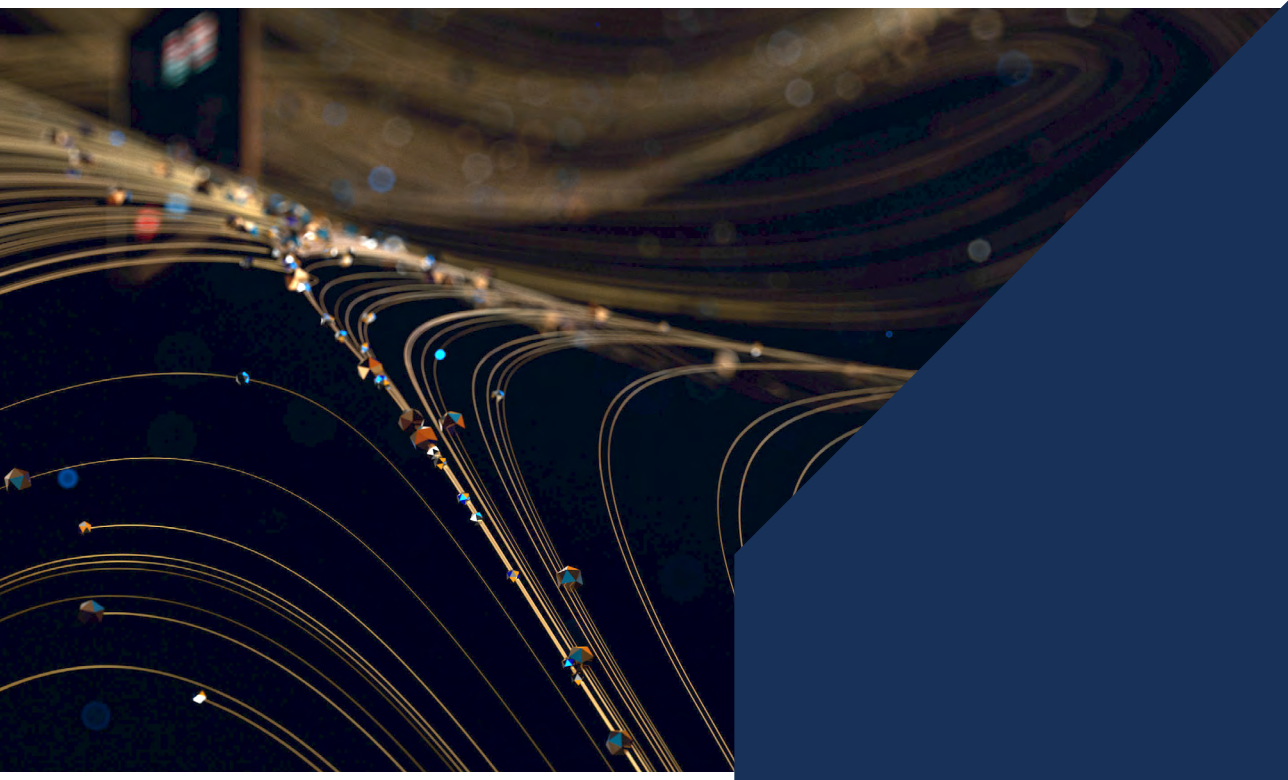
Informe Anual
2019

DISPOSITIVOS Y COMUNICACIONES MÓVILES

CCN-CERT IA-03/20

CENTRO
CRIPTOLÓGICO
NACIONAL

MARZO 2020



Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

Fecha de Edición: Febrero de 2020

Raúl Siles y Mónica Salas, Dino Security S.L., han participado en la elaboración y modificación del presente documento.

Índice

1. 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 a 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.

2. RESUMEN EJECUTIVO

La adopción de los dispositivos y comunicaciones móviles, tanto en el ámbito personal como profesional, ha alcanzado un nivel de madurez y estabilidad durante la última década 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 a los dispositivos móviles y a sus capacidades de comunicación inalámbricas, tanto en redes Wi-Fi y conexiones Bluetooth como en redes móviles celulares (2/3/4/5G), como uno de los objetivos principales de las ciberamenazas para el año 2020, consolidándose la tendencia de los últimos años.

El presente informe presenta algunas de las principales amenazas de seguridad y vulnerabilidades descubiertas a lo largo del año 2019 en los entornos de comunicaciones y dispositivos móviles, así como los avances y las tendencias más relevantes identificadas para este tipo de tecnologías para el año 2020.

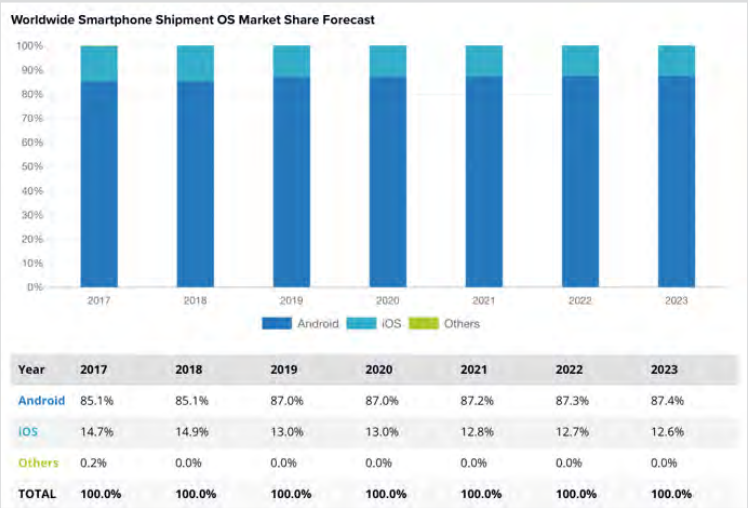
3. EVOLUCIÓN DEL MERCADO DE DISPOSITIVOS MÓVILES EN 2019

El año 2019 ha ratificado la disminución ya identificada en los dos años previos, 2017 y 2018, relativa al volumen de distribución y venta de dispositivos móviles por parte de todos los fabricantes a nivel global. En el segundo trimestre de 2019 (Q2 2019) el declive observado fue cercano al 2,7%, constituyéndose en el séptimo trimestre consecutivo en el que se reducen las ventas, con un total de 332 millones de unidades vendidas en un trimestre, frente a los 341 millones de unidades del año previo. La estimación de ventas totales en 2019 fue de 1.371 billones[1] de unidades [Ref.- 1] [Ref.- 2], según los estudios de IDC[2]. Se espera que haya un crecimiento en la segunda mitad de 2020 con la esperada llegada al mercado de nuevos terminales con soporte para 5G.

Algunos aspectos que han influido en este declive han sido las disputas por el mercado entre USA y China, con Huawei como principal fabricante afectado (analizados más en detalle posteriormente). Adicionalmente, se constituye como factor decisorio en la compra de dispositivos móviles su precio, lo que está abriendo la puerta a terminales de rango medio (el precio medio en 2019 rondó los $260). En esta gama media destacan los dispositivos que apuestas por Android One[3], garantizando nuevas versiones de Android y, especialmente, actualizaciones de seguridad durante 3 años.

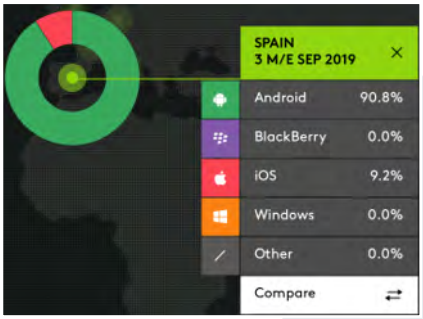
[1] Todas las referencias a billones en el presente informe corresponden a billones americanos, es decir, miles de millones de unidades.
[2] Datos obtenidos a finales de enero de 2020, sin las estadísticas consolidadas del último trimestre de 2019 (Q4 2019), pero teniendo en cuenta las estimaciones de previsiones para el global del año 2019 (posteriormente se facilitan los datos actualizados para Q3 2019, con un ligero cambio de tendencia).
[3] https://www.android.com/one/

La plataforma móvil Android mantiene la mayor cuota de mercado como líder indiscutible, ratificando los valores de años previos en torno al 87% de cuota de mercado global, con un ligero incremento asociado a las ventas de los primeros dispositivos con soporte para 5G en modo NSA (Non-Standalone), seguido por iOS con una cuota de un 13%. El resto de plataformas móviles existentes en el pasado, como Windows Phone o Blackberry, han desaparecido definitivamente del mercado. Por tanto, no hay novedades en la evolución de años previos, por lo que el presente informe se centra exclusivamente en las dos plataformas móviles relevantes a día de hoy, Android e iOS.



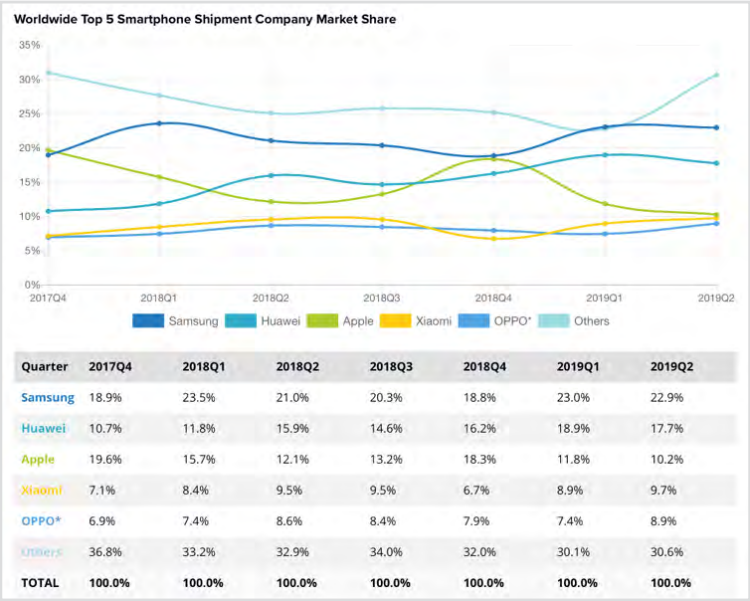
Year	2017	2018	2019	2020	2021	2022	2023
Android	85.1%	85.1%	87.0%	87.0%	87.2%	87.3%	87.4%
iOS	14.7%	14.9%	13.0%	13.0%	12.8%	12.7%	12.6%
Others	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
TOTAL	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Estas cifras globales se amplifican aún más con las estadísticas disponibles públicamente de manera específica para España, dónde en septiembre de 2019, la cuota de mercado de Android era de un 91% y la cuota de iOS de un 9% aproximadamente, desapareciendo toda presencia de cualquier otro sistema operativo móvil [Ref.- 3].

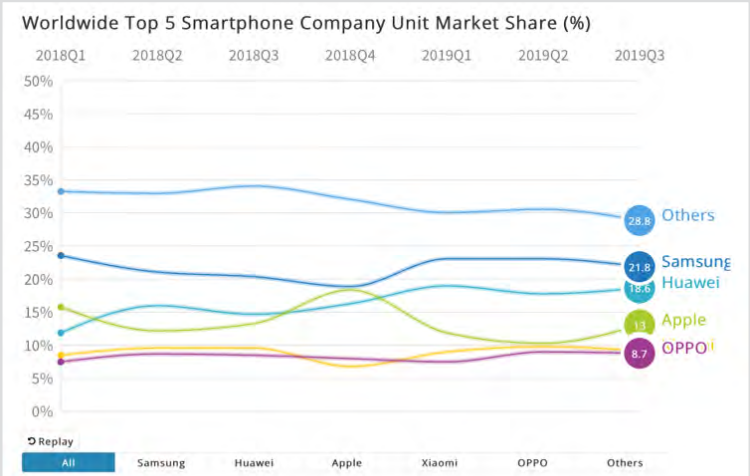


Pese al consolidado declive en el ritmo de adquisición de dispositivos móviles en la industria durante 2019, el crecimiento de ventas esperado por IDC para la segunda mitad de 2020 es más prometedor, con un ligero aumento entorno al 3,2% asociado a la demanda de terminales Android con soporte para las tecnologías de comunicación móvil 5G (ver apartado "11. Comunicaciones ") [Ref.- 1], quedando pendiente si Apple incorporará soporte para 5G en sus nuevos modelos de finales de 2020 (iPhone 12 y similares). Respecto a los fabricantes, cabe destacar que Samsung sigue liderando el mercado, con un 23% de cuota de mercado, y destaca como Huawei (pese a todas las tensiones comerciales y

controversias mediáticas entre China y USA del año 2019) sigue en el segundo puesto, con cifras cercanas al 17%, seguido de Apple con un 10% de cuota global (presentando una caída considerable del 18% respecto al año previo, debido al alto precio de sus últimos modelos de iPhone). Otros fabricantes de origen chino, como Xiaomi y Oppo, consolidan su cuarta y quinta posición, con una presencia relevante y creciente, y con cuotas de mercado medias del 10% y 9% respectivamente [Ref.- 2] (especialmente de Xiaomi en España[4], prácticamente igualando a Apple con un 18% de cuota de mercado, y de Oppo en China e India). Estos 5 fabricantes tienen una cuota conjunta del 70% del mercado.



Quarter	2017Q4	2018Q1	2018Q2	2018Q3	2018Q4	2019Q1	2019Q2
Samsung	18.9%	23.5%	21.0%	20.3%	18.8%	23.0%	22.9%
Huawei	10.7%	11.8%	15.9%	14.6%	16.2%	18.9%	17.7%
Apple	19.6%	15.7%	12.1%	13.2%	18.3%	11.8%	10.2%
Xiaomi	7.1%	8.4%	9.5%	9.5%	6.7%	8.9%	9.7%
OPPO*	6.9%	7.4%	8.6%	8.4%	7.9%	7.4%	8.9%
Others	36.8%	33.2%	32.9%	34.0%	32.0%	30.1%	30.6%
TOTAL	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%



Quarter	2018Q1	2018Q2	2018Q3	2018Q4	2019Q1	2019Q2	2019Q3
Samsung	23.5%	21.0%	20.3%	18.8%	23.0%	22.9%	21.8%
Huawei	11.8%	15.9%	14.6%	16.2%	18.9%	17.7%	18.6%
Apple	15.7%	12.1%	13.2%	18.3%	11.8%	10.2%	13.0%
Xiaomi	8.4%	9.5%	9.5%	6.7%	8.9%	9.7%	9.1%
OPPO*	7.4%	8.6%	8.4%	7.9%	7.4%	8.9%	8.7%
Others	33.2%	32.9%	34.0%	32.0%	30.1%	30.6%	28.8%
TOTAL	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Durante la fase final de elaboración del presente informe, IDC publicó los datos del tercer trimestre de 2019 [Ref.- 2], mostrando un ligero crecimiento global del 0.8% en la venta de dispositivos móviles, con un total de 358 millones de unidades vendidas en un trimestre, invirtiendo la tendencia a la baja de los últimos siete trimestres consecutivos. Respecto a la distribución de ventas entre los principales fabricantes, la tendencia previa se mantiene, destacando únicamente un ligero crecimiento de Apple (del 10% al 13%, detallado a continuación) frente a sus dos principales competidores, Samsung (que disminuye ligeramente, 1%, al igual que Xiaomi) y Huawei (que continua creciendo, 1%).

Las previsiones actualizadas a finales de enero de 2020 de cuota de mercado de IDC [Ref.- 1] para los diferentes sistemas operativos móviles no varían significativamente respecto a las cifras proporcionadas previamente, con una media para Android del 87% de cuota de mercado y de un 13% para iOS.

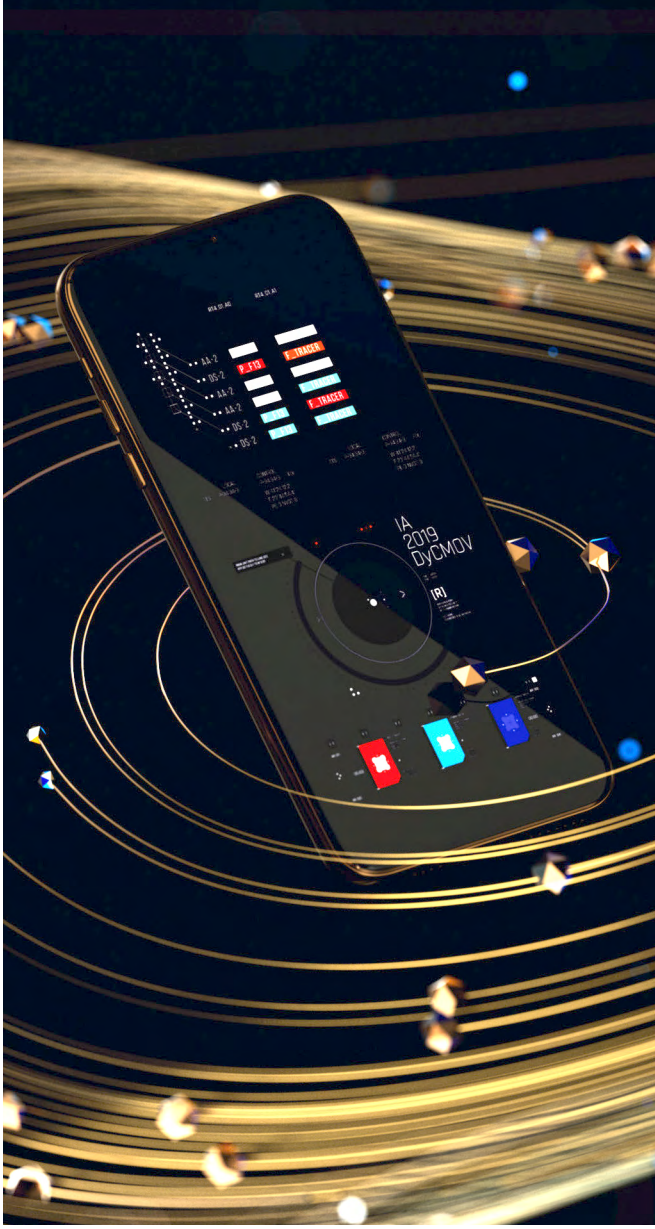
[4] http://gs.statcounter.com/vendor-market-share/mobile/spain

En contraposición a estos números y estimaciones, los resultados económicos publicados por Apple a finales de enero de 2020 ratifican un record histórico en ingresos en el primer trimestre de su año fiscal (último trimestre de 2019), con unas ventas trimestrales de casi 92 billones de dólares (un 9% de crecimiento respecto al pasado año), y unos beneficios netos de más de 22 billones (un 19% de crecimiento y también un record histórico), debido al éxito principalmente del iPhone 11 (y sus variantes), con más del 60% de ventas[5], de los Wearables (11%: Apple Watch, AirPods, etc.) y de sus servicios (14%) [Ref.- 14]. Estas cifras suponen la existencia de más de 1.500 millones de dispositivos Apple activos.

Dentro del año 2019 caben destacar las tensiones comerciales entre China y USA, que afectaron directamente a Huawei, tanto por su posición dominante en el tan ansiado control tecnológico de las ultra-valoradas futuras infraestructuras de las redes móviles 5G a nivel mundial, como por su relevante presencia en el ecosistema móvil, consolidado durante los últimos años como segundo fabricante de móviles, también a nivel mundial. De hecho, fue este último segmento el que fue utilizado como mecanismo de presión por parte del gobierno americano cuando Google anunció en mayo de 2019 [Ref.- 19] que suspendía todas sus operaciones comerciales y de negocios con Huawei, vetando el uso de los servicios de Google (incluyendo el mercado de Google Play y el resto de servicios: Gmail, YouTube, Maps, etc., que, por cierto, están prohibidos en China), vinculados muy estrechamente al sistema operativo Android, en los futuros dispositivos móviles de Huawei[6]. El impacto de esta noticia y el escándalo asociado tuvo repercusiones tremendas a nivel global, arrastrando a otras compañías americanas fabricantes de componentes hardware (como Intel, Qualcomm o Broadcom) a tampoco mantener sus negocios con el fabricante Chino.

Sin entrar en todas las connotaciones geopolíticas, vaivenes a nivel de negocio y consecuencias de este conflicto, incluidas las extensiones de EEUU de las prórrogas al veto[7] anunciadas a lo largo de todo el año 2019 (de 90 en 90 días, durante al menos 4 periodos hasta febrero de 2020), desde el punto de vista técnico, Huawei se vio avocada a anunciar en agosto de 2019 HarmonyOS [Ref.- 21], su nuevo sistema operativo para plataformas móviles (y muchos otros dispositivos inteligentes e IoT) diseñado para reemplazar a Android en todos sus productos, basado en un *microkernel* y distribuido. Curiosamente, en su lanzamiento se resaltaba la seguridad como uno de sus puntos clave y su integración con los TEE (Trusted Execution Environments). El primer producto comercial que hizo uso de este nuevo sistema operativo, en lugar de Android TV, fue la Honor TV[8]. Las previsiones para la llegada de HarmonyOS al mercado móvil son de marzo de 2020, de la mano del modelo Huawei P40[9]. La idea de disponer de un sistema operativo multidispositivo en los próximos años rivaliza con el futuro sistema operativo de Google Fuchsia OS [Ref.- 30], potencialmente buscando una "integración" de Chrome OS y Android, pero todavía en una fase experimental.

