Informe de Amenazas
CCN-CERT IA-06/17

Dispositivos y Comunicaciones Móviles
Informe Resumen 2016

Abril de 2017

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2017.05.04 10:58:45 +02'00'

ÍNDICE

1. SOBRE CCN-CERT

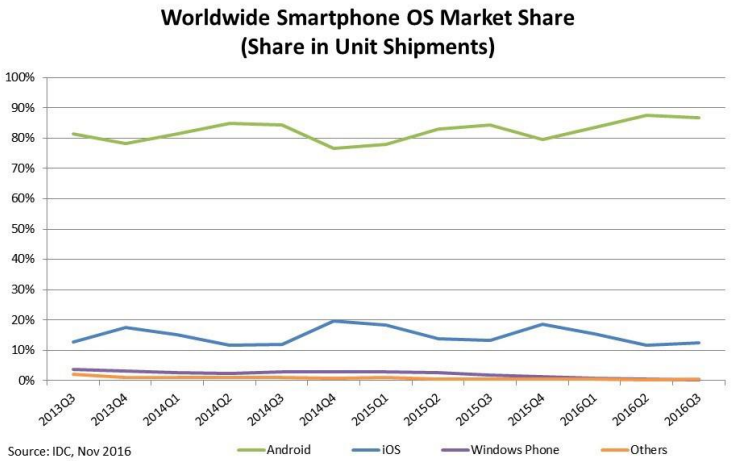
El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas del Sector Público**, a **empresas y organizaciones de interés estratégico** para el país y a cualquier sistema clasificado. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. RESUMEN EJECUTIVO

La madurez en la adopción de los dispositivos y comunicaciones móviles, tanto en el ámbito personal como profesional, ha alcanzado un nivel de estabilidad en el que resulta difícil imaginar la realización de las actividades cotidianas sin su utilización. El uso permanente de estas tecnologías confirma a los dispositivos móviles como uno de los **objetivos principales de las ciberamenazas para el año 2017**, consolidándose la tendencia de los últimos años.

A finales de 2016, se ha ratificado el ritmo de distribución con relación al año anterior por parte de todos los fabricantes de dispositivos móviles a nivel mundial, con una media de 360 millones de unidades por trimestre [Ref.- 1], según los estudios de IDC.



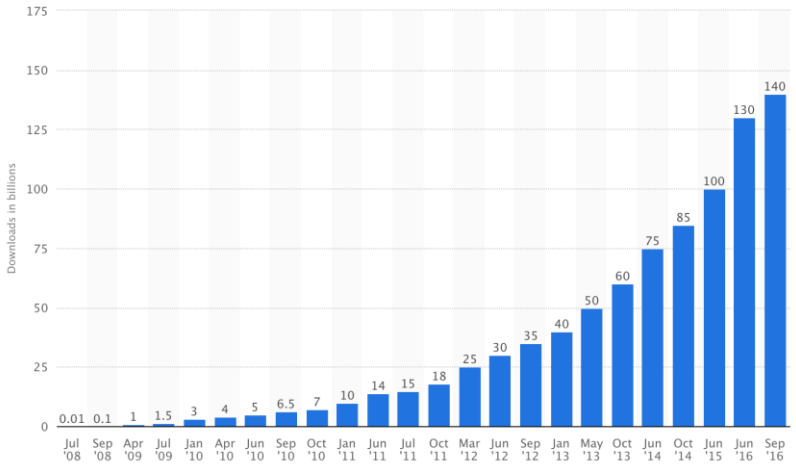
La plataforma móvil Android mantiene su cuota de mercado como líder indiscutible, con un ligero incremento que le sitúa en aproximadamente un 87% de la cuota de mercado, seguido por iOS con una cuota cercana al 13% y por Windows Phone, que ha disminuido aún más su cuota de mercado a cifras próximas al 0,3%, hecho que sí

parece confirmar el vaticinio de años previos de un declive en la presencia de este sistema operativo en el mercado de *smartphones* en el futuro.

En octubre del año 2016, continuando con la tendencia de estabilidad respecto al ritmo de adquisición de dispositivos móviles en la industria del trimestre anterior (que alcanzó su madurez en el año 2015), el crecimiento de ventas es prácticamente plano y sólo aumenta ligeramente en un 1% [Ref.- 2].

Respecto a los fabricantes, cabe destacar que Samsung sigue liderando el mercado (con un 21% de cuota de mercado), pese al conocido fiasco del modelo Note 7 en 2016, seguido por Apple (con un 13%) y de igual manera que los fabricantes de origen chino, como Huawei, OPPO o Vivo, presentan crecimientos y cuotas de mercado relevantes [Ref.- 3].

Las estadísticas del año 2016 reflejan el interés y crecimiento consolidado de los mercados de aplicaciones móviles (en adelante, *apps*), dónde la App Store alcanzó los 140 mil millones (billones[1]) de descargas totales en septiembre [Ref.- 4]. Por otro lado, Google Play ha llegado a superar los 2,2 millones de *apps*, mientras que la App Store ha alcanzado los 2 millones de aplicaciones móviles disponibles en junio de 2016 [Ref.- 5].



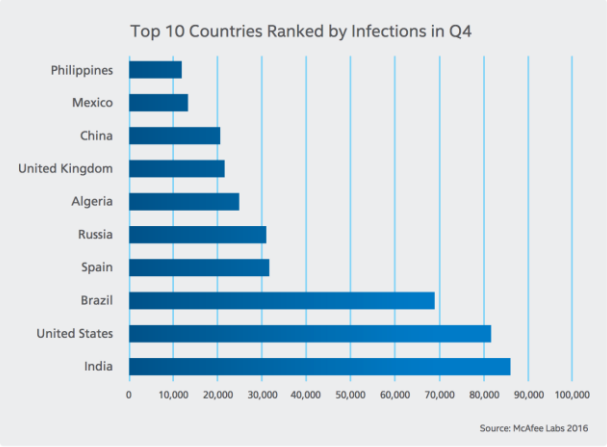
3. CÓDIGO DAÑINO PARA PLATAFORMAS MÓVILES

La importancia del código dañino para móvil como riesgo y amenaza real para los usuarios de dispositivos móviles se ve reflejada en la campaña de concienciación iniciada por Europol a finales de 2016, en concreto por el European Cybercrime Centre (EC3) dentro del mes de la ciberseguridad de Europa (octubre) [Ref.- 6]. En la misma estuvieron involucrados numerosos países, incluyendo a España, y agencias europeas.

[1] Las referencias a billones en el presente informe indican billones americanos, es decir, miles de millones.

Como denota el informe de la propia Europol [Ref.- 7], el malware para móvil juega un papel fundamental en numerosas investigaciones criminales realizadas en todo el territorio europeo, irrumpiendo en el dominio público.

Durante el año 2015 y principios de 2016 se ha identificado un incremento notable no sólo en el número de especímenes de código dañino para dispositivos móviles (*mobile malware*), sino también en su complejidad y sofisticación, encontrándose España entre los países más afectados a nivel mundial en base al número de infecciones únicas [Ref.- 8].



These numbers represent the total unique infections with repeated infections discarded.

Otras estadísticas también sitúan a España en el quinto lugar de los países con más detecciones de malware para Android [Ref.- 9].

Distribution of Android malware detections by country

1.	United States	12.74%
2.	Brazil	9.95%
3.	Indonesia	6.54%
4.	India	5.04%
5.	Spain	4.60%
6.	Philippines	4.25%
7.	France	4.24%
8.	Mexico	3.87%
9.	United Kingdom	3.59%
10.	Italy	2.79%

El malware para móvil continúa evolucionando y añadiendo técnicas para no ser detectado por los antivirus, mientras los usuarios siguen infectándose principalmente mediante la descarga de *app* de mercados no autorizados. Los países más afectados según otro estudio son Brasil, Indonesia, Filipinas y Méjico [Ref.- 10].

