Ciberseguridad

MARTIN ZORRILLA

Universidad Católica "Nuestra Señora de la Asunción"
Facultad de Ciencias y Tecnología
Teoría y Aplicación de la Informática II
Asunción, Paraguay

Abstract

Este documento pretende dar al lector una introducción a los conceptos de seguridad cibernética y las amenazas que existen, así como una breve historia sobre su origen y evolución en el tiempo, el estado del arte, la ventajas y desventajas de tener conocimientos sobre el tema así como las consecuencias que pueden provocar a las personas y a la sociedad. Por último se trata brevemente sobre las nuevas tendencias y las proyecciones para el futuro.

Keywords: ciberespacio, ciberamenazas, cibercriminales, exploit, malware.

1 Introducción

La rápida aceptación y el despliegue de internet ha transformado la forma en que creamos y compartimos información. Transacciones financieras, registros de salud, información personal y datos gubernamentales, todos esos datos pasan a través de sistemas tecnológicos a una velocidad que crece

exponencialmente. Las tecnologías informáticas, especialmente internet, han revolucionado la manera en que las personas se comunican, se administran los gobiernos, operan los comercios y cómo funciona la sociedad misma.

Con toda innovación siempre viene una serie de riesgos, las amenazas digitales parecen ser algo nuevo pero han estado presente desde hace mucho tiempo y en los últimos tiempos estas amenazas están en un estado constante de cambio y evolución y la carrera entre los guardianes y los criminales cibernéticos han estado aumentando de manera exponencial especialmente en la última década, aún más en los últimos años.

Se prevé que más de 20 billones de dispositivos estarán conectados solo en los próximos 4 años, forzando a los individuos y organizaciones a enfrentar un escenario de ataque que expande en un ciberespacio sin fronteras.

Es fundamental entender y adelantarse a las nuevas tendencias y estrategias que utilizan los cibercriminales en los años venideros, de manera a contar con los conocimientos para mantener la ventaja en esta carrera y evolucionar de manera proactiva las maneras en que vemos y desarrollamos todo tipo de actividades digitales.

2 Concepto

Ciberseguridad

El término ciberseguridad se escucha cada vez mas, otras palabras asociadas son ciberespacio, ciberamenazas, cibercriminales, ciberguardianes y conceptos similares. muchas veces el término ciberseguridad se utiliza como sinónimo de seguridad de la información, aunque esto no es totalmente correcto. La ciberseguridad está comprendida dentro de la seguridada de la información.

La ISACA (Information Systems Audit and Control Association) define a la ciberseguridad como:

"Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" [1].

La norma ISO 27001 define activo de información como los conocimien-

tos o datos que tiene valor para una organización, por otro lado, los sistemas de información comprende a las aplicaciones, servicios de tecnologías de la información u otros componentes que permiten manipular las mismas [2].

La ciberseguridad tiene como principal misión la protección de la información digital que se encuentra en los sistemas interconectados, por lo tanto está comprendida dentro de la seguridad de la información.

Seguridad de la información

El propósito principal de seguridad en todos los ámbitos de aplicación es el de reducir los riesgos hasta niveles mínimos aceptables, ya que seguridad total es una condición ideal, porque no es posible estar seguro de que se pueda evitar todos los riegos. La información digital es solo uno de los formatos en el que se puede encontrar los datos, existen otros como formatos físicos, bien sea escrita o impresa, además pueden estar de manera no representada, como las ideas o conocimientos de personas pertenecientes a una organización. Podemos citar rápidamente los formatos en lo que se pueden almacenar, procesar o transmitir la información:

Formato Electrónico.

Forma Verbal.

Mensajes Escritos.

Impresos.

Independientemente de la forma, la seguridad dela información requiere que se cumplan una serie de medidas de protección acorde a la importancia de la información.

Una forma de distinguir entre estos dos conceptos es analizar si se busca proteger el software, hardware, las redes o los servicios, estamos hablando de ciberseguridad. Cuando se incluyen medidas de seguridad relacionadas con la información que manejan todas la personas nos referimos a la seguridad de la información.

Diferencias entre ciberseguridad y seguridad de la información.

Ahora que se manejan los conceptos es posible identificar el momento

de aplicar uno u otro concepto. Hay que resaltar que la seguridad de la información abarca un ámbito más grande que el de la ciberseguridad, ya que la primera se enfoca en proteger la información de todo tipo de riegos, en diferentes estados y formas.

La seguridad de la información se sustenta de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, que soportan la idea de protección en las distintas facetas de la información; también involucra la aplicación y gestión de medidas de seguridad apropiadas, a través de un enfoque holístico.

Por otro lado, la ciberseguridad se enfoca en proteger la seguridad en formato digital y los sistemas interconectados que la procesan, transmiten o almacenan, por lo cual está más ligada a la seguridad informática. Con los avances tecnológicos que se incorporan dia a dia y la dependencia tecnológica aumenta, es necesario aplicarla ciberseguridad.

Malware

El malware o malicious software (Software malicioso) es un término colectivo para los virus informáticos, caballos de Troyas o Trojans, gusanos y otros softwares que pueden infectar una computadora, pero también otros dispositivos como servidores, smartphones, tablets y sistemas embebidos [3].

3 Breve Historia

Hoy en dia, los malwares son preocupaciones de todos los días, inclusive entre usuarios normales. Una enorme cantidad de dinero se pierde en el mundo cada día debido a los malwares y otros tipo de ataques, posiblemente billones, pero es difícil de cuantificar.

Lo que podría sorprender a algunos es que han existido desde al menos 1971, y han sido teorizados desde 1949, para tener en cuenta, Microsoft aún no existía hasta 1975.

1949 - John Von Neumann fue un matemático húngaro revolucionario que emigró a los estados unidos en el 1933. En 1948 Von Neumann empezó a hablar de un autómata celular, un complejo modelo matemático para funciones biológicas elementales. Para 1949 esas ideas evolucionaron en una serie de lecturas sobre los “Self-Reproducing Automata”. Estas ideas

estaban adelantadas a su época y se aplicaban a los microbios como los viruses biológicos. A partir de ahí, basado en su experiencia con ENIAC se imaginó un autómata auto reproducible que podría ser aplicable a estas nuevas "máquinas computacionales" [4].

1971 - Antes de los ataques avanzados como STUXNET, existían programas simples que replicaban juegos mensajes encriptados a los usuarios. El virus Creeper fue creado en 1971, una vez que infecta a una máquina enviaba un mensaje corto que desafiaba al usuario a atrapar al Creeper. Este fue creado como un experimento universitario y no causaba ningún tipo de daño, pero sí dio un adelanto del futuro de los malwares y las consecuencias en la ciberseguridad.

1978 - Es lanzado el primer troyano, un programa llamado ANIMAL. este no destruía el sistema, pero sí se replicaba a sí mismo en otras máquinas a través de copias en redes multi usuarios.

