bluetooth o GPS

De este modo, se evita la propagación de códigos maliciosos y el gasto innecesario de la batería.

9 Evitar utilizar redes inalámbricas públicas

De ser imprescindible, no usar servicios que requieran información sensible como transacciones bancarias, compras, etc.

10 Configurar adecuadamente las redes sociales

No compartir información de forma pública y limitar la cantidad de amigos.

11 No seguir hipervínculos sospechosos de correos, mensajes o sitios web

Incluso si estos mensajes provienen de contactos conocidos, pues ellos pueden estar infectados. Tampoco escanear cualquier código QR.

12 Ser cuidadoso con el dispositivo para evitar su robo o pérdida

No dejar el smartphone sin vigilar. Es recomendable utilizar la funcionalidad manos libres en lugares concurridos.

13 Entrenarse para detectar infecciones a tiempo

Acudir a un profesional en caso de notar comportamientos extraños del sistema o las aplicaciones, el historial de llamadas o mensajes posee entradas no conocidas, existe un excesivo uso de datos, se reciben mensajes extraños SMS, la boleta de gastos contiene movimientos sospechosos, o cualquier otro indicio similar.

Conclusión

Las estadísticas demuestran que el malware móvil se diversifica a una tasa constante, materializándose como un vector de ataque real. El punto de inflexión para la protección reside en la comprensión y asimilación de esta problemática, para luego evaluar correctamente todos los riesgos a los que se está expuesto y las barreras de protección disponibles para contrarrestarlos.

En la actualidad, los ciberdelincuentes concentran gran parte de sus recursos en la creación de amenazas para este mercado que crece a pasos agigantados. Por este motivo, si el uso que se le da a los dispositivos móviles es el incorrecto y no hay concientización acerca de las amenazas que existen ni se adoptan las medidas necesarias para resguardar la información, cualquier usuario podría convertirse en una nueva víctima.

En este contexto, resulta fundamental tomar conciencia de la información que se transporta y utiliza en este tipo de dispositivos, y poner en práctica medidas de precaución para resguardarla con el fin de no sufrir ningún incidente que podría ocasionar consecuencias indeseables.

www.eset-la.com

/esetla

@esetla

/company/eset-latinoamerica