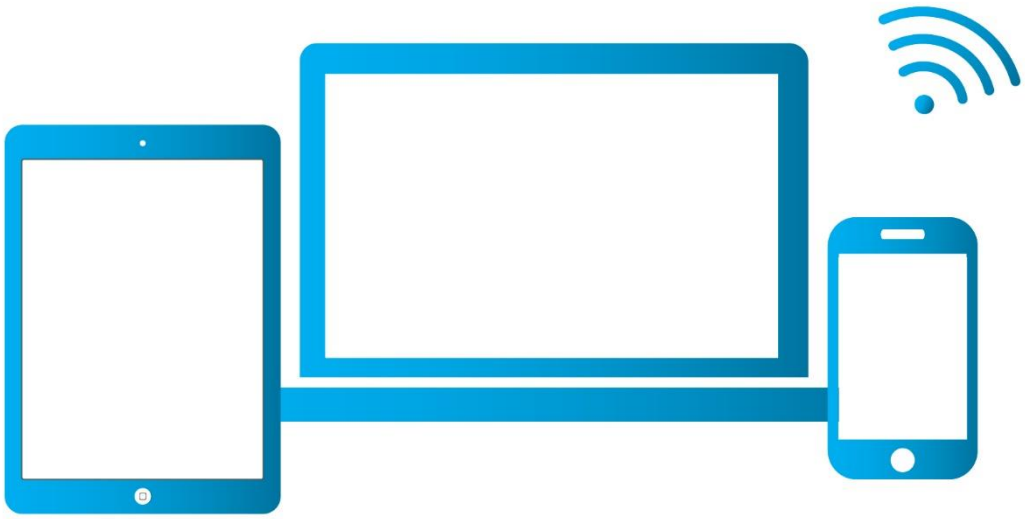
GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN-CERT centro criptológico nacional

CCN-CERT IA-10/18

Informe Anual 2017
Dispositivos y comunicaciones móviles



Mayo 2018

Edita:

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA DEL GOBIERNO
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

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
2018.05.10 13:07:42 +02'00'

© Centro Criptológico Nacional, 2018

Fecha de Edición: mayo de 2018

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL 4
2. RESUMEN EJECUTIVO 5
3. EVOLUCIÓN DEL MERCADO DE DISPOSTIVOS MÓVILES EN 2018 5
4. EVOLUCIÓN DE LOS MERCADOS OFICIALES DE APPS MÓVILES EN 2017 6
5. ADOPCIÓN DE LAS ÚLTIMAS VERSIONES DE LOS SISTEMAS OPERATIVOS MÓVILES 7
5.1 ANDROID GO 8
5.2 TREBLE 9
6. MECANISMOS DE AUTENTIFICACIÓN BIOMÉTRICA EN DISPOSITIVOS MÓVILES ... 11
6.1 FACE ID – IPHONE 11
6.2 ESCÁNER DE IRIS Y RECONOCIMIENTO FACIAL - SAMSUNG 13
6.3 INTELLIGENT SCAN - SAMSUNG 15
7. ADOPCIÓN DE NUEVAS TECNOLOGÍAS: INTELIGENCIA ARTIFICIAL 16
8. DESBLOQUEO DE DISPOSITIVOS Y EXTRACCIÓN FORENSE DE DATOS 19
9. CÓDIGO DAÑINO PARA PLATAFORMAS MÓVILES 23
10. COMUNICACIONES MÓVILES 37
ANEXO A. REFERENCIAS 41

SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación 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.

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, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la **información clasificada** (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo con esta normativa y la Ley 40/2015 de Régimen Jurídico del **Sector Público** es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de **operadores críticos del sector público** la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

1. RESUMEN EJECUTIVO

La adopción de los dispositivos y comunicaciones móviles, tanto en el ámbito personal como en el profesional, ha alcanzado un nivel de madurez y estabilidad en el que resulta difícil imaginar la realización de las actividades cotidianas sin hacer uso de estos. La utilización permanente y extensiva de estas tecnologías confirma que los dispositivos móviles son uno de los objetivos principales de las ciberamenazas para el año 2018, consolidándose así la tendencia de los últimos años.

El presente informe recoge algunas de las principales amenazas de seguridad y vulnerabilidades descubiertas a lo largo del año 2017 en los entornos de comunicaciones y dispositivos móviles, así como las tendencias más relevantes identificadas para el año 2018.

2. EVOLUCIÓN DEL MERCADO DE DISPOSTIVOS MÓVILES EN 2018

Curiosamente, y por primera vez en la historia, durante el año 2017 se identificó una muy ligera disminución (0,5%) respecto al año previo en el volumen de distribución de dispositivos móviles por parte de todos los fabricantes a nivel mundial, con una media de 365 millones de unidades por trimestre (1,46 billones americanos en total), según los estudios de IDC.

La plataforma móvil Android mantiene su cuota de mercado como líder indiscutible, ratificando los valores de años previos en torno al 85% de la cuota de mercado (Figura 3-1.); seguido por iOS, con una cuota cercana al 15%. Se confirma la casi definitiva desaparición de Windows Phone como sistema operativo en el mercado de *smartphones* futuro, debido a que ha disminuido aún más su cuota de mercado a cifras próximas al 0,1%, por la falta de acuerdos con fabricantes hardware de dispositivos para este sistema operativo.

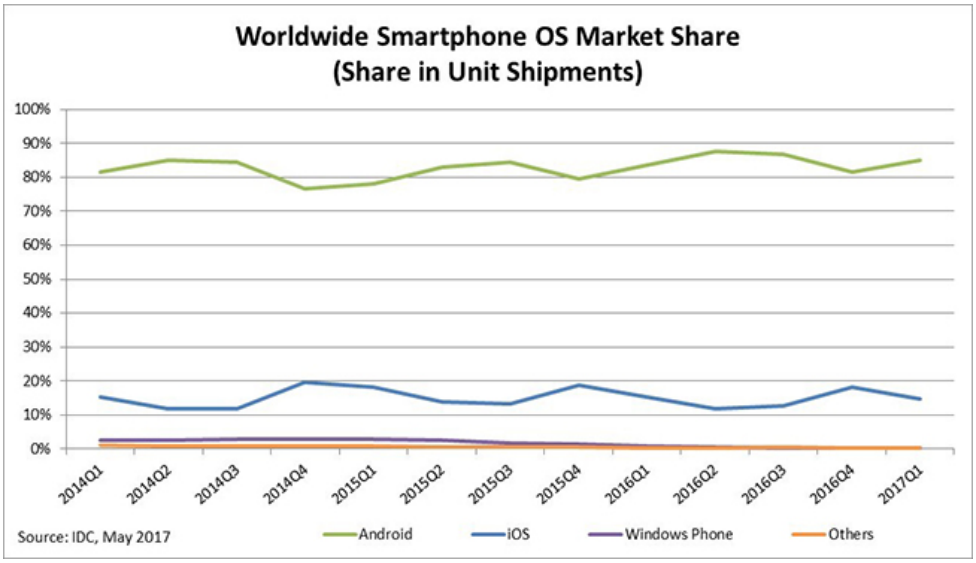


Figura 3-1.

En consecuencia, el presente informe sigue la evolución de los de años pasados, centrándose exclusivamente en las dos plataformas móviles relevantes a día de hoy, Android e iOS. Estas cifras globales se ratifican con las estadísticas disponibles públicamente, de manera específica para España, dónde a final de 2017 la cuota de mercado de Android era de un 87%; y la cuota de iOS, de un 13% aproximadamente.

Pese al ligero declive en el ritmo de adquisición de dispositivos móviles en la industria durante 2017, el crecimiento de ventas esperado en 2018 es prácticamente plano; con un reducido aumento asociado a la demanda de pantallas más grandes y de las tecnologías 5G. Respecto a los fabricantes, cabe destacar que Apple y Samsung siguen liderando el mercado −con entre un 12 y un 20% de cuota de mercado dependiendo del trimestre a lo largo de todo el 2017−, seguidos de los fabricantes de origen chino, como Huawei, OPPO o Xiaomi, con cuotas de mercado medias del 10%, 8% y 7% respectivamente.

Finalmente, con respecto a la comercialización de los dispositivos móviles, cabe destacar el incremento notable en el precio de los mismos, especialmente para los modelos de alta gama tanto de iOS como de Android, que ya se acercan o superan los mil euros.

3. EVOLUCIÓN DE LOS MERCADOS OFICIALES DE APPS MÓVILES EN 2017

Las estadísticas del año 2017 reflejan el ya conocido interés y crecimiento consolidado de los últimos años por parte de los mercados de aplicaciones móviles (en adelante, *apps*), dónde Apple Store alcanzó los 180 mil millones (billones[1]) de descargas totales en junio de 2017. (Figura 4-1)

Por otro lado, Google Play ha llegado a superar los 2,8 millones de apps disponibles, mientras que la App Store ha alcanzado los 2,2 millones de aplicaciones móviles en marzo de 2017.

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

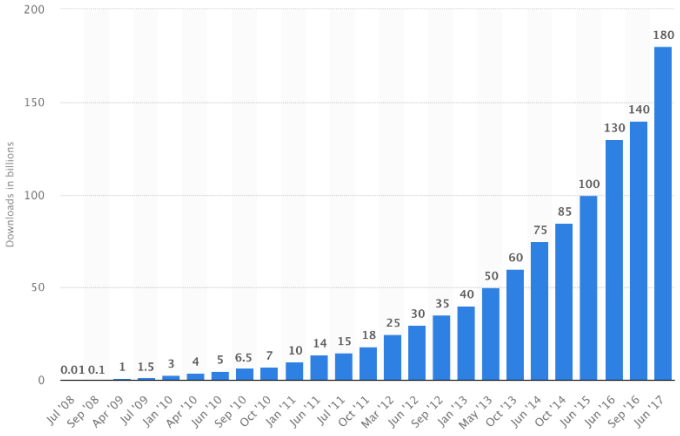


Figura 4-1.

4. ADOPCIÓN DE LAS ÚLTIMAS VERSIONES DE LOS SISTEMAS OPERATIVOS MÓVILES

La adopción de las nuevas versiones disponibles de los sistemas operativos móviles es crucial desde el punto de vista de seguridad, tanto para hacer uso de las nuevas funcionalidades y capacidades de protección introducidas por los fabricantes como Apple y Google, como para poder disponer de las últimas actualizaciones de seguridad frente a las vulnerabilidades públicas ampliamente conocidas.

La última versión del sistema operativo iOS 11.x, publicada por Apple a mediados de septiembre de 2017, estaba siendo utilizada por un 65% de usuarios cuatro meses después, en base a los datos oficiales obtenidos a través de la App Store de enero de 2018. (Figura 5-1.)

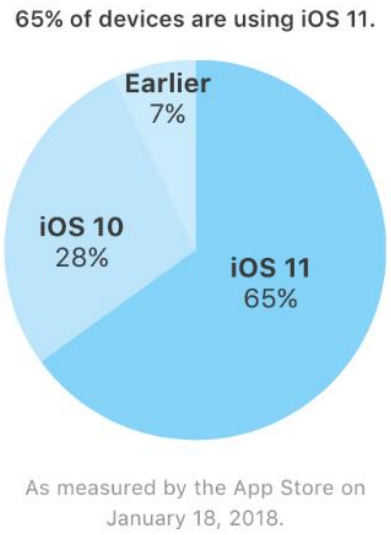


Figura 5-1.

En el caso de Android, la última versión del sistema operativo publicada a finales de agosto de 2017, Android 8.x (Oreo) ha presentado un nivel de adopción muy lento con respecto a versiones previas[2]. Pasados cinco meses desde su publicación, las estadísticas oficiales de Google del 5 de febrero de 2018 reflejaron que sólo el 1,1% de usuarios a nivel mundial disponía de la versión 8 de Android. Esta situación impide que los usuarios de Android puedan beneficiarse de todas las mejoras de seguridad introducidas en Android 8.x (Figura 5-2.)

Las versiones de Android más comúnmente utilizadas en la misma fecha eran Android 7.x, 6.x y, todavía, Android 5.x, con un 28,5%, 28,1% y 24,6% de cuota de mercado respectivamente. Este hecho ha incrementado aún más la fragmentación ya conocida de Android, con un impacto directo en la prevalencia de vulnerabilidades y en la limitada disponibilidad de actualizaciones de seguridad para esta plataforma para muchos usuarios.

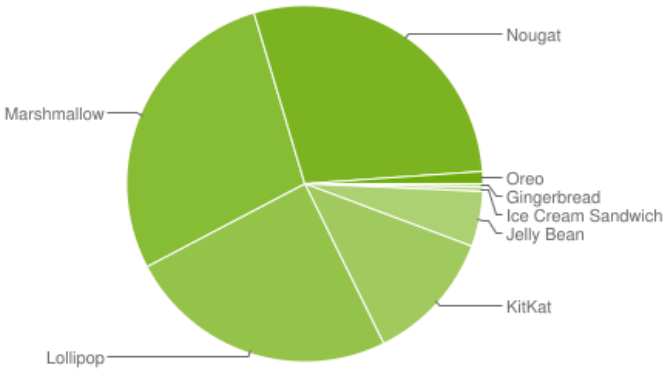


Figura 5-2.

Con el objetivo de mitigar la tan conocida fragmentación asociada a las diferentes versiones de Android utilizadas por los usuarios de este sistema operativo, Google está promoviendo dos iniciativas impulsadas junto a Android 8.x (Oreo): **Android Go** y el proyecto **Treble**.

4.1 Android Go

Mediante Android Go −anunciada en la conferencia Google I/O de 2017, y centrada en el software para complementar la antigua iniciativa Android One del año 2014, más centrada en el hardware− se pretende ofrecer actualizaciones de manera más ágil y continuada para dispositivos móviles de bajo coste, incluso pese a la existencia de personalizaciones de los fabricantes, adicionales a otras características.