En el primer trimestre de 2016, dentro de las diez (10) familias de especímenes de malware más relevantes (en función del número de ataques), cabe destacar la aparición de un malware móvil para Android denominado *HummingBad*, desconocido

hasta febrero de 2016, lo que refleja su velocidad de distribución y rápido crecimiento [Ref.- 11].

HummingBad dispone de capacidades para obtener permisos de *root* (de cara a obtener beneficios económicos por parte de sus creadores a través de anuncios), funcionalidad de *keylogger* y permite la instalación de otras *apps*, pudiendo evitar contenedores cifrados utilizados a nivel empresarial.

Una reciente investigación revela que el mismo equipo de hackers rusos relacionado con el ataque al Partido Demócrata en Estados Unidos durante las últimas elecciones presidenciales, estuvo también implicado en el seguimiento de unidades de artillería ucranianas entre los años 2014 y 2016 empleando un malware para Android [Ref.- 12].

Dicho malware estaba vinculado a una aplicación legítima desarrollada originalmente por un oficial ucraniano como elemento de apoyo para designación de objetivos por parte de una de las piezas de artillería en servicio (D-30), siendo utilizada por más de 9.000 militares dentro de la brigada de artillería del ejército ucraniano. El malware permitió obtener inteligencia sobre las tropas ucranianas, gracias a la intercepción de las comunicaciones y los datos de la localización de los dispositivos móviles infectados, y de esta manera combatir a la artillería en contra de los separatistas pro-rusos que estaban luchando en el este de Ucrania.

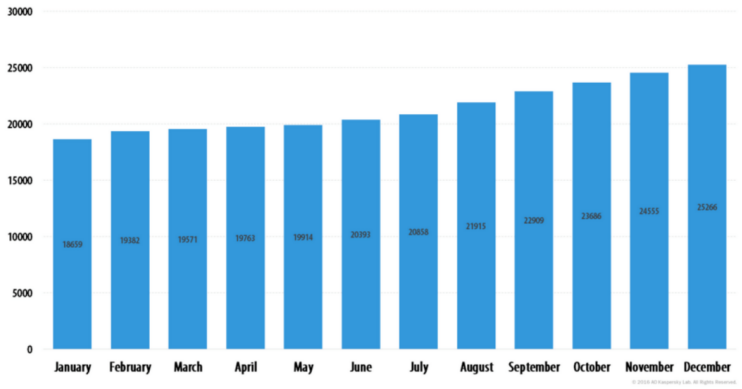
Se trata de una variante de malware de tipo *RAT* (Remote Access Tool) conocida como *X-Agent* y desarrollada y utilizada exclusivamente por el grupo *"Fancy Bear"* (APT 28), asociado con la agencia de inteligencia militar rusa (GRU). El malware fue distribuido de manera encubierta en foros de militares ucranianos como una *app* legítima, todo ello englobado claramente dentro de una operación militar a gran escala.

En enero de 2017, se desveló la existencia de un malware distribuido en la India a través de WhatsApp y cuyo principal objetivo eran los efectivos de policía, paramilitares y del ministerio de defensa, con capacidades para acceder a información personal del usuario, incluyendo credenciales [Ref.- 13].

El malware se remitía dentro de documentos Word, Excel y PDF mediante mensajes que parecían provenir de dos agencias gubernamentales, hacia personal potencialmente interesado en ambas, la National Defense Academy (NDA) y la National Investigation Agency (NIA).

La desenfrenada expansión del uso de los dispositivos móviles para el acceso a la banca electrónica, estimada en un 68 % entre jóvenes de entre 18 y 29 años, justifica el incremento en el número de troyanos bancarios móviles que han afectado al sector financiero desde finales de 2015 [Ref.- 14].

Como resultado, durante el verano de 2016, se corroboró la sofisticación y evolución de especímenes de malware como *Marcher*, un malware cuyo objetivo es obtener las credenciales bancarias del usuario y que expandió su lista de objetivos con nueve (9) nuevos bancos en Reino Unido (añadidos a los bancos ya existentes previamente de Alemania, Austria, Francia, Australia y Turquía) [Ref.- 15].



Number of mobile banking Trojans detected by Kaspersky Lab solutions in 2015

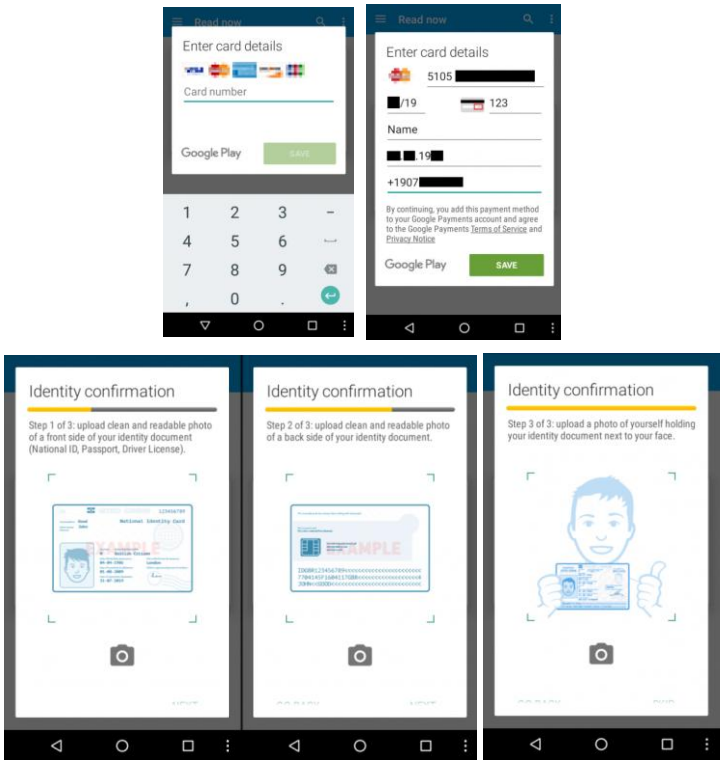
Marcher se identificó inicialmente en 2013 en foros rusos, centrado en el robo de tarjetas de crédito (junto a su fecha de expiración y código CVV2) mediante la superposición de una ventana cuando el usuario accedía a Google Play. En 2014 comenzó a incorporar instituciones financieras siendo su objetivo casi todas las versiones de dispositivos Android, con una distribución mayor en Jelly Bean, Kit Kat y Lollipop.

La distribución del mismo se lleva a cabo a través de mensajes de *phishing* camuflados como una actualización de *Adobe Flash*, que animan al usuario a infectarse en un proceso consistente en tres (3) pasos: permitir la instalación de *apps* de fuentes que no son de confianza, descargar e instalar la *app*. Algunas variantes de *Marcher*, además de atacar a *apps* y *URL* bancarias específicas (incluyendo, por ejemplo, el hacer uso directo del navegador web móvil con el banco), también atacan a *apps* de compañías aéreas, de pago y de comercio electrónico, obteniendo tanto las credenciales de autentificación como los códigos de un posible segundo factor de autentificación, manipulando los mensajes SMS y la redirección de llamadas de voz.

Asimismo, debido a que algunas instituciones financieras empiezan a hacer uso del escaneo de documentos oficiales para la identificación de sus clientes o de una verificación extensa de sus datos personales, el malware móvil está en continua evolución mejorando sus capacidades técnicas y de ingeniería social para suplantar a los usuarios.

Estos ejemplares de malware superponen su propia pantalla sobre la de la *app* bancaria legítima, para solicitar al usuario información adicional, que típicamente es empleada en el proceso de validación del usuario o para responder a las preguntas de seguridad.

Troyanos como *Acecard*, adicionalmente, solicitan al usuario información se su tarjeta de crédito (haciéndose pasar por Google Play), del segundo factor de autentificación e incluso una foto de la persona junto a su documento identificativo (DNI, pasaporte, carnet de conducir, etc.), para así disponer de todos sus datos [Ref.- 16].