1983 - El término virus es utilizado por primera vez para describir a un programa de computadora en una novela de Frederick Cohen.

1986 - El primer virus para una IBM-PC es lanzado.

1988 - Es creado el Morris Worm, este se esparce rápidamente en el mundo, convirtiéndose en el primer gusano en ser esparcido extensivamente vía internet.

2000 - ILOVEYOU, un gusano que infectó millones de máquinas Windows en solo unas pocas horas de ser liberado.

2000 - Un joven canadiense de 15 años hizo caer el sitio Yahoo.com mediante una ataque DDoS, en aquel momento Yahoo era el motor de busqueda nuemero uno.

2007 - Estonia es atacado deliberadamente por un ataque DDoS, bajando el sitio del primer ministro y de otras organizaciones como escuelas y bancos.

2008 - Aparecen los Scarewares, programas que lucen como programas anti-malwares pero que en realidad son un tipo de malware.

2010 - Aparece Stuxnet que tiene como objetivo las instalaciones nucleares Iraníes. Es conocido como el malware más avanzado alguna vez creado.

2012 - Zappos, una popular tienda de comercio electrónico especializada en zapatos es hackeada, 24 millones de datos de clientes son expuestos, como nombres, direcciones y tarjetas de créditos [5].

4 El ciclo de vida de una ataque avanzado

Lo componentes claves de de una estrategia avanzada de ataque incluyen infección, persistencia, comunicación y mando y control.

Infección.

La infección generalmente tiene un aspecto social, como el de lograr que un usuario haga clic en un enlace malo en un correo de suplantación de identidad, invitando a un sitio de red social, o enviándolo a un sitio web con una imagen infectada por ejemplo.

La mayoría de los exploits de hoy son usados para quebrar un objetivo e infectarlo con el malware, por ejemplo se ejecuta un exploit causando un overflow, lo que permite al atacante tener acceso al shell. Con el esto el atacante puede entregar prácticamente cualquier carga, ahora puede descargar el malware a través de la aplicación o de la conexión que ya se encuentra abierta. Esto se conoce como drive-by-download y es una de las estrategias más utilizadas.

Las infecciones se apoyan fuertemente en esconderse y evadir las herramientas de seguridad tradicionales, una técnica utilizada es crear malwares específicos para un cierto objetivo, el cual se sabe que no será detectado. otra técnica es la de infectar utilizando conexiones que las herramientas de seguridad no pueden analizar, como tráfico en transmisiones SSL, encriptaciones propietarias P2P y aplicaciones de mensajería instantánea.

La tendencia moderna es que los ataques no necesariamente vienen como ejecutables en un archivo adjunto de un correo electrónico. Un simple link es suficiente, es por esto por el cual las redes sociales, webmail y plataformas de microblogging como Twitter se está convirtiendo rápidamente en los vectores favoritos de infección para los atacantes.

Persistencia.

Una vez que la máquina está infectada, el atacante necesita asegurar

la persistencia, es decir que este pueda sobrevivir en la red en un periodo de tiempo. Para estos efectos, generalmente se instalan rootkits y bootkits en las máquinas infectadas. Un rootkit es un malware que provee accesos con privilegios como un usuario root en la computadora. Un bootkit es un variante modo-kernel del rootkit, usadas normalmente en máquinas que cuentan con protección del tipo full-disk encryption (encriptación a nivel de hardware).

Una puerta trasera o Backdoor permite al atacante saltarse los procedimientos normales de autenticación para obtener acceso a un sistema comprometido. Normalmente se utilizan en caso de que un malware es detectado y removido del sistema. Poison Ivy es un exemplo de backdoor que fue usado en el ataque a RSA.

Finalmente, puede ser instalado un anti-AV, de manera a desinstalar o deshabilitar cualquier software de antivirus en la máquina y evitar que el malware sea borrado. Usualmente esto se realiza infectando el MBR de la máquina objetivo.

Comunicación.

La comunicación es fundamental para que un APT(advanced persistent attack) resulte exitoso. si no es posible la comunicación, coordinar un ataque complejo a largo plazo tampoco lo es. El atacante debe poder comunicarse con otros sistemas infectados que permitan tomar mando y control, así como extraer los datos robados del sistema objetivo. Estos ataques y comunicaciones deben ser furtivos y no levantar sospechas en la red. Este tipo de tráfico es escondido generalmente usando técnicas que incluyen:

Encriptados con SSL, SSH o alguna aplicación específica. Encriptación propietaria también es usual en estos casos. Por ejemplo bitTorrent es conocido por usar encriptación propietaria y es una herramienta de preferencia tanto para infección como mando y control.

Burlar o esquivar mediante el uso de proxies, herramientas de acceso a escritorio remoto como LogMein, RDP. también utilizando aplicaciones de entunelamiento dentro de otras aplicaciones o protocolos que permitan esto.

Evasión de puertos usando anonimizadores de redes o salto de puertos a túneles sobre puerto abiertos.Por ejemplo, los botnets se caracterizan por

enviar instrucciones de mando y control sobre IRC(Internet Relay Chat) en puertos no estándares

Flujo rápido o DNS dinámicos a un proxy a través de múltiples hosts infectados y re enrutar el tráfico lo cual hace extremadamente difícil a los equipos forenses determinar a dónde está yendo realmente el tráfico

Mando y Control.

El mando y control se ubica por encima de la plataforma de comunicación que se ha establecido, pero en realidad se trata de asegurar que el ataque sea controlable, administrable y actualizable.

Mando y control generalmente se logra por medio de aplicaciones comunes como webmail, social media, P2P, redes, blogs. Este tráfico no sobresale si genera sospechas, por lo general es encriptado y utiliza backdoors y proxies.

5 Estado actual

El cambiante Rostro de los Cibercriminales

Los cibercriminales han evolucionado del proto-típico estudiante en un sótano, motivado más que nada por recibir notoriedad, a cibercriminales motivados por significativas ganancias financieras, muchas veces auspiciados por organizaciones criminales, grupos políticos e inclusive gobiernos. Los atacantes actuales se ajustan al siguiente perfil:

Tienen muchos más recursos disponibles para realizar los ataques.

Tienen grandes conocimientos técnicos y de mucha concentración.

Están bien financiados.

Están bien organizados.

Por qué es esto importante? por que si bien un estudiante o un joven en un sótano logra infiltrarse en una red corporativa y obtuviera por ejemplo un código fuente RSA, este no sabria que hacer con el. Por otro lado, una organización criminal o un estado sabe exactamente qué hacer o a quien vender dicha dicha propiedad intelectual, sea en el mercado gris o negro.