[5] https://www.xatakamovil.com/apple/record-ingresos-para-apple-wearables-servicios-iphone-11-tienen-culpa
[6] https://www.techradar.com/news/huawei-ban
[7] https://www.xataka.com/moviles/van-cuatro-estados-unidos-renueva-exencion-veto-a-huawei-que-afirma-que-eso-no-tendra-impacto-sus-negocios
[8] https://www.xda-developers.com/honor-vision-tv-huawei-harmony-os/
[9] https://www.xataka.com/moviles/nada-cambia-harmony-os-quiza-llegue-huawei-p40



Mientras tanto, durante el supuesto periodo de transición acontecido en el año 2019, Huawei comercializó en octubre el modelo Mate 30 Pro[10], todavía con Android, pero sin los servicios de Google ni Google Play (al no disponer de la licencia de los Google Play Services, o GPS). Un caso que no se había presentado durante la última década y que parece requerir que los usuarios de este dispositivo sean más avanzados y tengan suficiente nivel técnico para conocer Android en detalle y poder llevar a cabo tareas manuales como, por ejemplo, la instalación de los paquetes (APKs) de apps populares como WhatsApp, o la instalación de los Google Play Services extraoficialmente. Este modelo de funcionamiento y mercado tiene implicaciones de seguridad directas, ya que abre la puerta a que usuarios menos expertos acaben instalando apps de fuentes que no son de confianza, hasta que la tienda oficial de Huawei, denominada AppGallery[11], disponga de las apps deseadas por los usuarios. La respuesta oficial de Huawei ante este riesgo es que el dispositivo incluirá una licencia del antivirus Avast...

La indisponibilidad de una tienda o mercado oficial de apps reconocida en los dispositivos móviles inteligentes actuales sin Google Play, que disponga de miles de apps que permitan a los usuarios extender su funcionalidad de fábrica, es uno de los mayores retos para Huawei, con implicaciones relevantes de seguridad de cara a la distribución de apps de confianza. Actualmente Huawei es el principal afectado por el veto de EEUU, pero otros fabricantes chinos como Xiaomi, Oppo o Vivo temen verse afectados también. Por este motivo, los cuatro fabricantes chinos, con un 40% del mercado global [Ref.- 2], preparan una alianza para crear una alternativa a Google Play [Ref.- 31], denominada Global Developer Service Alliance (GDSA)[12]. Esta plataforma para desarrolladores distribuirá apps y otros contenidos multimedia o juegos, a nivel global, tanto dentro como fuera de China (inicialmente, en 9 regiones objetivo).

Para finalizar con el análisis de la evolución del mercado de dispositivos móviles en 2019, parece consolidarse la tendencia que lleva a la desaparición del tradicional conector de auriculares (minijack de 3,5 mm) frente al uso de Bluetooth (delegándose en los auriculares inalámbricos la calidad del sonido, en

[10] https://www.xataka.com/moviles/probando-mate-30-pro-entendemos-que-huawei-dice-que-su-gran-reto-apps-google-play-hay-que-saber-android-funcione
[11] https://huaweimobileservices.com/es/appgallery-esp/
[12] https://www.gdsa.com/en

lugar de en el terminal), aunque algunos dispositivos de 2020 de gama alta como el LG V60 ThinQ parece que incorporarán conector minijack. Debe tenerse en cuenta que la utilización generalizada de Bluetooth para el audio fuerza a los usuarios, al igual que ocurre con los dispositivos personales, como las pulseras o los relojes inteligentes (o *smart watch*), a tener activo el interfaz de Bluetooth permanentemente, con las implicaciones de seguridad asociadas, pudiendo ser utilizado para obtener detalles de los dispositivos Bluetooth o explotado en caso de ser vulnerables (ver apartado "10. Comunicaciones inalámbricas").

También destaca la reciente apuesta del Parlamento Europeo por estandarizar un conector de carga único y universal para los dispositivos móviles [Ref.- 32], actualmente teniendo el USB-C como referencia, propuesta a la que Apple inicialmente se ha opuesto, alegando que frena la innovación, en relación a su conector lightning; aunque los últimos iPad Pro hacen uso de un conector USB-C. El objetivo es reducir la cantidad de residuos electrónicos, simplificar su uso y aumentar la interoperabilidad, con carácter urgente (debiendo tomarse la decisión antes de julio de 2020). Un acuerdo similar fue tomado en 2009 para pasar de los más de 30 conectores propietarios diferentes existentes a un único conector estándar, el microUSB. En función de la decisión final, será interesante evaluar las implicaciones desde el punto de vista de seguridad, ya que el conector físico de los dispositivos móviles es utilizado tanto para cargar la batería como para transferencias de datos.

Asimismo, continua la tendencia a principios de 2020 con la aparición de múltiples modelos de dispositivos móviles con pantalla plegable, una tendencia que ya se mencionaba en el informe del pasado año 2018 [Ref.- 10], como el Samsung Galaxy Z Flip, Motorola Razr, Galaxy Fold, etc. Destaca igualmente el cierre de la compañía Essential tras sólo 3 años de vida, dejando a sus usuarios sin actualizaciones de seguridad después de febrero de 2020[13].

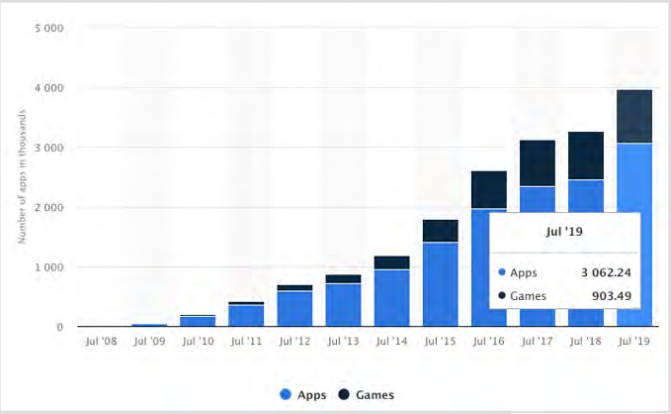
Por último, a lo largo de todo el mes de febrero de 2020 múltiples empresas tecnológicas anunciaron oficialmente la cancelación de su presencia en el Mobile World Congress (MWV) de Barcelona, el mayor evento de telefonía móvil a nivel mundial, debido a los riesgos de seguridad y contagio del coronavirus Wuhan (COVID-19), empezando por LG, ZTE (con confusión), Ericsson, NVIDIA, Amazon, Sony o Intel, una tendencia creciente según pasaban los días que acabó finalmente en la cancelación del congreso en su totalidad [Ref.- 120].

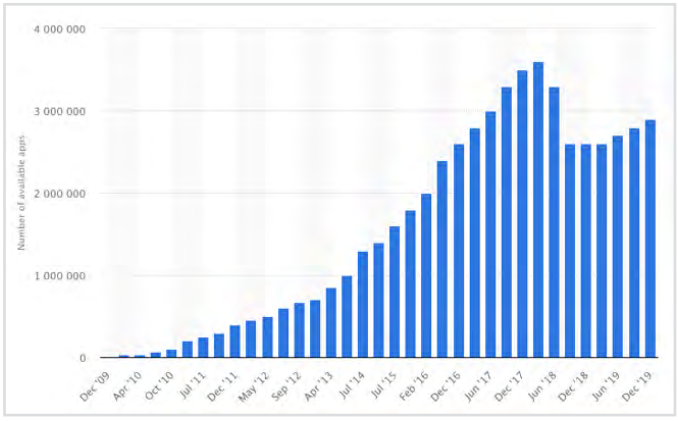
[13] https://www.xataka.com/moviles/essential-anuncia-su-cierre-tres-anos-despues-presentar-su-primer-smartphone (https://github.com/EssentialOpenSource)

4. EVOLUCIÓN DE LOS MERCADOS OFICIALES DE APPS MÓVILES EN 2019

Las estadísticas del año 2019 presentan un incremento notable respecto al número total de aplicaciones móviles (en adelante, apps) disponibles en los mercados oficiales (que se había ralentizado el pasado año 2018), dónde la Apple Store disponía de 900 mil juegos y 3 millones de aplicaciones móviles (no juegos) en el tercer trimestre de 2019 [Ref.- 9] (ver primera imagen inferior[14]), y Google Play disponía de 2,57 millones de apps [Ref.- 5], incrementando su número a 2,9 millones a finales de 2019 (ver segunda imagen inferior) [Ref.- 6].

Estas cifras (ligeramente variables según la fuente) reflejan como los mercados oficiales de apps han manifestado un nuevo crecimiento en 2019 tras el declive de 2018, incrementándose el número de apps existentes. A modo de referencia, Google ganó 8,8 billones de dólares a nivel mundial con Google Play en 2019 (en base a la comisión del 30% que aplica), incluyendo tanto apps como contenidos [Ref.- 31].





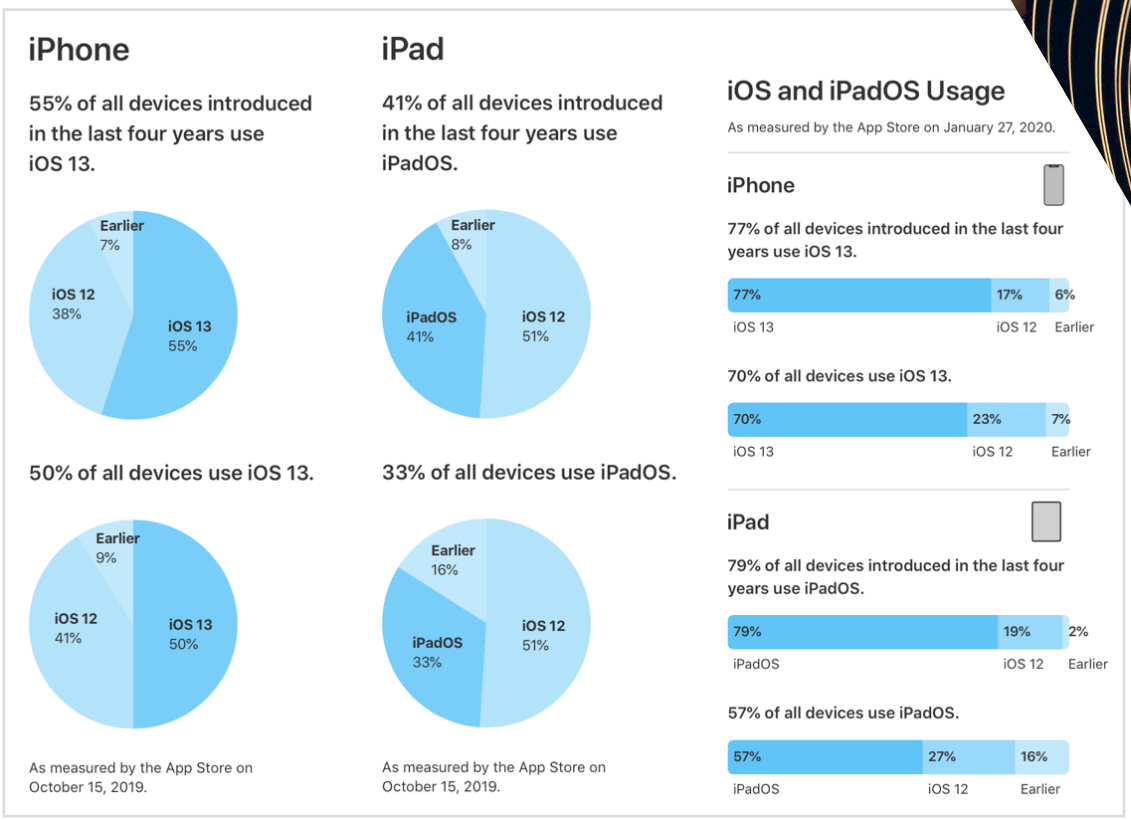
[14] Las estadísticas para la App Store de Apple de ambas referencias, provenientes de la misma fuente, son contradictorias, ya que reflejan unos 3,9 millones de apps (incluyendo juegos) [Ref.- 9] y, por otro lado, 1,84 millones de apps [Ref.- 5].

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

La adopción de las nuevas versiones disponibles de los sistemas operativos móviles, iOS y Android, 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, Apple y Google, como para poder disponer de las últimas actualizaciones de seguridad frente a vulnerabilidades públicamente conocidas.

Las últimas versiones del sistema operativo iOS 13.x para iPhone y iPadOS 13.x para iPad, liberadas por Apple a mediados de septiembre de 2019, a fecha 15 de octubre de 2019[15], es decir, un mes después, estaban siendo utilizadas por un 55% y un 41% respectivamente de usuarios con dispositivos móviles considerados recientes (es decir, comercializados en los últimos 4 años), y por un 50% y un 33% de usuarios totales, en base a los datos oficiales obtenidos a través de la App Store por parte de Apple [Ref.- 8].

[15] Desafortunadamente, y potencialmente influenciado por una reducida tasa de adopción respecto a años previos, a mediados de enero de 2020 no se dispone aún de estadísticas más actualizadas del nivel de adopción de iOS y iPadOS por parte de Apple, siendo las últimas del 15 de octubre de 2020.



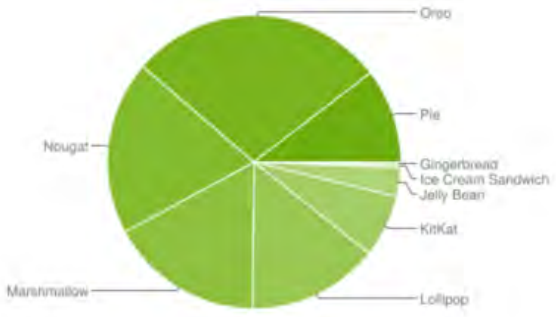
Durante el proceso de elaboración de la presente guía, Apple actualizó las estadísticas de adopción de iOS 13 (ver imagen superior derecha), lo que permite ver la evolución en el tiempo desde la fase inicial de comercialización hasta 4 meses después, 27 de enero de 2020. En ese momento, iOS y iPadOS 13 estaban siendo utilizadas por un 77% y un 79% respectivamente de usuarios con dispositivos móviles recientes, y por un 70% y un 57% de usuarios totales [Ref.- 8].

En septiembre de 2019, con la versión 13 de iOS, Apple ha independizado por primera vez el sistema operativo de los dispositivos móviles iPhone y iPad, publicando iPadOS 13[16] para estos últimos (soportado desde el iPad 2017 o 5ª generación, Air 2, mini 4 y Pro[17]). Ambos sistemas operativos, iOS y iPadOS son muy similares, pero el principal objetivo de Apple independizándolos es transformar el iPad en una alternativa a los portátiles, con un enfoque más profesional [Ref.- 22]. iPadOS presenta cambios en la pantalla de inicio con acceso rápido a los widgets, multitarea para la ejecución simultánea de varias apps, Exposé (como en macOS), la vista dividida con dos instancias de una misma app, soporte para trabajar con archivos externos (memorias USB, tarjetas SD, servidores SMB, iCloud Drive...), mejoras con Apple Pencil, el navegador web Safari, entre muchos otros.

[16] https://www.apple.com/ipados/
[17] https://www.xatakamovil.com/sistemas-operativos/ios-13-ipados-todos-dispositivos-compatibles-ultima-actualizacion-apple

En el caso de Android, la última versión del sistema operativo publicada a principios de septiembre de 2019, Android 10.x (sin nombre en código por primera vez en la historia), está presentando un nivel de adopción muy lento con respecto a versiones previas de Android, aunque similar a la adopción de Android 9.x en 2018. Tras 5 meses desde su publicación, las estadísticas oficiales de Google a finales de enero de 2020 no están disponibles, ya que quedaron congeladas en el 7 de mayo de 2019, donde lógicamente ni si quiera se refleja la existencia de la versión 10.0 de Android, lo que indica una adopción menor al 0,1% a nivel mundial [Ref.- 7]. En dichas estadísticas oficiales, Android 9.x (Pie), 9 meses tras su publicación disponía de un 10% de cuota de mercado, y Android 8.x (Oreo), más de 20 meses después de su publicación, disponía de una cuota de mercado de un 28% (incluyendo ambos Android 8.0 y 8.1). Esta situación impide, una vez más, que los usuarios de Android puedan beneficiarse de todas las mejoras de seguridad introducidas en las últimas versiones de Android.

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.3%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.2%
4.2.x		17	1.5%
4.3		18	0.5%
4.4	KitKat	19	6.9%
5.0	Lollipop	21	3.0%
5.1		22	11.5%
6.0	Marshmallow	23	16.9%
7.0	Nougat	24	11.4%
7.1		25	7.8%
8.0	Oreo	26	12.9%
8.1		27	15.4%
9	Pie	28	10.4%



Data collected during a 7-day period ending on May 7, 2019.
Any versions with less than 0.1% distribution are not shown.

Por tanto, las versiones de Android más comúnmente utilizadas en dicha fecha (7 de mayo de 2019) eran (por orden) Android 8.x, 7.x, 6.x y, todavía, Android 5.x, junto a Android 9.x, con un 28,3%, 19,2%, 16,9%, 14,5% y 10,4% de cuota de mercado respectivamente. Este hecho ha incrementado aún más la fragmentación de Android ya conocida en años previos, al existir 5 versiones distintas con porcentajes muy significativos, lo que tiene un impacto directo en la prevalencia de vulnerabilidades y en la limitada disponibilidad de actualizaciones de seguridad para esta plataforma para muchos usuarios. Cabe recordar que Google sigue proporcionando ciertas actualizaciones de seguridad para la plataforma Android a través de la actualización automática de otros componentes, como Google Play Services (GPS), aunque las mismas no conlleven ningún incremento de la versión del sistema operativo del dispositivo móvil.

El conocido problema de fragmentación de las versiones de sistema operativo en Android sigue estando muy presente y parece que aún, las medidas que se comenzaron a instaurar junto a Android 8.x (Oreo) con el objetivo de mitigar la tan conocida fragmentación asociada a las diferentes versiones de Android, por ejemplo, mediante el proyecto Treble (ver los detalles en el informe anual de 2017 [Ref.- 11]), o imponiendo requisitos más estrictos sobre los fabricantes de dispositivos móviles y el compromiso de publicar actualizaciones durante al menos 2 años para dispositivos “populares” (ver los detalles en el informe anual de 2018 [Ref.- 10]), no han dado sus frutos, aunque Google indica lo contrario (tal como se detalla en el apartado “8. Código dañino para plataformas móviles”). Será necesario esperar a los próximos años para comprobar realmente su efectividad.

6. DESBLOQUEO Y EXPLOTACIÓN DE DISPOSITIVOS MÓVILES, EXTRACCIÓN FORENSE DE DATOS Y *JAILBREAKS*

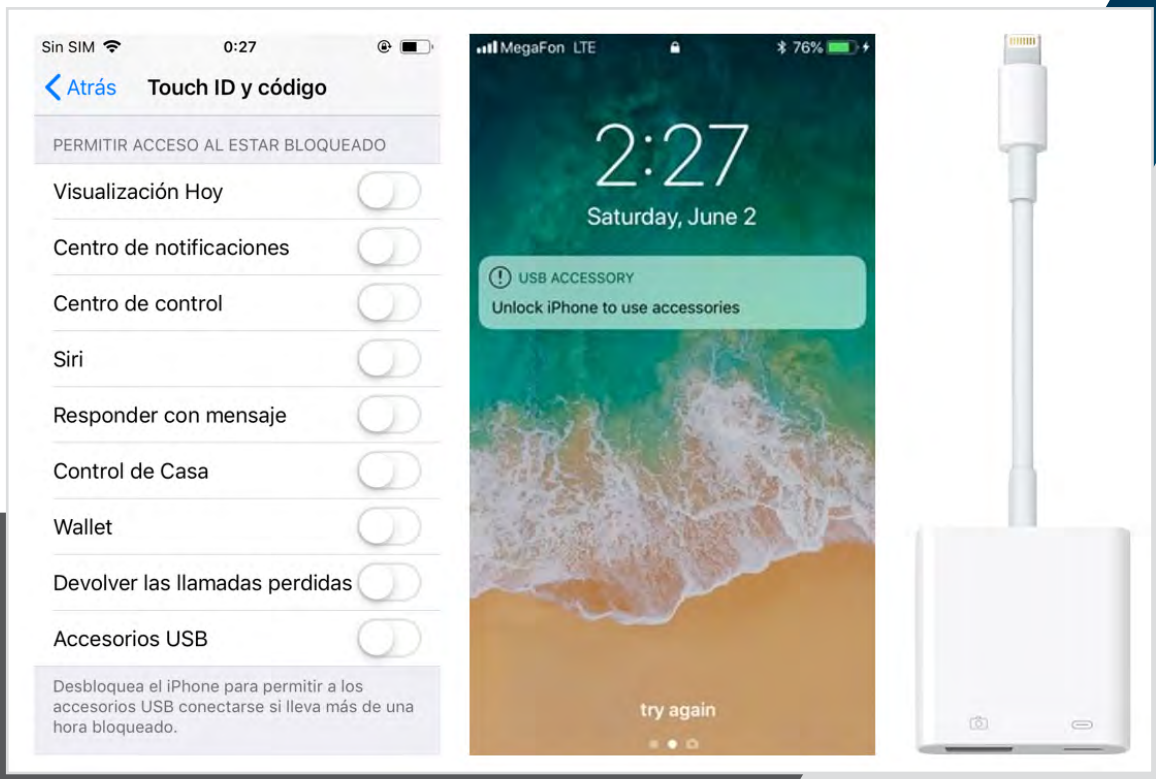
El informe anual de amenazas de 2017 y tendencias de 2018 de dispositivos y comunicaciones móviles publicado por el CCN-CERT hace dos años [Ref.- 11], junto al informe de 2018 del pasado año [Ref.- 10], ya reflejaban la relevancia que seguía tomando la posibilidad de evitar la pantalla de autentificación o bloqueo de los dispositivos móviles, junto a la extracción de datos de los mismos sin autorización y sin conocer el código de acceso, ya sea legítimamente por parte de los cuerpos y fuerzas de seguridad del estado en casos judiciales en los que están involucrados estas tecnologías, como ilegítimamente por parte de ciberdelincuentes.