Uno de los motivos que ha podido influir en la popularización de los troyanos bancarios para Android durante el año 2016 es la publicación del código Fuente relacionado con el *exploit kit* conocido como *GM Bot* [Ref.- 17].

Otras variantes de troyanos financieros móviles aparecidos a principios de 2016 como "*Android/Spy.Agent.SI*" (ESET), disimulados como supuestas actualizaciones de *Adobe Flash*, pueden obtener las credenciales bancarias de veinte (20) *apps* financieras de países como Australia, Nueva Zelanda o Turquía. Debido a sus capacidades para interceptar mensajes SMS, también pueden evitar el segundo factor de autentificación [Ref.- 18].

Alguno de los especímenes de malware identificados durante 2016, como *Godles*, dispone de capacidades para obtener privilegios como *root* en un 90% de los dispositivos móviles existentes en el mercado (especialmente con versiones de Android 5.1 o anteriores), mediante el uso de múltiples *exploits*, donde destacan *PingPongRoot* y *Towelroot*, de manera similar a un *exploit kit* (el mismo está basado en un *framework* de código abierto[2]). Las variantes iniciales de *Godles* incluían un *exploit* de *root* local, mientras que las nuevas versiones lo obtienen de manera remota intentando evitar así potenciales mecanismos de detección [Ref.- 19].

Godles ha sido distribuido a través de numerosos mercados, incluyendo Google Play, y podría haber afectado a unos 850.000 dispositivos móviles. *Godles* también dispone de capacidades de control remoto para realizar la instalación de otras *apps* de manera silenciosa.

[2] https://github.com/android-rooting-tools

Curiosamente, se han identificado múltiples *apps* benignas en Google Play firmadas con el mismo certificado de desarrollador que *Godles*, lo que permitiría al atacante infectar a usuarios que disponen actualmente de *apps* no maliciosas con su código dañino sin su conocimiento.

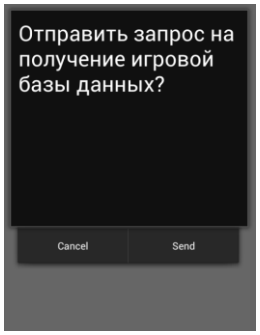
El interés de los troyanos para obtener privilegios de *root* en el dispositivo móvil del usuario víctima, mediante la ejecución de *exploits*, para así disponer de control completo del mismo, se ha incrementado notablemente a lo largo de todo el año 2016, especialmente, en los troyanos de anuncios asociados fundamentalmente a dos (2) familias de malware, *Ztorg* e *Iop* [Ref.- 20].

Estos privilegios les permiten, por un lado, ocultarse en el sistema y dificultar su eliminación (llegando algunos incluso a instalarse en la imagen de recuperación para sobrevivir incluso al proceso de restauración de los ajustes de fábrica), y por otro, disponer de la capacidad para instalar silenciosamente y ejecutar otras *apps* (e incluso comprar nuevas *apps* desde Google Play), que son las encargadas de mostrar los anuncios y obtener así beneficios económicos.

Las técnicas tan agresivas empleadas para mostrar anuncios hacen que en muchos casos el dispositivo móvil no pueda ser utilizado. Estas familias de malware se siguen distribuyendo a través de *apps* infectadas disponibles en Google Play.

En otros casos, como por ejemplo *Fusob* (analizado posteriormente), los *exploits* no son empleados para obtener privilegios de *root* sino para la distribución del malware. Asimismo, otros especímenes como *Svpeng* se distribuían a través de la red de anuncios legítima Google AdSense, lo que le convirtió en el troyano bancario móvil más popular en 2016.

Debido a que Android implementa nuevas medidas de seguridad, como por ejemplo la solicitud de permisos al usuario antes de enviar un SMS Premium, algunos especímenes de malware como el troyano *Tiny SMS* [Ref.- 20] superpone su propia ventana para que el usuario no pueda visualizar el mensaje original, pero sin cubrir los botones legítimos, para que el usuario pueda aprobar la solicitud de envío sin ser consciente de ello[3].

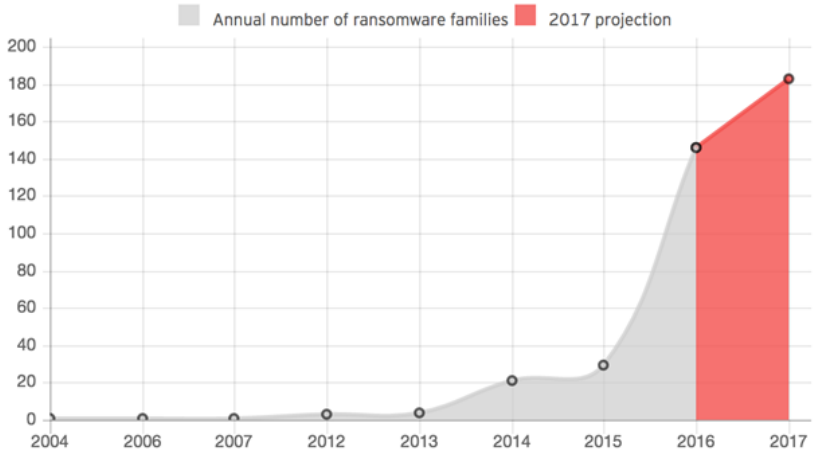


[3] https://cdn.securelist.com/files/2016/05/q1_2016_mw_en_9.png

Una técnica similar es empleada por *Asacub*[4], en este caso, para ocultar el hecho de que el usuario está facilitando privilegios de administrador al malware. Este troyano adicionalmente reemplaza la *app* de mensajería por defecto, para disponer de control completo sobre los mensajes SMS [Ref.- 20].

Desde un punto de vista global del malware (tanto tradicional como móvil), definitivamente el año 2016 ha sido el año del ransomware y la extorsión, con un incremento exponencial superior al 400% [Ref.- 21]. En 2017 se espera que se estabilice (con un crecimiento estimado del 25%), aunque los métodos de ataque y los objetivos (víctimas potenciales) se diversificarán.

Se espera que los incidentes que permitan acceder a datos de las compañías presentarán dos componentes, por un lado, la venta de dichos datos confidenciales, y por otro, su cifrado mediante ransomware para duplicar el beneficio tras el compromiso.



En el caso específico del malware móvil, según Quick Heal, ha habido un incremento del 200% destacando la utilización de **Ransomware-as-a-Service (RaaS)**, donde se venden los especímenes junto a kits de personalización en el mercado negro [Ref.- 22].

Estos datos se confirman por parte de Trend Micro, con un incremento 15 veces mayor de las amenazas asociadas a ransomware para Android en junio de 2016 respecto a abril de 2015 [Ref.- 23], distribuido habitualmente en mercados de terceros como *apps* legítimas, juegos populares, reproductores de Flash o de vídeo, o supuestas actualizaciones de sistema.

El ransomware móvil se puede clasificar principalmente en dos (2) categorías: aquel que bloquea el dispositivo móvil tras cambiar el código de acceso o PIN, empleando también la superposición de sus propias ventanas por encima de las de cualquier otra *app* (también conocido como *blocker*) y por otro lado aquel que cifra los ficheros del usuario, habitualmente almacenándolos en la tarjeta SD (también conocido como *cryptolocker*) solicitando una recompensa económica en ambos casos.

[4] https://securelist.com/blog/research/73211/the-asacub-trojan-from-spyware-to-banking-malware/

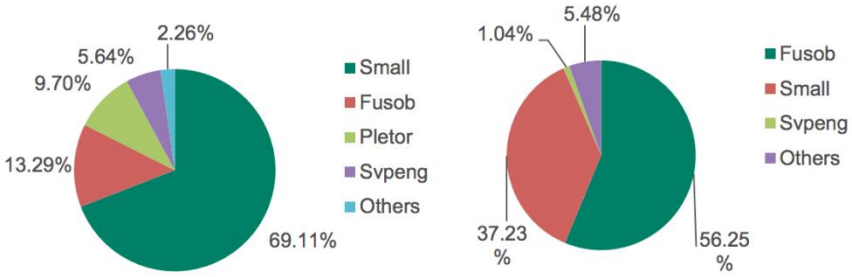
En el entorno más tradicional (ordenadores portátiles, equipos de escritorio, etc.), el segundo tipo es el más común, mientras que en el entorno móvil lo es el primer tipo.