Android Go proporciona las capacidades de seguridad y protección de Google Play Protect (GPP) a los dispositivos móviles bajo su ámbito. Durante 2017, Google ha

[2] https://en.wikipedia.org/wiki/Android_version_history & https://koz.io/mobile-os-version-adoption/

llevado a cabo la integración de múltiples de sus servicios y plataformas de seguridad bajo un mismo paraguas. Google Play Protect aúna múltiples capacidades y servicios previamente disponibles de manera individual en Android, cómo Verify Apps, Find My Device, Google Bouncer, Android Device Manager, SafetyNet, Google Safe Browsing (en Chrome), el servicio de reCAPTCHA, etc.

El objetivo es proporcionar un conjunto de servicios comunes para los dos billones de usuarios que hacen uso de Android a diario y proteger los dispositivos móviles, apps y los datos de los usuarios frente a las últimas amenazas de seguridad. Entre estos se incluye, por ejemplo, el análisis y escaneo de más de 50 billones[3] de apps diariamente. Estos números permiten hacerse una idea del volumen y complejidad del ecosistema móvil actual, en este caso, sólo de Android.

4.2 Treble

El propósito de este proyecto es minimizar algunos de los múltiples factores que promueven la fragmentación de Android, incluyendo la dificultad a la hora de adaptar las nuevas actualizaciones software del sistema operativo a las personalizaciones llevadas a cabo por los fabricantes (OEMs o *vendors*) y/o operadores de telecomunicaciones.

Para ello, Google ha creado una capa de hardware abstracta (HAL, Hardware Abstraction Layer) entre los drivers de software específicos de los fabricantes, necesarios para gestionar el hardware existente en los diferentes modelos de dispositivos móviles, y el propio sistema operativo Android. Al desacoplar Android de los componentes hardware y de sus detalles de implementación, se facilita la actualización del sistema operativo sin afectar a la funcionalidad. El interfaz estándar definido entre Android y el hardware, denominado "vendor interface" –validado por el Vendor Test Suite (VTS), análogo al Compatibility Test Suite (CTS)–, no se verá afectado por las actualizaciones, por lo que es posible aplicar actualizaciones de sistema operativo manera independiente y sin impactar al hardware, a diferencia de cómo ocurría anteriormente. (Figura 5-2.1)

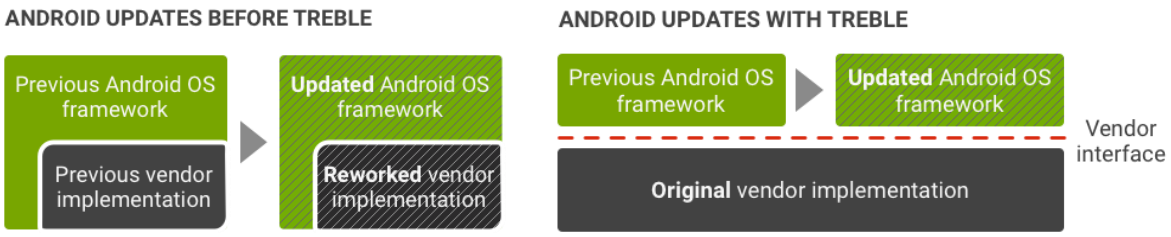


Figura 5-2.1

[3] Billones americanos, o miles de millones.

Sin embargo, la migración hacia la nueva arquitectura propuesta por Treble requiere que los fabricantes migren los drivers de todos sus componentes hardware, para cumplir con los requisitos y convenciones definidos por Treble. Google ha establecido Treble como obligatorio para todos los nuevos dispositivos móviles que disponen de Android 8.x desde fábrica, pero no obligatoriamente para los que se pueden actualizar a dicha versión. A día de hoy, algunos modelos como los Google Pixel 2 y Pixel, Sony Xperia XZ1, HTC U11 Plus o el Huawei Mate 9 ya disponen de soporte para Treble, con nuevos modelos incorporándose a la lista oficial (o extraoficial) de Treble[4] cada mes, por lo que recibirán actualizaciones futuras más ágilmente.

Solo el tiempo confirmará si la solución propuesta por Google tiene éxito y si los fabricantes, pese a soportar Treble, proporcionarán actualizaciones de manera ágil y frecuente para sus dispositivos, ya que estas actualizaciones en cualquier caso llegarán al usuario final a través de los fabricantes o los operadores, y no a través de Google directamente. Debido a que una de las principales motivaciones de negocio de los fabricantes es incrementar las ventas de los nuevos modelos de dispositivos móviles, ofrecer soporte y alargar la vida de modelos previos es contraproducente para cumplir ese objetivo.

Adicionalmente a la adopción de las últimas versiones del sistema operativo, Google está realizando un esfuerzo adicional para que los desarrolladores de aplicaciones móviles (apps) hagan uso también de las últimas APIs, librerías y capacidades disponibles en Android. Para ello, con la publicación de Android 8.x (Oreo), los desarrolladores deben de acomodar sus apps para las últimas APIs disponibles, a riesgo de que su app sea retirada de Google Play. El objetivo es que los dispositivos móviles más modernos dispongan de todas las funcionalidades y protecciones de seguridad disponibles a la hora de ejecutar las apps (como, por ejemplo, el control de permisos en tiempo de ejecución introducido en Android 6 o API 23) y, a su vez, reducir la fragmentación en el ecosistema de las apps de Android.

Los plazos establecidos por Google, que no afectan a la compatibilidad de las aplicaciones con dispositivos móviles más antiguos, requieren que las nuevas apps publicadas en Google Play a partir de agosto de 2018 hagan uso de la API 26 (Android 8.0) o posterior. Este requisito se aplicará a las apps existentes, para la distribución de nuevas actualizaciones, a partir de noviembre de 2018. A partir de 2019, las apps deberán hacer uso del nivel de API correspondiente a cada nueva versión de Android, que se incrementa anualmente. Un año después de la publicación de una nueva versión de Android, las apps deberán tener como objetivo, al menos, el nivel de API de dicha versión.

[4] https://www.xda-developers.com/list-android-devices-project-treble-support/

5. MECANISMOS DE AUTENTIFICACIÓN BIOMÉTRICA EN DISPOSITIVOS MÓVILES

5.1 Face ID – iPhone

En septiembre de 2017 con el anuncio del iPhone X por parte de Apple, y con la posterior comercialización en noviembre de 2017, se proporcionó a los usuarios de iOS un nuevo mecanismo de autentificación biométrica, adicional a la identificación por huella digital dactilar empleada ampliamente durante los últimos años por la industria móvil, tanto en iPhone y iPads, como en *smartphones* y *tablets* basados en Android.

Este nuevo mecanismo, denominado Face ID, reemplaza en el caso del iPhone X al mecanismo de autentificación mediante huella digital dactilar (conocido como Touch ID). Este se basa en el reconocimiento facial del usuario mediante un sistema de cámara (denominado TrueDepth), que hace uso de nuevas tecnologías para identificar la geometría en tres dimensiones (3D) de la cara del usuario −como son el análisis de una matriz de 30 mil puntos invisibles correspondientes al mapa de la cara (incluyendo información en relieve o con profundidad)−, junto a la captura por infrarrojos de ésta, y al uso de técnicas avanzadas de inteligencia artificial (IA) empleadas en los algoritmos de reconocimiento de la misma.

Adicionalmente, este mecanismo se adapta con el uso a los cambios en la apariencia del usuario. Desafortunadamente, este no permite elegir qué mecanismo de autentificación biométrico desea utilizar en el iPhone X, sino que hará uso de la cara o de la huella digital dactilar según el modelo de iPhone empleado.

Los datos de Face ID, junto a la representación matemática de la cara del usuario, son cifrados y almacenados con una clave protegida por el Secure Enclave Processor (SEP). Al igual que ocurría con Touch ID, Face ID puede ser empleado para autentificarse en el dispositivo móvil, para autentificarse en apps de Apple o de terceros, para autorizar compras en los diferentes mercados oficiales de Apple o para realizar pagos mediante Apple Pay, lo que denota la confianza que Apple ha puesto en este sistema.

El mismo mes de noviembre de 2017, una semana después del inicio de su comercialización, la firma vietnamita Bkav publicó una investigación que demostraba la posibilidad de construir una máscara tridimensional, con un coste aproximado de unos $200, a partir de la representación en tres dimensiones (3D) de la cara del usuario víctima, y que permitía a un potencial atacante hacer uso de esta máscara (o "gemelo artificial") para autentificarse con éxito a través de Face ID (Figura 6-1.1). La máscara original fue posteriormente mejorada a través de una segunda versión de la misma.

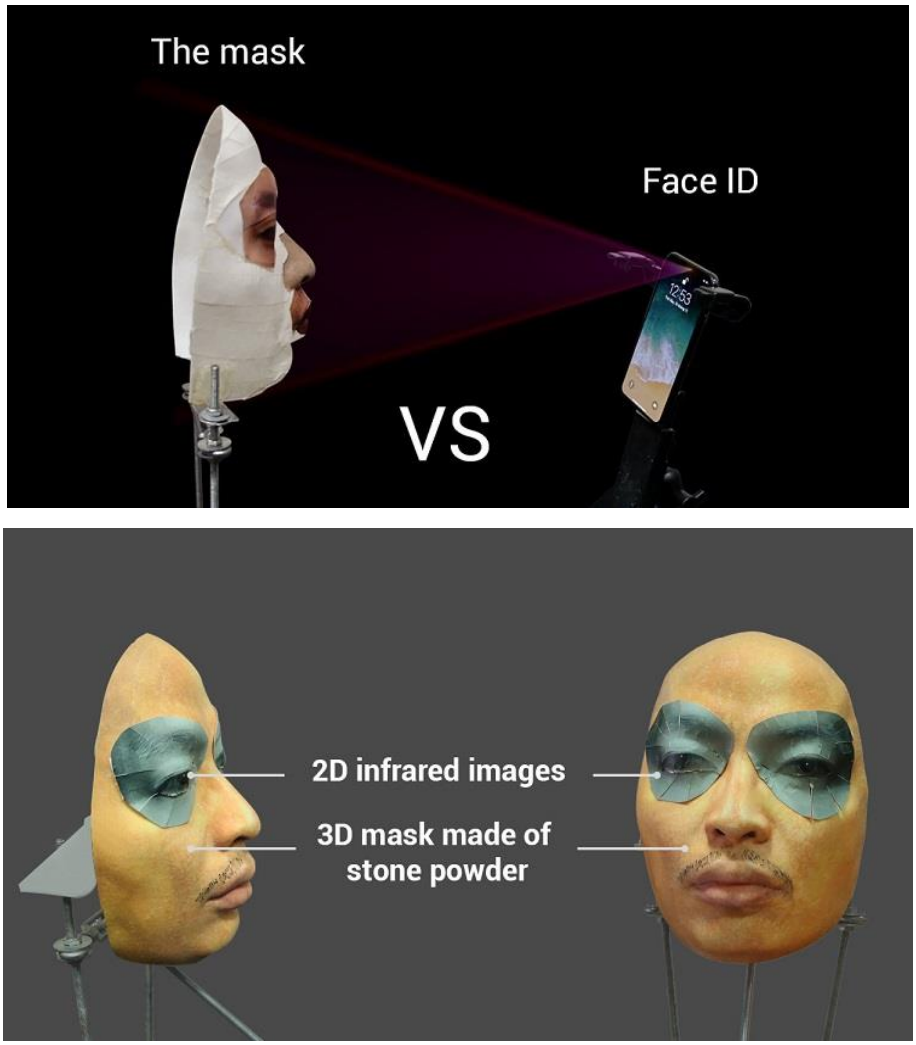


Figura 6-1.1

Supuestamente, la elaboración y composición en 3D de la máscara podría llevarse a cabo a partir del procesamiento de múltiples fotografías de la cara del usuario, tomadas desde distintos ángulos. Aunque la viabilidad de uso de esta técnica para ejecutar ataques reales por parte de un adversario, especialmente ataques dirigidos que permitan suplantar a un usuario respecto a Face ID, es limitada –tras cinco intentos fallidos el iPhone solicitará el código de acceso de respaldo–, la investigación vuelve a demostrar la posibilidad de saltarse los mecanismos de autentificación biométrica más avanzados, tal como ya ocurrió con Touch ID en septiembre de 2013.

La utilización de nuevos mecanismos de autentificación basados en la biometría se extendió a lo largo del año 2017 a otros dispositivos móviles, impulsada por el incremento de pagos móviles, e incluso como mecanismo de verificación o validación de

la identidad, por ejemplo, con "selfie pay" en Europa de la mano de Mastercard[5]. La biometría se ha constituido como un elemento clave en el año 2017 dentro de la industria móvil, y potencialmente se incorporará a más dispositivos a lo largo de 2018. Una tendencia que se consolidará en años venideros, ya que los usuarios prefieren hacer uso de estos mecanismos frente al tradicional código de acceso (o a la utilización de un usuario y contraseña en el caso de las apps).

5.2 Escáner de iris y reconocimiento facial - Samsung

Previamente al iPhone X, la comercialización del Samsung Galaxy S8 (S8+, y posteriormente el Note 8) en abril de 2017 introducía múltiples mecanismos de autentificación biométricos para desbloquear el dispositivo. Incluía el sensor de huella digital dactilar ya existente en modelos previos junto a un nuevo escáner de iris, que debutó con el Samsung Note 7, y un nuevo escáner de reconocimiento facial.

El escáner de reconocimiento facial de Samsung hace uso de la cámara frontal junto a una ingente cantidad de datos asociados a la cara del usuario para obtener propiedades y relaciones entre sus elementos, y permitir o denegar el acceso al dispositivo móvil.

El escáner de iris (Figura 6-2.1) hace uso de una cámara de iris dedicada que emplea filtros y tecnologías ópticas de luz infrarroja (leds) para obtener un patrón matemático a partir de imágenes detalladas del iris de uno o ambos ojos del usuario –aunque el aprendizaje del usuario se realiza sobre ambos ojos, es posible desbloquear el dispositivo móvil con un solo ojo–. En este caso, sólo un único usuario puede almacenar su información del iris en el dispositivo móvil.