Continuando con la tendencia de los últimos años dónde los dispositivos móviles basados en iOS han presentado numerosas vulnerabilidades que han permitido evitar la pantalla de desbloqueo sin disponer del código de acceso [Ref.- 12], iOS 12 y 13 han acumulado un total de 8 vulnerabilidades a lo largo del año 2019 y de 4 hasta principios del año 2020 respectivamente. Estas vulnerabilidades han permitido el acceso al contenido de contactos (viéndose este acceso afectado especialmente por numerosas vulnerabilidades) y fotos, conocer la última app utilizada, compartir contenidos, o conocer la dirección de e-mail utilizada para iTunes, entre otros. Este tipo de amenaza refleja los riesgos asociados a la pérdida o robo de los dispositivos móviles, siendo imprescindible tomar medidas de protección frente a accesos físicos no autorizados (incluso temporalmente o durante un breve espacio de tiempo). Igualmente, Android 10 presentó una vulnerabilidad en la pantalla de bloqueo que permitía añadir nuevos usuarios sin conocer el código de acceso[18].

[18] https://twitter.com/raulsiles/status/1173155293599076352

El año 2019 se ha caracterizado de nuevo por los avances y modificaciones realizados por Apple en las distintas versiones y subversiones de iOS, con el objetivo de restringir los posibles accesos no autorizados a través de USB por parte de las soluciones comerciales de análisis forense de dispositivos móviles, como los servicios de Cellebrite y el producto GrayKey de Grayshift [Ref.- 11], añadiendo a las últimas mejoras de iOS 12 [Ref.- 15] [Ref.- 17] nuevas capacidades en iOS 13, tal como se detalla en la guía práctica de seguridad de dispositivos móviles iPhone para iOS 13 del CCN-CERT [Ref.- 18].

En iOS 11.4.1 (o versiones posteriores) la activación del modo restringido USB se habilitaba automáticamente una hora después del último desbloqueo del dispositivo, y/o desde que el dispositivo móvil había sido desconectado de un accesorio USB. En iOS 12 la conexión de datos vía USB también se deshabilitaba inmediatamente tras el bloqueo del dispositivo si han pasado más de 3 días (72 horas) desde que el dispositivo hizo uso de una conexión de datos vía USB por última vez (por ejemplo, al no utilizarse estas conexiones frecuentemente), o si se han deshabilitado los mecanismos de autentificación biométrica y se requiere introducir el código de acceso (por ejemplo, al activar el modo de emergencia, o SOS, de iOS).



Entre las novedades introducidas en iOS 13 destaca que adicionalmente al establecimiento de emparejamientos o relaciones de confianza entre iOS y un ordenador, Apple ha introducido el concepto de emparejamiento con dispositivos USB [Ref.- 16]. En este segundo caso, no es necesario introducir el código de acceso y no existe ningún intercambio de claves criptográficas, pero el dispositivo móvil debe estar (o debe ser) desbloqueado, en cuyo caso se almacenará información sobre el dispositivo USB y éste pasará a ser un dispositivo USB de confianza. Durante el periodo de una hora en el que se permiten conexiones USB, si se conecta un dispositivo USB en iOS 13, éste es gestionado de manera diferente si se trata de un dispositivo USB de confianza previamente emparejado, o de un dispositivo nuevo. En el primer caso se permitirá la conexión de datos, mientras que en el segundo caso, las capacidades de datos del puerto USB serán restringidas, incluso dentro del periodo de una hora. En resumen, en iOS 13, de cara a poder extraer datos mediante técnicas forenses, cobra mayor importancia disponer de un dispositivo USB de confianza, que estuviese previamente emparejado con el dispositivo móvil objetivo, con la idea de potencialmente poder extender a más de una hora el periodo de extracción de evidencias (pero siendo mayor el riesgo de que se activen las restricciones USB en iOS 13).

En relación con las capacidades de análisis forense y extracción de datos y evidencias de los dispositivos móviles y, en concreto, de dispositivos que hacen uso de la última versión de iOS, 13, numerosas investigaciones y avances se han llevado a cabo a finales de 2019, promovidos por la existencia del *jailbreak* checkra1n [Ref.- 24].

A lo largo del año 2019, se han producido avances en herramientas de jailbreak ya existentes para diferentes versiones de iOS 11 y 12, tales como unc0ver[19] o Chimera[20], proporcionando una mayor estabilidad y soporte para poder obtener control completo del dispositivo móvil en nuevas versiones de iOS (especialmente dentro de iOS 12) y nuevos modelos de dispositivos. Sin embargo, el mayor impacto en la comunidad de Apple, de seguridad y de *jailbreak* se produjo a finales del mes de septiembre de 2019, cuando el investigador axi0mX publicaba el descubrimiento de un exploit épico en el BootROM, componente encargado del proceso de arranque inicial de los dispositivos móviles iOS y iPadOS, que afectaba a numerosos modelos de dispositivos y, en consecuencia, a cientos de millones de dispositivos existentes en el mercado [Ref.- 23].

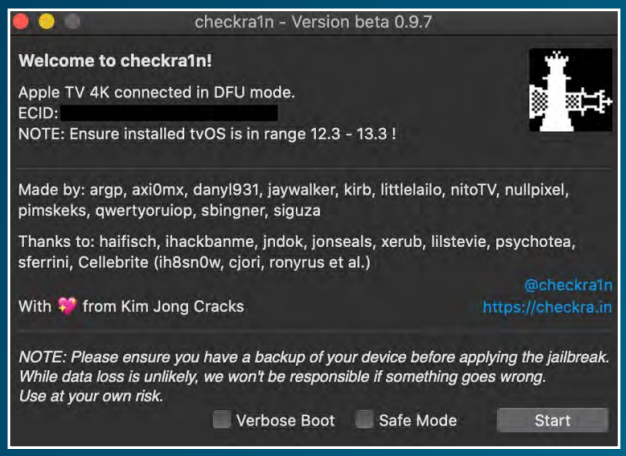
[19] https://unc0ver.dev (https://github.com/pwn20wndstuff/Undecimus)
[20] https://chimera.sh

El exploit checkm8 (“checkmate”), publicado abierta y gratuitamente, e implementado en el *jailbreak* checkra1n [Ref.- 24] (para iOS 12.3 y versiones superiores) afecta a múltiples generaciones de iPhones y iPads, desde el iPhone 5S (con el chip A7 de Apple) hasta el iPhone 8 y X (con el chip A11 Bionic de Apple). Únicamente los últimos modelos de hardware solucionan la vulnerabilidad asociada: desde el iPhone XS y XR, en adelante, y desde el iPad mini de 5ª generación, iPad Air de 3ª generación o el iPad Pro de 3ª generación, en adelante (con el chip A12 Bionic o posterior). Lo sorprendente, es que la vulnerabilidad (de tipo *use-after-free*) fue descubierta por el investigador analizando las diferencias en el BootROM entre la versión utilizada en modelos anteriores y la siguiente versión utilizada en el iPhone XS, concretamente, en las versiones beta de iOS 12 publicadas el verano de 2018. Apple había solucionado la vulnerabilidad de manera encubierta, sin haber anunciado ni si quiera su existencia (haciendo viable que otros investigadores ya la hubieran descubierto anteriormente y la estuvieran usando de manera privada). Se debe tener en cuenta que en los mercados de comercialización de vulnerabilidades y exploits de día cero (no publicados), este tipo de vulnerabilidades tienen un precio actualmente de entre 1 y 2 millones de dólares[21].

Checkm8 es similar a otra vulnerabilidad publicada en el año 2010 denominada limera1n[22], descubierta por geohot, que afectaba al iPhone 4 y al iPad 1 (entre otros). Es decir, hace 9 años que no se conocía públicamente la existencia de una nueva vulnerabilidad de BootROM, por lo que probablemente este descubrimiento es uno de los más relevantes en la historia del *jailbreak*, sino el más relevante. El impacto desde el punto de vista de seguridad de este tipo de vulnerabilidades en el

[21] https://zerodium.com/program.html
[22] https://www.theiphonewiki.com/wiki/Limera1n

BootROM (o vulnerabilidades hardware) es muy alto, ya que como su propio nombre indica, el BootROM dispone de una memoria de solo lectura (ROM, Read Only Memory), por lo que no puede ser modificada y, por tanto, no puede ser parcheada por Apple mediante una actualización software que solucione la vulnerabilidad. De hecho, el que el BootROM no se pueda modificar es uno de los mecanismos principales que proporcionan seguridad y confianza a los dispositivos de Apple, y a todo el sistema y cadena de firmado y verificación del código que será ejecutado por iOS y iPadOS. Como resultado, todos los dispositivos móviles vulnerables (según su modelo de fábrica), seguirán siendo vulnerables por el resto de sus días (independientemente de la versión de iOS de la que dispongan), y la única opción para usuarios finales y empresas de cara a no hacer uso de un dispositivo móvil vulnerable es sustituirlos por los nuevos modelos hardware de iPhone y iPad. Al tratarse de un exploit en el proceso de arranque, para poder sacar provecho del mismo es necesario interacción física con el dispositivo víctima durante el arranque, a través del conector de *lightning* USB (no pudiendo ser explotada remotamente).



Las capacidades de bajo nivel de checkra1n permiten desde volcar la memoria del SecureROM (este es el término empleado por Apple para el BootROM[23]), descifrar las keybags o incluso permitir interacciones hardware con los dispositivos mediante un interfaz JTAG. Adicionalmente, la versión publicada en febrero de 2020 añade soporte para Linux (junto al existente para macOS), incluye webra1n (un interfaz web que permite realizar el proceso de *jailbreak* desde un navegador web a través de la red interactuando con el ordenador conectado por USB al dispositivo víctima), y lleva a cabo las tareas de parcheo de bajo nivel mediante un nuevo sistema operativo denominado pongoOS [Ref.- 25].

[23] https://www.theiphonewiki.com/wiki/Bootrom

Curiosamente, esta vulnerabilidad casi coincidió en el tiempo con el anuncio por parte de Apple de un nuevo programa de recompensas (bug bounty) para investigadores de seguridad, denominado Apple Security Bounty, anunciado inicialmente en BlackHat USA en agosto de 2019 [Ref.- 27] y publicado oficialmente en diciembre de 2019 [Ref.- 29]. Este programa inicialmente privado (es decir, gestionado por invitación desde 2016) se abrió al público en 2019 e incorporó, además de iOS e iCloud, otras plataformas de Apple, como iPadOS, macOS, watchOS, o tvOS, aumentando el importe de las recompensas respecto a años previos, hasta un máximo de un millón y medio de dólares (considerando los bonus). Adicionalmente, Apple anunció la futura existencia en el año 2020 de dispositivos móviles iOS oficiales de investigación de Apple, con acceso de bajo nivel como root y capacidades de depuración (diferentes de los dispositivos de desarrollo o de producción), especialmente preparados para facilitar las investigaciones de seguridad en iOS, dentro de un programa denominado iOS Security Research Device.

Las capacidades de acceso completo a los dispositivos de Apple asociadas a los jailbreaks o a capacidades similares, es decir, obteniendo acceso como root, ha estado rodeada de gran controversia durante este año 2019 también debido a las disputas legales de Apple contra Corellium, que salieron a la luz públicamente a finales de diciembre de 2019 [Ref.- 26]. Corellium es una empresa que proporciona una plataforma de virtualización de iOS utilizada comercialmente por investigadores y analistas de seguridad para el análisis de apps y del ecosistema de iOS (constituyéndose potencialmente como la competencia frente a los dispositivos móviles de desarrollo de Apple anteriormente mencionados).

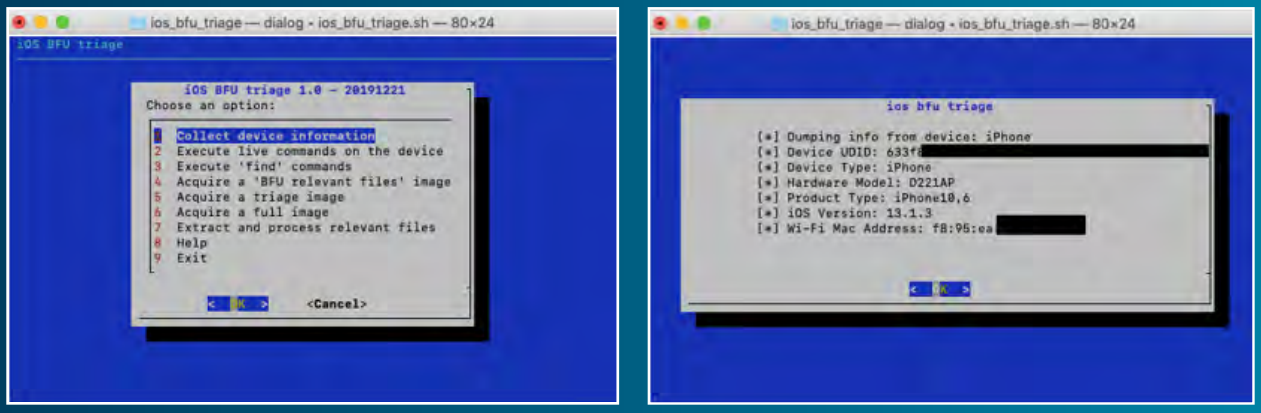
En la demanda interpuesta por Apple (inicial, y especialmente en su progresión) se puede ver como la compañía de la manzana defiende que la creación de un entorno de emulación de iOS que facilite la creación de herramientas de jailbreak infringe su copyright, referenciando el DMCA y mencionando explícitamente otras herramientas de jailbreak, algo que ha sido visto en la comunidad global de jailbreaks públicos como un ataque directo. La controversia a su vez radica en que durante todo el proceso legal, Apple ha animado a Corellium a seguir desarrollando su tecnología, incluyéndola en su Security Bounty Program privado, e incluso intentó su adquisición, que no prosperó por desacuerdos económicos, tras lo que demandó a la compañía. Desde un punto de vista general, es importante destacar como la existencia y disponibilidad de jailbreaks públicos para iOS (y ahora iPadOS), o soluciones similares, constituyen una herramienta fundamental para poder llevar a cabo análisis detallados y en profundidad de la seguridad de iOS y de las apps existentes por defecto y de terceros que ejecutan en este sistema operativo móvil. Un caso concreto utilizado como ejemplo para desenmascarar el uso y la existencia de apps de espionaje en la App Store es el análisis mediante el uso de un *jailbreak* de ToTok [Ref.- 28] (descrito posteriormente en este mismo apartado).

Una serie de estudios y publicaciones del Departamento de Seguridad Nacional (DHS) de EEUU detallan los resultados de las pruebas realizadas por el NIST en la adquisición forense de datos y extracción de

evidencias de dispositivos móviles mediante diferentes herramientas comerciales y sobre múltiples objetivos [Ref.- 88], una referencia actualizada en 2019 para analistas forenses[24].

Desde el punto de vista forense, la existencia de checkra1n abrió la puerta a la posibilidad de extraer datos y evidencias de dispositivos con iOS 13, y de analizar los detalles internos de esta nueva versión de sistema operativo liberada por Apple en septiembre de 2019. Checkra1n es un *jailbreak* de tipo *semi-tethered*, es decir, requiere explotar la vulnerabilidad durante el proceso de arranque desde un ordenador conectado por USB, y disponer de acceso completo al dispositivo. Una de sus características es que, la siguiente vez que el dispositivo móvil arranque, lo hará utilizando un arranque normal, sin dejar evidencias de cara al usuario de que había sido explotado y comprometido previamente.

Como resultado de las investigaciones de iOS 13 desde un punto de vista forense, destacando la importancia del *jailbreak* checkra1n para una extracción o adquisición física de datos, se han realizado avances significativos en 2019 respecto a la información y evidencias que están disponibles antes (BFU, Before First Unlock) y después (AFU, After First Unlock) del primer desbloqueo del dispositivo móvil tras el arranque. En primer lugar, la relevancia de checkra1n es que permite aplicar el mismo procedimiento de extracción (o uno muy similar) a multitud de modelos de dispositivos móviles de Apple (iPhones, iPad, Apple TV y Apple Watch) y sobre diferentes versiones de iOS (y del resto de sistemas operativos), incluyendo la versión más actual (algo que no es posible con otros *jailbreaks*) [Ref.- 33].



Si no se conoce el código de acceso del dispositivo, únicamente un conjunto reducido de datos, obtenidos a nivel de sistema de ficheros, estará disponible: logs, preferencias, bases de datos del sistema y temporales, buzón de voz, etc. Si se conoce el código de acceso, es posible obtener el contenido del sistema de ficheros completo y de la keychain. Por otro lado, si el dispositivo aún no ha sido desbloqueado

[24] https://www.vice.com/en_us/article/n7jevz/government-report-reveals-its-favorite-way-to-hack-iphones-without-backdoors

al menos una vez (BFU), la mayoría de los contenidos permanecen cifrados en iOS. Sin embargo, aún es posible (al igual que si el dispositivo ha sido deshabilitado por un elevado número de intentos de acceso fallidos, o si el modo restringido USB está activado) disponer de acceso a ciertas entradas de la keychain, incluyendo credenciales para cuentas de e-mail, nombres e identificadores de cuentas de usuario, y otros tokens de autentificación, accesibles por diseño para facilitar el proceso de arranque de iOS [Ref.- 34]. Asimismo, es posible acceder en modo BFU a contenidos del sistema de ficheros, como la lista de apps instaladas, datos de Wallet, la lista de conexiones Wi-Fi, ficheros multimedia, notificaciones, datos de localización, actividades de red de las apps, buzón de voz, etc. A finales de 2019 se publicaron una serie de artículos técnicos para la extracción de datos en iOS 13, detallando las capacidades forenses y listando los artefactos disponibles mediante checkra1n, una vez se proporciona acceso como root, y en diferentes escenarios BFU [Ref.- 35].

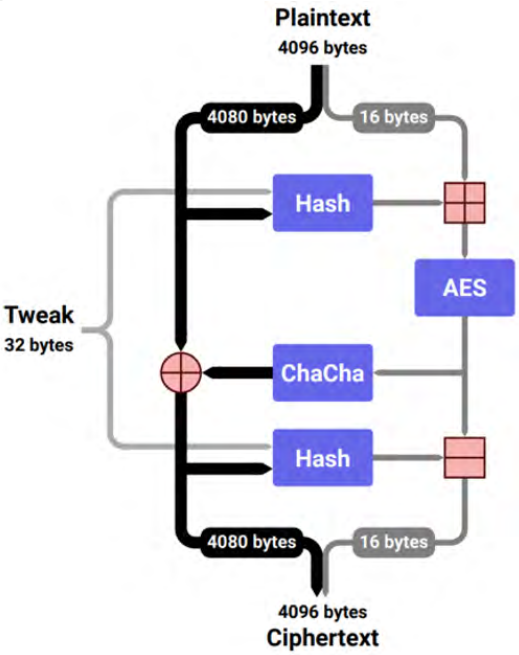
ToTok es el nombre de una app de espionaje publicada en la App Store [Ref.- 28], evitando todos los mecanismos de aprobación de Apple, y utilizada por los Emiratos Árabes Unidos (UAE), en concreto por la agencia de inteligencia de señales ubicada en Abu Dhabi, junto a la empresa Pax AI (especialistas en el procesamiento y análisis de datos), asociada a DarkMatter (con vinculación al proyecto Raven, también mencionado en el presente informe). El supuesto propósito legítimo de esta app era el de una app de mensajería estándar (texto y vídeo), incluso en un país donde otras apps populares como WhatsApp y Skype están restringidas, y presentaba millones de descargas en todo el mundo, tanto en la App Store como en Google Play (ambos mercados eliminaron la app tras desvelarse sus actividades). El análisis forense de la misma mediante técnicas de ingeniería inversa en un entorno con *jailbreak* permitió identificar sus capacidades para monitorizar masivamente las actividades de aquellos que la habían instalado: seguimiento de la localización a través de su servicio meteorológico, obtención de contactos con la excusa de poder conectar con conocidos, y el típico acceso al micrófono, cámara, calendario, y otros datos del teléfono. El análisis no clarifica si el gobierno de UAE disponía de capacidades para grabar las llamadas de audio y vídeo de los usuarios. Por supuesto, ToTok era anunciada (en campañas de marketing minuciosamente preparadas) como gratuita, rápida y segura, pero sin mención a ninguna capacidad de cifrado extremo a extremo (E2E), tan ampliamente utilizado hoy en día por otras apps de mensajería.