Además, estos estados u organizaciones cuentan con recursos financieros mucho más amplios que el de una sola persona. Se ha descubierto muchas actividades criminales operando con todos los componentes clásicos de un negocio legítimo, con oficinas, recepcionistas y cubículos completamente llenos de cibercriminales. Estas con empresas criminales en todo el sentido de la palabra, y por supuesto tienen un alcance mucho más amplio que el de una sola persona.

Pero no solo ha cambiado el rostro y la forma en que se organizan los cibercriminales, también ha sucedido lo mismo con el tipo de información que está siendo tratada como objetivo. Estos grupos pueden hacer cosas muy interesantes con información aparentemente sin importancia.

Así también han cambiado las estrategias, en vez de los tradicionales ataques directos a un servidor o un recurso de alto perfil o valor, las estrategias actuales emplean por sobre todo mucha paciencia y procesos de varios pasos que mezclan exploits, malwares y evasión en ataques coordinados.

Por ejemplo, un ataque muchas veces se inicia seduciendo a un individuo en hacer clic en un link infectado. La página resultante toma control de la computadora del usuario y por detras descarga un malware, luego el malware actúa como un punto de control dentro de la red, permitiendo al atacante expandir el ataque y buscar otros recursos en la red interna, escalando privilegios en la máquina infectada o creando nuevas cuentas administrativas, por nombrar alguna de las estrategias.

La clave se encuentra en que en vez de tomar al malware y a los exploit de redes como disciplinas separadas como en el pasado, están ahora integrados en un proceso continuo. es más, estos dos en conjunto no son el fin del ataque, sino que simplemente habilita el siguiente paso de un plan de ataque mucho más complejo.

El malware, el cual es cada vez más especializado para evitar la detección, provee a un atacante remoto de un mecanismo de persistencia, y la red habilita al malware a adaptarse y reaccionar al ambiente que ha infectado

Casos de Estudio.

Los ataques actuales son más sofisticados que nunca, todo tipo de empresas e información está siendo determinada como objetivo. Cada dia, mas

y mas ataques logran realizarse de forma satisfactoria, produciendo brechas e intrusiones. Algunos ejemplos:

Sony PlayStation. En abril de 2011, hackers lograron infiltrarse en la red de Sony PlayStation, robando potencialmente información de tarjetas de crédito e información personal, incluyendo nombres, fechas de nacimientos, direcciones físicas y de correo, passwords, IDs y otros datos de más de 100 millones de suscriptores. El valor de estos datos personales para futuros actos criminales, tanto cibernéticos como tradicionales(secuestro, extorsión) podría fácilmente superar el valor de las tarjetas de crédito robadas, ya que se maneja que estos datos se venden en el mercado negro a 1 USD aproximadamente.

Senado de los EE.UU. En junio del 2011, el grupo cibercriminal LulzSec se introdujo en el sitio web del senado y publicó una lista de archivos-no clasificados ni sensibles- en línea. Otros ejemplos de "Hacktivistas" políticos perpetrados por grupos criminales incluye ataque contra los sitios webs del servicio público de difusión de los EE.UU(PBS), la compañía difusora FOX, MasterCard, Visa y PayPal por tomar medidas negativas o prensa negativa en contra de WikiLeaks [6].

RSA. En marzo del 2011, RSA Security, fue infiltrada por un atacante que envió un correo Phishing de suplantación de identidad con un documento adjunto de Microsoft Excel a varios funcionarios de RSA. El archivo infectado contiene un malware que utiliza un exploit dia zero de adobe flash para instalar una puerta trasera o backdoor, establecer control y robar passwords así como datos sensibles.

Comodo. En el mismo mes un intruso comprometió la red de un revendedor y robo 9 certificados de seguridad que luego podrían ser emitidos de forma fraudulenta para hacerse pasar por sitios webs operados por Google, Microsoft, Skype entre otros. Esto dejó a la vista el potencial para los atacantes de obtener información sensible indirectamente, atacando uno de los puntos débiles en un ecosistema de negocios.

Stuxnet. En 2010 sale a la luz stuxnet, un malware que se conoce como el más avanzado hasta el momento. El objetivo principal de este malware era el de retrasar el programa nuclear iraní. Esta central usaba centrifugadoras para enriquecer el uranio.

La primera versión tenía como objetivo los controladores industriales

Siemens S7-417, los encargados de controlar las válvulas y sensores de presión de las centrifugadoras. La infección se realizó de forma manual, es decir alguien tuvo que llevar el archivo en un USB o en uno de los portátiles que se usaban para configurar los sistemas y abrirlo manualmente. Cuando se cargaba el archivo, el código tomaba el control pero de forma muy discreta. Reemplaza las lecturas de los sensores y dejaba que todo se ejecutase normalmente como si nada pasara.

Los creadores de Stuxnet podría haber destrozado las instalaciones nucleares,pero no lo hicieron porque para conseguir sus propósitos era mejor retrasar el programa iraní. Un fallo catastrófico había llevado a los ingenieros a analizar exhaustivamente que había pasado y probablemente habrían detectado y corregido el problema, lo cual no hubiese supuesto un retraso demasiado grande.

En una segunda versión, se menciona que si bien stuxnet parece estar hecha por un grupo de expertos industriales y programadores, en la segunda se aprecia la influencia de gente relacionada con el mundo de la seguridad, los ingenieros de la NSA. La primera diferencia es el metodo de propagacion, usando cuatro vulnerabilidades zero-day, infecta unidades usb para transmitirse de un ordenador a otro, también utilizaba firmas con certificados digitales robados, por lo tanto windows lo detectaba como un driver legítimo y confiable. Aun así este no encontraba en las instalaciones nucleares, esto lo hizo mediante contratistas externos que trabajaban para la central y que tenían dispositivos menos protegidos, a partir de ahí solo era cuestión de tiempo para que un contratista conecte su USB o portátil a la red de la central, luego Stuxnet sería capaz de llegar a su objetivo, los controladores Siemens.

Stuxnet se puede considerar una ciberarma y es el pionero en este mundo. Señala varias ideas y conceptos en los que se centraran sus sucesores en el futuro.

Tesla. Hackers toman control de los frenos de un vehículo Tesla en movimiento.

En el 2016 un equipo Chino de investigación de seguridad lograron tomar control de un Tesla Model S desde una distancia de 12 metros, interfiriendo con los frenos del auto, el bloqueo de puertas, la pantalla de entretenimiento y otras funcionalidades controladas electrónicamente en el auto. El ataque se enfocó en el Can Bus, la red de computadoras conectadas

que se encuentra en los modelos de vehículos modernos, controlando desde señaleros hasta los frenos. El ataque requiere que el auto se conecte a un hotspot Wifi malicioso configurado por el equipo de hackeo, y solo puede ser disparado cuando el navegador web del auto está siendo utilizado. Los investigadores actuaron de forma responsable en descubrir las vulnerabilidades y presentarlas a la compañía Tesla. Luego se creó una actualización de software que fue entregada por aire a todos los vehículos. Este es un caso de Ethical Hacking que será abordado con más detalle más adelante [7].