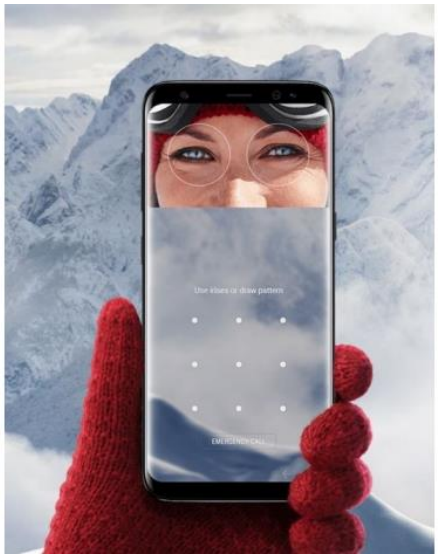


Figura 6-2-1.

[5] https://www.engadget.com/2016/10/04/mastercard-online-selfie-pay-europe/

Los datos biométricos, de la huella digital dactilar, de la cara o del iris, son procesados mediante algoritmos específicos para obtener una representación binaria de las características físicas del usuario, que es cifrada y almacenada en la TrustZone del dispositivo móvil Samsung, protegida por Knox.

Estas capacidades biométricas están integradas en diferentes servicios de Samsung para la autentificación del usuario –como por ejemplo Secure Folder, un contenedor para la gestión segura de ficheros y apps privadas–. Asimismo, se integran dentro de Samsung Pass, para hacer uso de autentificación biométrica en apps de banca móvil y en sitios webs mediante el navegador web de Samsung, y pueden ser empleadas también para autorizar pagos mediante Samsung Pay.

Al igual que otras tecnologías de autentificación biométrica, los nuevos escáneres de iris y de cara de Samsung han sido vulnerados. Por un lado, el sistema de reconocimiento facial proporciona un nivel de seguridad bajo (tal como ha reconocido el propio Samsung) y puede ser engañado con una fotografía en alta resolución del usuario, ya que sólo crea un mapa bidimensional (2D) de la cara de este, de manera parecida a como ocurría con el mecanismo de Face Unlock estándar de Android.

Por otro lado, el escáner de iris fue engañado en mayo de 2017 por investigadores del CCC (Chaos Computer Club), el mismo grupo que demostró por primera vez cómo saltarse el Touch ID del iPhone en 2013. Para ello, emplearon una lente de contacto para replicar la curvatura del globo ocular (Figura 6-2.2), y la fotografía de infrarrojos del ojo del usuario –tomada a cinco metros de distancia empleando el modo nocturno de una cámara digital, aunque potencialmente también se podría hacer uso de una fotografía de alta resolución obtenida de Internet–, demostrando que no era necesario extraer físicamente el ojo del usuario víctima para suplantarle.

Adicionalmente, el escáner de iris de Samsung fue también vulnerado por Bkav en junio de 2017 empleando un método más sencillo, basado también en el uso de una cámara de infrarrojos para posteriormente imprimir una representación del ojo y cubrirla con una fina capa de pegamento transparente.

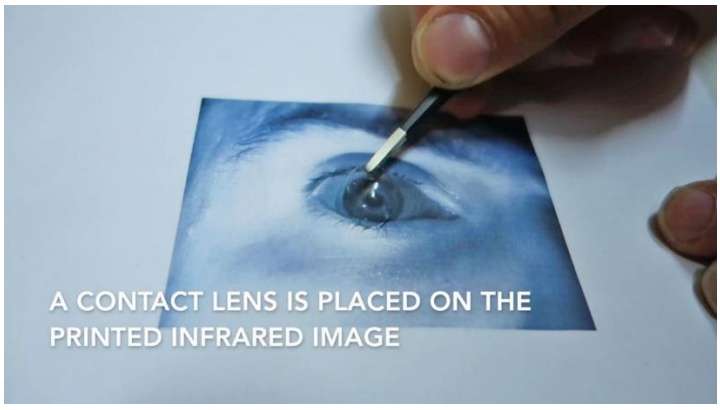


Figura 6-2.2

En resumen, los mecanismos biométricos basados en el uso de la cámara (como el reconocimiento facial y el escáner de iris) dejan más expuestos los "datos" del usuario frente a potenciales atacantes, como la posible obtención de imágenes a distancia; frente al uso de la huella digital dactilar (que requiere una obtención más próxima)[6]. Asimismo, todas estas vulnerabilidades asociadas a los sistemas de biometría aún plantean si el uso de un código de acceso robusto no sigue constituyendo un mecanismo de acceso a los dispositivos móviles más seguro, aunque más incómodo para el usuario[7].

5.3 Intelligent Scan - Samsung

Complementariamente, el Samsung S9 (y S9+) incorpora un nuevo sistema de autentificación denominado "Intelligent Scan". Este sistema se erige como competidor más directo de Face ID[8] que el S8 por robustez y prestaciones, debido a que combina un sistema de reconocimiento facial mejorado con el escáner de iris (también mejorado para trabajar a mayores distancias). Dispone también de capacidades biométricas más rápidas y sofisticadas a la hora de completar el proceso de verificación y de seleccionar el mecanismo de autentificación más óptimo en función del entorno y de las condiciones de uso (por ejemplo, en escenarios con iluminación reducida).

Estas capacidades serán integradas también en los servicios previamente descritos, como Samsung Pass. Sin embargo, las debilidades de ambos sistemas permanecen. Por esta razón, y por seguridad, los servicios más críticos como Secure Folder y Samsung Pay hacen uso sólo del escáner de iris (o de la huella digital dactilar), más preciso y fiable que el reconocimiento facial. Quizás el motivo por el que aún el S9 dispone de un sensor de huella digital dactilar es porque Samsung es consciente de las debilidades de seguridad de los nuevos sistemas biométricos.

Por otro lado, el Samsung S9 dispone de un sensor de huella mejorado que agiliza el proceso de registro, e introduce la tecnología "Dedicated Fingerprint" que permite seleccionar una huella digital dactilar dedicada para Secure Folder, pudiendo desbloquear el dispositivo móvil con esta y acceder directamente a este entorno privado de almacenamiento de datos.

Aunque aún es temprano para confirmarlo, el futuro de la biometría en dispositivos móviles podría pasar a hacer uso de un lector de huella digital dactilar integrado en la propia pantalla del dispositivo móvil. Esta implementación, que ya está disponible en el primer prototipo de móvil de Vivo[9], hace uso de un sensor óptico de

[6] http://www.bbc.com/news/technology-40012990
[7] https://www.theverge.com/2017/4/21/15360584/samsung-galaxy-s8-unlock-face-iris
[8] http://www.iphonehacks.com/2018/03/iphone-x-face-id-vs-galaxy-s9-intelligent-scan-differences-explained.html
[9] https://mobileidworld.com/vivo-display-sensor-tech-412151/

imágenes de Synaptics[10], a diferencia del sensor ultrasónico anunciado por Qualcomm y Fingerprint Cards[11].

Adicionalmente, en el futuro se podrá hacer uso incluso de nuevas características físicas de los usuarios, tal como demuestra la patente de Samsung asociada a un mecanismo de autentificación basada en propiedades de los flujos sanguíneos del usuario. Un sensor podría medir el flujo de sangre del usuario y extraer parámetros únicos del mismo, fisiológicos y morfológicos, que podrían ser empleados para su autentificación, o ser combinados con los mecanismos biométricos ya existentes en el dispositivo móvil.

6. ADOPCIÓN DE NUEVAS TECNOLOGÍAS: INTELIGENCIA ARTIFICIAL

El año 2017, y las tendencias previstas para el año 2018, han incrementado el uso de nuevas tecnologías de inteligencia artificial (IA, *Artificial Intelligence* o AI) en los dispositivos móviles, asociadas en muchos casos a sus capacidades de seguridad. Por ejemplo, el iPhone X de Apple hace uso de un nuevo procesador A11 Bionic diseñado especialmente para la ejecución de algoritmos de *Machine Learning (ML),* empleados en el proceso de verificación de la cara del usuario, cuando se emplea Face ID como mecanismo de autentificación biométrica. Con el objetivo de evitar ataques de suplantación, se hace uso de redes neuronales a través de un motor neuronal específico, protegido por el Secure Enclave Processor, que transforma los datos del relieve y de las imágenes de infrarrojos de la cara del usuario en su representación matemática.

La introducción de los **algoritmos de ML**, dentro del ámbito y mercado de la IA, se ha extendido también a entornos móviles, en concreto a las apps móviles y a numerosas aplicaciones prácticas relacionadas, constituyéndose como la tendencia de moda (Figura 7-1.). Estos algoritmos ofrecen capacidades de análisis y predicción en base al estudio y modelización de cantidades ingentes de datos o muestras[12].

[10]https://mobileidworld.com/vivo-demos-display-fingerprint-scanner-ces-901101/ https://mobileidworld.com/synaptics-display-sensor-mass-production-012121/
[11] https://mobileidworld.com/fpc-announces-display-fingerprint-sensor-tech-011012/
[12] https://theappsolutions.com/blog/development/machine-learning-in-mobile-app/

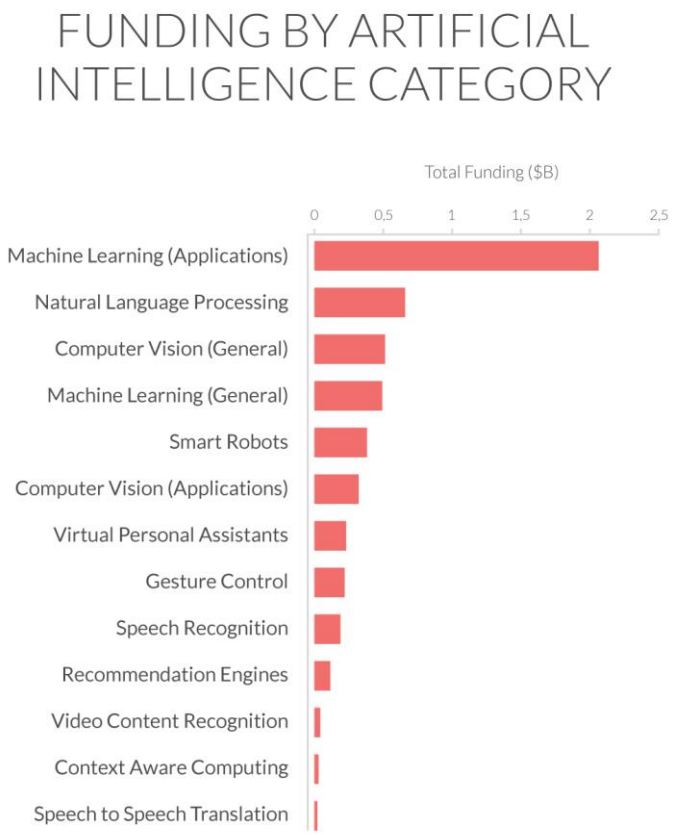


Figura 7-1.

Algunos casos prácticos de estas tecnologías integradas con "la nube" y el ecosistema móvil lo constituyen los **asistentes inteligentes digitales personales** que interactúan con el usuario mediante la voz, como Google Assistant, Alexa o Siri, extendidos posteriormente también a dispositivos IoT para el hogar. Destaca también la introducción por parte de Apple del SDK o kit de desarrollo de Siri, pudiendo las apps ofrecer capacidades propias a través de este asistente digital.

Asimismo, destaca cómo Google ha extendido la disponibilidad del asistente en Android Go para dispositivos móviles con 1 GB de memoria RAM o menos, con idea de hacerlo aún más universal. Las soluciones de ML también son empleadas para el reconocimiento y clasificación de las fotos del usuario, tanto en iOS, iCloud Photos, como en Android, Google Photos, utilizando diferentes categorías o sistemas de búsqueda.

Esta tendencia abre la puerta a nuevos tipos de ataques, centrados en la manipulación de la tecnología a través de la voz, sin interacción física directa con los dispositivos, y a la sutil manipulación de los algoritmos de IA para que proporcionen resultados inesperados.

Un ejemplo del primer tipo de ataque sigue siendo viable hoy en día (marzo de 2018), al existir la posibilidad de acceder a información sensible a través de las notificaciones de apps de terceros en iOS 11.3 ,al menos hasta su versión beta, y en versiones previas. Un potencial atacante con acceso físico a un dispositivo móvil iOS puede interactuar con Siri para que el asistente virtual lea el contenido de las notificaciones ocultas, incluso con la pantalla del dispositivo móvil bloqueada. Esta vulnerabilidad se une a la larga lista de vulnerabilidades similares descubiertas en versiones previas de iOS, que permiten evitar la pantalla de bloqueo manipulando la interacción del dispositivo con Siri.

Por otro lado, Google ha publicado el software, **Tensor Flow Lite**, disponible tanto para Android como para iOS. Este hace uso de redes neuronales específicamente optimizadas para su ejecución dentro de los propios dispositivos móviles, como precursor del "Artificial intelligence of Things (AioT)" del futuro, y **no requiere de conexión a Internet o a "la nube"** para hacer uso de ML[13], si hace uso de las capacidades de cálculo actuales de los dispositivos. Estas capacidades pueden ser empleadas, por ejemplo, para la traducción de idiomas.

Android 8.1, de hecho, introduce una nueva librería nativa, Neural Networks API (NNAPI)[14], para el desarrollo de apps y soluciones basadas en ML y que requieren de tareas intensivas de computación en los propios dispositivos móviles. Android Studio 3.0 proporciona soporte para esta API, junto al nuevo lenguaje de programación para Android, denominado Kotlin, e introducido por Google en 2017. Desde el punto de vista de seguridad, están aún por ver las implicaciones de seguridad de este lenguaje, que tiene que ser muy tenido en cuenta, al igual que Swift en iOS, sustituto de ObjectiveC, debido a la tendencia a que un mayor número de apps móviles hagan uso del mismo en el futuro, en lugar de Java.

La utilización de los algoritmos de ML está también asociada directamente a las capacidades de protección frente a software malicioso o dañino (o *malware*) móvil en soluciones como Google Play Protect. Para ello, se identifican y aplican mejoras en tiempo real en base al análisis de comportamiento y a las detecciones diarias de apps dañinas, empleando técnicas avanzadas de análisis y visualización de grandes volúmenes de datos con múltiples dimensiones, obtenidos del ecosistema Android global −mediante, por ejemplo, la Google Machine Learning -SNE[15] Cloud−. Otros fabricantes de seguridad, como por ejemplo Kaspersky también referencian ML en sus

[13]https://www2.deloitte.com/content/dam/insights/us/articles/machine-learning-mobile-applications/DUP_2830_Machine-learning_vFINAL.pdf
[14] https://developer.android.com/ndk/guides/neuralnetworks/index.html
[15] SNE: -Distributed Stochastic Neighbor Embedding

soluciones empleadas a lo largo de 2017 para la identificación y detección de malware móvil.