7. MECANISMOS DE SEGURIDAD AVANZADOS EN DISPOSITIVOS MÓVILES

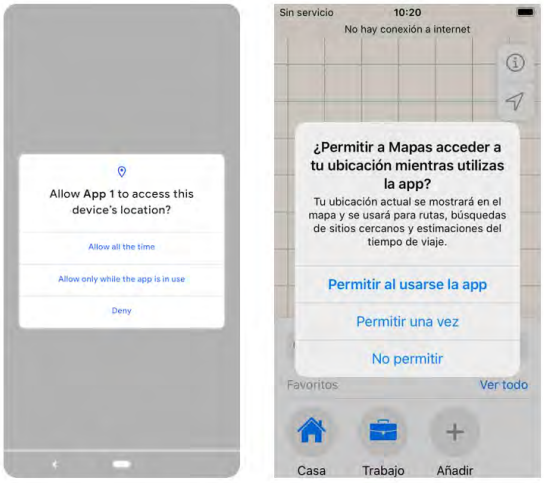
Con el objetivo de proteger los datos almacenados en los dispositivos móviles Android mediante nuevas capacidades de cifrado en reposo, y complementando las capacidades de cifrado de los servicios de almacenamiento en la nube asociadas al servicio Cloud Key Vault (CKV) de Google (Google Cloud Platform, o GCP) descritos en el informe anual del pasado año 2018 [Ref.- 10], Google anunció a principios de 2019 cambios relevantes para todos los dispositivos móviles Android 9, especialmente para aquellos sin aceleración criptográfica hardware (es decir, sin soporte hardware AES en sus CPUs), típicamente dispositivos móviles de gama baja englobados en la iniciativa Android Go, o dispositivos IoT (relojes, TVs...) con CPUs como el ARM Cortex-A7 [Ref.- 36]. El objetivo de Google con esta iniciativa es asegurar que todos los dispositivos móviles Android hacen uso de cifrado a partir de Android 9 o versiones posteriores, reemplazando AES (en caso de ser necesario) con un nuevo algoritmo criptográfico más ligero y eficiente, denominado Adiantum, con un impacto mínimo en el rendimiento, pero con robustez similar.

El cifrado de disco presenta ciertos desafíos al tenerse que proteger sectores de disco de tamaño fijo (4.096 bytes), siendo necesario que el tamaño del contenido cifrado y sin cifrar sea el mismo. En AES este requisito se soluciona empleando modos de operación que preservan la longitud de los contenidos, como AES-XTS o AES-CBC-ESSIV. En el caso de Adiantum, y ante la imposibilidad de usar ChaCha20 y Poly1305 en el modo estándar definido en el RFC 7539, se hace uso de un nuevo modo de uso de ChaCha que preserva la longitud de los contenidos y que proporcionan un incremento de velocidad cinco veces superior a AES-256-XTS en los dispositivos objetivo. Para ello se combinan hashes (basados en NH y Poly1305) junto al cifrado de flujo de ChaCha12.

En el año 2019 Google ha progresado en los avances de seguridad en sus últimos dispositivos móviles, continuando con la tendencia de 2018 (ver el informe anual de 2018 [Ref.- 10]), actualizando y publicando a principios de 2020 su guía "Android Enterprise Security White Paper" [Ref.- 38], centrada en las capacidades de seguridad empresariales de Android, similar a la guía oficial de seguridad de plataformas de Apple (también renovada, como se describe a continuación). Complementariamente, Google publicó el modelo de seguridad de la plataforma móvil Android (publicación científica), empleando un modelo formal más abstracto que ejemplifica los casos de uso habituales, las amenazas (y el modelo de amenazas formal) a las que Android está expuesto y que intenta mitigar en diferentes escenarios, y sus implicaciones, intentando encontrar el equilibrio entre seguridad, privacidad y usabilidad, y posicionar las últimas versiones de Android a través de sus nuevas capacidades de seguridad y privacidad en el segmento más corporativo de los dispositivos móviles [Ref.- 37].



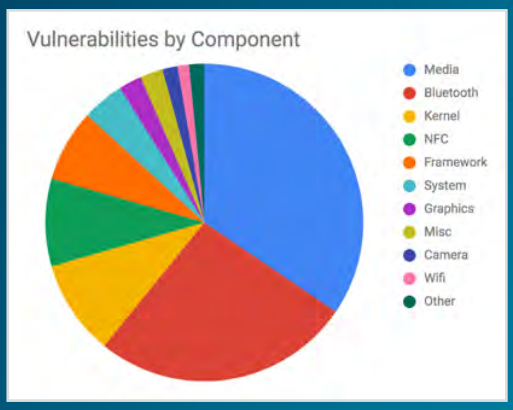
Android 10 ha introducido mejoras en la API de KeyChain, una nueva implementación para la autentificación facial, protegiendo el proceso de autentificación mediante una integración vía hardware en aquellos dispositivos que lo soportan, extiende los controles de privacidad sobre los datos y la ubicación del usuario, junto a otros cambios de privacidad en el modelo de permisos existente en versiones de Android previas. Específicamente, Android 10 ha mejorado el control del que disponen los usuarios para gestionar sus datos de localización, que siempre han sido considerados como uno de los datos más sensibles y han estado involucrados en numerosos escándalos (ver los detalles del The Times Privacy Project en el apartado "9. Privacidad del usuario en las plataformas móviles"). En versiones previas de Android el usuario únicamente disponía de un permiso para proporcionar o no acceso a la localización a las apps. En Android 10 los permisos de localización se hacen más granulares [Ref.- 40], permitiendo acceso a la localización a las apps todo el tiempo (incluso cuando están ejecutando de fondo o en segundo plano), cuando están siendo utilizadas (es decir, en primer plano), o nunca. Este modelo se asemeja más al modelo existente en iOS 13, aunque en iOS también se dispone de la opción de proporcionarle acceso a la localización a las apps una única vez [Ref.- 18].

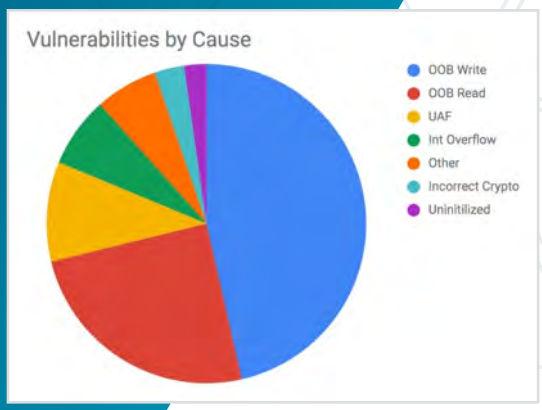


Igualmente, y en relación con la privacidad y el potencial seguimiento de los usuarios, Android 10 por defecto aleatoriza la dirección MAC del dispositivo en los escaneos Wi-Fi. En relación a las capacidades de cifrado de Android, junto a la opción de Adiantum descrita previamente, es importante destacar como Android 10 introduce el modelo de File Based Encryption (FBE) por defecto.

Las nuevas capacidades de seguridad de Android 10 [Ref.- 41] incluyen, adicionalmente a Adiantum, la activación por defecto de TLS 1.3, nuevas protecciones a nivel de plataforma [Ref.- 42], aislando aún más los codecs multimedia en su propio *sandbox* (fuera del servicio *mediacodec* - destacando la evolución de la seguridad y la reducción de privilegios de este componente en Android desde Android 6 a Android 10), verificaciones para componentes que procesan contenido no fiable (mediante BoundSan e IntSan, *sanitizers*), protecciones de bajo nivel en el kernel, como Shadow Call Stack (SCC), protecciones de ASLR frente a filtraciones de memoria mediante XOM (eXecute-Only Memory), o un nuevo gestor de la memoria *heap* (Scudo).

Concretamente, en Android 10 [Ref.- 42] muchas de estas medidas de protección de bajo nivel han sido aplicadas a la pila Bluetooth, lo que potencialmente ha permitido reducir el impacto de vulnerabilidades que fueron descubiertas posteriormente, como BlueFrag (descrita en el apartado "11. Comunicaciones inalámbricas"). El motivo por el que el foco en Android 10 se ha centrado en los componentes o *frameworks* multimedia, Bluetooth y el kernel es porque la mayoría de vulnerabilidades que han afectado a esta plataforma móvil implican a estos elementos, junto a NFC, siendo la causa del 90% de estas vulnerabilidades problemas de tipo *out of bounds* (OOB) *reads/writes*, *use-after-free* (UAF), e *integer overflows*.





Las capacidades de autentificación biométrica de Android, introducidas en Android 9 a través de la BiometricPrompt API, fueron descritas en gran nivel de detalle en el informe anual de 2018 [Ref.- 10], dentro de un apartado específico denominado "Mecanismos de autentificación biométrica en dispositivos móviles". En el informe de este año no se ha considerado necesario incidir de nuevo en estas capacidades, que siguen estando presentes y formando parte del día a día de los usuarios en los ecosistemas tanto de iOS como de Android. Android 10, sin embargo, actualiza dicho subsistema con soporte para huella dactilar digital y reconocimiento facial, así como nuevos casos de uso tanto implícitos como explícitos [Ref.- 41]. El flujo de autentificación explícito, empleado por defecto y recomendado para transacciones más críticas, como pagos, requiere que el usuario lleve a cabo una acción de verificación para proceder, como proporcionar su huella dactilar, o pulsar un botón adicional en el caso de reconocimiento facial. El flujo de autentificación implícito no requiere la intervención directa del usuario y se recomienda para operaciones menos críticas, como el proceso de *login* o el autorelleno de datos. Adicionalmente, las nuevas capacidades de BiometricPrompt permiten verificar si un dispositivo móvil dispone de las capacidades biométricas necesarias antes de hacer uso de este subsistema, pudiendo eliminar referencias a biometría si el dispositivo no la soporta.

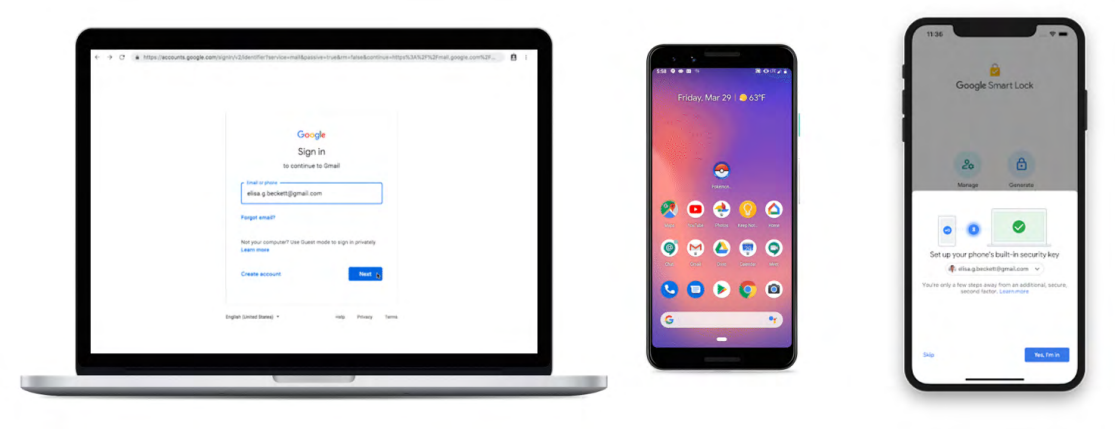
Dejando a un lado el programa de recompensas general de Google para investigadores de seguridad[25], destacan en 2019 los cambios introducidos en el programa de recompensas de seguridad de Google Play (Google Play Security Reward Program, GPSRP), que se extiende a todas las apps con 100 millones de instalaciones o más, y que se añade al programa que pueda tener la empresa desarrolladora de la app [Ref.- 43]. Google se beneficia de las vulnerabilidades reportadas al poder automatizar escaneos en busca de vulnerabilidades similares en todo Google Play. Sólo en 2018 el programa ayudó a 30 mil desarrolladores para arreglar problemas de seguridad en unas 75 mil apps. Adicionalmente, en agosto de 2019 Google lanzó un nuevo programa de recompensas para la protección de datos por parte de los desarrolladores (Developer Data Protection Reward Program, DDPRP), con el objetivo de identificar abusos con datos de usuario (entre otros) en apps de Android [Ref.- 43].

En relación con la integración de los dos principales ecosistemas móviles actuales, Android e iOS, Google publicó a comienzos de 2020 una serie de recomendaciones para que los usuarios de dispositivos móviles de Apple puedan proteger su cuenta de usuario de Google, mediante el Advanced Protection Program

[25] https://security.googleblog.com/2020/01/vulnerability-reward-program-2019-year.html

[Ref.- 44]. La importancia y criticidad a la hora de proteger la cuenta de usuario de Google queda puesta de manifiesto a lo largo de la guía CCN-STIC 456 de la cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android, publicada por el CCN-CERT en septiembre de 2018 [Ref.- 20]. Este programa de protección avanzado de Google ha sido diseñado para aquellos usuarios que requieren de niveles superiores de seguridad o se pueden ver amenazados más frecuentemente, como periodistas, activistas, personas de negocios relevantes o políticos. Sus nuevas capacidades requieren el uso de llaves de seguridad hardware (*security keys*, como las del estándar FIDO[26] U2F, Universal 2nd Factor) como segundo factor de autentificación (2FA, Two-Factor Authentication) o de verificación (2SV, Two-Step Verification) para la protección de las credenciales del usuario, por ejemplo, frente a ataques de *phishing*. Este 2FA es más robusto que el uso de mensajes SMS de verificación o de notificaciones *push*.

A lo largo de 2019 Google convirtió los dispositivos móviles Android, con versión 7 o superior, en llaves de seguridad hardware, pudiendo ser utilizados como 2FA sin requerir llevar encima dispositivos adicionales, aparte del móvil [Ref.- 45]. Al acceder a la cuenta de usuario de Google [Ref.- 20] desde un ordenador con 2FA activo, el dispositivo móvil Android puede ser utilizado directamente como llave de seguridad a través de Bluetooth. Inicialmente Android actuaba de llave de seguridad para Chrome OS, macOS y Windows 10 (mediante el navegador web Chrome), y posteriormente se extendió el modelo a iPads y iPhones [Ref.- 46] (mediante la app Google Smart Lock[26]).

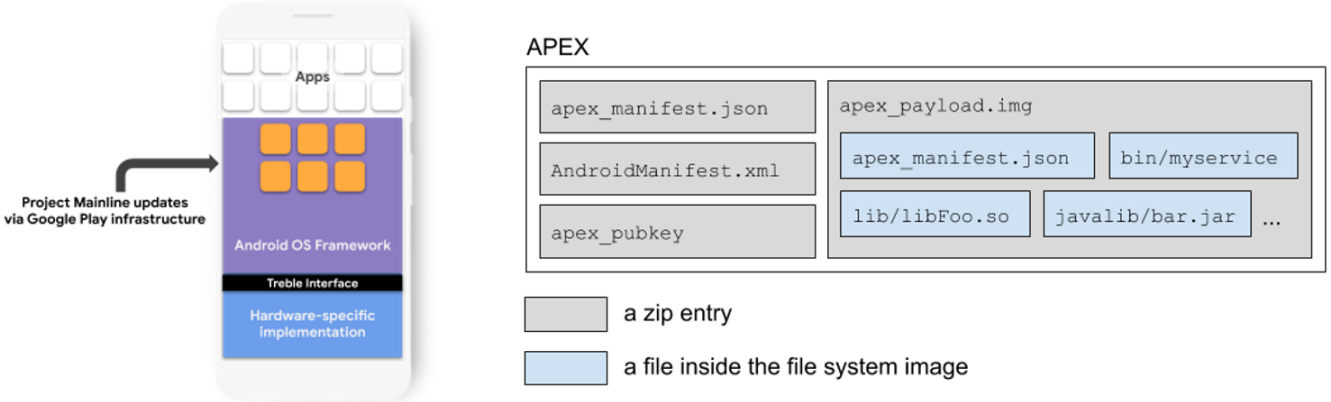


En 2020, Google amplió estas capacidades de llave de seguridad a los dispositivos móviles iOS [Ref.- 44], Complementariamente, con versión 10 o superior, mediante la app Google Smart Lock[27], que también hace uso de Bluetooth durante el proceso de autentificación para actuar de llave de seguridad para otro dispositivo: Chrome OS, macOS, Windows 10, etc. (haciendo uso del navegador web Chrome).

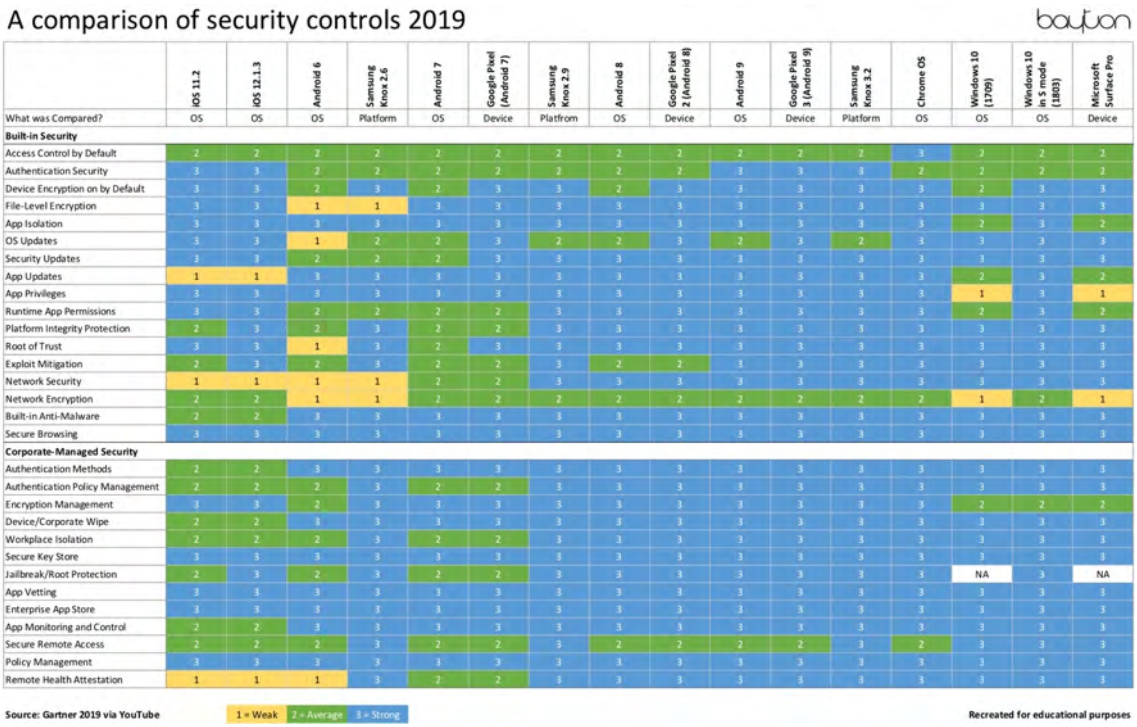
[26] https://fidoalliance.org/how-fido-works/
[27] https://apps.apple.com/es/app/google-smart-lock/id1152066360

Complementariamente, con el objetivo de proporcionar mecanismos de autentificación más sencillos y robustos, pero en este caso únicamente para el ecosistema Android, Google introdujo capacidades de autentificación y verificación local del usuario mediante FIDO2 en Android[28], inicialmente en los dispositivos Pixel pero posteriormente para Android versión 7 o superior, que permiten verificar la identidad del usuario en algunos servicios de Google (potencialmente tanto desde apps como desde servicios web) empleando la autentificación biométrica (huella dactilar digital) o el desbloqueo de la pantalla del dispositivo móvil, en lugar de la contraseña de la cuenta de usuario de Google [Ref.- 47].

Complementando el Proyecto Treble (mencionado en el apartado "8. Código dañino para plataformas móviles"), Google publicó el proyecto Mainline [Ref.- 48], cuyo objetivo principal es agilizar la distribución de actualizaciones en el ecosistema Android (especialmente de seguridad, pero también permite la incorporación de mejoras, por ejemplo, en el modelo de permisos del sistema), en concreto, para componentes críticos del sistema operativo, pero sin necesidad de llevar a cabo una actualización completa (u OTA) del mismo, sino empleando el modelo de actualizaciones parciales de las apps, a través de Google Play. Para ello, Android 10 proporciona una serie de componentes con soporte para Mainline (como los *codecs* multimedia, el proveedor de seguridad de Java Conscrypt, el controlador de permisos, componentes de red y resolución DNS, etc.), con capacidad para recibir a través de APKs o APEX componentes y actualizaciones dinámicas que pasarán a formar parte del sistema operativo.