Ethical Hacking.

Un hacker ético es un experto en sistemas informáticos y redes de computadoras que sistemáticamente que intenta penetrar en un sistema informático o red en nombre de sus propietarios o empleadores, con el fin de encontrar vulnerabilidades de seguridad que un hacker malicioso potencialmente pueda aprovechar.

Los hackers éticos utilizan los mismos métodos y técnicas para probar y eludir las defensas de un sistema que sus contrapartes menos éticos, pero en lugar de tomar ventaja de las vulnerabilidades encontradas, documentan y proporcionan asesoramiento sobre cómo solucionarlos de forma que la organización pueda mejorar su la seguridad general.

El propósito de hacking ético es evaluar la seguridad de una red o infraestructura del sistema. Implica encontrar y tratar de explotar cualquier vulnerabilidad para determinar si es posible el acceso no autorizado o de otras actividades maliciosas. Las vulnerabilidades tienden a encontrarse en configuración del sistema en mal estado o inadecuada, fallas de hardware o software conocidos y desconocidos y debilidades operativas en los procesos o en las contramedidas adoptadas.

Uno de los primeros ejemplos de hacking ético se produjo en la década de 1970, cuando el gobierno de los Estados Unidos utilizó grupos de expertos llamados "equipos rojos" para piratear sus propios sistemas informáticos.

Este se ha convertido en un sub-sector considerable en el mercado de seguridad de la información y se ha ampliado para abarcar también los elementos físicos y humanos de las defensas de una organización. Una prueba con éxito no significa necesariamente una red o un sistema totalmente seguro, pero debe ser capaz de resistir los ataques de los piratas informáticos automatizados y no cualificados.

Actualmente, se ofrecen varios cursos gratuitos y pagos para certificar en esta área de la informatica, asi como herramientas libres que permiten iniciarse en el campo.

6 Tendencias

Incrementan las amenazas a smartphones.

Aunque nos suene un raro y poco común, los ataques a teléfonos inteligentes y tablets existen y están en aumento. ¿Por qué? solo es cuestion de analizar lo siguiente, los dispositivos móviles actuales contienen demasiada información personal, muy relevante sobre nosotros, que en manos ajenas podría valer mucho, ya sea individualmente o en conjunto.

Si bien los fabricantes se esfuerzan cada año en implementar formas de bloqueo más robustos. Cada vez hay más ciberataques dirigidos a estos dispositivos. La idea acerca de que los ciberdelincuentes únicamente atacan a los ordenadores es falsa. Solo en el tercer trimestre se han registrado en españa casi 6.400 nuevas amenazas para Android,el sistema operativo para dispositivos móviles más extendido en el mundo.

La firma de seguridad informática Sophos, prevé que el próximo año se verá un aumento en el número de vulnerabilidades en los dispositivos Android que, a su vez, podrían ser realmente aprovechadas por los hackers [8].

Ya se han detectado muestras de la complejidad en las nuevas técnicas utilizadas para esquivar la detección y filtrado en la App Store, algunas aplicaciones son capaces de camuflarse en juegos inofensivos que, posteriormente, descargan un componente malicioso.

Cada dia salen al mercado grandes cantidades de aplicaciones propiciando que los cibercriminales prueben suerte esquivando los mecanismos de detección de la App Store, pero la naturaleza de Android, y su soporte flexible para App Stores de terceros, contribuye a que android sea un blanco más fácil que iOS, aunque el segundo tampoco está libre de ataques.

Un nuevo objetivo - El internet de las cosas

Los dispositivos interconectados a través de internet ya sea por ethernet o wifi, conocido como the internet of things, han conseguido ofrecer nuevas

posibilidades, no solo a los usuarios, sino también a los hackers. Como ya es apreciable a estas alturas, ningún aparato está exento de sufrir un ataque desde el momento que se conecta a internet. Cada dia insertamos más tecnología a nuestra vida cotidiana.

Se estima que para 2020 habrá 50.000 aparatos conectados. Cada vez dependemos más de la tecnología y esta dependencia puede conllevar nuevos riesgos. Ante estas nuevas amenazas será necesario establecer nuevas medidas de protección, que hasta ahora es contemplada por poca personas, prácticamente solo las que están en el área de seguridad.

Si aún no se están explotando mucho las vulnerabilidades del Internet de las Cosas es sencillamente porque los cibercriminales aún no han encontrado el modelo de negocio que les permita hacer dinero. En la medida que aumente la diversidad de las aplicaciones de estos dispositivos la probabilidad de que estos puedan emerger será mucho mayor.

Técnicas más inteligentes

Así como la ciberseguridad empieza tomar notoriedad y las personas y organizaciones toman conciencia de los peligros que conllevan no tomar las medidas necesarias, la ingeniería social sigue evolucionando y cada vez de invertir más para protegerse de estos ataques. Según expertos, el ransomware -que restringe el acceso- continuará predominando en 2016 hasta el punto que solo será cuestión de tiempo que se vean cosas más allá del rescate por secuestro de datos.

Es fácil imaginar un ransomware aplicado a un hackeo a un vehículo como se mencionó el caso de los vehículos Tesla y tendríamos un escenario donde el atacante podría tomar control de un vehículo en movimiento y pedir un rescate para devolver el control, este es solo un escenario, se podría aplicar el concepto para smartphones, casas etc. Los atacantes aumentarán las amenazas de hacer públicos los datos privados, en lugar de tenerlos como rehén. Precisamente, está previsto que los creadores de malware comercial también continuarán invirtiendo fuertemente.

Ataques en la nube

La virtualización de las infraestructuras y los servicios cloud computing es otra de las tendencias actuales en la digitalización de las empresas. Será otro de los focos de atención por parte de los ciberdelincuentes. La vulnera-

bilidad Venom que se produjo este año dio una pista sobre el potencial del malware para escapar desde un hipervisor y acceder al sistema operativo host en un entorno virtualizado [8].

7 Malware para Moviles

Encontramos que el escenario de los malwares para dispositivos móviles, al igual que los malwares tradicionales, continúan creciendo y evolucionando con varios factores que contribuyen a este fenómeno. El incremento en la velocidad, poder de cómputo y espacio de almacenamiento en dispositivo móviles ha permitido a un mayor número de personas a utilizar sus dispositivos para realizar variadas tareas como compras en línea, administrar sus finanzas y pagar cuentas.

Como consecuencia, los móviles se han convertido en objetivos mucho más valiosos para los cibercriminales. En el 2015 se ha encontrado vulnerabilidades en Android OS que ha cambiado la forma en que Google maneja sus actualizaciones de seguridad. También se ha visto un incremento en la cantidad de malwares avanzados con los que se ha lidiado desde hace bastante tiempo en el mundo de las PC's y que están aterrizando en el mundo de los móviles. Ransomware, fraudes bancarios y RATs (remote access tools) han incrementado su presencia en el mundo de los dispositivos móviles.