La posibilidad de manipular o atacar los algoritmos de ML (*Adversarial Machine Learning*) empieza a ser estudiada por los investigadores de seguridad ya que, debido a su complejidad, es difícil evaluar desde el punto de vista de seguridad la efectividad real de estas soluciones.

7. DESBLOQUEO DE DISPOSITIVOS Y EXTRACCIÓN FORENSE DE DATOS

La posibilidad de disponer de acceso no autorizado a un dispositivo móvil, suplantando a su propietario, ya sea legítimamente por parte de los cuerpos y fuerzas de seguridad del estado a la hora de solventar un caso judicial en el que están involucradas estas tecnologías, como ilegítimamente por parte de ciber-delincuentes, sigue siendo una de las áreas de mayor interés en el ecosistema móvil a nivel internacional.

Este interés se ve especialmente incrementado en el caso de aquellos dispositivos móviles dónde se considera más difícil vulnerar la pantalla de autentificación o desbloqueo sin disponer del código de acceso, como pueden ser los dispositivos móviles de Apple basados en iOS, como iPhones y iPads. Contradictoriamente a esta creencia generalizada, a lo largo de los años los dispositivos móviles basados en iOS han presentado numerosas vulnerabilidades que han permitido evitar la pantalla de desbloqueo sin disponer del código de acceso, permitiendo así el acceso a información parcial o total almacenada en los mismos. La versión 11 de iOS parece mantener la tendencia existente en versiones de iOS de años previos.

Esta amenaza enfatiza los riesgos asociados a la pérdida o robo de los dispositivos móviles, siendo imprescindible tomar medidas de protecciooón frente a accesos físicos no autorizados incluso temporalmente o durante un breve espacio de tiempo, especialmente en iOS. Algunos ejemplos centrados en evitar la pantalla de bloqueo de iOS tuvieron especial relevancia mediática, como el caso entre Apple y el FBI (junto al DoJ de USA) en relación al ataque terrorista de San Bernadino, California, del año 2016[16]. Este caso enfatizó de nuevo el debate centrado en si los dispositivos móviles deberían implementar una puerta trasera para permitir el acceso a los cuerpos y fuerzas de seguridad del estado, y cómo debería implementarse esta, de ser posible, para no poner en riesgo la seguridad del resto de usuarios de dichos dispositivos móviles.

Ante la negativa de Apple, en el caso de San Bernardino, lograron desbloquear con éxito el iPhone 5C del terrorista Syed Rizwan Farook. Para ello emplearon (potencialmente) una novedosa técnica hardware basada en desoldar del dispositivo

[16] La investigación por parte del FBI se llevó a cabo en el año 2016, aunque el ataque terrorista tuvo lugar en diciembre del año 2015.

móvil el **chip de memoria NAND del iPhone**, en el que se almacena el número de intentos fallidos de la pantalla de bloqueo −concretamente en un fichero de propiedades o plist−, conocida como "NAND mirroring"−ya referenciada brevemente en el informe del pasado año −.

Mediante el almacenamiento previo del contenido cifrado de dicho chip de memoria, y su posterior restauración −en realidad, realizando la restauración únicamente del bloque de datos asociado al contador de intentos−, era posible llevar a cabo un número ilimitado de intentos de desbloqueo, al poder realizar cinco intentos y resetear el contador a cero, como si no se hubiera realizado ningún intento de acceso fallido. Como resultado, la técnica permitía la realización de ataques de fuerza bruta para obtener el código de acceso legítimo en un breve espacio de tiempo, especialmente si se trata de un PIN de cuatro dígitos.

Sin embargo, esta técnica sólo era aplicable a los dispositivos móviles iOS previos al iPhone 5S, en los que se introdujo el procesador A7 que dispone de un procesador criptográfico, conocido como el Secure Enclave Processor (SEP). Debido a que el contador de intentos fallidos de la pantalla de desbloqueo se almacena en el SEP, se evita así su manipulación externa mediante la técnica basada en restaurar la memoria NAND (previamente descrita).

A finales de 2017 y principios de 2018, Cellebrite[17] publicitó la posibilidad de desbloquear cualquier dispositivo móvil iPhone (y iPad), incluyendo hasta la última versión de iOS 11 en ese momento, a través de sus servicios avanzados de desbloqueo y extracción de datos ("**Advanced Unlocking and Extraction Services**").

Este servicio relativamente económico, con un coste de unos $1.500-$5.000 por dispositivo[18] qué también está disponible para los últimos dispositivos móviles Android, requiere que el cliente envíe físicamente el dispositivo a los laboratorios de Cellebrite, dónde aplican el proceso de desbloqueo, para permitir al cliente o a ellos mismos extraer los datos del dispositivo. Las técnicas empleadas para disponer de este acceso no autorizado a los dispositivos móviles iOS son un objetivo que cada vez se vuelve más complejo con el paso del tiempo debido a que las medidas de protección que se van introduciendo en las nuevas versiones no han sido desveladas. Este servicio ha sido empleado también en casos de secuestro y/o desaparición de personas en España[19], por ejemplo, para el análisis del iPhone 6 de Diana Quer.

Alternativamente, la compañía Grayshift comenzó a comercializar a finales de 2017 un producto denominado **GrayKey**, que también permite a sus clientes llevar a

[17] https://media.cellebrite.com/wp-content/uploads/2017/12/advanced-unlocking-extraction-datasheet-jan2018.pdf
[18] El precio del servicio de $1.500 ha sido también referenciado en el pasado para versiones previas de iOS: https://www.forbes.com/sites/thomasbrewster/2016/03/23/cellebrite-apple-iphone-fbi-syed-farook-alexander-boettcher/
[19] http://www.elmundo.es/sociedad/2017/07/06/595e193f22601d5a068b45ce.html

cabo el desbloqueo de las últimas versiones (hardware y software) de los dispositivos móviles iOS en sus propias instalaciones (a diferencia del servicio de Cellebrite) y completar el proceso de extracción de datos de los mismos.

GrayKey, muy similar en formato a soluciones existentes de años previos como IP-Box, permite obtener el código de acceso tras varias horas o días, según su complejidad y longitud. El producto está disponible en dos versiones, ambas con licencia anual: una *online,* que requiere de conectividad a Internet para funcionar con un número de usos limitado a 300 y que solo puede ser empleada desde una ubicación, con un precio de $15.000； y otra *offline,* más flexible, sin todas esas limitaciones −y que hace uso de segundo factor de autentificación, con un coste de $30.000−.

Igualmente, las técnicas empleadas por GrayKey para vulnerar la seguridad de iOS no han sido desveladas. El interés, de nuevo por parte del FB, junto a muchas otras organizaciones y unidades[20], en este tipo de soluciones queda patente mediante, por ejemplo, la existencia de un proceso de compra público de seis unidades del modelo *offline* de GrayKey[21].

Desde un punto de vista legítimo, estas técnicas de desbloqueo por parte de los cuerpos y fuerzas de seguridad del estado se unen a la capacidad de poder hacer uso de los mecanismos biométricos de autentificación con la "ayuda" del sospechoso, ya sea mediante la identificación de su rostro si se utiliza Face ID, o la utilización de su huella dactilar para Touch ID (incluso en el caso de fallecidos[22]). Debe tenerse en cuenta, adicionalmente, que desde el punto de vista legal, la quinta enmienda de la constitución de EE.UU. no protege los mecanismos de autentificación biométrica, pudiendo por tanto

[20] https://motherboard.vice.com/en_us/article/vbxxxd/unlock-iphone-ios11-graykey-grayshift-police
[21]https://www.fbo.gov/index.php?s=opportunity&mode=form&id=0766508fa6330e948f73924cd68c27f0&tab=documents&tabmode=list
[22] https://www.forbes.com/sites/thomasbrewster/2018/03/22/yes-cops-are-now-opening-iphones-with-dead-peoples-fingerprints/

forzar a un sospechoso a desbloquear su dispositivo móvil empleando estos mecanismos, tal y como ha ocurrido en casos judiciales previos datados en 2016[23].

En relación con el desbloqueo de los dispositivos móviles, y más concretamente con la posible extracción de datos de los mismos, la última versión de iOS 11, por un lado, aumenta el nivel de seguridad al establecer una relación de confianza a través de la conexión USB con un ordenador. iOS 11 requiere no sólo que el usuario apruebe dicha relación de confianza (como en versiones previas), sino que introduzca el código de acceso, no pudiéndose por tanto hacer uso simplemente del desbloqueo mediante mecanismos biométricos.

Por otro lado, iOS 11 reduce el nivel de seguridad al permitir, desde el propio dispositivo móvil una vez desbloqueado, resetear la contraseña empleada para las copias de seguridad (o backups) de iTunes (Figura 8-1.) y, por tanto, la realización de un nuevo backup no cifrado (sin contraseña), facilitando la extracción lógica de sus datos desde el punto de vista forense.

Figura 8-1.

En versiones previas de iOS, al hacer uso de backups cifrados mediante iTunes, la contraseña empleada se almacenaba en el dispositivo móvil y se utilizaba para cifrar los datos antes de que estos fueran enviados y almacenados en el ordenador, o para restaurar un backup previo. La eliminación de la contraseña sólo era posible introduciendo la contraseña actual, único escenario que permitía la realización de un nuevo backup no cifrado o cifrado con una nueva contraseña, o también restaurando el

[23] https://www.forbes.com/sites/thomasbrewster/2016/10/16/doj-demands-mass-fingerprint-seizure-to-open-iphones/

dispositivo móvil a fábrica, pero con la consiguiente pérdida de los datos. En iOS 11 es posible restaurar los ajustes de configuración desde el propio dispositivo y, como consecuencia, eliminar el requisito que impone el uso de una contraseña previamente establecida para realizar un backup.

Por último, las implementaciones de Android desde la versión 6.x en dispositivos móviles que disponen de un **modulo TEE (Trusted Execution Environment)** hardware, almacenan tanto el código de acceso como el patrón de desbloqueo mediante un hash HMAC, basado en una clave disponible únicamente en el TEE. Este módulo hardware se encarga también de realizar los cálculos durante el proceso de autentificación, lo que aumenta la seguridad de Android; especialmente cuando se hace uso de un patrón de desbloqueo, ya que en versiones previas de Android éste se almacenaba empleando un hash sin semilla.

8. CÓDIGO DAÑINO PARA PLATAFORMAS MÓVILES

La importancia del código dañino para dispositivos móviles (*mobile malware*, en adelante malware móvil) como riesgo y amenaza real para los usuarios de dispositivos móviles sigue prevaleciendo en 2017, como en años previos, con un crecimiento continuado tanto en el número total de muestras como en el número de nuevas muestras, especialmente a finales de 2017. (Fugura 9-1.)

Por otro lado, el número de infecciones por malware móvil del tercer trimestre de 2017 superó los 16 millones, casi duplicando el número de infecciones identificadas un año antes. La evolución del malware móvil continúa su progresión: fueron necesarios 20 años para alcanzar los dos millones de muestras de malware en los equipos tradicionales (PCs), mientras que esa cifra se ha alcanzado en el ecosistema móvil en tan sólo cinco años.

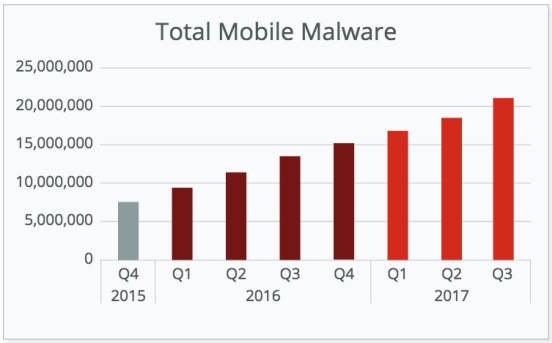


Figure 4. Total malware samples from 2015 – 2017.

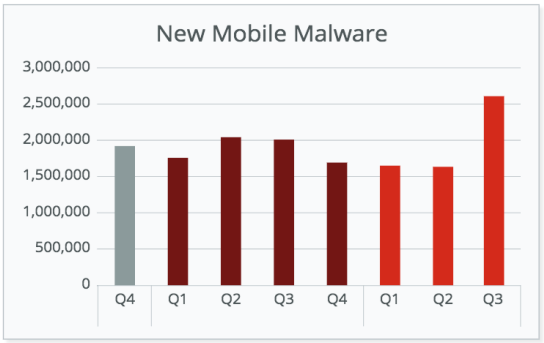


Figure 5. New malware samples from 2015 – 2017.

Figura 9-1.

Las estadísticas recopiladas por Sophos ratifican este incremento continuado del malware móvil para Android, siendo **Rootnik** la familia de malware más activa, con un 42% del malware identificado por Sophos, seguido por **PornClk** (14%) y por Axent, SLocker y Dloadr, con un 9%, 8% y 6% respectivamente (Figura 9-2.). Múltiples apps disponibles en Google Play estaban infectadas por Rootnik, y se identificaron, además, variantes de este, junto a otros especímenes de malware como **ZNIU**[24], que explotaba la vulnerabilidad del kernel de Linux conocida como DirtyCOW a finales de septiembre de 2017. Su objetivo era escalar privilegios y tomar control completo de los dispositivos móviles víctima obteniendo acceso como root.

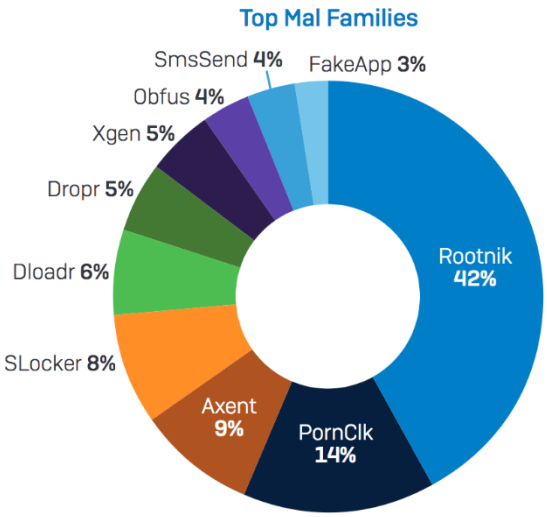


Figura 9-2.