[28] https://fidoalliance.org/android-now-fido2-certified-accelerating-global-migration-beyond-passwords/



A comparison of security controls 2019

What was Compared?	iOS 11.2 OS	iOS 12.1.3 OS	Android 6 OS	Samsung Knox 2.6 Platform	Android 7 OS	Google Pixel (Android 7) Device	Samsung Knox 2.9 Platfrom	Android 8 OS	Google Pixel 2 (Android 8) Device	Android 9 OS	Google Pixel 3 (Android 9) Device	Samsung Knox 3.2 Platform	Chrome OS OS	Windows 10 (1709) OS	Windows 10 in S mode (1803) OS	Microsoft Surface Pro Device
Built-in Security																
Access Control by Default	2	2	2	2	2	2	2	2	2	2	2	2	3	2	2	2
Authentication Security	3	3	2	2	2	2	2	2	2	3	3	3	2	2	2	2
Device Encryption on by Default	3	3	2	3	2	3	3	2	3	3	3	3	3	2	3	3
File-Level Encryption	3	3	1	1	3	3	3	3	3	3	3	3	3	3	3	3
App Isolation	3	3	3	3	3	3	3	3	3	3	3	3	3	2	3	2
OS Updates	3	3	1	2	2	3	2	2	3	2	3	2	3	3	3	3
Security Updates	3	3	2	2	2	3	3	3	3	3	3	3	3	3	3	3
App Updates	1	1	3	3	3	3	3	3	3	3	3	3	3	2	3	2
App Privileges	3	3	3	3	3	3	3	3	3	3	3	3	3	1	3	1
Runtime App Permissions	3	3	2	2	2	2	3	3	3	3	3	3	3	2	3	2
Platform Integrity Protection	2	3	2	3	2	2	3	3	3	3	3	3	3	3	3	3
Root of Trust	3	3	1	3	2	3	3	3	3	3	3	3	3	3	3	3
Exploit Mitigation	2	3	2	3	2	2	3	2	2	3	3	3	3	3	3	3
Network Security	1	1	1	1	2	2	3	3	3	3	3	3	3	3	3	3
Network Encryption	2	2	1	1	2	2	2	2	2	2	2	2	2	1	2	1
Built-in Anti-Malware	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Secure Browsing	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Corporate-Managed Security																
Authentication Methods	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Authentication Policy Management	2	2	2	3	2	2	3	3	3	3	3	3	3	3	3	3
Encryption Management	3	3	2	3	3	3	3	3	3	3	3	3	3	2	2	2
Device/Corporate Wipe	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Workplace Isolation	2	2	2	3	2	2	3	3	3	3	3	3	3	3	3	3
Secure Key Store	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Jailbreak/Root Protection	2	3	2	3	2	2	3	3	3	3	3	3	3	NA	3	NA
App Vetting	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Enterprise App Store	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
App Monitoring and Control	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Secure Remote Access	2	2	2	3	2	2	3	2	2	2	2	3	2	3	3	3
Policy Management	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Remote Health Attestation	1	1	1	3	2	2	3	3	3	3	3	3	3	3	3	3

Source: Gartner 2019 via YouTube — 1 = Weak, 2 = Average, 3 = Strong — Recreated for educational purposes

A lo largo de los años se ha seguido alimentando el debate de qué plataforma móvil es más segura, existiendo la creencia generalizada de que iOS es probablemente la plataforma móvil más segura, y más adecuada a nivel corporativo o empresarial, debido al férreo control que Apple tiene sobre el ecosistema (hardware, sistema operativo, apps, servicios, etc.), que le permite disponer de mayor control y de una integración más directa entre todos los componentes. Sin embargo, en los últimos años el posicionamiento de Google dirigido a integrar su propio hardware (dispositivos móviles Pixel o chips de seguridad específicos como el Titan M; ver el informe anual de 2018 [Ref.- 10]) y el sistema operativo Android ha hecho que éste se sitúe al mismo nivel que iOS. El informe de Gartner de mayo de 2019 (bajo suscripción) así lo ratifica [Ref.- 49]. En el mismo se pretende cuantificar a través de 30 categorías el nivel, o postura, de seguridad ofrecido por defecto por el sistema operativo de las plataformas móviles, desde el diseño y en base a los controles de seguridad existentes, así como las capacidades de gestión empresariales que estas ofrecen. El informe refleja [Ref.- 49] (ver la tabla comparativa superior) el progreso desde Android 6 a Android 9, especialmente en los dispositivos Pixel de Google, junto a detalles de entornos Android específicos como Samsung Knox[29].

[29] https://image-us.samsung.com/SamsungUS/samsungbusiness/solutions/samsung-knox/pdf/Gartner-Report-Knox-3-2-Security-Controls-0611.pdf

Apple ha proporcionado en iOS desde sus comienzos capacidades de protección de la integridad del código, pero inicialmente, antes de iOS 9, sólo a nivel de software. En iOS 9 se introdujo KIP (*Kernel Integrity Protection*) a nivel del kernel en una primera versión software, v0, para monitorizar ciertas estructuras de memoria críticas del kernel frente a modificaciones. Estas capacidades han ido evolucionando con el tiempo (a través de diferentes versiones), por ejemplo mediante KIP v1 en el iPhone 7, con la integración de protecciones hardware entre la CPU y el kernel. Adicionalmente, el iPhone XS implementa KIP v2 [Ref.- 27], con nuevas garantías a nivel de hardware frente a modificaciones del kernel (debido a la estrecha integración entre hardware y software que maneja Apple en su ecosistema móvil), así como mecanismos de protección de memoria como PPL (Page Protection Layer, basado en KIP y APRR) para asegurar la integridad del código de las apps una vez verificado su código. Complementariamente, el control del flujo de ejecución en el procesador se gestiona desde iOS 12 con Pointer Authentication Codes (PAC) en ARM v8.3 (ver el informe anual del pasado año 2018 [Ref.- 10]), haciendo uso de 5 tipos de claves criptográficas en iOS. En iOS 13 PAC ha sido mejorado para proteger más componentes del sistema operativo [Ref.- 27] (como por ejemplo todas las extensiones del kernel, la gestión de excepciones, o el motor JIT de JavaScript), y el objetivo de Apple es extender estas protecciones a otras estructuras de datos sensibles (de alto valor), no sólo código o punteros, mediante una futura actualización de iOS 13.

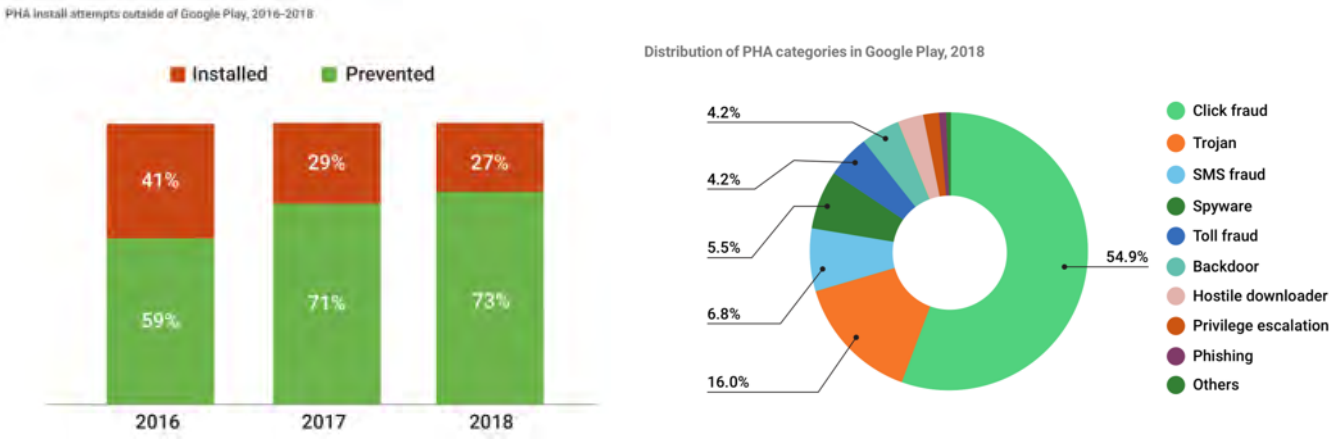
Finalmente, en el año 2019 Apple ha unificado su guía técnica oficial de seguridad de iOS en un nuevo y único documento que aglutina todos los aspectos de seguridad de sus diferentes plataformas y dispositivos, incluyendo tanto equipos tradicionales como móviles, y todos los sistemas operativos iOS, iPadOS, watchOS, tvOS y macOS. Es cada vez más común que tanto portátiles como dispositivos móviles compartan elementos de seguridad software y hardware como, por ejemplo, capacidades biométricas mediante Touch ID o los chips de seguridad como el SEP (Security Enclave Processor) en dispositivos móviles o el chip de seguridad T2 en portátiles [Ref.- 13]. La guía aborda la seguridad hardware, de sistema, la protección de datos mediante cifrado, a nivel de aplicaciones y de los servicios propietarios de Apple.

8. CÓDIGO DAÑINO PARA PLATAFORMAS MÓVILES

El software malicioso para dispositivos móviles, o malware móvil, sigue en constante evolución, identificándose numerosos especímenes a lo largo del año, tanto de malware como de spyware, cada vez más complejos y sofisticados. Los ejemplos detallados a continuación sólo constituyen una reducida muestra del amplio abanico de especímenes que son descubiertos cada año en campañas y operaciones activas para infectar a los usuarios. Desde una perspectiva más global, y tal como ha venido ocurriendo en el último par de años, los dispositivos móviles son uno más de los objetivos de las amenazas y el malware, identificándose campañas específicas tanto para Android como para iOS.

Desafortunadamente, al igual que ocurría el pasado año [Ref.- 10], en el momento de elaboración del presente informe, aún no se disponía del informe anual de seguridad del ecosistema Android para 2019, siendo el último publicado por Google en marzo de 2019 el del año 2018, "Android Security & Privacy 2018 Year in Review" [Ref.- 39], incorporando la privacidad junto a la seguridad como elemento clave del informe (en su 5ª edición, junto a la celebración de los 10 años de Android). Sin embargo, sí se dispone de un avance oficial de Google con las tendencias del malware móvil de 2019 [Ref.- 51] (detallado posteriormente).

En el mismo, Google ratifica (de manera similar a en años previos) que el ecosistema Android actual, con más de 2 billones de dispositivos activos en todo el mundo, dispone de un "bajo" índice de apps maliciosas, o PHAs (Potentially Harmful Applications), en Google Play frente a otros mercados de distribución de apps (con una tasa 8 veces mayor). Por este motivo, Google Play Protect (GPP) escanea todas las apps instaladas en un dispositivo independientemente de su origen, en global, unos 50 billones de apps escaneadas al día. En 2018, GPP previno la instalación de 1,6 billones de PHAs asociadas a mercados distintos a Google Play. Adicionalmente a las apps que ponen en riesgo los datos de usuario, como troyanos, spyware o apps de *phishing*, en 2018 se incluyó como categoría de PHAs las apps de fraude de anuncios y *clicks*, y GPP también notifica a los usuarios cuando identifica apps que deshabilitan mecanismos de seguridad de Android, como SELinux, o rootean el dispositivo (englobadas dentro de una categoría de apps deseadas por el usuario intencionadamente, *user-wanted* PHAs). Asimismo, Google introduce el concepto de software móvil no deseado (MUwS, Mobile unwanted Software), que recolecta identificadores o información sobre el usuario, las apps o el dispositivo. En 2019 Google anunció que por defecto GPP está activo en todos los dispositivos móviles Android, a través de la app Google Play Store[30].



La introducción del proyecto Treble [Ref.- 48] (ya descrito en el informe anual de 2017 [Ref.- 11]), y del programa de dispositivos Android empresariales recomendados por Google[31] (ya mencionado en el informe anual de 2018 [Ref.- 10]), parece empezar a dar sus frutos según Google, ya que en el último trimestre de 2018 las estadísticas de Google reflejan que un 84% más de dispositivos recibieron una actualización de seguridad con respecto al pasado año. Estas cifras sin embargo no llegan a reflejarse en la adopción de las nuevas versiones de Android, tal como se describe en el apartado "5. Adopción de

[30] https://security.googleblog.com/2019/02/google-play-protect-in-2018-new-updates.html
[31] https://www.android.com/enterprise/recommended/

las últimas versiones de los sistemas operativos móviles". Sin duda, se benefician de estas capacidades los dispositivos más modernos, tal como reflejan los datos de que en diciembre de 2018, un 95% de los Google Pixel 3 y 3 XL disponían de una actualización de seguridad publicada durante los últimos 90 días.

Algunas de las familias de malware móvil (PHAs) identificadas por Google incluyen: Snowfox, un SDK de anuncios que roba tokens OAuth, o realiza fraude de clicks, instalado más de 16 millones de veces. BreadSMS con unos 11 millones de instalaciones, la mayoría (98%) desde Google Play, que aprovecha el fraude por SMS y WAP, y con capacidades de ofuscación ante su análisis. Otros SDK de anuncios son View SDK (con 5,2 millones de instalaciones), CardinalFall (impactando a usuarios víctima de más de 10 países), FlashingPuma (distribuido principalmente fuera de Google Play), o Idle Coconut (enrutando adicionalmente tráfico de una VPN comercial a través de los dispositivos móviles víctima).

Por otro lado, Google ha intentado reducir la presencia de PHAs en software y apps pre-instaladas por parte de los fabricantes de los dispositivos desde fábrica, concretamente en sus imágenes del sistema operativo Android que incorporan los servicios de Google, previniendo la comercialización de 242 imágenes de Android contaminadas. Dentro de estas se encontraban familias como Cosiloon (pero en dispositivos Android no certificados) o Triada, junto a Chamois o EagerFonts. La primera de estas últimas con casi 200 millones de instalaciones, existiendo hasta 5 variantes de este malware, con capacidades para dificultar su análisis y que hace uso de servidores de comando y control (C&C) para gestionar sus acciones: fraude de anuncios y SMS o carga dinámica de código. La segunda de ellas es un SDK incluido en las apps de fuentes, presente en unos 12 millones de dispositivos de cientos de fabricantes y OEMs. De nuevo, hace uso de un servidor remoto para descargar plugins que ejecuta dinámicamente dentro de la app original, sin instalar nuevas apps maliciosas [Ref.- 39]. La existencia de PHAs pre-instaladas ha sido uno de los grandes cambios de tendencia de 2018, junto a la existencia de kits de desarrollo (SDK) con puertas traseras (*backdoors*), es decir, capacidades que permiten realizar muchas más acciones de las que el desarrollador era consciente (presentándose muy diversos escenarios). Como es de esperar, las estadísticas de Google ratifican que la presencia de PHAs en versiones más actuales de Android es menor, influenciadas por las nuevas capacidades, mejoras y restricciones de seguridad de Android 8 y 9.

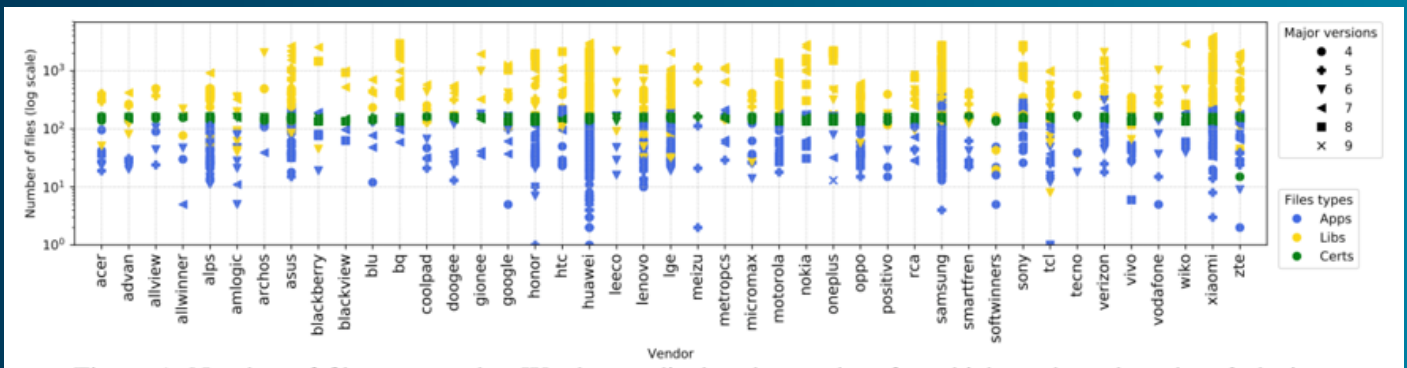


Figure 1: Number of files per vendor. We do not display the vendors for which we have less than 3 devices.

Esta amenaza de apps pre-instaladas maliciosas ya fue analizada en más detalle en el informe anual de 2018 [Ref.- 10], mencionándose ejemplos concretos como Adups o Riskware. Debe recordarse que el principal diferenciador de estas apps es que suelen disponer de permisos y privilegios de ejecución elevados a nivel del sistema. Tal como predecía dicho informe, esta tendencia de infección se materializó aún más a lo largo de 2019, con múltiples detalles de la realidad del ecosistema de apps pre-instaladas en Android reflejados en el estudio publicado en mayo de 2019 por múltiples investigadores, entre otros, de la Universidad Carlos III de Madrid [Ref.- 50]. La investigación, realizada a gran escala en dispositivos de más de 200 fabricantes, exponía la gran variedad de versiones y adaptaciones del sistema operativo Android publicadas por los fabricantes de dispositivos móviles, y las adaptaciones posteriores de los operadores de telecomunicaciones, así como todos los artefactos adicionales que son incorporados a las imágenes de fábrica, muchos de ellos con implicaciones directas en la privacidad del usuario, en la seguridad del dispositivo móvil, y con capacidades para la monitorización y recolección de datos de numerosas actividades del usuario. En resumen, el estudio refleja la ausencia de transparencia y control en qué componentes software residen en los dispositivos móviles Android que adquiere el usuario final.

Los dos principales vectores de entrada de las apps pre-instaladas maliciosas son su instalación desde fábrica, por que su creador consigue introducir la app en la cadena de suministro o fabricación del dispositivo móvil, o su distribución a través de actualizaciones OTA del sistema, no requiriendo ninguno de estos vectores la interacción por parte del usuario.

El avance oficial de Google respecto a las tendencias del malware móvil de 2019 publicado en febrero de 2020 [Ref.- 51], complementando el publicado en febrero de 2019[32], detalla cómo las estadísticas oficiales de Google Play Protect (GPP) indican que se escanean unos 100 billones de apps al día, un incremento notable (del doble) respecto al pasado año, previniendo la instalación de 1,9 billones de PHAs. En 2019 Google ha focalizado sus esfuerzos principalmente en proteger a los menores y las familias en Google Play [Ref.- 52], mediante las nuevas políticas publicadas en mayo de 2019 para los desarrolladores de apps Android (debiendo estos establecer una audiencia objetivo en sus apps, que incluya o no a menores, obligatoriamente desde el 1 de septiembre de 2019), y asegurando que las apps para menores proporcionan los contenidos adecuados, anuncios apropiados, y gestionan la información personal correctamente. En consecuencia, el proceso de revisión de este tipo de apps en Google Play (y de sus actualizaciones) se puede extender a 7 días, o incluso más.

Adicionalmente, se han tomado medidas para proteger la privacidad de los usuarios, especialmente en Android 10, con nuevos permisos o permisos más restringidos de cara a las apps, motivados entre otros por el Proyecto Strobe[33] (que dio lugar al cierre del servicio o red social Google+), y accesos más granulares por parte de las apps a la cuenta de Google del usuario y a su información [Ref.- 53]. El proceso de revisión

[32] https://android-developers.googleblog.com/2019/02/how-we-fought-bad-apps-and-malicious.html
[33] https://www.blog.google/technology/safety-security/project-strobe/

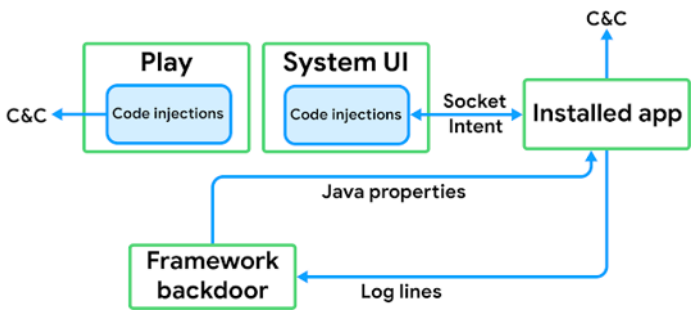
de las apps se ha intentado mejorar de cara a ofrecer más información a los desarrolladores de porqué una app es rechazada, y gestionar adecuadamente la suspensión o el bloqueo de cuentas de desarrolladores en Google Play.

Las nuevas políticas de Google Play han permitido reducir el número de apps que tienen acceso a los SMS y al histórico de llamadas del usuario, así como vetar casi 800 mil apps antes de su publicación con un proceso de revisión más estricto.