Android

El malware dirigido solo a teléfonos inteligentes Android ha crecido un 76 porciento en los últimos meses, amenazando así a la seguridad de Android; las demás plataformas también son vulnerables.

Muchas de estas amenazas, como la que supone hacer clic en un vínculo peligroso de un correo electrónico o de los resultados de búsqueda, son las mismas que podrían detectarse en un equipo, pero hay otras que solo afectan a los dispositivos móviles.

Por ejemplo, podría descargar accidentalmente una aplicación maliciosa que accediera a su información personal y la enviará a un ciberdelincuente. También podría descargar una aplicación peligrosa que marcará números de tarifa especial en su teléfono, de forma que se sumarán cargos elevados a la factura de su teléfono móvil. Otros programas maliciosos pueden alterar la funcionalidad de su teléfono y hacer que pierda toda su utilidad.

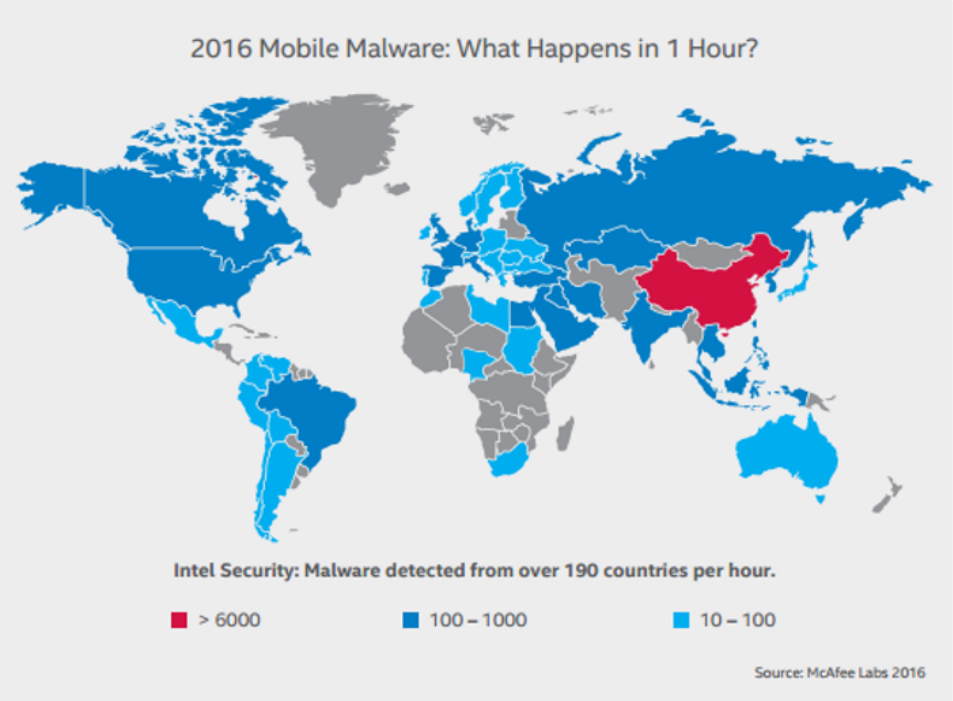

Figure 1: Lo que ocurre en una hora en el mundo. [9]

También es posible que reciba mensajes de texto o de voz de empresas aparentemente legítimas en los que le soliciten información personal.

Si detecta alguna de estas amenazas para dispositivos móviles, los riesgos están claros: podría perder su dinero, su identidad y su información privada; además, si su dispositivo deja de funcionar, podría perder también todos los datos almacenados en él, incluidas las fotos, los contactos y los correos electrónicos. Por esta razón, es importante adoptar medidas para protegerse del malware de dispositivos móviles. [9]

Stagefright: Configurando el escenario para incrementar la seguridad.

Se llama Stagefright a la colección de bugs que llevan a vulnerabilidades encontrados en el sistema operativo Android, estos son códigos del sistema que trabajan por debajo de las aplicaciones y son compartidos por muchas aplicaciones. Estas vulnerabilidades son bastante interesantes ya que permite al atacante ejecutar remotamente códigos en los teléfonos enviando un MMS especial.

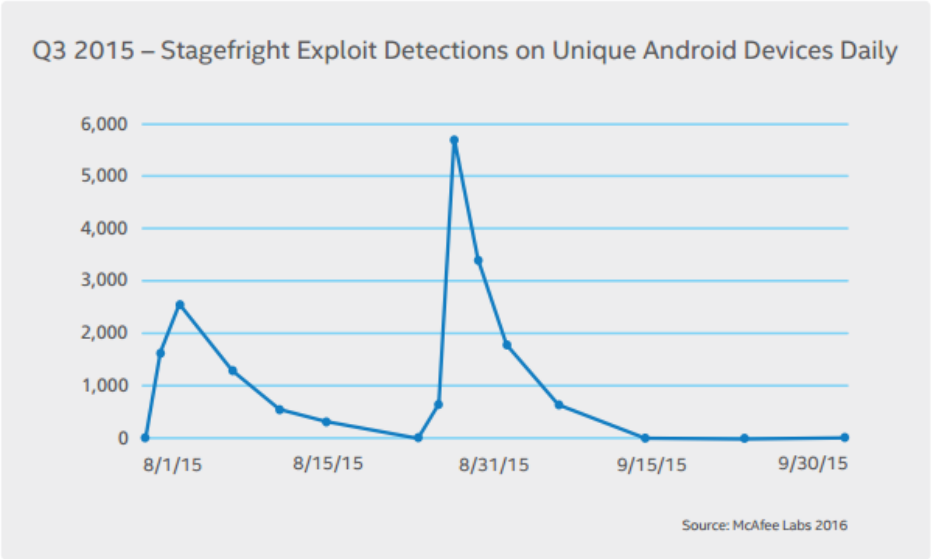

Figure 2: Stagefright Exploits. [9]

Típicamente, se intentará engañar al usuario para que haga clic en un link malicioso o instalando una aplicación infectada. Aún más preocupante es que dada la naturaleza de estos bugs, un atacante con solo saber el número de teléfono del objetivo deseado, puede hackear un teléfono, implantar un RAT y cubrir todo rastro del ataque, todo esto mientras el teléfono de la víctima quedo cargando la batería durante la noche.

Un estudio del laboratorio de McAfee Mobile del 2015 revela el número de dispositivos reportando ataques del tipo Stagefright, llegando a un poco más de 5000 dispositivos atacados hacia el final de agosto. Esto ocurrió solo dos semanas después de haber descubierto una vulnerabilidad Stagefright adicional.