Sin embargo, el número de apps potencialmente no deseadas o PUAs (Potentially Unwanted Applications) disminuyó en 2017 de 1,4 a un millón de muestras, acabando con la tendencia creciente de años previos. (Figura 9-3.)

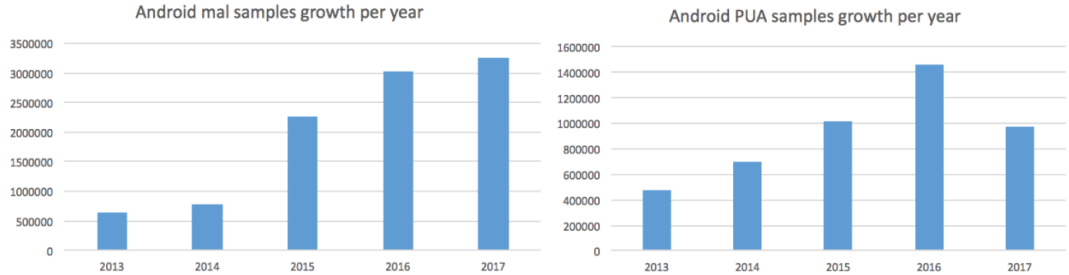


Figura 9-3.

[24] https://nakedsecurity.sophos.com/2017/09/29/android-malware-zniu-exploits-dirtycow-vulnerability/

Una de las vulnerabilidades principales durante el año 2017 en el ecosistema Android con implicación directa en la explotación por parte del código dañino para móviles ha sido **Cloak & Dagger**. Esta vulnerabilidad permite múltiples ataques mediante la manipulación de las capacidades de accesibilidad de Android, disponibles para adecuar las apps a usuarios con discapacidades visuales.

Una app maliciosa puede tomar el control completo del interfaz gráfico de usuario (UI, *User Interface*) del dispositivo móvil, de manera transparente para el usuario. La realización de los ataques requiere únicamente que la app disponga de alguno de los dos siguientes permisos: SYSTEM_ALERT_WINDOW ("draw on top") o BIND_ACCESSIBILITY_SERVICE ("a11y"). En caso de haber sido obtenida de Google Play, serán otorgados automáticamente al pertenecer a la categoría de permisos especiales. Los ataques se basan en la capacidad que tiene una app dañina para superponer contenidos y componentes encima del UI legítimo, engañando al usuario para que realice acciones o proporcione datos sin ser consciente de lo que está haciendo, o de a quién le está facilitando su información sensible.

Dentro de los ataques, o acciones maliciosas posibles, estarían ataques prácticos de **clickjacking o superposición de contenidos** encima de otras apps o del sistema (Figura 9-4.); captura de las pulsaciones del teclado, incluyendo contraseñas; *phishing*; instalación silenciosa de apps con todos los permisos habilitados; o el desbloqueo del dispositivo móvil manteniendo la pantalla apagada.

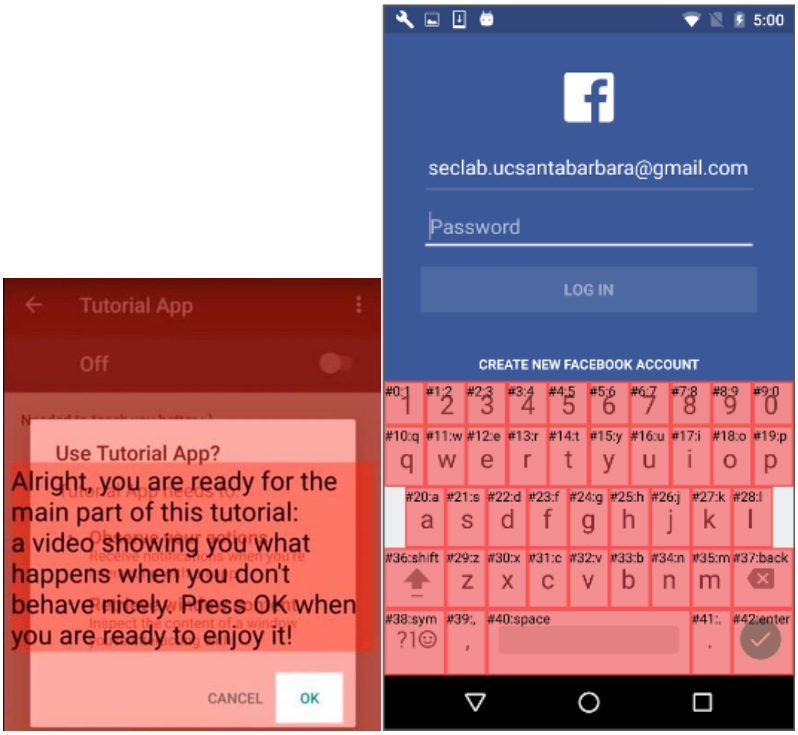


Figura 9-4.

Cloak & Dagger ha afectado a múltiples versiones de Android, desde 5.x hasta 7.1.2. Google ha tomado medidas para mitigar su impacto en Android 8.x (Oreo), al introducir limitaciones que no permiten la superposición de ventanas y contenidos sobre la app de ajustes del sistema debido a que explotan o abusan de características del diseño del UI de Android. En Android 8.x, para que una app pueda emplear los servicios de accesibilidad, debe de obtener explícitamente la aprobación del usuario a través de un privilegio existente en los ajustes de accesibilidad.

Dado que numerosas apps disponibles en Google Play hacen uso de los servicios de accesibilidad para otras tareas y mejoras de su funcionalidad, Google está contactando a los desarrolladores de las apps que hacen uso del permiso BIND_ACCESSIBILITY_SERVICE para que justifiquen su utilización dentro de la app para que lo eliminen, o para que eliminen la app en caso de no estar siendo empleado para ofrecer facilidades a usuarios discapacitados[25].

Con el objetivo de limitar la distribución de código dañino en Android de manera generalizada, el ajuste de configuración existente en versiones previas de Android que permite la instalación de apps desde orígenes que no son de confianza, ha sido restringido en Android 8.x. El ajuste ya no existe, y en su lugar se ha creado un nuevo permiso denominado **REQUEST_INSTALL_PACKAGES**, que incrementa la granularidad para poder gestionarlo por cada app.

Es decir, se debe otorgar la capacidad de instalar apps de terceros provenientes de fuera de Google Play de manera individualizada a cada app, por ejemplo, al navegador web Chrome para la descarga de APKs desde páginas web. Por tanto, los usuarios de Android 8.x pueden definir qué apps pueden instalar otras apps de terceros, en lugar de disponer únicamente de un ajuste global común a todo el sistema.

Por otro lado, aunque las nuevas capacidades de Android para ejecutar apps instantáneamente, conocidas como Instant Apps, anticipaban potencialmente un nuevo mecanismo para la distribución de malware en esta plataforma móvil pese a sus limitaciones, aún no se han identificado especímenes de software malicioso que hagan uso de esta funcionalidad.

A finales del año 2017 y principios de 2018, una de las campañas de malware móvil más relevantes, según McAfee, fue **Android**. El objetivo de esta campaña era la distribución de apps no deseadas en los dispositivos móviles de los usuarios víctimas, en un modelo de estafa conocido como pago por descargas (pay-per-download). Se eliminaron un total de 144 apps de Google Play, con una estimación de 17,5 millones de descargas por parte de los dispositivos móviles y usuarios afectados.

[25]https://www.reddit.com/r/Android/comments/7c4go5/is_google_play_really_going_to_suspend_all_app/

El ecosistema móvil también se ha visto involucrado en una tendencia cada vez más creciente dentro de las acciones dañinas llevadas a cabo por el software malicioso (malware) y la utilización de los recursos de computación del usuario víctima, en este caso del dispositivo móvil, para el minado de criptomonedas, como por ejemplo Bitcoin o Monero. Esta tendencia creciente, pero todavía en una fase incipiente o temprana, ya se reflejaba en el informe de malware móvil afecta a Google Play. El documento elaborado por McAffe, con datos del primer trimestre de 2018, destaca adicionalmente el fraude en anuncios, el spyware (o software espía), la actividad de botnets y centros de comando y control (C&C), y los troyanos bancarios. (Figura 9-5.)

Este tipo de ataques ha sustituido a otras acciones dañinas empleadas más frecuentemente en el pasado, como el **envío de mensajes SMS a servicios *premium***, o el fraude mediante llamadas a números de teléfono de pago. En el último año se ha identificado un incremento del 70% en el **minado de criptomonedas** (de un 5% dentro de Google Play), estando el foco principal en Bitcoin. Además, han crecido un 60% los **troyanos bancarios**, como Android/Marcher, que suplantaba a otras apps legítimas. Los troyanos bancarios, como FakeToken, han tenido como objetivo no sólo instituciones financieras, sino otros servicios de pago, como reserva de taxis, transporte, hoteles, entradas, etc.

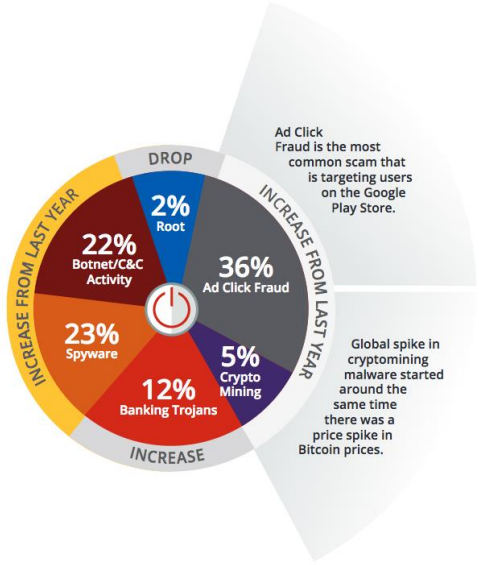


Figure 1. Chart: A breakdown of last year's campaigns vs. threats targeting Google Play in 2016. We have seen growth in several threat vector categories.

Figura 9-5.

Se estima que las campañas de malware móvil actuales centradas en el fraude en anuncios, pago por descargas o troyanos bancarios pueden proporcionar a sus autores unos ingresos de entre uno y dos millones de dólares, pudiendo incrementarse

estas cifras en un par de años (2020) si la tendencia del impacto y propagación de estos especímenes de malware continúa evolucionando según la progresión actual. Sin duda, la existencia de cinco billones[26] de usuarios de dispositivos móviles a nivel mundial en 2017 constituye un mercado potencial muy suculento.

Entre enero y septiembre de 2017 se han identificado, por parte de Sophos, 32 amenazas relevantes en Google Play (Figura 9-6.), duplicando los números para el mismo periodo del año anterior. Cabe destacar que el **malware Judy** infectó a 36,5 millones de usuarios entre mayo y septiembre; que el malware **Xavir(Ad)** había infectado a más de 800 apps de Android; y que **WireX**, potencialmente la botnet de DDOS de mayor tamaño en Android hasta el momento, había infectado 140.000 dispositivos en 100 países en agosto de 2017.

WireX obtiene sus objetivos dinámicamente mediante una conexión web, empleando una WebView en Android. Haciendo uso de 50 hilos (o *threads*) simultáneos, lanza ataques de DDoS enviando 512 bytes 10 millones de veces por cada hilo (generando varios Gbytes). Curiosamente, versiones previas de WireX no disponían de capacidades DDoS, estas fueron añadidas a finales de julio, sino que su objetivo era el fraude en anuncios.

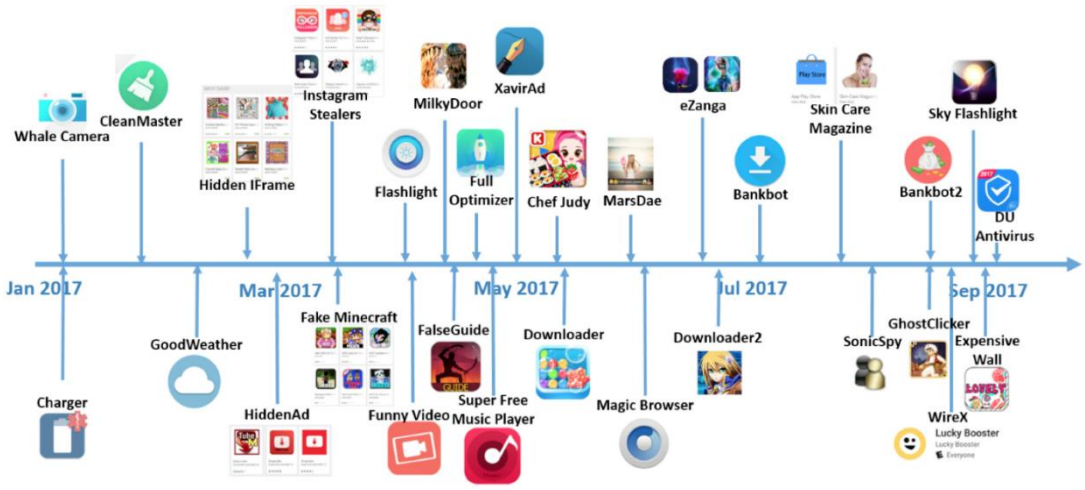


Figura 9-6.

Uno de los casos más significativos de distribución de malware en 2017 a través de Google Play fue **Lipizzan**, un spyware que solo infectó a 100 dispositivos a través de unas 20 apps diferentes. Su reducido volumen se debe a que estaba focalizada en un ataque muy dirigido, con referencias a una compañía de ciberarmas que trabaja para

[26] Todas las referencias a billones hacen mención a billones americanos, es decir, miles de millones.

gobiernos y agencias de inteligencia, entre otros clientes. En Google Play estas apps aparecían como benignas para copias de seguridad, limpieza del dispositivo móvil o para tomar notas, pero realmente disponían de múltiples capacidades para monitorizar al usuario víctima y exfiltrar sus datos, tanto del propio dispositivo como de apps de terceros.