Durante los años 2014 y 2015 existían fundamentalmente cuatro (4) familias de ransomware móvil dominando el mercado de este tipo de malware móvil: *Svpeng*, *Pletor*[5], *Small*, y *Fusob*[6] [Ref.- 24].

Actualmente, *Pletor* ha detenido su expansión, ya que sus creadores se han focalizado en el troyano *Acecard* (descrito anteriormente). Igualmente, los desarrolladores de *Svpeng* han centrado sus objetivos en la versión bancaria del troyano.

Svpeng ha atacado fundamentalmente a usuarios en Estados Unidos (97 %), aunque en abril de 2016 fue identificado en nueve (9) países diferentes. Dispone de capacidades para bloquear el acceso al dispositivo móvil y solicita una recompensa de 500 $. Como otras familias de ransomware, su método de distribución principal es a través de sitios web pornográficos.

Por tanto, en los años 2015 y 2016 existen principalmente dos (2) familias de ransomware móvil, *Small* and *Fusob*, que representan más del 93% del mercado, atribuidos a grupos cibercriminales de Rusia [Ref.- 24].



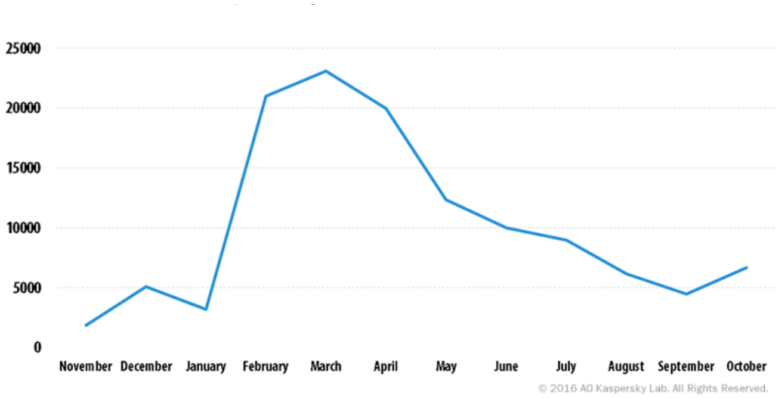
Ambas familias de ransomware muestran pantallas falsas indicando que a menos que el usuario pague la multa económica, se abrirá un caso criminal debido a haber cometido delitos menores.

Fusob identifica el idioma del dispositivo móvil, no llevando a cabo ninguna acción si es uno de los asociados a las repúblicas post-soviéticas. En caso contrario, muestra un mensaje asociado a la NSA solicitando un rescate de entre 100 $ y 200 $. La mayoría de sus víctimas son de origen alemán, inglés o americano (un 67 % en total), aunque ha afectado a más de 100 países distintos.

Para evitar ser eliminado, el malware bloquea el acceso a los ajustes del dispositivo superponiendo su propia ventana por encima de la ventana legítima. Adicionalmente, dispone de capacidades para hacer uso de la cámara del dispositivo móvil y para instalar otras *apps*.

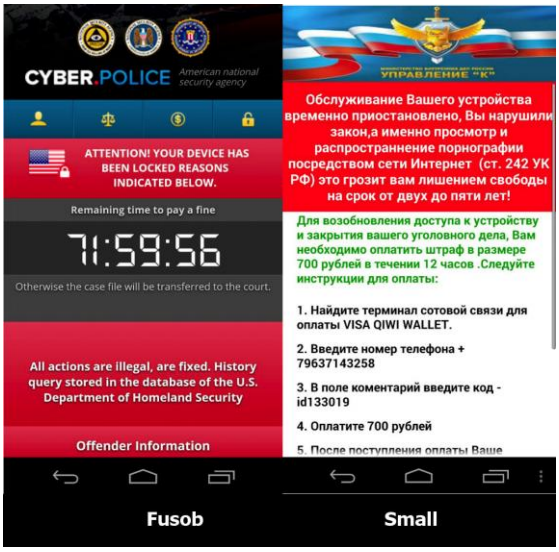
[5] https://blog.kaspersky.com/ransomware-outbreak/5045/
[6] https://securelist.com/analysis/kaspersky-security-bulletin/73839/mobile-malware-evolution-2015/

En algunos incidentes, se ha identificado el uso de un *exploit kit* para la distribución de *Fusob*[7]. La mayor actividad de *Fusob* [Ref.- 20] tuvo lugar durante la primera mitad del año 2016.



Number of unique users attacked by Trojan-Ransom.AndroidOS.Fusob

Por otro lado, *Small* (en su versión rusa) muestra un mensaje asociado al gobierno solicitando un rescate de entre 10 $ y 50 $. El 99 % de sus víctimas son de Rusia, Kazajistán y Ucrania.

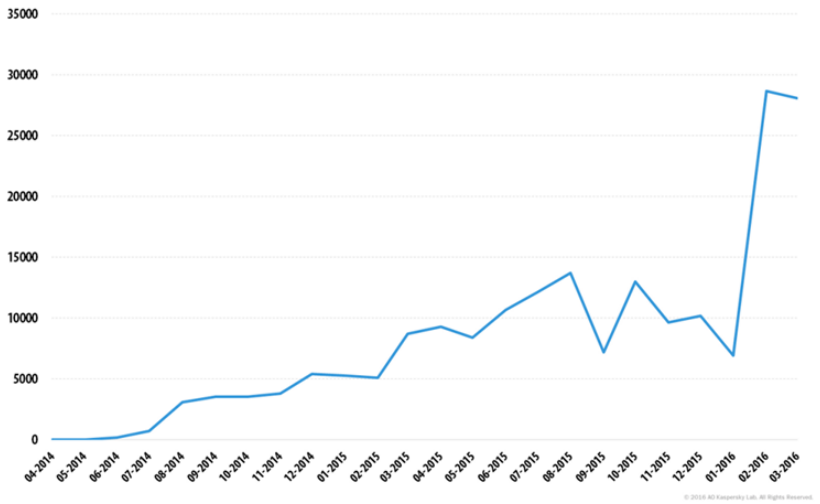


La versión inglesa de *Small* menciona al FBI y solicita un rescate de 300 $. Otra variante de *Small* dispone de capacidades de cifrado de la tarjeta SD del usuario víctima. *Fusob* solicita el pago mediante tarjetas regalo prepago de iTunes, mientras que *Small* ofrece la opción de pagar vía Kiwi o cupones de MoneyPak [Ref.- 24].

Las estadísticas recopiladas por Kaspersky indican que entre un 10 % y un 20 % de víctimas de malware para móvil, dependiendo del país, se ven afectadas por ransomware móvil y confirman su crecimiento desorbitado durante 2016.

[7] https://www.bluecoat.com/security-blog/2016-04-25/android-exploit-delivers-dogspectus-ransomware

En el caso de España, el porcentaje entre abril de 2015 y marzo de 2016 era sólo ligeramente superior al 5%, afectando más a países con infraestructuras consolidadas de pagos móviles y electrónicos, como Alemania, Canadá, Reino Unido y Estados Unidos [Ref.- 24].



Charger es un ransomware móvil que fue detectado en Google Play, en lugar de en mercados de terceros, empaquetado junto a otra *app* denominada *EnergyRescue* y haciendo uso de técnicas avanzadas de ofuscación y cifrado para evitar ser reconocido por sistemas de detección como *Bouncer*, y que se hacía pasar por una *app* para la gestión de la batería del dispositivo móvil [Ref.- 25].