Finalmente, con el objetivo de luchar contra el malware móvil (apps maliciosas) de manera más global, a finales de 2019 se anunció la App Defense Alliance [Ref.- 54], un acuerdo entre Google, ESET, Lookout y Zimperium para colaborar con la industria en la detección temprana de nuevas amenazas y la identificación de PHAs, bloqueando su publicación en Google Play. Para ello, se están integrando en GPP los motores de detección de los diferentes colaboradores, proporcionando cada uno de ellos una evaluación del riesgo para cada app que debe ser publicada. Los diferentes motores combinan *machine learning*, junto a técnicas de análisis estático y dinámico, para detectar comportamientos anómalos. Google espera que el uso de diferentes heurísticas mejore la eficiencia de detección de apps maliciosas.

En enero de 2019 Google comenzó la publicación de una serie de artículos destacando familias concretas de malware móvil, o PHAs, denominados "PHAs Family Hightlights". La primera familia que fue descrita es Zen [Ref.- 55], un malware que hace uso de privilegios de root para crear un servicio que crea cuentas de usuario de Google falsas, mediante el abuso de los servicios de accesibilidad. Para obtener permisos como root, Zen hace uso de un troyano en su cadena de infección, intentando obtener persistencia a través de la partición de sistema (en dispositivos móviles Android que no disponen de las protecciones de Verified Boot). No se profundiza en los detalles de esta familia para proceder a describir a continuación otras familias que han sido publicadas más recientemente.

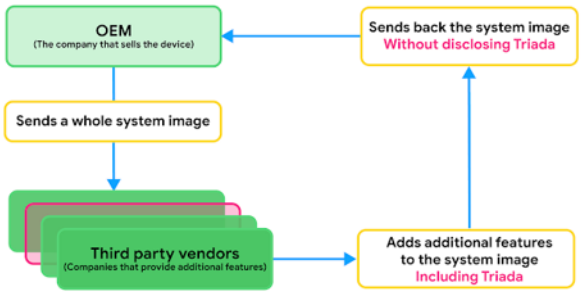
Una de las familias de malware móvil destacadas por Google a mitad de 2019 fue Triada [Ref.- 56], conocida desde 2016, y centrada en la instalación de apps de spam[34] para el envío de mensajes no solicitados a los contactos del usuario, o para el envío de e-mails no solicitados. Estas apps adicionalmente muestran anuncios, mecanismo empleado por los atacantes para monetizar este esquema de infección. Adicionalmente, Triada inyectaba código en los navegadores web para sustituir los anuncios legítimos por otros que beneficiaran financieramente a sus autores. Las comunicaciones entre el malware y los servidores de comando y control (C&C) estaban cifradas mediante mecanismos propietarios (doble XOR con dos claves diferentes); este cifrado también era empleado para ofuscar *strings* por parte de la app.



[34] https://developers.google.com/android/play-protect/phacategories#spam

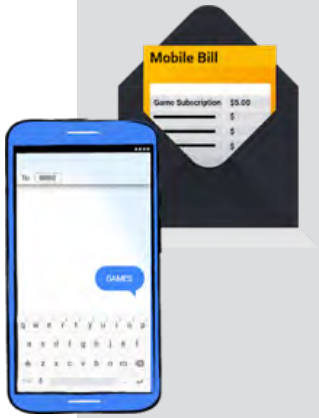
Inicialmente Triada actuaba como un troyano con capacidades para rootear los dispositivos móviles víctima (habitualmente antiguos), ocultando sus actividades mediante la obtención de código dinámicamente y mediante la instalación de otras apps, y evolucionando (en el verano de 2017) a ser una puerta trasera pre-instalada en las imágenes de sistema operativo de algunos fabricantes, y que se ejecutaba cada vez que cualquier app hacía uso del log de Android, pudiendo ejecutar con los privilegios y en el contexto de dicha app [Ref.- 56]. Su principal objetivo eran SystemUI como app del sistema, y la app de Google Play, para poder gestionar e instalar nuevas apps. Asimismo, las nuevas apps podían comunicarse con la puerta trasera a través del log de Android, empleando una etiqueta y mensaje específicos, empleando un mecanismo de comunicación encubierto bastante complejo (ver imagen previa), ya que las respuestas se realizaban a través de propiedades de Java dentro del contexto de la app objetivo. La evolución de Triada en el tiempo confirmó la aplicación de buenas prácticas de la industria por parte de sus autores, por ejemplo, pasando de usar MD5 a SHA1.

Las infecciones en las imágenes de sistema operativo de algunos fabricantes parecen estar asociadas a la interacción con terceros, que deben proporcionar la integración de ciertos componentes hardware o funcionalidades, para lo cual requieren realizar modificaciones en la imagen completa de sistema operativo. Se identificaron como origen de algunas infecciones fabricantes bajo el nombre de Yehuo o Blazefire.



A principios de enero de 2020 Google también destacaba la familia de malware móvil Bread [Ref.- 57], centrado en sus orígenes (2017) en fraude vía SMS, y que ha ido evolucionando a lo largo de los años para adecuarse a las nuevas restricciones de Google Play (como por ejemplo las limitaciones en el envío de SMSs por parte de las apps), intentando ofuscar y ocultar su comportamiento malicioso para no ser detectado. Las variantes más recientes se han centrado en el fraude a través de pagos o facturación mediante WAP, es decir, servicios de pagos móviles proporcionados por los operadores de telecomunicaciones a través de páginas web, autentificando al usuario mediante la red móvil de datos y su número de teléfono. El proceso de pago verifica el dispositivo móvil involucrado, pero no es necesaria la intervención del usuario, por lo que el esquema de fraude tiene éxito. El malware ha ido evolucionando para acomodar distintos flujos de pago de diferentes operadores móviles, incluyendo incluso la resolución de CAPTCHAS básicos. Tras verificar el operador móvil utilizado por el dispositivo, se descarga del servidor de comando y control (C&C) la configuración del flujo adecuado para el mismo y que contiene en JavaScript la serie

de pasos (accesos a diferentes URLs y su secuencia correcta) que se deben ejecutar. Si la app no dispone de soporte para el operador de la víctima, oculta sus actividades maliciosas y tiene un comportamiento benigno, para pasar desapercibida.

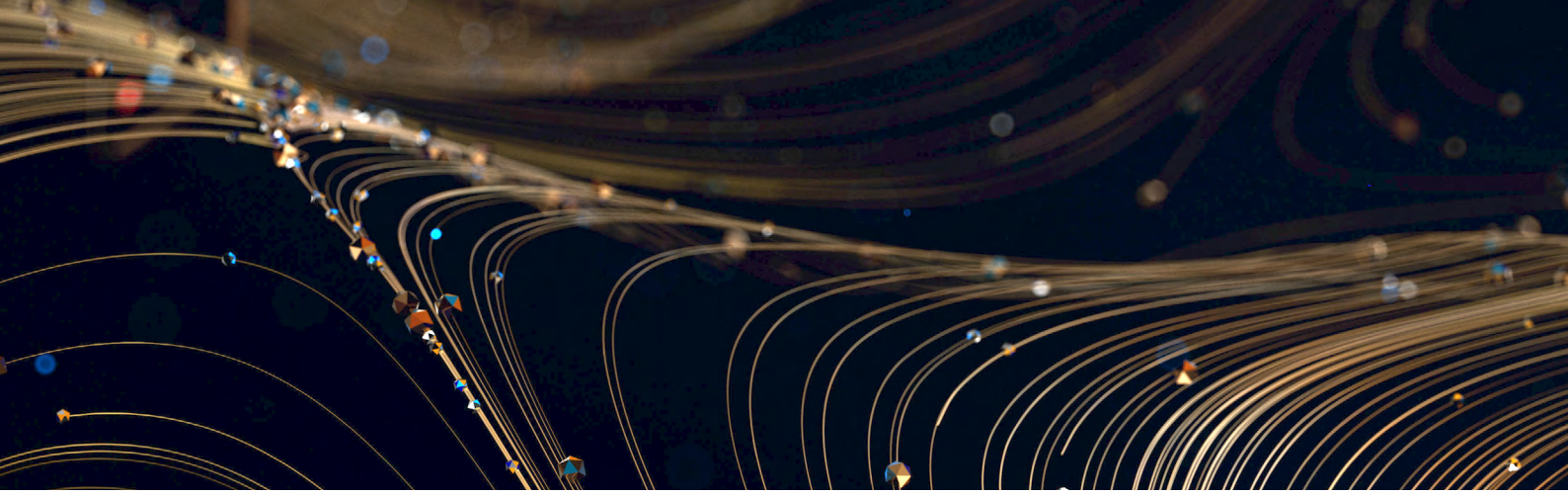


Dentro de las técnicas de ofuscación de este malware móvil se hace uso de cifrado, estándar (AES, Blowfish o DES), propietario (XOR), o de fragmentos y concatenación de cadenas de caracteres y de delimitadores, para ocultar sus *strings* [Ref.- 57]. Adicionalmente se ofuscan las llamadas a las librerías de Android (APIs) relacionadas con el fraude SMS o de servicios de pagos móviles mediante reflexión de Java, código nativo (JNI) o código JavaScript en WebViews, invocado desde los interfaces con Java existentes en Android. Bread es a su vez empaquetado en ocasiones con packers comerciales, como Qihoo360, AliProtect o SecShell. En los momentos de más actividad de esta campaña se han llegado a identificar hasta 23 variantes diferentes de la familia Bread subidas a Google Play a lo largo de un mismo día.

El lector interesado dispone de más detalles respecto a otras campañas móviles de infección que han sido descubiertas a lo largo del año 2019, por ejemplo, asociadas al phishing móvil [Ref.- 89], así como de los informes generales de tendencias y del panorama global del malware móvil de principios y mediados de 2019 de CrowdStrike [Ref.- 91], Positive Technologies [Ref.- 92], McAfee [Ref.- 93], Zimperium [Ref.- 94], o Wandera [Ref.- 95], entre otros[35].

A continuación se analizan vulnerabilidades más críticas de ambas plataformas móviles, Android e iOS, que han sido identificadas a lo largo de 2019 por haber sido utilizadas en ataques reales. En octubre de 2019 Google publicó la existencia de una vulnerabilidad de escalada de privilegios local (CVE-2019-2215), de tipo UAF (use-after-free), en el Binder del kernel de Android [Ref.- 58], junto al parche asociado. La misma permite obtener los máximos privilegios en un dispositivo vulnerable y parece que había estado siendo utilizada en ataques reales como 0-day dentro de la solución Pegasus de NSO Group. Incluso Android 10 con los parches de septiembre de 2019 estaba afectada, de ahí la máxima prioridad que se le dio a la hora de solucionarla. Curiosamente, pese a su impacto en la seguridad de Android, la vulnerabilidad venía heredada del kernel de Linux desde noviembre de 2017, pero no había sido etiquetada como un bug de seguridad, por lo que no había sido solucionada previamente ni había acabado en los boletines oficiales de seguridad de Android y, por tanto, no había sido aplicada globalmente en todas las versiones de Android existentes a través de los niveles de parches de seguridad correspondientes.

[35] La obtención de algunos de estos informes requiere de registro gratuito.



A mediados del año 2019, en concreto en el mes de julio, dos investigadores del Proyecto Zero de Google anunciaron la existencia inicialmente de 6 vulnerabilidades diferentes que permitían la realización de ataques sobre dispositivos móviles iOS sin la interacción del usuario, y que podían ser explotadas a través de la app iMessage [Ref.- 60]. Estas vulnerabilidades venían a confirmar sospechas previas sobre las capacidades de explotar dispositivos iOS remotamente a través de vulnerabilidades no publicadas en iMessage y utilizadas en ataques reales como el "Karma Hack", debido al nombre de la herramienta o plataforma empleada, Karma, aprovechada por una unidad de operaciones conocida como "Project Raven" (posteriormente trasladada a DarkMatter), compuesta por ex-hackers y ex-oficiales de inteligencia del gobierno Americano y la NSA, y creada por los Emiratos Árabes Unidos (UAE) [Ref.- 59] para monitorizar y espiar a cientos de objetivos (en una intensa competición por conseguir ciberarmas en Oriente Medio entre UAE, Arabia Saudí y Qatar, supuestamente en poder de unas pocas naciones como USA, Rusia y China). Karma permitía obtener acceso remoto a los dispositivos móviles iOS de los objetivos simplemente proporcionando el número de teléfono o la dirección de e-mail de la víctima, sin la intervención del usuario, potencialmente explotando vulnerabilidades en iMessages o Mail, al menos, durante los años 2016 y 2017.

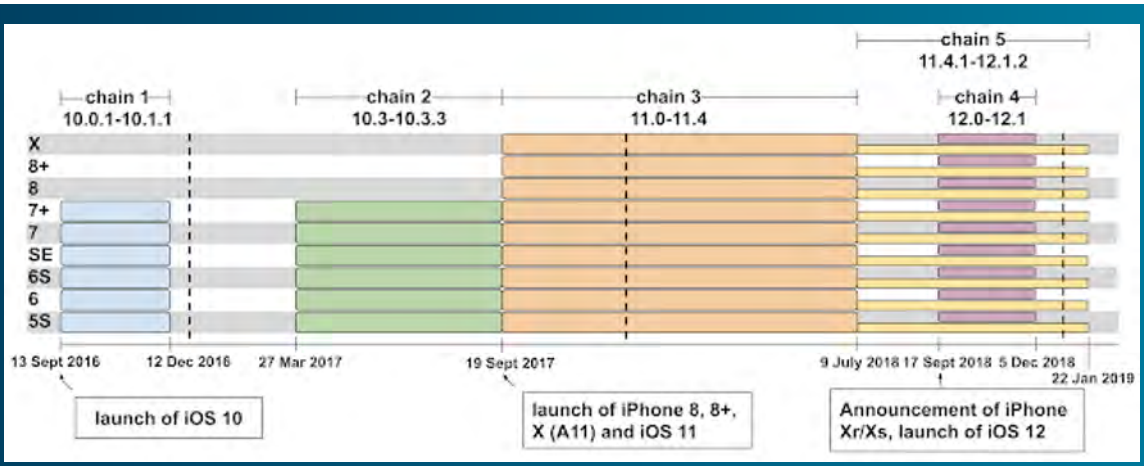
En su conjunto, el valor de estas vulnerabilidades en brokers o intermediarios en la venta de vulnerabilidades de seguridad se estimó por encima de los 5 millones de dólares, en base a los precios oficiales en aquel momento de brokers como Zerodium o Crowdfense. Cuatro de estas vulnerabilidades permitían la ejecución remota de código mediante el envío de un mensaje malformado al dispositivo móvil víctima, mientras que las otras dos permitían la extracción de información. Todas las vulnerabilidades fueron solucionadas por Apple en la actualización a la versión 12.4 de iOS [Ref.- 61], una actualización crítica debido a las numerosas y variadas vulnerabilidades de seguridad que solucionaba. Debido a que la versión 12.4 no solucionaba completamente las vulnerabilidades, los detalles técnicos no fueron publicados hasta posteriormente, una vez que se solucionó la vulnerabilidad CVE-2019-8641 en la versión 12.4.2[36] de iOS a finales de septiembre de 2019 y en iOS 13 a mediados del mismo mes (actualización que únicamente solucionaba esta vulnerabilidad de seguridad debido a su criticidad).

La relevancia de estas vulnerabilidades fue complementada con las correspondientes pruebas de concepto (PoCs), la presentación llevada a cabo por los investigadores en Black Hat USA en agosto de 2019 [Ref.- 62] y por diferentes artículos del Proyecto Zero publicados ese mismo mes [Ref.- 63], centrados en resaltar los potenciales vectores de ataque remotos en iOS a través de SMS, MMS, mensajes de voz,

[36] https://support.apple.com/es-es/HT210590

iMessage e e-mails y, específicamente, de la vulnerabilidad CVE-2019-8646 de iMessage [Ref.- 64], que permitía la lectura remota de ficheros de un dispositivo iOS víctima (mediante la concatenación de una serie de bugs en iOS). Los detalles técnicos publicados se centran en la superficie de ataque remota de los dispositivos móviles, empleando mecanismos de comunicación tan habituales como los SMS, que también han sido analizados para Android en otras publicaciones del año 2019 [Ref.- 65], e-mails o mecanismos propietarios de mensajería, como iMessage. Fue este mecanismo el principal objetivo de otros análisis más en profundidad y del descubrimiento de diferentes vulnerabilidades, debido a su integración a bajo nivel en iOS y con SpringBoard, su exposición a través de extensiones y *plugins* hacia otras apps, las numerosas operaciones de deserialización y procesamiento de mensajes, etc., dando lugar finalmente a un total de 10 vulnerabilidades distintas.

Complementando sus propias investigaciones de vulnerabilidades, otra unidad conocida como TAG (Threat Analysis Group) del Proyecto Zero de Google publicó también en agosto de 2019 una serie de artículos [Ref.- 67] detallando diferentes cadenas de explotación sobre iOS que habían sido identificadas en el mundo real, y utilizadas a través de sitios web comprometidos y utilizados como vector inicial de ataque (o *watering whole*) contra sus visitantes mediante exploits de día cero (0-day), o desconocidos hasta ese momento, para iOS. Las campañas identificadas no empleaban ataques dirigidos contra víctimas específicas, sino ataques masivos contra todos los visitantes, estimados en miles cada semana. En el caso de tener éxito con cualquiera de las cinco cadenas de explotación identificadas, dirigidas a diferentes versiones de iOS 10, 11 y 12, durante un periodo continuo de unos 2 años (lo que demuestra el interés y esfuerzo existente detrás de estas campañas ofensivas), se instalaba un implante para la monitorización remota de los dispositivos móviles afectados y de las actividades privadas de sus propietarios.

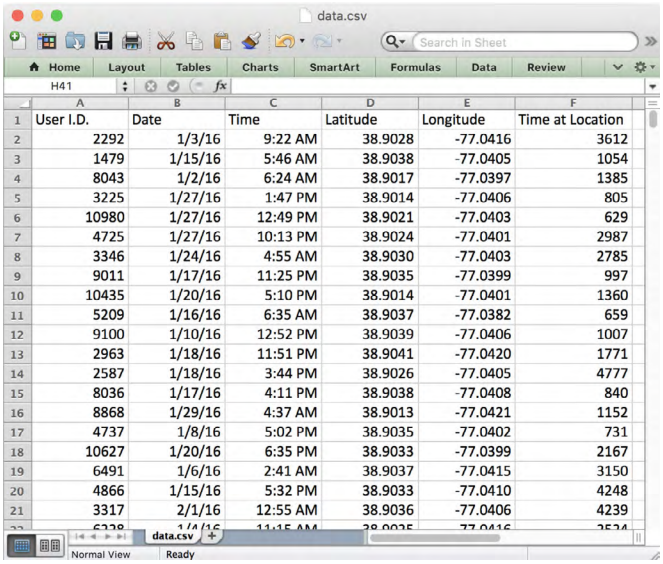


Las cinco cadenas de explotación suman un total de 14 vulnerabilidades que afectan al navegador web Mobile Safari, al kernel o técnicas para escapar del sandbox (o entorno restringido de ejecución) de una app, notificadas y corregidas por Apple en febrero de 2019. Los artículos publicados detallan los elementos técnicos de las cinco cadenas de explotación, del implante utilizado en los ataques reales y de los exploits de navegador web utilizados como vector de entrada inicial.

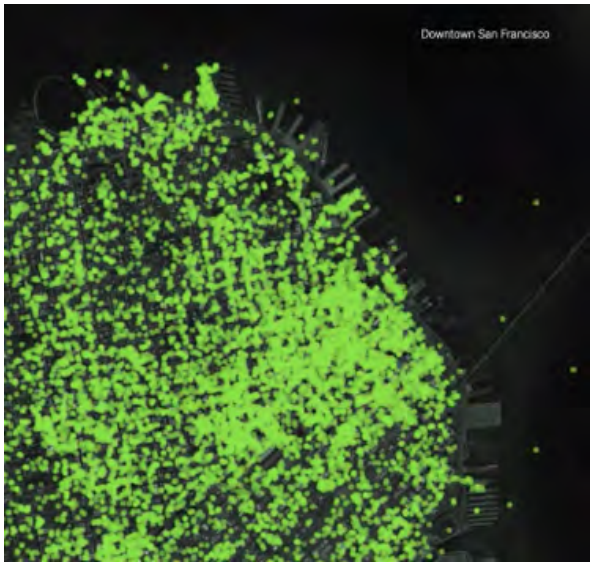
9. PRIVACIDAD DEL USUARIO EN LAS PLATAFORMAS MÓVILES

Complementando los análisis de las innumerables capacidades de la plataformas móviles, Android e iOS, y sus servicios en la nube asociados, para monitorizar las actividades de sus usuarios, vulnerando su privacidad, y los escándalos de casos públicamente conocidos que han afectado a la privacidad de los usuarios en 2018, como el de la app de actividad física y deportiva Strava, tal como se detallaba en el informe anual de 2018 [Ref.- 10], es importante destacar el estudio realizado por el New York Times (NY Times) a finales de 2019 dentro de su proyecto de privacidad o The Times Privacy Project . En el mismo [Ref.- 68], se refleja como los datos de geolocalización de decenas de millones de usuarios son almacenados por múltiples compañías (pertenecientes específicamente a una industria que comercializa los datos de ubicación de los usuarios, *location tracking industry*), sin ningún tipo de regulación o escrutinio, en ficheros de datos enormes que permiten monitorizar sus movimientos mediante sus dispositivos móviles. Un ejemplo de uno de esos ficheros (que no había sido obtenido de un operador de telecomunicaciones ni de un gigante tecnológico de la industria), perteneciente a un periodo de varios meses entre 2016 y 2017, contiene más de 50 billones de datos de localización, pertenecientes a más de 12 millones de ciudadanos americanos, y facilita su seguimiento en ciudades Washington, Nueva York, San Francisco o Los Ángeles. Este tipo de información permite identificar qué usuarios acceden a qué propiedades, identificando sus residencias o relaciones con los propietarios, y a muchos otros lugares, que desvelan de forma precisa muchos detalles de su vida (incluyendo famosos, gente influyente y VIPs). Se debe tener en cuenta que la información de ubicación es solicitada y procesada por numerosas apps, desde apps de información meteorológica, a apps de noticias, de cupones de descuento, ocio, restauración, etc. El estudio proporciona multitud de ejemplos particulares de ciudadanos que han sido identificados, con nombres y apellidos, simplemente mediante el análisis de los datos recolectados y contenidos en el fichero previamente mencionado.