En octubre otra ronda de vulnerabilidades Stagefright fue lanzada, apodada Stagefright 2, esta vez utilizando archivos mp3 y mp4 especialmente diseñados para explotar vulnerabilidades en el núcleo de una librería de Android (libutils) que existía desde el primer lanzamiento de Android. Esto implica que dispositivos corriendo Android 1.5 a 5.1 eran vulnerables a estos ataques, aproximadamente 1 billón de dispositivos.

Debido a que el rango de dispositivos vulnerables es mucho mayor, esta

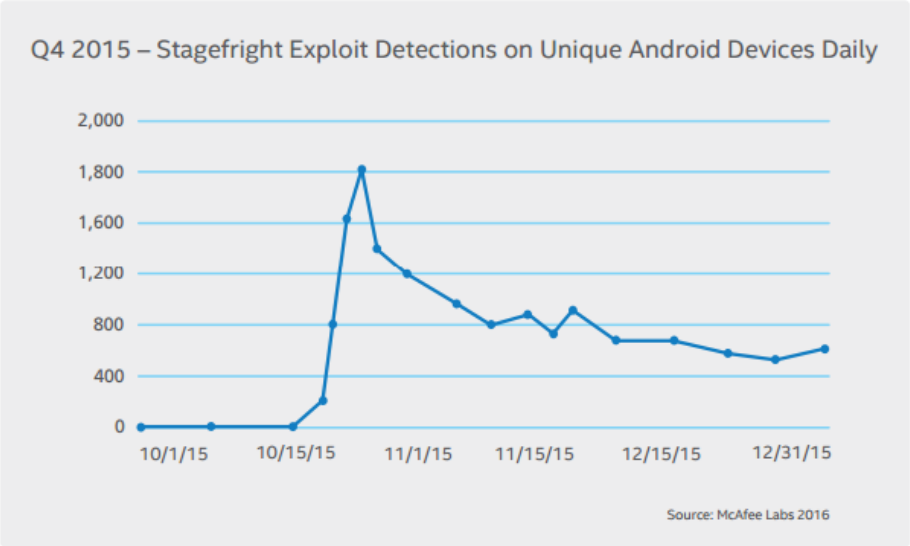

Figure 3: Stagefright 2.0 Exploits. [9]

nueva versión resultó en otro crecimiento de malwares basados en Stagefright de forma continua hasta el final del 2015.

¿Qué significa esto para el consumidor?

Stagefright resultó en un cambio dramáticamente la forma en que Google maneja sus parches de seguridad. Históricamente no existía una agenda para las actualizaciones, pero luego de los eventos a inicio del 2015 Google se ha comprometido a lanzar actualizaciones cada mes. De todas formas, es importante mencionar que las actualizaciones son distribuidas a las diferentes marcas y compañías telefónicas o portadoras, y depende de estas compañías la provisión de estas actualizaciones. Mirando el lado positivo, ahora existen actualizaciones mensuales, pero por el lado negativo, estas actualizaciones pueden tomar tiempo en llegar a los dispositivos Android. Como se puede ver en las gráficas anteriores, los ataques de este tipo son continuos y no decrecen. Algunas recomendaciones para dispositivos Android que aún cuentan con versiones viejas y sin los parches de actualización son: [9]

Desactivar los mensajes MMS

Actualizar el software del dispositivo

No abrir mensajes de desconocidos

Utilizar un software de seguridad

Malwares en iOS

Los dispositivos de Apple son conocidos por ser inmunes a malwares, si bien esto no es del todo cierto, es importante destacar que el número de malwares y ataques exitosos para esta plataforma es mucho menor al de Android, esto gracias a que Apple realiza un proceso detallado de verificación antes de disponibilizar una aplicación en el App Store y existe una menor cantidad de dispositivos desbloqueados (jailbreak). [10]

La mayoría de los malwares para iOS se basan en explotar vulnerabilidades en dispositivos desbloqueados(jailbroken) pero también se han entrado malwares que pueden realizar ataques a dispositivos no desbloqueados utilizando certificados empresariales, los cuales son diseñados para que las empresas distribuyan aplicaciones en sus propios teléfonos. [11]

AceDeceiver

También existen otros mecanismos de ataque, la compañía Palo Alto Security descubrió un malware capaz de infectar iPhones ya sean desbloqueados o no, este malware explota algunas vulnerabilidades en el mecanismo DRM (Digital rights management) de Apple. Este malware conocido como AceDeceiver aprovecha algunos errores de diseño en el sistema de protección DRM de Apple para instalar apps maliciosas en estos dispositivos. Actualmente se vio siendo utilizado solo en china, pero esto fácilmente podría cambiar y utilizarse en cualquier lugar.

El mecanismo utilizado es sencillamente un ataque MITM (man in the middle), que normalmente se utiliza para distribuir aplicaciones piratas, pero es la primera vez que se utiliza para instalar malware. el mecanismo es el siguiente:

Apple permite a sus usuarios comprar y descargar una aplicación para iOS desde su App Store a través de iTunes en la computadora. Luego el usuario puede utilizar la computadora para instalar la aplicación en sus dispositivos iOS, estos dispositivos solicitan un código de autorización para cada app instalada para demostrar que la app fue comprada realmente.

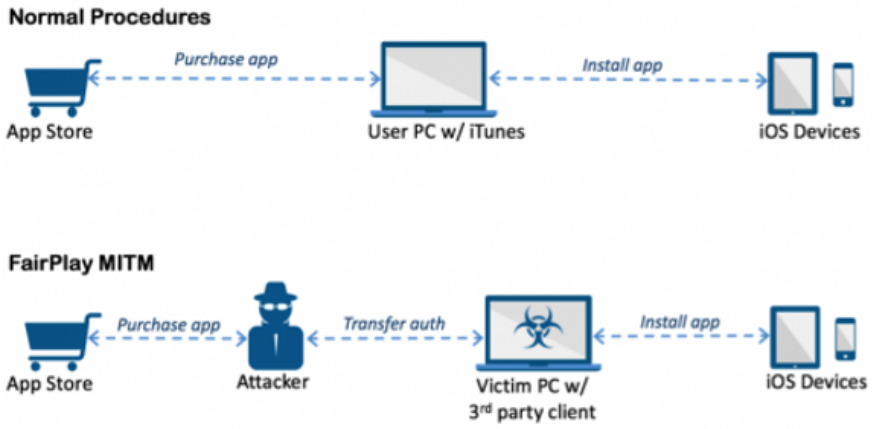

Figure 4: Procedimiento de un ataque MITM. [12]

En el ataque MITM, el atacante compra una app del App Store e intercepta y guarda el código de autorización. Luego se desarrolla o utiliza un software para computadoras, el cual simula el comportamiento de un cliente iTunes y engaña al dispositivo iOS para que crea que la app fue comprada realmente por la víctima. Por lo tanto, el usuario puede instalar apps que realmente nunca fueron compradas por él, y el creador del software potencialmente puede instalar aplicaciones maliciosas sin el conocimiento del usuario. [10]

Pegasus

Este malware fue descubierto por los laboratorios Citizen Lab y Lookout luego de que un activista de los derechos humanos haya recibido un enlace a un sitio web malicioso permitiendo desbloquear el dispositivo y la instalación de herramientas de monitoreo. Una investigación vincula al malwares con NSO como sus creadores, una organización israelí con dueños estadounidenses.