Entre estas capacidades se encontraba la posibilidad de grabar llamadas de teléfono, capturar la pantalla del dispositivo, tomar control del micrófono (convirtiéndose en un bug de escucha), obtener la localización del usuario, el registro de SMS y llamadas, extraer los datos multimedia y de apps de terceros como Gmail, Hangouts, LinkedIn, Messenger, Skype, Snapchat, Telegram, Viber, WhatsApp, etc. La app hacía uso de cifrado mediante AES para el despliegue y carga del código con sus capacidades adicionales, así como de técnicas anti-depuración y anti-emulador, para dificultar las tareas de análisis e ingeniería inversa sobre la misma.

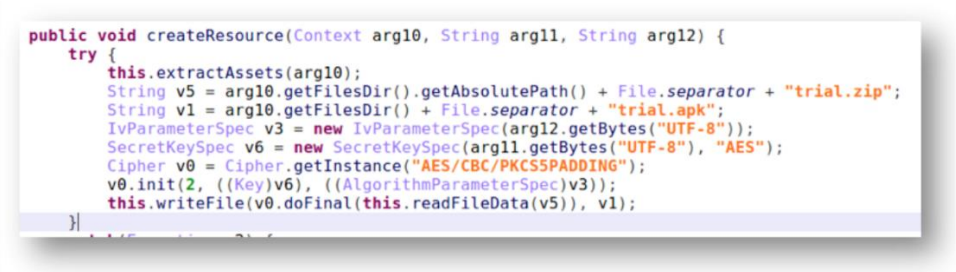


Figura 9-7.

Una vez descubierta, Google bloqueó las cuentas de los desarrolladores asociados y eliminó las apps tanto de Google Play como de los dispositivos móviles infectados mediante Google Play Protect –una capacidad ya conocida y ejercitada por Google en el pasado en casos críticos de infección por malware –. En abril de 2017, Google también bloqueó otro spyware dirigido, conocido como **Chrysaor**[27], con un número reducido de infecciones, menos de 36, en países muy concretos (Figura 9-8.) y asociado a NSO Group. Además, parecía estar vinculado al spyware Pegasus dirigido contra dispositivos móviles iOS en agosto de 2016, ya descrito en el informe del pasado año.

Adicionalmente a la exfiltración de datos propia de cualquier Spyware, Chrysaor intentaba elevar privilegios para tomar control completo del dispositivo móvil obteniendo acceso como root mediante el exploit Framaroot. Las actividades de lucha contra el malware móvil dirigido, llevadas a cabo por Google a través de sus servicios,

[27] https://android-developers.googleblog.com/2017/07/from-chrysaor-to-lipizzan-blocking-new.html

centradas en Chrysaor fueron detalladas en una presentación durante la conferencia BlackHat USA 2017.La investigación de Chrysaor permitió la identificación de Lipizzan.

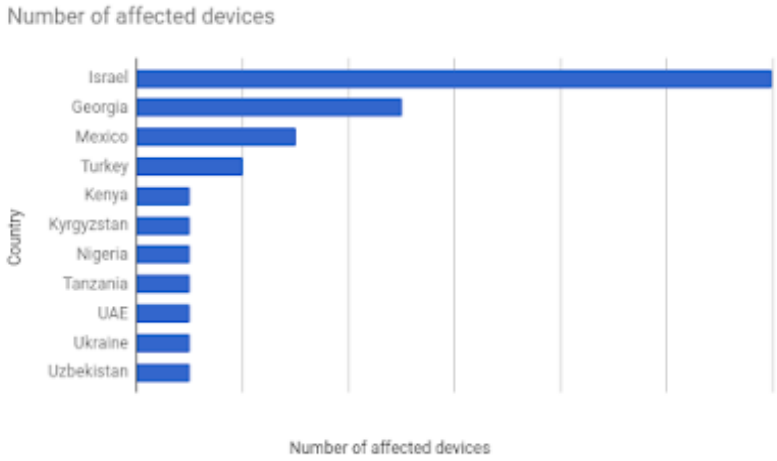


Figura 9-8.

Las recomendaciones de Google para evitar ser víctima de estos ataques, o cualquier otro malware móvil en general, pasan por **instalar apps sólo de fuentes de confianza** como Google Play, disponer de un código de acceso robusto, mantener el dispositivo móvil actualizado, habilitar Verify Apps y disponer de la capacidad de localizar el dispositivo móvil a través del Android Device Manager (ambas capacidades englobadas dentro de Google Play Protect)[28]. Estas sugerencias están alineadas con las recomendaciones de buenas prácticas y el decálogo de seguridad, recogidos por el CCN-CERT a través del **"Informe CCN-CERT BP-03/16 Buenas Prácticas en Dispositivo móviles",** publicado en octubre de 2016. (Figura 9-9.)

[28] https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html

	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.

Figura 9-9.

Durante 2018 se han identificado campañas que combinan el **fraude en anuncios por pulsaciones o *clicks***, una industria estimada actualmente en el rango del billón de dólares con el minado de criptomonedas, con el objetivo de proporcionar el mayor beneficio económico a los atacantes. Otras campañas de malware móvil, cuyo objetivo también son las criptomonedas, no se centran en el minado, sino en la distribución de monederos virtuales falsos para móviles, o en el robo de carteras de criptomonedas, tanto a usuarios finales como a instituciones financieras.

Esta tendencia se mantiene en 2018, dónde se han identificado apps, que lógicamente se distribuyen fuera de Google Play, cuyo propósito parece ser "hackear" o **manipular el comportamiento de otras apps** para obtener algo gratuitamente, aunque en realidad "hackean" al usuario víctima con capacidades para minar criptomonedas. Un

ejemplo es la app **"Lyft Hack"** (Figura 9-10.), centrada en el servicio de transporte entre particulares de Lyft, que una vez instalada y ejecutada, anima al usuario a instalar otras apps para desbloquear los contenidos *premium*. Como resultado, la nueva app no tiene asociado ningún icono y su único propósito es ejecutar tareas vinculadas al minado de criptomonedas empleando los recursos del dispositivo móvil víctima, ya sea mediante código propio o empleando un minador en JavaScript para Monero.

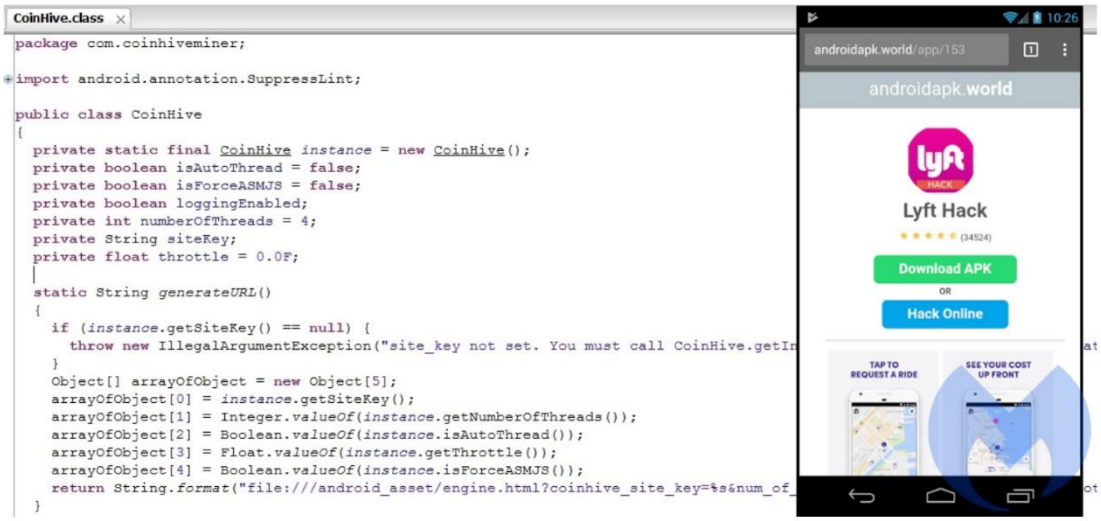


Figura 9-10.

En septiembre de 2017, Coinhive lanzó un nuevo servicio que proporcionaba una **API web para el minado de la criptomoneda Monero** (XMR) desde los navegadores web. Este servicio ha dado lugar a una explosión de herramientas o código de minado, muchas de ellas abusan de su funcionalidad para lanzar ataques dirigidos por el minado (o drive-by mining), en las que el visitante de una página web es forzado a minar una criptomoneda sin su aprobación y/o conocimiento.

Una de las campañas de este tipo, orientada a usuarios de Android que comenzó en noviembre de 2017 y seguía presente en enero de 2018, dirigió a millones de usuarios a páginas web que realizaban tareas de minado de Monero. Curiosamente, se presentaba un CAPTCHA al usuario para que confirmase que se trataba de un humano y no de un bot o herramienta automatizada y, mientras tanto y hasta que no se introducía el código, el dispositivo estaba minando la criptomoneda. (Figura 9-11.)

Los análisis llevados a cabo parecen confirmar que los usuarios de Android eran redirigidos a dichas páginas web no sólo a través del navegador web (por ejemplo, Chrome), sino también a través de apps gratuitas infectadas con módulos de anuncios maliciosos. Posteriormente se identificaron diferentes dominios que hacían uso de la

misma página web de validación de CAPTCHA (o plantilla), pero que minaban la criptomoneda Monero para diferentes claves o direcciones de Coinhive.

Las estadísticas de únicamente dos de los dominios más activos de esta campaña permiten hacerse una idea de su alcance, con unas 800.000 visitas diarias combinadas, y con una media de cuatro minutos en la página de minado por visita. Se estima, de manera conservadora, que los procesadores ARM estándar podrían minar unos 10 hashes por segundo, por lo que en base a todas las cifras previas (número de visitas, tiempo por visita, y capacidad de procesamiento), los ingresos por este tipo de actividades todavía son reducidos −de sólo unos miles de dólares al mes−. Esta tendencia muy posiblemente cambiará en los próximos años, siendo este tipo de ataques mucho más prevalentes y de mayor alcance.

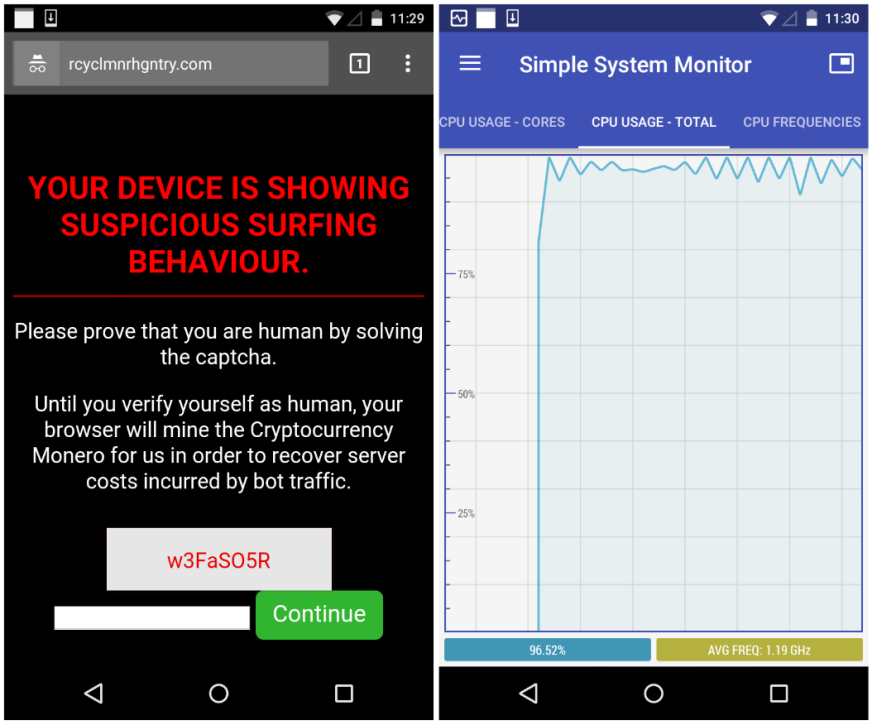


Figura 9-11.

Adicionalmente, las capacidades asociadas a ataques de ransomware por parte del malware móvil sigue en aumento en 2017. El crecimiento del ransomware se ha visto potenciado por un nuevo modelo de negocio, conocido como **RaaS (Ransomware as a Service)**, y asociado a la propagación de kits de explotación.

Por ejemplo, el malware para Android LokiBot extiende las capacidades de Marcher con funcionalidad de ransomware mediante el cifrado de ficheros y el bloqueo del dispositivo móvil. Este espécimen tenía como objetivo más de 100 instituciones financieras a nivel mundial, y se estima que ha generado unos beneficios estimados de dos millones de dólares sólo mediante la venta del kit de explotación asociado en la "dark web". Asimismo, intenta condicionar a los usuarios a que hagan uso de sus apps

de banca móvil, y dispone de capacidades para suplantar la dirección IP del dispositivo víctima para realizar otras acciones fraudulentas.

Una muestra de malware para Android, que se hace pasar por una app para la lectura de la bíblica coreana, y que tenía como objetivo usuarios de Corea del Sur con el fin de incorporar los dispositivos infectados a una botnet, se cree que ha sido la primera muestra de la incursión del grupo de cibercrimen Lazarus en el ecosistema móvil. Este grupo está asociado a Corea del Norte es conocido por sus actividades dentro del malware tradicional, como por ejemplo WannaCry, que impactó a la industria en la primera mitad de 2017.

El incremento de ransomware, también en entornos móviles, ha destacado a finales de 2017, dónde más del 30% del malware identificado por Sophos en el mes de septiembre era ransomware, como por ejemplo malware oculto en versiones falsas del popular juego chino King of Glory[29] (Figura 9-12.). La pantalla de aviso de la infección al usuario era muy similar a la de WannaCry, haciendo creer a las víctimas que habían sido infectadas por éste. Para la obtención de los pagos, el malware empleaba los medios de pago de Wechat, Alipay y QQ.