EnergyRescue roba los contactos y mensajes SMS del usuario e intenta obtener permisos de administrador (como ya ha sido habitual en otras muestras de malware para Android en el pasado). Si obtiene dichos permisos, bloquea el dispositivo móvil y solicita al usuario una recompensa de 0,2 Bitcoins (unos 250 $) y le amenaza con que se venderá su información personal cada 30 minutos en el mercado negro si no paga. Aunque los mensajes mostrados al usuario indican lo contrario, el malware no cifra realmente los ficheros del usuario.

McAfee vaticina que en 2017 seguirá evolucionando el malware de Android, especialmente el ransomware, los troyanos bancarios y las herramientas de acceso y control remoto (RAT, Remote Access Tools) [Ref.- 26].

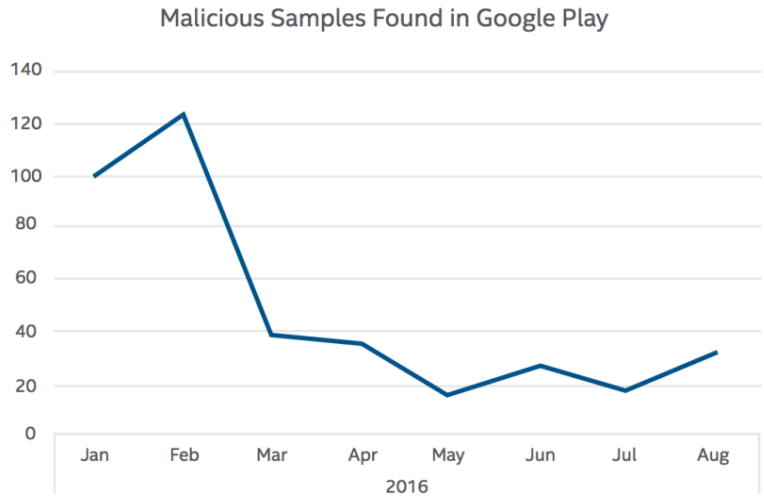
Una de las variantes de ransomware más destacadas en el segundo y tercer trimestre de 2016 es *Jisut*, que modifica el código de acceso del dispositivo móvil y solicita una recompensa mediante Bitcoins o tarjetas de prepago.

Debido a que muchos dispositivos móviles hacen copias automáticas de seguridad de sus datos en la nube, el beneficio asociado a los rescates por cifrado de los mismos es limitado. Por este motivo, se espera que en 2017 sigan prevaleciendo las técnicas de bloqueo de la pantalla de acceso, junto al robo de credenciales.

Un ejemplo de esa evolución es *Svpeng* (descrito previamente), que ha mutado de ransomware a troyano bancario [Ref.- 26].

La proliferación de RAT para Android durante 2016, enmascaradas como herramientas de soporte, ha empleado mercados de terceros y redes sociales para su distribución.

Aunque es más seguro llevar a cabo la descarga e instalación de *apps* desde los mercados oficiales, estos tampoco están exentos, tal como demuestran las estadísticas de *apps* maliciosas identificadas en Google Play, especialmente elevadas a comienzos del año 2016, aunque sean eliminadas por Google de manera ágil una vez detectadas [Ref.- 26].



4. OTROS RIESGOS ASOCIADOS A PLATAFORMAS MÓVILES

Dejando a un lado las amenazas asociadas directamente al malware para móvil, el año 2016 también ha presentado otros riesgos de seguridad relevantes en los entornos y tecnologías móviles.

Los dispositivos móviles son frecuentemente utilizados para establecer comunicaciones personales y profesionales con conocidos a través de las aplicaciones de mensajería, ya sea mediante el envío y recepción de mensajes SMS (o MMS), o mediante el uso de otros servicios de mensajería como WhatsApp, Telegram, Line, etc.

A través de estos servicios es posible recibir mensajes con enlaces web que albergan código dañino, con el objetivo de infectar y comprometer el dispositivo móvil del usuario víctima. Estos ataques basados en enlaces maliciosos distribuidos a través de las *apps* de mensajería se suelen referenciar como *SMiShing*[8][9], en lugar de *phishing* (término empleado en su distribución mediante correo electrónico).

[8] https://www.osi.es/es/actualidad/blog/2013/09/09/fraudes-online-vii-smishing-estafa-que-llega-traves-de-un-sms
[9] http://horajaen.com/detienen-a-siete-jiennenses-por-una-estafa-de-pishing/

El ataque apodado como *Pegasus* [Ref.- 27] que tuvo lugar en agosto de 2016 contra Ahmed Mansoor, un defensor de los derechos humanos de reconocido prestigio a nivel internacional y residente en los Emiratos Árabes Unidos, utilizó técnicas basadas en el envío de un mensaje SMS dañino para intentar infectar el iPhone de la víctima y tomar control completo del mismo mediante un software de espionaje (spyware) sofisticado, empleando tres nuevas vulnerabilidades para iOS desconocidas públicamente con anterioridad (0-days), y cuyo valor en el mercado de vulnerabilidades (tal como se detallará posteriormente) es muy elevado.

Pegasus, probablemente uno de los ataques más sofisticados de la historia [Ref.- 28], dispone de la capacidad de comprometer un dispositivo móvil iOS, con la última versión disponible en el momento de su utilización, con una sola pulsación en un enlace web por parte del usuario víctima. Las tres vulnerabilidades explotadas por Pegasus fueron resueltas por Apple en iOS 9.3.5 y, finalmente, de nuevo, en iOS 10.0.1.

En realidad, en el caso de iOS, Pegasus puede ser englobado dentro de una categoría de malware asociado al ciberespionaje móvil patrocinado por gobiernos [Ref.- 29]. Por otro lado, en el caso de Android, en 2016 también se ha descubierto Exaspy, un software comercial de ciberespionaje móvil cuyo objetivo eran altos ejecutivos de compañías privadas y corporaciones [Ref.- 30]. Exaspy dispone de numerosas capacidades para obtener los datos y actividades del usuario víctima.

Las predicciones para 2017 [Ref.- 31] parecen confirmar:

- La expansión de nuevas campañas de ciberespionaje móvil en entornos corporativos, con herramientas cada vez más simples de usar y más económicas.
- La proliferación de ataques más sofisticados y con un mayor nivel de comprometimiento y control sobre los dispositivos móviles afectados, con el

objetivo de ocultar su presencia y actividades persistiendo durante mayores periodos de tiempo.

Los atacantes seguirán aprovechando las oportunidades disponibles, tal y como ocurrió en 2016 con el popular juego Pokemon Go, para el que existían versiones falsas y maliciosas del mismo 48 horas después de su lanzamiento.

Los riesgos asociados a la pérdida o robo de los dispositivos móviles siguen siendo una realidad a tener en cuenta que hace imprescindible tomar medidas de protección frente a accesos físicos no autorizados (incluso temporalmente o durante un breve espacio de tiempo), especialmente en iOS.

Aunque la versión 9 de iOS se vio afectada por un menor número de vulnerabilidades que permiten evitar la pantalla de bloqueo del dispositivo móvil con respecto a las versiones de iOS 7 e iOS 8. iOS 10, únicamente durante el último mes de 2016 y primer mes de 2017, se ha visto afectada por más vulnerabilidades de este tipo que iOS 9 en su totalidad [Ref.- 32].

Esta sigue siendo una de las debilidades más significativas de esta plataforma a lo largo de los años, tal como denota el conjunto acumulado de vulnerabilidades en la pantalla de desbloqueo de las diferentes versiones de iOS.

Estos riesgos asociados a la pérdida o robo, incluso si el dispositivo móvil iOS está protegido por un código de acceso, pueden presentarse también a través de la tarjeta SIM asociada al servicio de telefonía móvil, si la misma no está correctamente protegida, tal como denota el siguiente incidente de seguridad publicado a finales de 2016 [Ref.- 33].