El malware aprovecha vulnerabilidades zero-day para desbloquear el teléfono remotamente e instalar un paquete de herramientas de monitoreo en el dispositivo de la víctima. Uno de los procesos claves es tomar ventaja de un error de corrupción de memoria en el Webkit Safari. La vulnerabilidad permite al atacante descargar un malware cuando la víctima hace clic en un link que lo re direcciona a una web maliciosa.

Una vez instalado, Pegasus aprovecha fallas en el kernel para escalar privilegios, permitiendo al atacante interceptar mensajes de texto, email, acceder a los contactos y robar información de una serie de apps incluyendo Gmail, Facebook, WhatsApp, WeChat y muchos más [13].

Apple parchea la vulnerabilidad lanzó IOS 9.3.5.

Otros Malwares iOS

Como se puede apreciar en los reportes, el mayor porcentaje de malwares está destinado a dispositivos Android, pero eso no significa que no existan malwares para iOS como muchos creen, iOS tampoco es inmune a estos males. Más abajo se encuentra un resumen de otros malwares para esta plataforma además de los mencionados anteriormente.

Name	Discovery date	Presumed origin	Devices	Type
iOS/Trapsms.Altr.spy	June 2009	Russia?	Jailbroken	SMS Forwarder
Spy/MobileSpyIiPhoneOS	Aug 2009	USA	Jailbroken	Spyware
iOS/Eeki.Aiworm	Nov 2009	Australia (Ashley Towns)	Jailbroken	Worm Proof of Concept
iOS/Eeki.Biworm	Nov 2009	The Netherlands	Jailbroken	Mobile banking malware
iOS/Toires.Altr.spy	Nov 2009	Switzerland (Nicolas Seriot)	Any (jailbroken or not)	Rogue application - Proof Of Concept
Adware/LBTMIiOS	Sep 2010	France	Any (jailbroken or not) - Was found (and removed) in the official AppStore	Call premium phone number
Spy/iKeyGuardIiPhoneOS	Apr 2011	Czech Rep.	Jailbroken	Keylogger
iOS/FindCall.Altr.spy	July 2012	Russia?	Any (jailbroken or not) - Was found (and removed) in the official AppStore	Privacy trojan
Riskware/KillmobIiOS	July 2013	USA	Jailbroken	Spyware
iOS/AdThief.Altr	Mar 2014	China	Jailbroken	Ad revenue hijacking
iOS/SSLCreds.Altr.pws	Apr 2014	China	Jailbroken	Password stealer

Figure 5: iOS Malware List. [14]

Peligros en la App Store

Como hemos visto, tanto Android como iOS no son inmunes a los malwares y muchos de estos se encuentran en las respectivas Apps Stores. En los últimos años, centenares de apps fueron removidas de las Apps Stores por razones de seguridad. Para iOS, este año su mayor amenaza provino de una aplicación con adware extremadamente agresivo y para Android una buena cantidad de aplicaciones infectadas. Tanto Google como Apple han sido bastante rápidos en remover rápidamente aplicaciones maliciosas en sus respectivas App Stores, pero de todas formas es inevitable que algunas apps infectadas esquiven el proceso de verificación.

Se puede observar el resultado de un análisis de las App Stores realizado en el primer semestre del 2016 por McAfee.

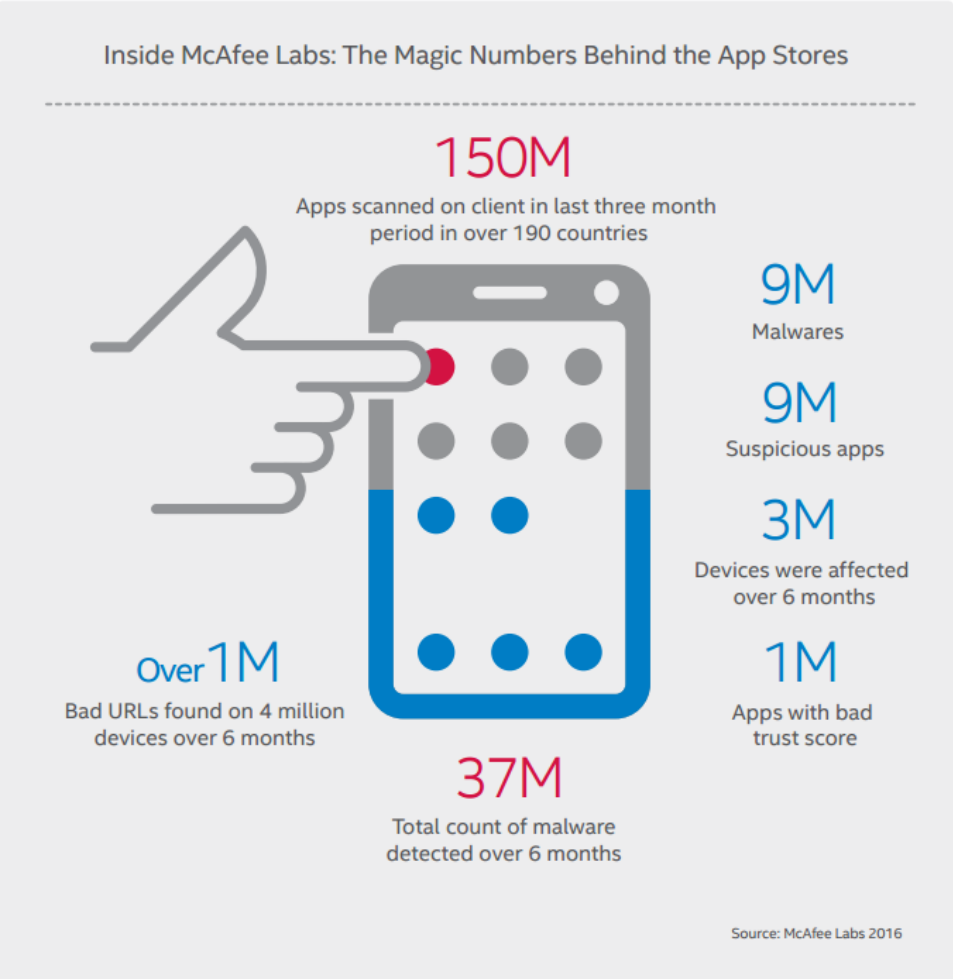

Figure 6: Análisis de las App Stores realizado en el primer semestre del 2016 por McAfee. [9]