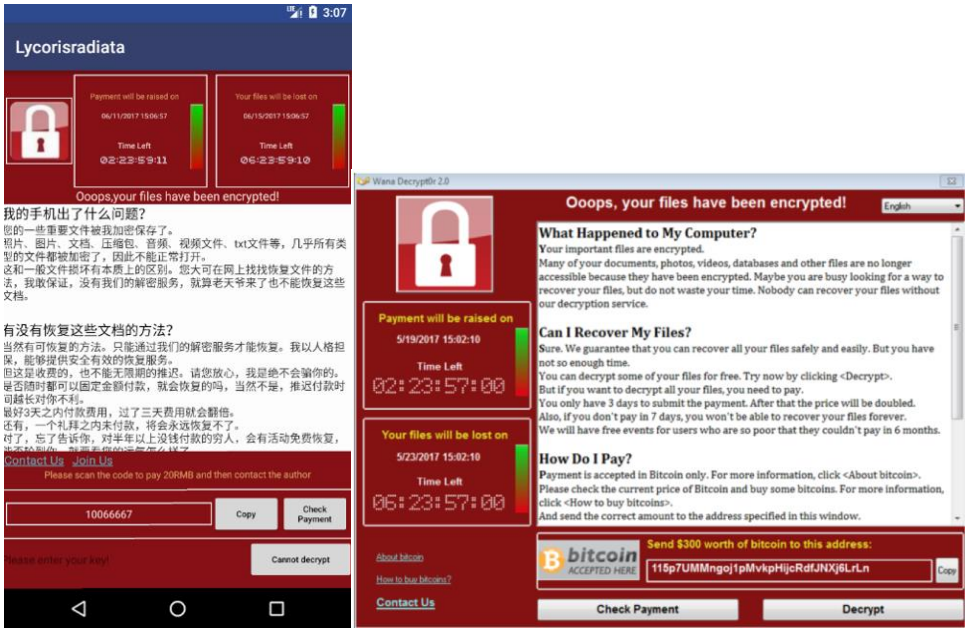


Figura 9-12.

También durante la primera mitad de 2017 se identificó una actividad notable del ransomware móvil debido a una familia conocida como **Congur**, centrada en el bloqueo de la pantalla de acceso del dispositivo móvil, que totalizó el 83% de instalaciones de este tipo a lo largo de todo el año según Kaspersky.(Figura 9- 13.)

[29] https://nakedsecurity.sophos.com/2017/06/09/android-ransomware-hides-in-fake-king-of-glory-game/

Figura 9-13.

Las dos técnicas empleadas por el ransomware en Android no han cambiado respecto a años previos, debido a que son simples pero efectivas: **bloqueo de la pantalla de acceso al dispositivo móvil** o **cifrado de los datos del usuario**. La primera de ellas suele cambiar el código de acceso (o PIN), no pudiendo el usuario hacer uso de su dispositivo móvil, aunque en algunos casos el malware emplea siempre el mismo valor de PIN que, una vez obtenido, permite desbloquear todos los dispositivos infectados sin pagar el rescate. La segunda técnica, empleada por ejemplo por Svpeng y Faketoken, cifra los ficheros del usuario existentes en el almacenamiento compartido −como por ejemplo fotografías y documentos descargados−, debido al modelo de permisos de Android.

Dada la extensa fragmentación de Android en el ecosistema actual, donde muchos dispositivos móviles no reciben las últimas actualizaciones de seguridad y, por tanto están expuestos a vulnerabilidades conocidas públicamente, a lo largo de 2017 se ha popularizado el malware móvil que intenta aprovecharse de esta situación y explotar las vulnerabilidades existentes.

Se estima que casi la mitad del malware móvil, recogido en el Top 20 de Kaspersky, dispone de estas capacidades. Además, han aumentado significativamente los ejemplares de malware móvil que disponen de **exploits para intentar *rootear*** el dispositivo víctima y tomar control completo del mismo, pudiendo llevar a cabo cualquier acción posteriormente. **Ztorg**[30] fue distribuido en casi 100 apps a través de Google Play, algunas de ellas descargadas más de un millón de veces, intentan lograr la persistencia, y la infección permanece incluso tras restaurar el dispositivo a fábrica. Otro ejemplo es Dvmap, que inyecta su código malicioso en las librerías del sistema y también fue distribuido a través de Google Play, con más de 50 mil descargas.

[30] https://securelist.com/ztorg-money-for-infecting-your-smartphone/78325/

En contradicción, el número de víctimas afectadas por este tipo de malware ha disminuido respecto al pasado año, especialmente al disminuir el número de dispositivos móviles con una versión significativamente antigua de Android, como Android 5.0 o inferior. Sin embargo, se debe tener en cuenta, tal como se detallaba inicialmente, que todavía a mediados de 2017 un 35% de usuarios hacían uso de Android 5.x.

Igualmente, durante 2017 se identificó un incremento del malware móvil focalizado en la obtención de beneficios a través de **pulsaciones en suscripciones WAP**, normalmente combinado con fraude en anuncios por pulsaciones o *clicks*, o con el envío de mensajes SMS a servicios *premium*. Las suscripciones WAP (o WAP billing) son un sistema de pago móvil que imputa los cargos directamente en la factura de telefonía móvil del usuario, asociada a su contrato de la tarjeta SIM y del servicio de telefonía con el operador de telecomunicaciones. Las páginas de facturación mediante WAP normalmente redirigen al usuario a un servicio del operador para que el usuario confirme que desea pagar por el servicio, pulsando en un botón o enlace para aceptar el cargo.

Este tipo de malware, como por ejemplo Ubsod o Autosus, está diseñado para aceptar el pago por estos servicios suplantando al usuario mediante código JavaScript específico. Algunas muestras incluso eliminan los mensajes SMS indicativos de los gastos asociados. Para asegurar su éxito, el malware deshabilita el interfaz Wi-Fi y activa el interfaz de datos de telefonía móvil, ya que este es el mecanismo de comunicación empleado por WAP para identificar al usuario y poder proceder al pago.

Algunas variantes de este tipo de malware, como Xafekopy, distribuido como app para la optimización de la batería, tienen similitudes con otras familias de malware, como Ztorg, ambos potencialmente creados por autores chinos y con la India y Rusia como principales objetivos. En julio de 2017 se identificaron más de 5.000 víctimas de 48 países diferentes.

Un ejemplo de malware móvil que aprovechaba las debilidades proporcionadas por los servicios de accesibilidad en Android, previamente descritas, fue **Svpeng**. El informe del pasado año profundizaba en esta familia de malware, asociada inicialmente al ransomware y que en 2016 se centraba en el sector financiero como troyano bancario.

En julio de 2017, se identificaron variantes de Svpeng que hacían uso de los servicios de accesibilidad para auto-otorgarse múltiples permisos que les permitiesen llevar a cabo las acciones deseadas en la plataforma Android, como el envío o recepción de SMSs, la realización de llamadas, o la lectura de los contactos. Asimismo, el malware se añadía a los administradores del dispositivo simulando ser Adobe Flash Player para evitar su desinstalación.

Otras variantes de Svpeng identificadas en agosto de 2017 volvían a sus orígenes y ejecutaban ataques de ransomware, bloqueando el acceso al dispositivo móvil, cifrando los ficheros y solicitando un rescate al usuario en Bitcoins. (Figura 9-14.)

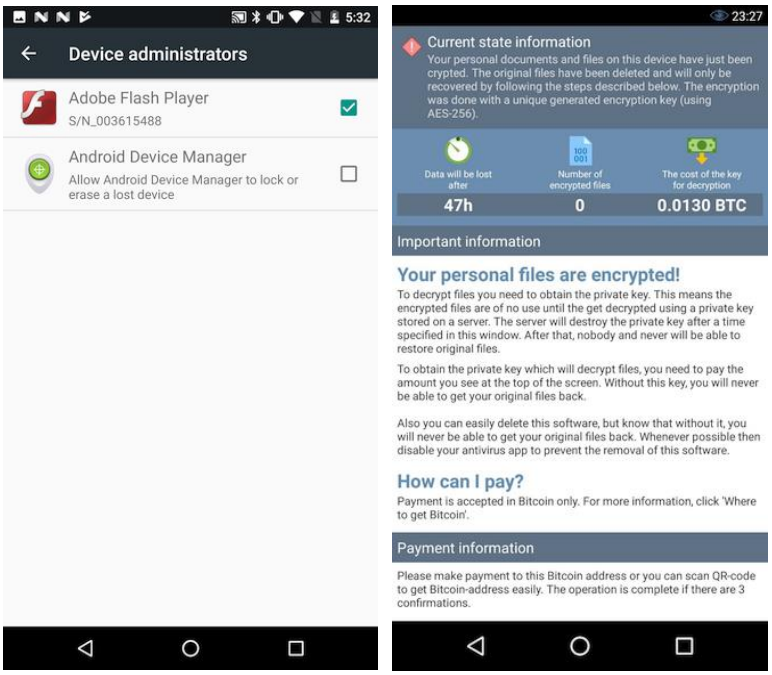


Figura 9-14.

9. COMUNICACIONES MÓVILES

El año 2017 ha estado marcado por vulnerabilidades de seguridad muy relevantes que han impactado a los dispositivos y entornos móviles. Entre estas, cabe destacar especialmente BlueBorne (Figura 10-1.), asociada a las tecnologías Bluetooth; y KRACK (Figura 10-2.), asociada a las tecnologías Wi-Fi. Curiosamente estas dos vulnerabilidades coincidieron casi en el tiempo con un cambio significativo en el comportamiento de los dispositivos móviles de Apple, que se introdujo en iOS11 a la hora de gestionar los interfaces Bluetooth y Wi-Fi desde los ajustes del centro de control, dónde realmente los interfaces inalámbricos no son deshabilitados completamente[31].

[31] https://motherboard.vice.com/en_us/article/evpz7a/turn-off-wi-fi-and-bluetooth-apple-ios-11

Figura 10-1.

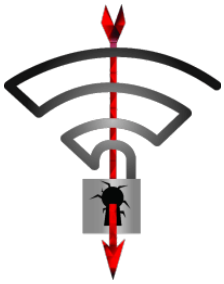


Figura 10-2.

La **vulnerabilidad BlueBorne** es en realidad un conjunto inicial de ocho vulnerabilidades −más otras identificadas posteriormente que afectaban a dispositivos IoT, algunos basados también en Android como variantes del Amazon Echo o Google Home−, que incluía múltiples debilidades en la pila de comunicaciones Bluetooth de numerosos sistemas operativos y dispositivos, incluyendo iOS y Android. Dentro de estas vulnerabilidades se englobaban la posibilidad de ejecutar ataques de interceptación de tráfico (o MitM, Man-in-the-Middle), la capacidad de revelar los contenidos de la memoria del dispositivo víctima, o incluso la ejecución remota de código. Algunas semanas después de la publicación inicial se disponía de pruebas de concepto que permitían explotar con éxito las más críticas de estas vulnerabilidades y ejecutar código de manera remota en los dispositivos móviles vulnerables como, por ejemplo, Android 7.1.2 sin las actualizaciones de seguridad de septiembre de 2017 (o posteriores).

El principal problema con este tipo de vulnerabilidades, Blueborne o KRACK, es que en los próximos años aún habrá en funcionamiento numerosos dispositivos vulnerables, que nunca recibirán actualizaciones para mitigar el impacto y riesgo de las mismas.

La **vulnerabilidad KRACK** es en realidad un conjunto de 10 vulnerabilidades, que afectó a los mecanismos de seguridad más robustos existentes para las redes Wi-Fi, WPA(2), tanto en su versión personal (PSK) como empresarial (Enterprise). Como consecuencia se vieron afectados tanto puntos de acceso Wi-Fi como clientes Wi-Fi, incluyendo dispositivos móviles como iOS o, especialmente, Android 6.0 o versiones posteriores, que podían llegar a reinstalar una clave con valor cero.

Lo más paradójico de la vulnerabilidad KRACK es que el intercambio en cuatro pasos o mensajes de WPA(2) para la negociación de una nueva sesión había sido matemáticamente probado. Sin embargo, el alcance o ámbito de dicho análisis formal se centraba en verificar que la clave negociada permanecía en secreto y que no se podían manipular los mensajes, pues no contemplaba aspectos, que posteriormente dieron lugar a la vulnerabilidad, como saber si la clave era instalada sólo una vez.

Como consecuencia indirecta de esta vulnerabilidad, a lo largo de 2018, la Wi-Fi Alliance planea publicar una nueva especificación de seguridad Wi-Fi, denominada WPA3, que introduce nuevas mejoras de seguridad en los protocolos para diferentes escenarios de uso.

Desde el punto de vista de las tecnologías de comunicaciones móviles, asociadas a los operadores de telecomunicaciones**, se estima que la adopción de 5G comenzará a finales de 2018**, al menos en forma de pilotos en algunas regiones, como USA o Korea del Sur, mostrando una progresión mucho más acelerada que la de tecnologías pasadas, como 4G. **El uso de 5G extenderá los riesgos actuales de seguridad y privacidad** asociados a las comunicaciones móviles, debido a que ampliará su ámbito de actuación a muchos más escenarios y dispositivos asociados al Internet de las Cosas (IoT) o a los coches conectados, y gestionará mayores volúmenes de datos. Estos riesgos también aumentan debido a que los operadores de telecomunicaciones cada vez permiten la interconexión de más entidades o terceros a sus redes, pudiendo estos identificar u obtener datos privados de los usuarios.

Sin embargo, **la tecnología 5G podría proporcionar mecanismos de seguridad** frente a ciertas amenazas conocidas, como por ejemplo el uso de estaciones base falsas, como *IMSI catchers* o *stingrays* empleadas para la identificación, obtención de la ubicación, seguimiento, monitorización y captura del tráfico de dispositivos móviles y usuarios víctima.