Si un potencial atacante obtiene acceso a la tarjeta SIM y ésta no dispone de un código de acceso, puede obtener fácilmente el número de teléfono del usuario. Con el mismo, es posible tener acceso a ciertas apps y servicios, como por ejemplo WhatsApp.

El uso de WhatsApp (en concreto mediante un mensaje a un grupo desde la pantalla de bloqueo) permitiría obtener el nombre completo del usuario, asumiendo que no se conocía previamente, y con esos datos (número de teléfono y nombre completo), es posible obtener la dirección de e-mail del usuario víctima en servicios como Google. Una vez conocida dicha dirección, es posible resetear su contraseña mediante un código SMS que también es enviado al número de teléfono del usuario comprometido.

Si la cuenta de Google está asociada al Apple ID (o cuenta en Apple) del usuario, sería posible obtener acceso a la misma mediante el proceso de recuperación de contraseña. Empleando esta cuenta, es posible resetear remotamente el dispositivo móvil a sus ajustes de fábrica y activarlo posteriormente, disponiendo de control completo sobre el mismo para su posterior venta o utilización.

Este escenario ejemplifica la necesidad de proteger las tarjetas SIM y la criticidad de los códigos SMS, ampliamente empleados como segundo factor de autentificación o como mecanismo de recuperación de contraseñas, al menos, al mismo nivel que los dispositivos y cuentas que protegen y a los que están asociados.

Asimismo, demuestra la criticidad de mostrar notificaciones en la pantalla de bloqueo de los dispositivos móviles, por muy conveniente que sea esta práctica en las actividades diarias.

5. VULNERABILIDADES EN IOS

Por otro lado, la vulnerabilidad en el proceso de actualización de iOS (CVE-2014-4383), mencionada en el informe de amenazas 2014 y tendencias 2015, que permitía a un potencial atacante congelar las actualizaciones de sistema del dispositivo móvil, y que no había sido completamente solucionada por Apple en las versiones 8 y 9 de iOS, finalmente fue solucionada en iOS 10 (CVE-2016-4741) mediante el uso de HTTPS para el intercambio del tráfico asociado a la comprobación de actualizaciones [Ref.- 34].

Este ejemplo confirma que la resolución de algunas vulnerabilidades en los sistemas operativos móviles puede requerir de varios años, con la consiguiente exposición para sus usuarios durante todo ese tiempo.

Sin lugar a dudas, uno de los casos estrella acontecidos a lo largo del año 2016 en la industria móvil es el asociado al caso de San Bernardino (California), y la supuesta disputa por la privacidad de los usuarios entre Apple y el FBI [Ref.- 35].

En resumen, debido a las mejoras en los mecanismos de seguridad y cifrado introducidas durante los últimos años en los dispositivos móviles (iPhone, en este caso), cada vez es más difícil disponer de acceso a los datos almacenados de manera cifrada en los mismos, incluso para las fuerzas y cuerpos de seguridad del estado en sus investigaciones.

Pese a la solicitud por parte de la justicia americana, Apple se erigió como defensor y estandarte de la privacidad de sus usuarios, aunque técnicamente sí dispondría de capacidades para tener acceso a los datos contenidos en un dispositivo móvil cifrado. Curiosamente, finalmente el FBI encontró, a través de una novedosa técnica de análisis forense, la posibilidad de obtener el código de acceso del iPhone involucrado en la investigación, y como consecuencia, la capacidad para acceder y analizar sus contenidos.

Una de las vulnerabilidades presentes en iOS 10, en concreto junto a la versión de iTunes asociada, está relacionada con la facilidad para llevar a cabo ataques de cracking o adivinación de la contraseña empleada en las copias de seguridad cifrados de iOS realizados con iTunes.

En versiones previas de iTunes, se hacía uso de un proceso de derivación de la clave de cifrado empleando la contraseña del usuario y el algoritmo PBKDF2 con 10.000 iteraciones. En la nueva versión de iTunes para iOS 10 se hace uso únicamente de una iteración mediante SHA-256, lo que hace que el proceso de cracking sea 2.500 veces más rápido [Ref.- 36]. Esta vulnerabilidad fue solucionada por Apple posteriormente en iOS 10.1 (CVE-2016-4685).

La oferta de *Zerodium*, una compañía que comercializa vulnerabilidades y *exploits* no públicos, de finales del año 2015 para iOS 9 aumentó a lo largo de 2016 para iOS 10. El valor de las nuevas vulnerabilidades que permitan disponer de control remoto

completo de un dispositivo móvil iOS de Apple se incrementó de un millón de dólares a un millón y medio de dólares [Ref.- 37].

Este hecho sólo ratifica el interés de la industria por disponer de acceso no autorizado a este tipo de dispositivos móviles, considerados por muchos como unos de los más seguros.

Un estudio publicado en enero de 2017 [Ref.- 38] confirma que la privacidad y seguridad proporcionada por las soluciones y aplicaciones móviles asociadas a las comunicaciones a través de VPN (Virtual Private Networks, o redes privadas virtuales) en Android presenta carencias significativas.

Del total de 283 *apps* de VPN analizadas, instaladas por decenas de millones de usuarios, el 18 % no cifraban correctamente el tráfico del usuario y un 38 % inyectaba malware o anuncios. Adicionalmente, el 80 % de las *apps* solicitaban acceso a datos sensibles, como la cuenta del usuario o los mensajes de texto (o SMS), recopilando información personal del usuario.

Este estudio refleja la importancia de la reputación a la hora de instalar únicamente *apps* conocidas, de prestigio consolidado y publicadas por compañías o desarrolladores de confianza, así como la necesidad de verificar cuidadosamente los permisos solicitados por las mismas.

6. EMPLEO DE HTTPS EN TRÁFICO DE APLICACIONES MÓVILES

En 2017 se confirma la tendencia, e importancia, de hacer uso de HTTPS (mediante TLS) para autentificar y cifrar adecuadamente las comunicaciones y el tráfico intercambiado entre las *apps* móviles y los servicios remotos.

En este sentido, Apple anunció durante su conferencia de desarrolladores WWDC de junio de 2016 que el uso de HTTPS a través de Apple, *App Transport Security* (ATS) sería obligatorio para todas las *apps* publicadas en la App Store desde finales de año: "*Today, I'm proud to say that at the end of 2016, App Transport Security (ATS) is becoming a requirement for App Store apps*" (Apple's head of security engineering and architecture, Ivan Krstic).

ATS es un mecanismo introducido para iOS 9 en 2015, y que hace uso de HTTPS con requisitos de seguridad elevados (empleando TLS 1.2, *forward secrecy*, y al menos claves RSA de 2.048 bits o ECC de 256 bits, y algoritmos de hashing mediante SHA-256 o superior).

Desafortunadamente, la complejidad de dicho cambio, y la lenta adopción de HTTPS por parte de los desarrolladores de las *apps*, ha obligado a Apple a anunciar el 21 de diciembre de 2016 una extensión de la fecha límite de aplicación de dicho requisito, hasta una nueva fecha (no especificada) [Ref.- 39].

Asimismo, la versión 6.x de Android introdujo una nueva característica que permite a las *apps* declarar, y monitorizar, si generan o no tráfico sin cifrar [Ref.- 40]. Complementariamente, la versión 7.x de Android añade un nuevo fichero de configuración de seguridad de red más exhaustivo [Ref.- 41] que permite a las *apps*

individualmente definir las autoridades certificadoras (CA), así como otros escenarios, en los que confían, sus capacidades de *certificate pinning*, y si desean hacer un uso exclusivo de HTTPS.

7. BUENAS PRÁCTICAS EN EL USO DE DISPOSITIVOS MÓVILES

Desde el punto de vista defensivo, cabe destacar la publicación por parte del CCN-CERT en el mes de octubre de 2016 del "Informe CCN-CERT BP-03/16 Buenas Prácticas en Dispositivo móviles", con recomendaciones de seguridad para los usuarios finales y las organizaciones, incluyendo un decálogo de seguridad que debe ser tenido en cuenta por cualquier usuario de dispositivos móviles [Ref.- 42].