Figure 7: Amenazas Móviles más destacadas en el último trimestre del 2015. [9]

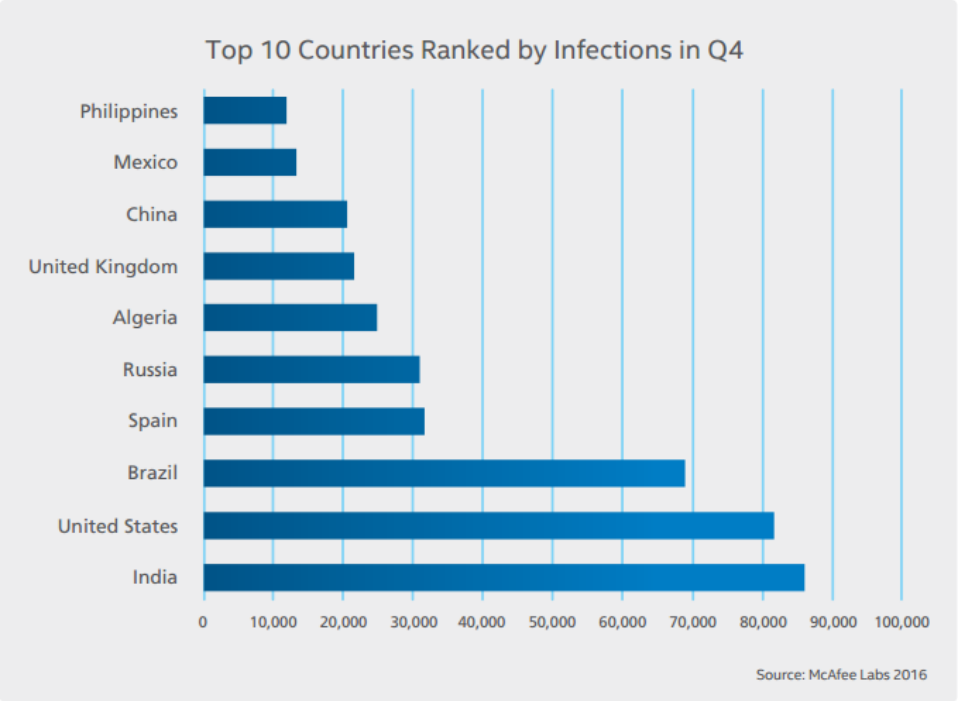

Figure 8: Estos números representan el total de infecciones únicas con infecciones repetidas descartadas. [9]

Consejos para esquivar los malwares para móviles

Estos son algunos consejos que puede seguir para asegurarse de que su información y su dispositivo están a salvo:

Descargue únicamente aplicaciones de app Stores con buena reputación, y lea las opiniones de otros usuarios antes de descargarlas para comprobar que son seguras.

Antes de descargar una aplicación, lea detenidamente su política de privacidad para asegurarse de que no compartirá su información personal.

Revise periódicamente las facturas de su teléfono móvil para comprobar que no hay cargos sospechosos. Si ve cargos que no se corresponden con nada que haya hecho, póngase en contacto inmediatamente con el proveedor del servicio.

Busque y descargue aplicaciones solo a través de una red inalámbrica segura.

No responda nunca a mensajes de texto o de voz facilitando información personal. Si se pone en contacto con usted alguien que dice ser de un banco o de un importante minorista o proveedor de servicios, llame directamente a su número de teléfono legítimo para verificar su identidad.

Cuando navegue por Internet, compruebe siempre que el nombre del dominio del sitio que visita es legítimo.

Nunca haga clic en un correo electrónico, un sitio de red social o un mensaje de alguien que no conoce.

Utilice un producto como un antivirus para dispositivos móviles, protección antimalware y búsqueda segura como McAfee mobile Security, Kaspersky Internet Security for Android o algún software similar. [9]

8 Conclusion

Con el aumento de la dependencia tecnológica y el acceso a dispositivos interconectados por más personas cada día, es fundamental que se tome conciencia sobre los riesgos de los ciberataques, las consecuencias y las medidas a tomar para minimizar estos eventos. Esto debe empezar por los actores involucrados en el área técnica pero debe llegar a todos los actores de la sociedad, ya que todos estamos expuestos a este tipo de problemas.

Desde sus inicios hasta hoy, las estrategias fueron evolucionando no solo en las técnicas y herramientas utilizadas, sino los mismos datos objetivos son cada vez más extensos, desde datos personales, tarjetas de crédito y hasta le georeferenciación de personas puede ser utilizada de distintas maneras por los criminales, ya sea para su uso directo o para la venta de estos datos.

En los últimos años vemos que con el incremento de los smartphones y de dispositivos en la Internet of Things, están apareciendo cada vez más ataques dirigidos a este tipo de dispositivos.

References

1. PMG-SSI. (2015) Ciberseguridad. [Online]. Available: http://www.pmg-ssi.com/2015/06/iso-27001-diferencia-entre-ciberseguridad-y-seguridad-de-la-informacion/
2. IsoTools. (2015) Riesgo y seguridad. [Online]. Available: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/
3. Iso.org. (2015) iso27001. [Online]. Available: http://www.iso.org/iso/iso27001
4. LavaSoft. (2015) History of malware. [Online]. Available: http://www.lavasoft.com/mylavasoft/company/blog/history-of-malware
5. Radware. (2015) Malware time line. [Online]. Available: http://www.radware.com/Resources/malwaretimeline.aspx
6. R. Centric. (2015) Cybersecurity. [Online]. Available: http://www.redcentricplc.com/media/2632/cybersecurity-for-dummies.pdf
7. T. Guardian. (2016) Tesla model s hacked. [Online]. Available: https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes
8. Abc.es. (2016) Ciberseguridad - tendencias 2016. [Online]. Available: http://www.abc.es/tecnologia/redes/abci-ciberseguridad-tendencias-marcara-2016-201512280112noticia.html
9. McAfee. (2016) The mobile report. [Online]. Available: http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf
10. 9tomac. (2016) iphone malware. [Online]. Available: https://9to5mac.com/2016/03/17/acedeceiver-iphone-malware/

11. Apple. (2016) Apple developers. [Online]. Available: https://developer.apple.com/programs/enterprise/

12. P. A. Security. (2016) Drm exploit on ios. [Online]. Available: http://researchcenter.paloaltonetworks.com/2016/03/acedeceiver-first-ios-trojan-exploiting-apple-drm-design-flaws-to-infect-any-ios-device/

13. A. insider. (2016) Pegasus. [Online]. Available: http://appleinsider.com/articles/16/09/01/pegasus-ios-malware-package-also-found-to-impact-os-x-apple-issues-patch

14. Fortinet. (2016) ios malware. [Online]. Available: https://blog.fortinet.com/2014/06/09/ios-malware-does-exist