[37] https://www.nytimes.com/privacy-project



	A	B	C	D	E	F
1	User I.D.	Date	Time	Latitude	Longitude	Time at Location
2	2292	1/3/16	9:22 AM	38.9028	-77.0416	3612
3	1479	1/15/16	5:46 AM	38.9038	-77.0405	1054
4	8043	1/2/16	6:24 AM	38.9017	-77.0397	1385
5	3225	1/27/16	1:47 PM	38.9014	-77.0406	805
6	10980	1/27/16	12:49 PM	38.9021	-77.0403	629
7	4725	1/27/16	10:13 PM	38.9024	-77.0401	2987
8	3346	1/24/16	4:55 AM	38.9030	-77.0403	2785
9	9011	1/17/16	11:25 PM	38.9035	-77.0399	997
10	10435	1/20/16	5:10 PM	38.9014	-77.0401	1360
11	5209	1/16/16	6:35 AM	38.9037	-77.0382	659
12	9100	1/10/16	12:52 PM	38.9039	-77.0406	1007
13	2963	1/18/16	11:51 PM	38.9041	-77.0420	1771
14	2587	1/18/16	3:44 PM	38.9026	-77.0405	4777
15	8036	1/17/16	4:11 PM	38.9038	-77.0408	840
16	8868	1/29/16	4:37 AM	38.9013	-77.0421	1152
17	4737	1/8/16	5:02 PM	38.9035	-77.0402	731
18	10627	1/20/16	6:35 PM	38.9033	-77.0399	2167
19	6491	1/6/16	2:41 AM	38.9037	-77.0415	3150
20	4866	1/15/16	5:32 PM	38.9033	-77.0410	4248
21	3317	2/1/16	12:55 AM	38.9036	-77.0406	4239

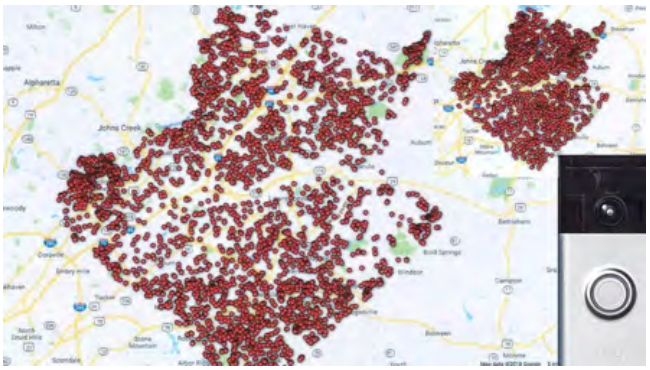


Es interesante reflexionar como hemos aceptado como sociedad a nivel global que cualquier ciudadano, a partir de los 12 años de edad (o incluso antes), lleve encima consigo un dispositivo de seguimiento, los dispositivos móviles, que permite conocer su ubicación las 24 horas del día, y sin que ningún gobierno se lo imponga, cediendo dicha información a compañías de las que no conocen ni su existencia. Las actividades para recolectar y vender esta información de seguimiento de personas siguen siendo legales hoy en día en muchos países. Un patrón de identificación muy habitual basado únicamente en dos ubicaciones es el asociado al hogar y a la oficina de un usuario, sin incluir el colegio de los hijos, ya que no es común que ambos se repitan simultáneamente, siendo prácticamente imposible anonimizar los datos, por mucho que los servicios traten de tranquilizar a los usuarios con este tipo de mensajes. En ocasiones, adicionalmente la información de localización se comercializa junto con identificadores de las plataformas de anuncios, lo que facilita la identificación de los usuarios, y otros datos personales, de manera más precisa. Esta información, a su vez, permite establecer relaciones entre las actividades online de los usuarios y sus actividades en el mundo real.

Otro de los grandes escándalos de 2019 asociado a la privacidad de los usuarios, en relación con las apps y servicios móviles, y con el Internet de las Cosas (IoT), fue el de los timbres inteligentes y cámaras de seguridad de Ring (compañía adquirida por Amazon en febrero de 2018 por aproximadamente 1,5 billones de dólares). La Electronic Frountier Foundation (EFF) [Ref.- 69], al igual que muchos otros medios como Motherboard [Ref.- 70], difundió en agosto de 2019 los riesgos y recomendaciones de seguridad y privacidad oportunos para que los usuarios fuesen plenamente conscientes de las implicaciones en su privacidad al hacer uso de este tipo de dispositivos y servicios, especialmente si no han sido configurados y restringidos convenientemente por alguien con los conocimientos adecuados.

Los vídeos grabados por las cámaras, al accionarse el timbre o detectarse movimiento, eran distribuidos al dispositivo móvil del usuario, pero también a la nube de Amazon, y a los departamentos de la policía local en USA, facilitando la monitorización completa de vecindarios enteros (desvelando la existencia

de estrechas relaciones y acuerdos entre ambas instituciones, Amazon y las fuerzas de orden público, sin ninguna transparencia y con implicaciones de privacidad y comerciales, incluyendo incentivos económicos o incluso subvencionando parte del coste de las cámaras con dinero estatal[38]). Las apps para establecer redes sociales locales en el vecindario y conocer y discutir que está ocurriendo en los alrededores, acceder a las últimas noticias y tendencias locales, notificar comportamientos sospechosos, especialmente relacionados con el crimen, la seguridad y la protección del barrio, como Neightborgs (Amazon), Nextdoor o Citizen, han demostrado su intrusismo en la privacidad de los vecinos, así como casos de racismo y xenofobia. Algunas de estas apps se han extendido y promocionado también localmente en España, a través de mensajería postal, no únicamente en USA. Sorprendió a la opinión pública el acceso sin limitaciones, ni regulación, con ilimitados derechos (según los términos del servicio), del que disponían Amazon y cientos de agencias de policía estadounidenses[39] (sin autorización judicial) a todos los contenidos, grabaciones y vídeos, incluyendo su localización proporcionada a través de un mapa local, adquiridos a través de estas cámaras a través de la plataforma en la nube de Amazon. Incluso los ciudadanos que no hacen uso de estas cámaras serán monitorizados a través del creciente número de cámaras instaladas por sus vecinos, creando un sistema masivo de vigilancia de vídeo. Como consecuencia de todos estos descubrimientos y fallos de seguridad, en febrero de 2020 Ring anunció actualizaciones en su app móvil y servicios que proporcionaban al usuario un mayor control sobre su privacidad y seguridad, incluyendo sus datos y sus dispositivos, a través de un nuevo centro de control [Ref.- 96].



Colateralmente, Ring sufrió en diciembre de 2019 un incidente de seguridad que permitió el acceso a los datos de más de 3.600 usuarios, así como su suplantación en la plataforma[40], mediante la obtención de sus credenciales de acceso a través de los volcados de usuarios y contraseñas asociados a otros incidentes de seguridad, enfatizándose la importancia de no reutilizar contraseñas entre diferentes servicios. Los

[38] https://www.vice.com/en_us/article/d3ag37/us-cities-are-helping-people-buy-amazon-surveillance-cameras-using-taxpayer-money
[39] https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/?arc404=true
[40] https://www.eff.org/deeplinks/2019/12/ring-throws-customers-under-bus-after-data-breach

últimos detalles técnicos de todos estos casos asociados al servicio Ring de Amazon desvelan como la app Ring para Android hace uso de hasta cuatro soluciones de seguimiento y monitorización de compañías de análisis de datos y marketing (Branch, MixPanel, AppsFlyer y Facebook, junto a Crashlytics) para recabar información personal del usuario, incluyendo nombres, direcciones IP privadas, operador móvil, identificadores persistentes y datos de los sensores del dispositivo móvil, permitiendo obtener una huella identificativa del mismo [Ref.- 71]. Adicionalmente, se dispone públicamente de numerosas y detalladas noticas describiendo este caso, así como numerosos otros casos de intrusiones a estos dispositivos IoT, incluyendo las grabaciones de vídeo de las cámaras de hogares y familias que no son conscientes de que sus dispositivos han sido accedidos ilegalmente y están siendo monitorizados[41].

[41] Basta con buscar en Internet por “ring hacked camera”.

10. COMUNICACIONES INALÁMBRICAS

AirDrop es un mecanismo propietario de Apple para el intercambio inalámbrico de ficheros y datos entre dispositivos Apple que hace uso de tecnologías Bluetooth Low Energy (Bluetooth LE o BLE) para el descubrimiento de dispositivos, y de tecnologías Wi-Fi extremo a extremo (sin un punto de acceso Wi-Fi) para la transferencia de información entre los dispositivos implicados, empleando posteriormente tráfico Bonjour (DNS) para el descubrimiento de servicios (como el servicio de AirDrop) y tráfico HTTP dentro de un túnel TLS con certificados digitales en ambos extremos para autentificar y cifrar las comunicaciones. Estos certificados están asociados a identidades relacionadas con la cuenta de iCloud de los usuarios [Ref.- 72]. Concretamente, AirDrop hace uso de un protocolo inalámbrico propietario de Apple denominado AWDL (Apple Wireless Direct Link)[42], que es empleado ampliamente para las comunicaciones entre dispositivos Apple, es decir, en más de un billón de dispositivos, tanto en AirDrop como en otros servicios de Apple como AirPlay o el desbloqueo de macOS mediante un AppleWatch.

En agosto de 2019 se publicó una extensa investigación de seguridad y privacidad, por parte de investigadores alemanes y estadounidenses, que resaltaba la existencia de múltiples vulnerabilidades en AirDrop, incluyendo AWDL y su integración con BLE, tanto a nivel de diseño como de implementación [Ref.- 73]. Entre estas vulnerabilidades se encontraba la posibilidad de llevar a cabo varios ataques de denegación de servicio (DoS), sobre las comunicaciones de AWDL y sobre los propios dispositivos móviles (causando que estos se reiniciasen), ataques de Man-in-the-Middle (MitM), permitiendo la interceptación y el reemplazo silencioso por parte de un atacante de los ficheros intercambiados mediante AirDrop, y ataques para el potencial seguimiento de usuarios. Estos últimos permiten la identificación de los usuarios a través de los mensajes intercambiados, potencialmente desvelando el nombre del propietario (a través del *hostname* del dispositivo), y permitiendo obtener la dirección MAC del AP Wi-Fi al que está conectado (BSSID) y la dirección MAC Wi-Fi real del dispositivo, incluso aunque el dispositivo Apple haga uso de una dirección MAC aleatoria. Múltiples vulnerabilidades[43] relacionadas fueron corregidas por Apple en iOS

[42] https://owlink.org/wiki/#what-is-apple-wireless-direct-link-awdl
[43] https://owlink.org/publications/

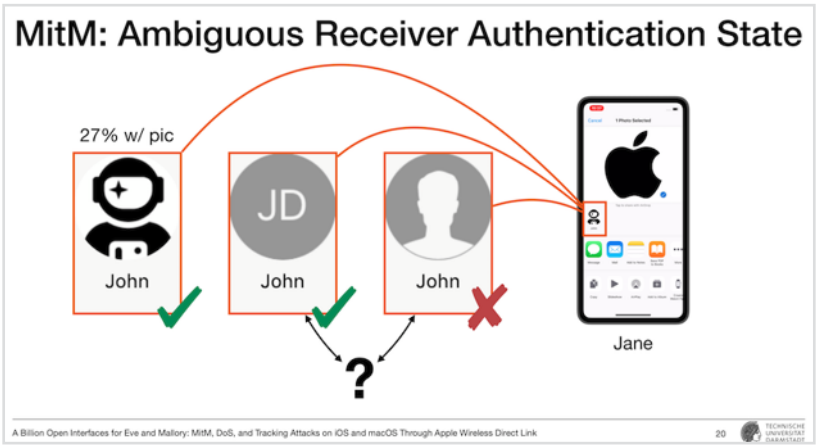
12.1 (DoS mediante tramas corruptas, CVE-2018-4368[44]), 12.2 (“activación” remota de AWDL vía BLE, sin CVE, y la obtención de la dirección MAC del interfaz Wi-Fi del dispositivo vía AWDL, CVE-2019-8567, en iOS 12.2, y del BSSID del AP Wi-Fi, CVE-2019-8620, en iOS 12.3) y 12.3 (DoS en las comunicaciones mediante desincronización, CVE-2019-8612), y en iOS 13.1 (revelación del *hostname*, CVE-2019-8799, pasando a ser un UUID aleatorio) y 13.2 (revelación de memoria, CVE-2019-8787, normalmente dentro del apartado de Wi-Fi), aunque la corrección de otras requiere rediseñar el servicio AirDrop, con las implicaciones de compatibilidad asociadas.

Específicamente para la vulnerabilidad de obtención de información y “activación” remota de AWDL, cuando se hace uso del icono para compartir contenidos en iOS, potencialmente a través de AirDrop (o a través del resto de mecanismos de compartición), el dispositivo emisor envía tramas BLE para notificar a los dispositivos cercanos. Según si estos admiten conexiones AirDrop de cualquiera o sólo de contactos, compartirán su información de identificación de vuelta con el emisor. Sin embargo, debido a que el identificador empleado en la fase de descubrimiento de AirDrop mediante BLE (detallado de nuevo posteriormente para otras investigaciones y vulnerabilidades), únicamente emplea los dos primeros bytes del SHA256 (short hash o hash corto) para los diferentes identificadores del usuario (AppleID, números de teléfono del usuario, y direcciones de e-mail; se permiten un máximo de 4 identificadores o hashes cortos) hace que sólo existan 65.536 posibilidades (16 bits). Por tanto, si un potencial atacante realiza un ataque mediante fuerza bruta y envía esos 65.536 valores posibles utilizando anuncios BLE, acción que puede ser completada en unos 30 segundos, cualquier dispositivo con AirDrop habilitado sólo para los contactos responderá indicando que ha identificado la petición como proveniente de uno de sus contactos. Cuantos más contactos tenga la victima en su dispositivo, mayor será la probabilidad de recibir antes un identificador que coincida con uno de ellos, reduciendo el tiempo necesario para completar el ataque.

Específicamente para la vulnerabilidad de MitM[45], en un escenario con dos dispositivos víctima que hacen uso de AirDrop sólo para sus contactos, un atacante puede llevar a cabo un ataque de DoS sobre el receptor para que no responda en la fase de descubrimiento, forzando a que el emisor no vea al destinatario y éste acabe permitiendo conexiones de cualquiera para intentar solucionar el problema. Como resultado, el emisor enviará el fichero al supuesto destinatario, no siendo consciente de que un atacante ha suplantado al destinatario con este ataque MitM, haciendo de intermediario (o *relay*), por lo que no sólo recibirá el fichero legítimo del emisor víctima, sino que además podrá reemplazarlo por un fichero diferente de cara al receptor, y lo más interesante para el atacante es que la previsualización del fichero en el receptor muestra el fichero original, aunque realmente se recibe el fichero reemplazado.

[44] https://www.youtube.com/watch?v=M5D9NeKapUo
[45] https://www.youtube.com/watch?v=5T7Qatoh0Vo

Desde el punto de vista de seguridad, para evitar este tipo de ataques se debe prestar especial atención a los iconos mostrados por el interfaz gráfico de usuario de iOS para AirDrop, de cara a confirmar si un usuario ha sido autentificado en el proceso: si se muestra la foto del contacto, su identidad ha sido validada, al igual que si se muestran las iniciales del contacto (debido a que el contacto no tiene una foto asociada). Sin embargo, si se muestra el icono genérico con la silueta de una persona en color gris y blanco, la identidad del otro usuario no ha sido verificada [Ref.- 72].

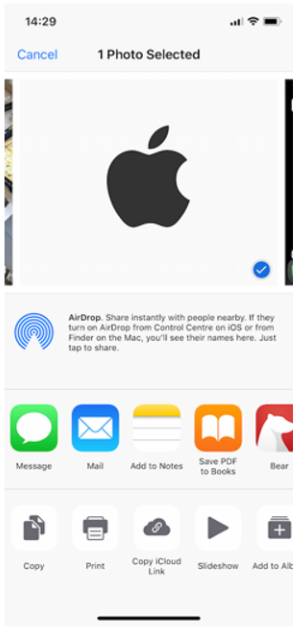


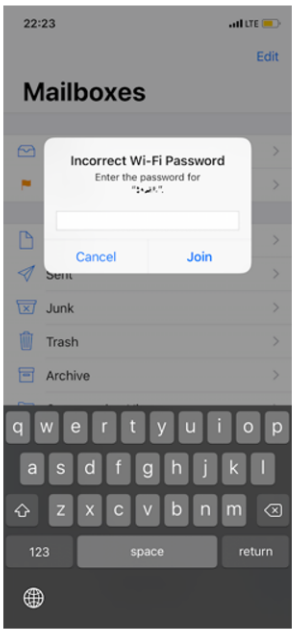
Circunstancialmente, en el año 2017 ya se publicaron investigaciones asociadas al descubrimiento automático de servicios que analizaban las implicaciones de privacidad, descubrimiento y autentificación en protocolos del Internet de las cosas (IoT), en concreto, analizando las debilidades de AirDrop [Ref.- 74]. Estas investigaciones han sido complementadas por otros estudios más recientes (de junio de 2019) centrados en el análisis desde el punto de vista de seguridad del protocolo Continuity de Apple, diseñado para proporcionar interoperabilidad y comunicaciones entre dispositivos Apple tradicionales (macOS) y móviles (iOS y iPadOS), también basado en Bluetooth LE [Ref.- 75]. En resumen, la conveniencia, facilidad de uso y fluidez en el intercambio de información entre dispositivos Apple tiene un alto coste en la privacidad y en la información sensible y datos de comportamiento que son desvelados (prácticamente de manera continua) a potenciales adversarios. La ausencia de detalles técnicos respecto al funcionamiento de AirDrop y AWDL, disponible desde 2014, parece haber centrado la atención de la comunidad de seguridad a lo largo del año 2019, intentando entender mejor su comportamiento y las debilidades en los mecanismos de seguridad existentes, dada la creciente preocupación al respecto teniendo en cuenta el amplio número de servicios que se basan en estas tecnologías dentro del ecosistema de Apple.

Como resultado de la investigación se dispone de documentación más detallada y código asociados a AWDL y a su implementación de código abierto Open Wireless Link (OWL) [Ref.- 76]. Debido a la adopción de AWDL por parte de la Wi-Fi Alliance dentro del estándar Neighbor Awareness Networking (NAN), también conocido como “Wi-Fi Aware”, potencialmente los dispositivos móviles Android también se podrían ver afectados por vulnerabilidades similares.

Las implicaciones de seguridad de servicios como AirDrop son cada vez más relevantes si se tiene en cuenta que cuando se dispone de iCloud activo, Apple ofrece la posibilidad de compartir credenciales a través de AirDrop con otros dispositivos, incluyendo el sitio web objetivo y el usuario y contraseña asociados. Estas capacidades sólo funcionan entre contactos (equivalente al modo sólo contactos), independientemente del modo en el que AirDrop esté configurado. Las credenciales recibidas, tras ser aceptadas por el usuario, son almacenadas en el dispositivo receptor en la Keychain de autorelleno de contraseñas del usuario [Ref.- 13].