	Decálogo de seguridad de los dispositivos móviles
1	El dispositivo móvil debe de estar protegido mediante un código de acceso robusto asociado a la pantalla de bloqueo (o en su defecto, una huella dactilar digital). El código de acceso debe ser solicitado inmediatamente tras apagarse la pantalla, que debería de bloquearse automáticamente lo antes posible si no hay actividad por parte del usuario. No se debe dejar el dispositivo móvil desatendido sin bloquear.
2	Se debe hacer uso de las capacidades nativas de cifrado del dispositivo móvil con el objetivo de proteger todos los datos e información almacenados en el mismo.
3	El sistema operativo del dispositivo móvil debe estar siempre actualizado, al igual que todas las aplicaciones móviles (*apps*).
4	No conectar el dispositivo móvil a puertos USB desconocidos y no aceptar ninguna relación de confianza a través de USB si no se tiene constancia de estar conectando el dispositivo móvil a un ordenador de confianza.
5	Deshabilitar todos los interfaces de comunicaciones inalámbricas del dispositivo móvil (NFC, Bluetooth y BLE, Wi-Fi, servicios de localización, etc.) que no vayan a ser utilizados de forma permanente por parte del usuario. Deberían habilitarse únicamente cuando vayan a ser utilizados, y volver a deshabilitarse al finalizar su uso.
6	No conectar el dispositivo móvil a redes Wi-Fi públicas abiertas (o *hotspots* Wi-Fi) que no implementan ningún tipo de seguridad.
7	No instalar ninguna aplicación móvil (*app*) que no provenga de una fuente de confianza, como los mercados oficiales de *apps* (Google Play, App Store, etc.).
8	Se recomienda no otorgar permisos innecesarios o excesivos a las *apps*, limitando así los datos y la funcionalidad a la que éstas tendrán acceso.
9	Siempre que sea posible se debe hacer uso del protocolo HTTPS (mediante la inserción del texto "https://" antes de la dirección web del servidor a contactar). Nunca se debería aceptar un mensaje de error de certificado digital inválido.
10	Se deben realizar copias de seguridad (*backups*) periódicas, y preferiblemente automáticas, de todos los contenidos del dispositivo móvil que se desea proteger y conservar.

8. TENDENCIAS 2017

Pese a que el malware móvil no está tan extendido como el malware tradicional, su continuada progresión debe ser tenida en cuenta, ya que la madurez de las empresas para analizar y gestionar un incidente asociado a malware para móvil es también limitada, no disponiendo de la misma agilidad, procedimientos y conocimientos técnicos para llevarla a cabo que en el caso del malware tradicional [Ref.- 43].

Según un informe que analiza los incidentes de seguridad de 2016, una de cada cinco organizaciones sufrió un incidente relacionado con la movilidad, y un 39 % mencionan la seguridad como un impedimento para implantar entornos BYOD [Ref.- 44].

Las predicciones de Gartner respecto a la seguridad móvil para 2017 reflejan un incremento en los ataques y sofisticación de los mismos e incluyen recomendaciones para que las organizaciones no retrasen la implantación de iniciativas que afronten y permitan defenderse frente a las amenazas móviles, acuñadas bajo el término Mobile Threat Defense (MTD) [Ref.- 45], complementando las posibles soluciones de gestión (MDM) ya existentes.

Según Gartner, las soluciones MTD parecen constituirse por tanto como el siguiente escalón en las organizaciones frente a la frenética búsqueda de mecanismos para proteger sus entornos de movilidad [Ref.- 46].

En resumen, la tendencia de las principales amenazas móviles para el año 2017:

- Parece seguir evolucionando hacia escenarios más complejos, avanzados y profesionalizados de ataque.
- Apunta hacia una masificación y sofisticación del ransomware, la infección desde mercados de terceros principalmente.
- Los troyanos bancarios y malware cuyo objetivo son las *apps* de pagos.
- Y ataques dirigidos de espionaje a través de los dispositivos móviles.

ANEXO A. REFERENCIAS

[Ref.- 1] "Smartphone OS Market Share, 2016 Q3". IDC. 2016.
URL: http://www.idc.com/promo/smartphone-market-share/os

[Ref.- 2] "Worldwide Smartphone Shipments Up 1.0% Year over Year in Third Quarter Despite Samsung Galaxy Note 7 Recall". IDC. 26 Oct 2016.
URL: https://www.idc.com/getdoc.jsp?containerId=prUS41882816

" Worldwide Smartphone Volumes Relatively Flat in Q2 2016 Marking the Second Straight Quarter Without Growth". IDC. 28 Jul 2016.
URL: http://www.idc.com/getdoc.jsp?containerId=prUS41636516

[Ref.- 3] "Smartphone Vendor Market Share, 2016 Q3". IDC. 2016.
URL: http://www.idc.com/promo/smartphone-market-share/vendor

[Ref.- 4] "Cumulative number of apps downloaded from the Apple App Store from July 2008 to September 2016 (in billions)". Statista. Sep 2016
URL: https://www.statista.com/statistics/263794/number-of-downloads-from-the-apple-app-store/

[Ref.- 5] "Number of apps available in leading app stores as of June 2016". Statista. Jun 2016
URL: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

[Ref.- 6] "Malware Has Gone Mobile. Stop.Think. Connect. to keep cybercriminals out of your mobile device". Europol. Oct 2016. URL: https://www.europol.europa.eu/newsroom/news/malware-has-gone-mobile-stopthinkconnect-to-keep-cybercriminals-out-of-your-mobile-device

[Ref.- 7] "The Internet Organised Crime Threat Assessment (IOCTA) 2016". Europol.
URL: https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016

[Ref.- 8] "Mobile Threat Report. What's on the Horizon for 2016". McAfee Labs (Intel). 2016.
URL: http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf

[Ref.- 9] "2017 - State of Malware Report". Malwarebytes Labs.
URL: https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdf

[Ref.- 10] "2016-2017 State of Malware Report". MalwareBytes Labs.
URL: https://blog.malwarebytes.com/malwarebytes-news/2017/02/2016-state-of-malware-report/
URL: https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdf

[Ref.- 11] "HummingBad: A Persistent Mobile Chain Attack". Checkpoint. Feb 2016.
URL: http://blog.checkpoint.com/2016/02/04/hummingbad-a-persistent-mobile-chain-attack/

[Ref.- 12] "'DNC hackers' used mobile malware to track Ukrainian artillery – researchers". The Register. Dec 2016. URL: http://www.theregister.co.uk/2016/12/22/android_malware_tracked_ukrainian_artillery/
URL: https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

[Ref.- 13] "Mobile malware disguised as Microsoft docs spread via WhatsApp". SC. Jan 2017. URL: https://www.scmagazine.com/indian-whatsapp-users-targeted-by-mobile-malware/article/629335/

[Ref.- 14] "Financial Malware and its Tricks: Mobile Malware". F5. Aug 25, 2016. URL: https://f5.com/about-us/blog/articles/financial-malware-and-their-tricks-mobile-malwares-21708

[Ref.- 15] "This sneaky mobile malware just evolved into something even nastier" (Marcher). ZDNet. Jun 2016.
URL: http://www.zdnet.com/article/this-sneaky-mobile-malware-just-evolved-into-something-even-nastier/
URL: https://securityintelligence.com/marcher-mobile-bot-adds-uk-targets-steps-up-banking-fraud-capabilities/
URL: http://blog.checkpoint.com/2016/04/28/marcher-marches-on-the-anatomy-of-a-banker-malware/

[Ref.- 16] "Android Banking Trojan Asks for Selfie With Your ID". McAfee. Oct 2016. URL: https://securingtomorrow.mcafee.com/mcafee-labs/android-banking-trojan-asks-for-selfie-with-your-id/