Las propuestas de seguridad[32], qué están siendo evaluadas actualmente por el 3GPP para la estandarización final de 5G en el año 2019, podrían evitar este tipo de amenazas mediante el uso de un Subscription Permanent Identifier (SUPI, identificador único compuesto por el IMSI y potencialmente por el identificador de la red o NAI), que sería cifrado con la clave pública del operador, para no enviar el IMSI en claro por el aire, existiendo además un proceso de autentificación para que el dispositivo pueda verificar que la red móvil es legítima. Estas capacidades ya existen en 4G, pero el objetivo es que en 5G se aumente la protección de los datos intercambiados por el aire, por ejemplo, mediante el uso de un Subscription Concealed Identifier (SUCI, versión cifrada del SUPI), y además evitando que la red pueda forzar el uso de un cifrado nulo, es decir, hacer uso de comunicaciones sin cifrar. La nueva vulnerabilidad de las librerías (CoreText), que gestionan los contenidos del interfaz de usuario de los dispositivos móviles iOS, no está directamente asociada a una vulnerabilidad en las comunicaciones, pero sí realizaba a través de estas su distribución y explotación. De nuevo, y de manera similar a la vulnerabilidad que se explotó en el año 2013 mediante la utilización de caracteres

[32]https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionUid=SP-180056 & https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045

árabes Unicode, en el mes de febrero de 2018 se descubrió una nueva vulnerabilidad explotable remotamente mediante un carácter Unicode en el lenguaje indú Telugu.

Los dispositivos móviles con iOS 11 (anteriores a la versión 11.2.6) sufrían una denegación de servicio al recibir dicho carácter e intentar mostrarlo en pantalla sin éxito (Figura 10-3.) Este tipo de vulnerabilidades puede ser explotada a través de múltiples vectores de ataque, incluyendo comunicaciones inalámbricas Bluetooth o Wi-Fi, al intentar mostrar el nombre del dispositivo Bluetooth o de la red Wi-Fi maliciosos; o a través de contenido distribuido mediante páginas web, e-mails, redes sociales, SMS, o las múltiples apps de mensajería existentes.

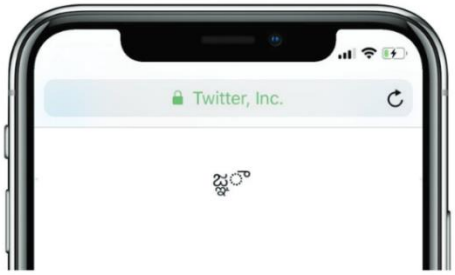


Figura 10-3.

ANEXO A. REFERENCIAS

[Ref.- 1]	**"Smartphone OS Market Share, 2017 Q4". IDC. 2017.** http://www.idc.com/promo/smartphone-market-share/os
[Ref.- 2]	**"Smartphones Hit Pivotal Stage as Worldwide Shipment Volumes Decline 0.5% in 2017, But Return to Growth is Expected, According to IDC". IDC. 27** Febrero de 2018. https://www.idc.com/getdoc.jsp?containerId=prUS43591418
[Ref.- 3]	**"Smartphone Vendor Market Share, 2017 Q4". IDC. 2017.** https://www.idc.com/promo/smartphone-market-share/vendor
[Ref.- 4]	**"Cumulative number of apps downloaded from the Apple App Store from July 2008 to June 2017 (in billions)". Statista.** Abril de 2018. 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 March 2017". Statista.** Abril 2018. https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/
[Ref.- 6]	**"Android vs. iOS. Smartphone OS sales market share evolution". Kantar Worldpanel.** https://www.kantarworldpanel.com/global/smartphone-os-market-share/
[Ref.- 7]	**"Android Dashboards. Platform Versions". Android Developers.** https://developer.android.com/about/dashboards/index.html
[Ref.- 8]	**"Support – App Store". Apple Developer.** https://developer.apple.com/support/app-store/
[Ref.- 9]	**"Google Play Protect". Google.** https://www.android.com/play-protect/
[Ref.- 10]	**"Mobile Threat Report. The Next 10 Years". McAfee Labs (Intel). 2018**. https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2018.pdf
[Ref.- 11]	"**Double Stuffed Security in Android Oreo". Android Developers Blog.** Diciembre de 2017. https://android-developers.googleblog.com/2017/12/double-stuffed-security-in-android-oreo.html
[Ref.- 12]	**"Android Oreo (Go edition)". Google.** https://www.android.com/versions/oreo-8-0/go-edition/ https://www.androidpit.com/what-is-android-go
[Ref.- 13]	**"About Face ID advanced technology". Apple.**https://support.apple.com/en-us/HT208108
[Ref.- 14]	**"Bypassing iOS Lock Screens: A Comprehensive Arsenal of Vulns". DinoSec**. Abril de 2018. http://blog.dinosec.com/2014/09/bypassing-ios-lock-screens.html
[Ref.- 15]	**"Informe de Amenazas CCN-CERT IA-06/17: Dispositivos y Comunicaciones Móviles Informe Resumen 2016". CCN-CERT.** Abril 2017. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2215-ccn-cert-ia-06-17-dispositivos-y-comunicaciones-moviles-informe-resumen-2016-1.html
[Ref.- 16]	**"Treble". Google.** https://source.android.com/devices/architecture/treble https://android-developers.googleblog.com/2017/05/here-comes-treble-modular-base-for.html
[Ref.- 17]	**"Improving app security and performance on Google Play for years to come". Android Developers Blog. Dec 2017.** https://android-developers.googleblog.com/2017/12/improving-app-security-and-performance.html
[Ref.- 18]	"**Bkav's new mask beats Face ID in "twin way": Severity level raised, do not use Face ID in business transactions". Bkav**. Noviembre de 2017. http://www.bkav.com/dt/top-news/-/view_content/content/103968/bkav%EF%BF%BDs-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions https://youtu.be/rhiSBc061JU

	https://www.wired.com/story/hackers-say-broke-face-id-security/
[Ref.- 19]	**"Informe de Amenazas CCN-CERT IA-03/14: Ciberamenazas 2013 y Tendencias 2014". CCN-CERT.** Octubre de 2014. https://www.ccn-cert.cni.es/publico/dmpublidocuments/CCN-CERT_IA-03-14-Ciberamenazas_2013_Tendencias_2014-publico.pdf
[Ref.- 20]	**"[In-Depth Look] Samsung's Biometric Technologies Bring Added Security and Convenience to the Galaxy S8". Samsung**. Marzo de 2017. https://news.samsung.com/global/in-depth-look-samsungs-biometric-technologies-bring-added-security-and-convenience-to-the-galaxy-s8
[Ref.- 21]	**"What are biometrics and biometric solutions?". Samsung Developers.** http://developer.samsung.com/tech-insights/pass/what-are-biometrics-and-biometric-solutions
[Ref.- 22]	**"Galaxy S8 bloqueo facial explicado". MarcianoTech.** Marzo de 2017. https://www.youtube.com/watch?v=S3rCOZNqYq0 https://arstechnica.com/gadgets/2017/03/video-shows-galaxy-s8-face-recognition-can-be-defeated-with-a-picture/
[Ref.- 23]	**"Chaos Computer Clubs breaks iris recognition system of the Samsung Galaxy S8". CCC.** Mayo 2017. https://www.ccc.de/en/updates/2017/iriden https://media.ccc.de/v/biometrie-s8-iris-en https://www.engadget.com/2017/05/23/galaxy-s8-iris-scanner-hacked/
[Ref.- 24]	"**Galaxy S8 Iris Scanner bypassed by glue". Bkav.** Junio de 2017. https://www.youtube.com/watch?v=Z9PumZZoOu4 http://www.bkav.com/top-news
[Ref.- 25]	**"[In-Depth Look #3] How Samsung Streamlined the Galaxy S9's Security Features". Samsung.** Febrero de 2018. https://news.samsung.com/global/in-depth-look-3-how-samsung-streamlined-the-galaxy-s9s-security-features
[Ref.- 26]	"**Real Time Authentication Based On Blood Flow Parameters". WIPO** Enero de 2018 https://patentscope.wipo.int https://www.androidpit.com/samsung-biometry-unlock-intelligent-scan-blood-flow
[Ref.- 27]	**"TensorFlow Lite". Google.** https://www.tensorflow.org/mobile/tflite/
[Ref.- 28]	**"Machine Learning aplicado a ciberseguridad". Alfonso Muñoz. OWASP Madrid.** Diciembre 2017. https://www.slideshare.net/owaspmadrid/machine-learning-aplicado-a-ciberseguridad-limitaciones-y-seguridad-ofensiva https://www.youtube.com/watch?v=ItC7mKm2d5g
[Ref.- 29]	**"My Take on FBI's "Alternative" Method". Jonathan Zdziarski.** Marzo de 2016. https://www.zdziarski.com/blog/?p=5966 https://www.zdziarski.com/blog/?p=6015 https://www.zdziarski.com/blog/?p=6020 https://www.youtube.com/watch?v=HG7JlDDX_RM
[Ref.- 30]	**"The Feds Can Now (Probably) Unlock Every iPhone Model In Existence -- UPDATED ". Forbes**. Febrero de 2018. https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite
[Ref.- 31]	**"GrayKey iPhone unlocker poses serious security concerns". Malware Bytes Labs.** Marzo de 2018. https://blog.malwarebytes.com/security-world/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns/ https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/ https://graykey.grayshift.com
[Ref.- 32]	**"New Security Measures in iOS 11 and Their Forensic Implications". Elcomsoft.** Septiembre de 2017.

	https://blog.elcomsoft.com/2017/09/new-security-measures-in-ios-11-and-their-forensic-implications/
[Ref.- 33]	**"iOS 11 Horror Story: the Rise and Fall of iOS Security". Elcomsoft.** Noviembre de 2017. https://blog.elcomsoft.com/2017/11/ios-11-horror-story-the-rise-and-fall-of-ios-security/ https://support.apple.com/en-us/HT205220
[Ref.- 34]	**"Gatekeeper Password Storage: How Android Secures Devices". Magnet Forensics**. Abril de 2017. https://www.magnetforensics.com/blog/gatekeeper-password-storage-android-secures-devices/
[Ref.- 35]	**"Cloak & Dagger".** Mayo de 2017. http://cloak-and-dagger.org
[Ref.- 36]	**"Making it safer to get apps on Android O". Android Developes Blog.** Agosto 2017. https://android-developers.googleblog.com/2017/08/making-it-safer-to-get-apps-on-android-o.html
[Ref.- 37]	**"Android Instant Apps is open to all developers. Start building today!". Android Developers Blog.** Mayo 2017. https://android-developers.googleblog.com/2017/05/android-instant-apps-is-open-to-all.html
[Ref.- 38]	**"Lipizzan spyware linked to cyberarms firm plunders SMS, logs and photos". Sophos.** Julio 2017. https://nakedsecurity.sophos.com/2017/07/28/lipizzan-spyware-linked-to-cyberarms-firm-plunders-sms-logs-and-photos/
[Ref.- 39]	**"From Chrysaor to Lipizzan: Blocking a new targeted spyware family". Android Developers Blog.** Julio 2017. https://android-developers.googleblog.com/2017/07/from-chrysaor-to-lipizzan-blocking-new.html
[Ref.- 40]	**"Fighting Targeted Malware In The Mobile Ecosystem". BlackHat USA 2017. Google & Lookout.** Jul 2017. https://www.blackhat.com/docs/us-17/wednesday/us-17-Ruthven-Fighting-Targeted-Malware-In-The-Mobile-Ecosystem.pdf
[Ref.- 41]	**"Bogus hack apps hack users back for cryptocash". Malwarebytes Labs.** Febrero de 2018. https://blog.malwarebytes.com/cybercrime/2018/02/bogus-hack-apps-hack-users-back-for-cryptocash/
[Ref.- 42]	**"Informe CCN-CERT BP-03/16: Buenas Prácticas en Dispositivo móviles". CCN-CERT.** Octubre de 2016. https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4058-como-usar-nuestro-movil-de-forma-segura-y-evitar-ciberataques.html https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1757-ccn-cert-bp-03-16-dispositivos-moviles/file.html
[Ref.- 43]	**"The state of malicious cryptomining". Malwarebytes Labs.** Febrero de 2018. https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/
[Ref.- 44]	**"Drive-by cryptomining campaign targets millions of Android users". Malwarebytes Labs.** Febrero de 2018. https://blog.malwarebytes.com/threat-analysis/2018/02/drive-by-cryptomining-campaign-attracts-millions-of-android-users/
[Ref.- 45]	**"SophosLabs 2018 Malware Forecast". Sophos.** Noviembre de 2017 https://www.sophos.com/en-us/en-us/medialibrary/PDFs/technical-papers/malware-forecast-2018.pdf https://nakedsecurity.sophos.com/2017/11/07/2018-malware-forecast-the-onward-march-of-android-malware/
[Ref.- 46]	**"Mobile malware evolution 2017". Kaspersky.** Marzo de 2018. https://securelist.com/mobile-malware-review-2017/84139/

[Ref.- 47]	**"WAP-billing Trojan-Clickers on rise". Kaspersky**. Agosto de 2017. https://securelist.com/wap-billing-trojan-clickers-on-rise/81576/
[Ref.- 48]	**"A new era in mobile banking Trojans". Kaspersky**. Julio de 2017 https://securelist.com/a-new-era-in-mobile-banking-trojans/79198/
[Ref.- 49]	**"Blueborne". Armis.** Sep 2017. https://www.armis.com/blueborne/
[Ref.- 50]	**"KRACK (Key Reinstallation AttaCKs) Attacks". Mathy Vanhoef.** Octubre de 2017. https://www.krackattacks.com
[Ref.- 51]	**"Wi-Fi Alliance® introduces security enhancements". Wi-Fi Alliance.** Enero de 2018. https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements
[Ref.- 52]	**"Stingray spying: 5G will protect you against surveillance attacks, say standards-setters". ZDNet.** Marzo de 2018. https://www.zdnet.com/article/stingray-spying-5g-will-protect-you-against-surveillance-attacks-say-standards-setters/
[Ref.- 53]	**"Protecting 5G against IMSI catchers". Ericsson Research Blog.** Junio de 2017. https://www.ericsson.com/research-blog/protecting-5g-imsi-catchers/ https://www.surrey.ac.uk/sites/default/files/5GIC-SSG-Security-Overview-WhitePaper-2017-08-02.pdf
[Ref.- 54]	**"Apple Telugu exploitation (CVE-2018-4124)". Raul Siles. DinoSec.** Febrero de 2018. https://twitter.com/raulsiles/status/966339511717330944