[Ref.- 17] "Android Malware About to Get Worse: GM Bot Source Code Leaked". IBM. Feb 2016.
URL: https://securityintelligence.com/android-malware-about-to-get-worse-gm-bot-source-code-leaked/

[Ref.- 18] "Android banking trojan masquerades as Flash Player and bypasses 2FA". WeLiveSecurity. Mar 2016. URL: http://www.welivesecurity.com/2016/03/09/android-trojan-targets-online-banking-users/ URL: http://www.virusradar.com/en/Android_Spy.Agent.SI/description

[Ref.- 19] "'GODLESS' Mobile Malware Uses Multiple Exploits to Root Devices". Trend Micro. Jun 2016. URL: http://blog.trendmicro.com/trendlabs-security-intelligence/godless-mobile-malware-uses-multiple-exploits-root-devices/

[Ref.- 20] "Kaspersky Security Bulletin 2016". Kaspersky. Dec 2016. URL: https://kasperskycontenthub.com/securelist/files/2016/12/KASPERSKY_SECURITY_BULLETIN_2016.pdf

[Ref.- 21] "The Next Tier: 8 Security Predictions for 2017". Trend Micro. URL: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017

[Ref.- 22] "Mobile ransomware increases 200 percent". HelpNetSecurity. Sep 2016. URL: https://www.helpnetsecurity.com/2016/09/02/mobile-ransomware-increases-200-percent/

[Ref.- 23] "Mobile Ransomware: The Fast Growing Yet Unknown Threat". Trend Micro. Sep 22, 2016.
URL: http://blog.trendmicro.com/mobile-ransomware-fast-growing-yet-unknown-threat/

[Ref.- 24] "Ransomware on mobile devices: knock-knock-block". Kaspersky. June 29, 2016.
URL: https://blog.kaspersky.com/mobile-ransomware-2016/12491/
URL: https://securelist.com/analysis/publications/75183/ksn-report-mobile-ransomware-in-2014-2016/

[Ref.- 25] "Charger Mobile Ransomware Removed from Google Play". Threat Post. Jan 25, 2017.
URL: https://threatpost.com/charger-mobile-ransomware-removed-from-google-play/123321/
URL: http://blog.checkpoint.com/2017/01/24/charger-malware/

[Ref.- 26] "McAfee Labs 2017 Threats Predictions". McAfee. November 2016.
URL: https://www.mcafee.com/mx/resources/reports/rp-threats-predictions-2017.pdf

[Ref.- 27] "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender". Citizenlab. Aug 2016.
URL: https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
URL: https://blog.lookout.com/blog/2016/08/25/trident-pegasus/
URL: https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-how-to-tell-impacted.pdf

[Ref.- 28] "PEGASUS iOS Kernel Vulnerability Explained". Stefan Esser. Sep 2016.
URL: https://sektioneins.de/en/blog/16-09-02-pegasus-ios-kernel-vulnerability-explained.html
URL: https://sektioneins.de/en/blog/16-09-05-pegasus-ios-kernel-vulnerability-explained-part-2.html

[Ref.- 29] "Mobile Cyber Espionage is Real!". Skycure. Aug 2016.
URL: https://www.skycure.com/blog/mobile-cyber-espionage-is-real/

[Ref.- 30] "Exaspy – Commodity Android Spyware Targeting High-level Executives". Skycure. Nov 2016. URL: https://www.skycure.com/blog/exaspy-commodity-android-spyware-targeting-high-level-executives/

[Ref.- 31] "2017 Mobile Security Predictions – Some Good With The Bad". Skycure. Dec 2016.
URL: https://www.skycure.com/blog/2017-mobile-security-predictions/
URL: http://es.slideshare.net/skycure/mobile-security-2016-wrapup-and-2017-predictions

[Ref.- 32] "Bypassing iOS Lock Screens: A Comprehensive Arsenal of Vulns". Raúl Siles. DinoSec. September 204 (updated: January 2015). URL: http://blog.dinosec.com/2014/09/bypassing-ios-lock-screens.html

[Ref.- 33] "The 'Sin' Card: How criminals unlocked a stolen iPhone 6S". Morphus Labs. Oct 2016.
URL: https://www.linkedin.com/pulse/sin-card-how-criminals-unlocked-stolen-iphone-6s-renato-marinho

[Ref.- 34] "iOS: Back To The Future". Raul Siles. DinoSec. June 2014.
URL: http://blog.dinosec.com/2014/06/ios-back-to-future.html
"iOS: Back To The Future II". Raul Siles. DinoSec. January 2015.
URL: http://blog.dinosec.com/2015/01/ios-back-to-future-ii_25.html
"iOS 10: CVE-2016-4741". Apple.
URL: https://support.apple.com/es-es/HT207143
URL: https://www.dinosec.com/docs/iOS-includingOrdinarySecurity_RaulSiles_DinoSec_NN6ed.pdf

[Ref.- 35] "Everything you need to know about the Apple versus FBI case". Troy Hunt. Feb 2016.
URL: https://www.troyhunt.com/everything-you-need-to-know-about-apple/

[Ref.- 36] "iOS 10: Security Weakness Discovered, Backup Passwords Much Easier to Break". Elcomsoft. Sep 2016.
URL: http://blog.elcomsoft.com/2016/09/ios-10-security-weakness-discovered-backup-passwords-much-easier-to-break/
URL: https://support.apple.com/es-es/HT207271 (iOS 10.1 - CVE-2016-4685)

[Ref.- 37] "Zerodium iOS 9 Bounty". Zerodium.
URL: https://www.zerodium.com/ios9.html
URL: https://zerodium.com/program.html
URL: https://www.wired.com/2016/09/top-shelf-iphone-hack-now-goes-1-5-million/

[Ref.- 38] "Tinker, Torrentor, Streamer, Spy: VPN privacy alert". CSIRO. Jan 25, 2017.
URL: https://blog.csiro.au/tinker-torrentor-streamer-spy-vpn-privacy-alert/
URL: https://research.csiro.au/ng/wp-content/uploads/sites/106/2016/08/paper-1.pdf

[Ref.- 39] "Supporting App Transport Security (ATS)". Apple. Dec 21, 2016.
URL: https://developer.apple.com/news/?id=12212016b

[Ref.- 40] "Protecting against unintentional regressions to cleartext traffic in your Android apps". Android Devloper's Blog. Apr 2016.
URL: http://android-developers.blogspot.com.es/2016/04/protecting-against-unintentional.html

[Ref.- 41] "Configuración de seguridad de la red". Android Developers.
URL: https://developer.android.com/preview/features/security-config.html

[Ref.- 42] "Informe CCN-CERT BP-03/16: Buenas Prácticas en Dispositivo móviles". CCN-CERT. Octubre 2016.
URL: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4058-como-usar-nuestro-movil-de-forma-segura-y-evitar-ciberataques.html
URL: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1757-ccn-cert-bp-03-16-dispositivos-moviles/file.html

[Ref.- 43] "Mobile Malware State of Play". Contextis. Nov 2016.
URL: https://www.contextis.com/resources/blog/mobile-malware-state-play/

[Ref.- 44] "BYOD & Mobile Security Spotlight Report". 2016.
URL: http://www.crowdresearchpartners.com/wp-content/uploads/2016/03/BYOD-and-Mobile-Security-Report-2016.pdf

[Ref.- 45] "It starts now: 2017 mobile security predictions from Gartner". Lookout. Dec 2016.
URL: https://blog.lookout.com/blog/2016/12/01/gartner-mobile-security-predictions/
URL: https://www.gartner.com/doc/3512932?ref=AnalystProfile&srcId=1-4554397745

[Ref.- 46] "Market Guide for Mobile Threat Defense Solutions". Gartner. xxx
URL: https://www.lookout.com/info/gartner-market-guide-report-lp
URL: https://www.gartner.com/doc/3393617/market-guide-mobile-threat-defense