En relación con las capacidades de Bluetooth, y también de AirDrop, de los dispositivos Apple, Hexway publicó una investigación en octubre de 2019, conocida como Apple Bleee y que afecta a iOS 10.3.1 o superior (aunque dependiente del modelo de dispositivo), que permite obtener información sobre el estado del dispositivo móvil (si está en *standby*, en la pantalla de bloqueo, en la pantalla principal, recibiendo una llamada, etc.) o detalles de otros dispositivos Bluetooth como la carcasa de los AirPods, el nivel de batería, nombre del dispositivo, estado del interface Wi-Fi (realmente AirDrop, encendido o apagado), versión de iOS e, incluso, conocer el número de teléfono móvil [Ref.- 77]. El análisis se centra en las comunicaciones Bluetooth LE (BLE) generadas por los dispositivos de Apple, tradicionales y móviles, y obtiene los cambios de estado e información a través de estas. Dado que AirDrop hace uso de un hash SHA256 del número de teléfono del usuario como identidad del remitente a la hora de enviar un fichero, es posible crear una base de datos de hashes para identificar potenciales números de teléfono de una ciudad o país concretos. En el caso de AirDrop, a diferencia de la compartición de contraseñas Wi-Fi descrita a continuación, durante la fase de identificación únicamente se envían mediante BLE los dos primeros bytes del SHA256 (short hash) para los diferentes identificadores del usuario: AppleID, números de teléfono del usuario, y direcciones de e-mail. Durante la fase de autentificación posterior, a la hora por ejemplo de enviar un fichero, se envía el hash SHA256 completo (long hash).






```
python ble_adv_search.py -m 54:69:F1:23:2B:47
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
...
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
[54:69:F1:23:2B:47] 0e02011a0aff4c0010050b1c0fc556
...
```

Por otro lado, desde la versión 11 de iOS es posible compartir contraseñas de redes Wi-Fi con otros usuarios. Para ello, una vez seleccionada la red Wi-Fi a la que se desea conectar el usuario, su dispositivo móvil comienza a emitir tramas BLE solicitando la contraseña a otros dispositivos cercanos. Para que los receptores puedan identificar al dispositivo o usuario solicitante, las tramas incluyen de nuevo un hash SHA256 del número de teléfono del usuario, del AppleID y del e-mail, así como del SSID de la red Wi-Fi. Sólo se envían los primeros 3 bytes de los hashes, pero estos permiten obtener el número de teléfono mediante servicios de consulta HLR (Home Location Register), junto al estado y región. Debido a que los dispositivos de Apple no solo envían, sino que también reciben y procesan tramas BLE, es posible manipular dichas tramas para suplantar a otros dispositivos Bluetooth (por ejemplo, AirPods, y los niveles de batería) u obtener la contraseña de una red Wi-Fi enviando solicitudes mediante la suplantación de un contacto. La contramedida de seguridad a aplicar para evitar el intercambio de toda esta información pasa por deshabilitar el interfaz de Bluetooth. Como resultado de esta investigación pionera, en 2019 se han publicado otras herramientas evolucionando las originales, como Airdrop Crazy [Ref.- 78].

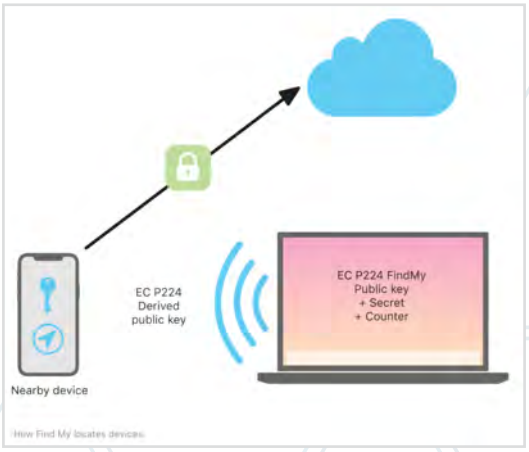
En diciembre de 2019 Apple corrigió en iOS 13.3 una nueva vulnerabilidad de denegación de servicio (DoS) asociada a AirDrop, denominada AirDoS [Ref.- 79], que permitía a un potencial atacante (haciendo uso de una herramienta de código abierto disponible públicamente) enviar ficheros de manera continua a todos los dispositivos en su área de alcance, especialmente si permitían la recepción de ficheros vía AirDrop por parte de cualquiera. Como resultado, el usuario del dispositivo víctima recibe el mensaje de confirmación para autorizar o no la recepción del fichero, bloqueándose el interfaz gráfico de usuario (GUI) y cualquier otra actividad que se esté llevando a cabo. Debido a que iOS, y iPadOS, no limitaba el número de peticiones de recepción de ficheros que podían ser procesadas, el atacante puede remitir estas peticiones de manera continua haciendo que se generen mensajes de autorización ilimitados, denegando el uso del dispositivo. El ataque podía ser mitigado deshabilitando el interfaz de Bluetooth y/o la funcionalidad de AirDrop en los dispositivos víctima, aunque una vez lanzado el ataque esta opción no era sencilla de llevar a cabo en la zona del ataque. La versión 13.3 soluciona la vulnerabilidad estableciendo un límite en el número de peticiones aceptadas en un breve espacio de tiempo (tras denegar el usuario la petición 3 veces, iOS automáticamente deniega el resto de peticiones), aunque Apple decidió no asignar un CVE a la misma ni reflejarla en el boletín oficial de seguridad de iOS/iPadOS 13.3[46] (aunque Apple sí menciona al investigador por su contribución).

Durante el año 2019, Apple introdujo en iOS 13 una innovadora opción para poder encontrar los dispositivos Apple que no disponen de conexión a Internet dentro de los servicios asociados a “Buscar” (o “Find My (iPhone, iPad, Apple Watch o Mac)” en inglés), denominada “Offline Finding” o “Encontrar sin conexión” [Ref.- 72], que permite la localización de un dispositivo perdido o robado aunque no disponga de conexión a una red de datos (Wi-Fi o móvil) [Ref.- 27]. Adicionalmente, iOS 13 unifica la funcionalidad de Find My iPhone y Find My Friends en una única app, Find My (*device*).

[46] https://support.apple.com/en-us/HT210785

Esta funcionalidad, anunciada inicialmente en la conferencia WWDC de junio de 2019 [Ref.- 80], y que requiere disponer de un segundo dispositivo vinculado al mismo Apple ID, ha sido diseñada con la privacidad y el anonimato en mente, con el objetivo de evitar que se pueda realizar un seguimiento de los usuarios y sus dispositivos perdidos (con iOS, iPadOS, macOS, etc.), y rastrear su localización, tanto mediante las señales Bluetooth como por parte de Apple, y que no se revele a Apple la identidad de los dispositivos que encuentran el dispositivo perdido, empleando mecanismos criptográficos complejos [Ref.- 13]. Para no comprometer el consumo de batería de los dispositivos implicados, la cantidad de datos intercambiados es mínima y se incluyen en otro tráfico de red de iCloud ya existente.

Para ello se hace uso de comunicaciones Bluetooth empleando identificadores dinámicos, en concreto claves públicas efímeras (de curva elíptica) que cambian o rotan a lo largo del tiempo (aproximadamente cada 15 minutos) y que son difundidas por el dispositivo perdido, ya que cualquier identificador estático permitiría realizar el seguimiento del dispositivo asociado. Los dispositivos Apple cercanos reciben dicha clave vía Bluetooth, obtienen su localización (es decir, la ubicación aproximada del dispositivo perdido) y una referencia horaria, la cifran con dicha clave, y transmiten la información cifrada a los servidores de Apple de iCloud [Ref.- 81]. Para identificar o vincular esos datos de localización con el dispositivo perdido se envían junto a un hash de la clave pública recibida por Bluetooth y utilizada para cifrarlos.



El propietario del dispositivo perdido puede posteriormente consultar a los servidores de Apple de iCloud mediante un segundo dispositivo vinculado al mismo Apple ID y obtener los datos cifrados. Para ello proporciona el hash de la clave pública como identificador para obtener sus datos de localización, que una vez descifrados con la clave privada asociada a dicha clave pública (en realidad, el conjunto de claves públicas yendo hacia atrás en el tiempo en intervalos de 15 minutos), y que es compartida entre todos los dispositivos vinculados al mismo Apple ID del usuario a través de iCloud (en concreto, mediante un canal cifrado extremo a extremo implementado a través de la iCloud Keychain), le permiten conocer la localización del dispositivo.

En relación con las tecnologías inalámbricas Bluetooth, la versión iOS 12.4 liberada en julio de 2019 solucionó la vulnerabilidad conocida como KNOB, Key Negotiation of Bluetooth Attack (CVE-2019-9506) [Ref.- 61], que permitía forzar, mediante un ataque MitM, a que la negociación de las conexiones Bluetooth haga uso de claves de cifrado débiles (de 8 bits o 1 byte), facilitando ataques de fuerza bruta [Ref.- 82]. Esta vulnerabilidad también fue resuelta en los parches de seguridad de Android de agosto de 2019, afectando desde Android 7 a 9, al igual que a muchos otros dispositivos Bluetooth de numerosos fabricantes. El impacto de esta vulnerabilidad fue muy elevado, ya que afectaba a la especificación de Bluetooth desde hace 12 años (no así a BLE) y, por tanto, a todos los dispositivos y chips compatibles que la implementaban. Su descubrimiento fue posible gracias a la existencia de nuevas herramientas Bluetooth de bajo nivel publicadas en 2018, como InternalBlue, que permiten interactuar con la capa de enlace de la tecnología Bluetooth (LMP, Link Manager Protocol).

Durante el año 2019 el mercado de productos con soporte para WPA3 (Wireless Protected Access 3) [Ref.- 66], el nuevo estándar de seguridad para redes Wi-Fi personales y empresariales ratificado y publicado en junio de 2018, y que fue ya introducido en el informe anual del pasado año [Ref.- 10], ha ido madurando. Prueba de ello es el soporte para WPA3 dentro del ecosistema móvil, más concretamente, en Android 10 e iOS 13 [Ref.- 83]. A principios de 2020 el número de productos certificados por la Wi-Fi Alliance con soporte para WPA3 disponibles es cercano a los 600[47], incluyendo dispositivos móviles de Oppo, Vivo, ZTE, Samsung, LG, Motorola, entre otros, junto a varios chipsets de Qualcomm. Sin embargo, los productos con soporte para Wi-Fi Easy Connect (o DPP), uno de los cuatro mecanismos principales anunciados originalmente en WPA3, sigue siendo muy limitado, con únicamente dos productos.

Android 10 [Ref.- 84] proporciona soporte para WPA3 personal (SAE, Simultaneous Authentication of Equals) y empresarial (modo 192 bits) y para Wi-Fi Enhanced Open (OWE, Opportunistic Wireless Encryption) [Ref.- 85], incluyendo el modo de transición de WPA2 a WPA3 y de redes abiertas a OWE. Sin embargo, iOS 13 [Ref.- 86] proporciona únicamente soporte para WPA3 personal (SAE) y empresarial, junto al modo de transición de WPA2 a WPA3.

Sin duda, este pasado año 2019 ha demostrado la relevancia desde el punto de vista de seguridad de las tecnologías inalámbricas en los dispositivos móviles, incluyendo Bluetooth, BLE, Wi-Fi y tecnologías propietarias derivadas de éstas, como AirDrop, así como las tecnologías móviles celulares (ver siguiente apartado). Esta tendencia parece que tendrá continuidad en el año 2020, y futuros años, tal como demuestra una nueva vulnerabilidad para Android publicada en febrero de 2020 (mes en la que fue solucionada por Google[48]), aunque descubierta en noviembre de 2019 por ENRW, denominada BlueFrag (CVE-2020-0022).

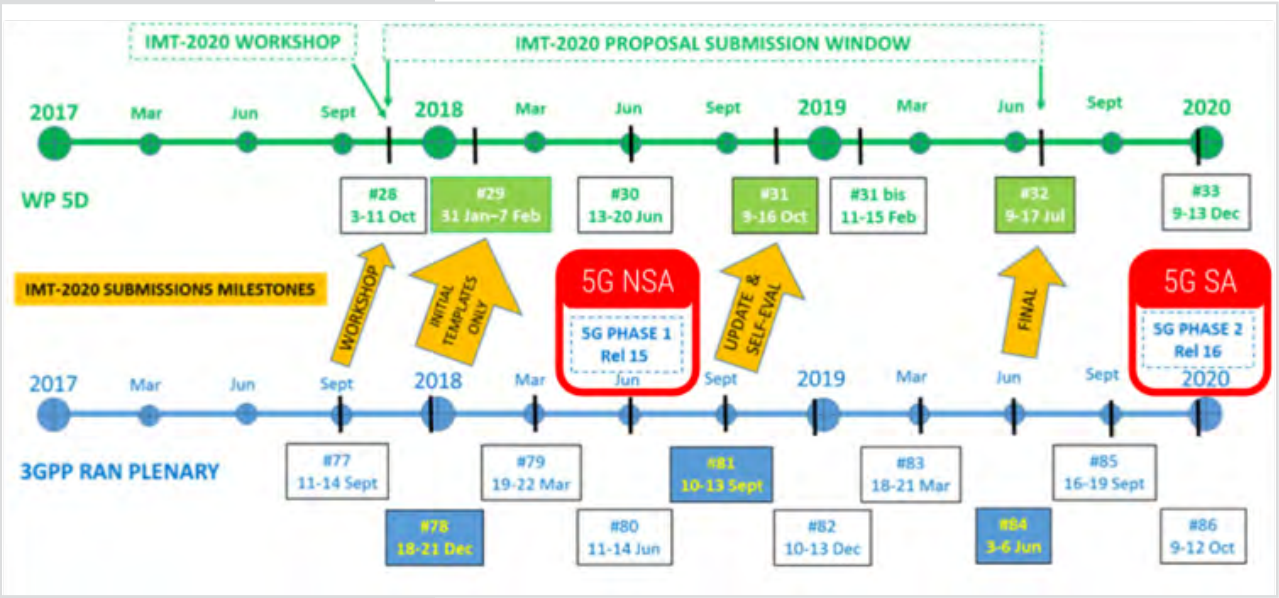
[47] https://www.wi-fi.org/product-finder-results?sort_by=certified&sort_order=desc&capabilities=16
[48] https://source.android.com/security/bulletin/2020-02-01.html

BlueFrag [Ref.- 87] permite la ejecución remota de código en dispositivos Android 8, 8.1 y 9, y realizar denegaciones de servicio (DoS) en Android 10. Para explotar esta vulnerabilidad no se requiere interacción por parte del usuario y lo único que se necesita es que el interfaz de Bluetooth esté activo y conocer la dirección Bluetooth (BD_ADDR, Bluetooth Address) del dispositivo víctima, haciendo que se asemeje mucho a la vulnerabilidad BlueBorne del año 2017.

11. COMUNICACIONES MÓVILES

Tal como se detallaba en el informe anual de 2018 [Ref.- 10] las tecnologías 4G o LTE (Long Term Evolution) siguen siendo el mecanismo de comunicación móvil o celular principal empleado hoy en día por los dispositivos móviles, pero 2019 se ha constituido como el año de comienzo de la transición a las tecnologías y redes 5G del futuro, cuya evolución continuará en 2020, y despegará definitivamente en el año 2021. El presente apartado profundiza en la evolución y riesgos de seguridad de las tecnologías 5G, así como en otros descubrimientos de seguridad del año 2019 en las comunicaciones genéricas de los dispositivos móviles, como apps de mensajería ampliamente utilizadas.

La tecnología 5G se está desplegando en dos fases: 5G NSA (Non-Standalone) o 5G no autónomo, una fase de transición que funciona sobre la infraestructura de las redes 4G+, y 5G SA (Standalone) o 5G completo, una fase de consolidación que hace uso de una nueva infraestructura 5G con un despliegue de antenas mucho más denso que el actual [Ref.- 97].



Desde el punto de vista de los dispositivos móviles, en 2019 ya se comercializaron algunos modelos con soporte para 5G, como el Samsung Galaxy S10 5G, LG V50 ThinQ, Xiaomi Mi 9 Pro 5G o el Xiaomi Mi MIX 3 5G, pero desafortunadamente, sólo para la modalidad NSA (hasta 2 Gbps de descarga), con los módems 5G Exynos 5100 o Snapdragon X50 (asociado al procesador Snapdragon 855). Por tanto, estos modelos no podrán ser utilizados en las redes 5G SA futuras (aunque potencialmente podrán mediante actualizaciones software del módem), que proporcionarán el prometido ancho de banda de descarga de 20 Gbps. Únicamente en 2019 el modelo Huawei Mate 20X era compatible con ambas fases gracias al módem Balong 5000. Los diferentes análisis realizados en medios tecnológicos generalistas[49] detallan como podría ser conveniente esperar hasta disponer de un despliegue más amplio de la red real 5G, SA, de cara a adquirir dispositivos con soporte completo 5G y poder sacarle todo el partido a esta tecnología.

Posteriormente, a principio de 2020 se han anunciado y/o comercializado modelos como el Samsung Galaxy S20 (y sus variantes)[50] con soporte para 5G, también NSA (aunque también se comercializan en modelos sin 5G más económicos), a través del procesador Exynos 990, y del módem 5G NSA multibanda Sub-6, es decir, por debajo de la banda de frecuencias de 6 GHz (denominado Exynos Modem 5123)[51]. El Xiaomi Mi 10 (y Pro) también incluye soporte 5G mediante el procesador Snapdragon 865[52], con un incremento significativo de su precio frente a sus predecesores, siendo el soporte para 5G uno de los argumentos. Este procesador, que proporciona soporte tanto para NSA como para SA, también es utilizado por el ZTE Axon 10s Pro o el Realme X50 Pro 5G (complementando el Realme X50 5G, o el OPPO Reno3 (Pro), ambos con Snapdragon 765G y el módem Snapdragon X52, también con soporte NSA y SA). El Honor View30 (Pro) también proporciona soporte 5G completo NSA y SA a través del procesador Kirin 990.

Desde el punto de vista de las redes móviles 5G, las preocupaciones de Europa y EEUU asociadas a la hegemonía de los elementos de red 5G por parte de fabricantes chinos como Huawei, con unos precios sin competencia, y la controversia con EEUU ya mencionada al inicio del presente informe, presentan implicaciones de seguridad incluso a nivel de la seguridad nacional de muchos países (llegándose incluso a involucrar la OTAN[53]). Estas se vieron alimentadas en 2019 por la publicación de documentos secretos que desvelaban las supuestas operaciones de Huawei para construir la red celular de Korea del Norte [Ref.- 98], con la potencial violación asociada de las leyes y controles de exportación americanos.

[49] https://www.xataka.com/tag/5g
[50] https://www.xataka.com/moviles/samsung-galaxy-s20-galaxy-s20-plus-caracteristicas-precio-ficha-tecnica
[51] https://www.xataka.com/componentes/exynos-990-exynos-5123-procesador-modem-5g-multibanda-7-nanometros-para-buques-insignia-samsung-2020
[52] https://www.qualcomm.com/products/snapdragon-865-5g-mobile-platform
[53] https://www.ituser.es/actualidad/2019/12/la-otan-se-compromete-a-garantizar-la-seguridad-de-5g

En el caso de España, complementando la primera convocatoria que Red.es lanzó en 2018, y cuya resolución se publicó en abril de 2019[54], el Consejo de Ministros autorizó en octubre de 2019 la segunda convocatoria de ayudas (45 millones de €) para el desarrollo de proyectos piloto de tecnologías 5G[55], junto a los avances necesarios en el plan técnico de la TDT (con la liberación de la banda de 700 MHz y el Segundo Dividendo Digital) para acomodar el desarrollo de las redes 5G en nuestro país[56].

Desde el punto de vista de seguridad y privacidad, la tecnología 5G es uno de los elementos más relevantes en la actualidad, ampliamente analizada por diferentes actores[57]. Los Estados miembros de la Unión Europea (UE) han llevado a cabo un análisis de los riesgos de seguridad de 5G, publicando un informe en octubre de 2019 (junto a ENISA) del que se ha hecho eco tanto el CCN-CERT como el DSN (Departamento de Seguridad Nacional) [Ref.- 99], concluyendo con la necesidad de llevar a cabo evaluaciones de los perfiles de riesgo de proveedores de 5G y la aplicación de restricciones a aquellos considerados de alto riesgo. Las medidas identificadas también consideran la exclusión de proveedores de la provisión de equipamiento y servicios a redes consideradas críticas o sensibles. También se recomienda diversificar entre distintos proveedores la compra de equipamiento y servicios. Esta evaluación de riesgos de las infraestructuras de red 5G se debe a la recomendación planteada por la Unión Europea en marzo de 2019, reflejada en el BOE en el caso de España [Ref.- 100].

El informe, basado en los resultados de las evaluaciones nacionales de riesgos en materia de ciberseguridad realizadas por todos los Estados miembros de la UE, determina los principales riesgos y amenazas, los activos más delicados, los principales puntos vulnerables, tanto técnicos como de otro tipo (como la interferencia de terceros países en la cadena de suministro), y una serie de riesgos estratégicos. El despliegue de las redes 5G podría conllevar una superficie mayor de ataque a proteger, especialmente de ciertos elementos muy críticos en la arquitectura 5G (como las estaciones base o los sistemas de gestión y orquestación), una mayor dependencia de los fabricantes o proveedores de los componentes y elementos de la red, preocupando no sólo la confidencialidad de las comunicaciones, sino también su integridad y disponibilidad, al esperar que constituyan la espina dorsal de las futuras economías y sociedades completamente digitalizadas. Complementariamente, en enero de 2020 la Comisión Europea aprobó un conjunto de instrumentos común con las medidas de reducción de riesgo acordadas por los diferentes Estados miembros de la UE, debido a su importancia estratégica [Ref.- 101]. Las medidas de seguridad concretas a implantar deberán ser definidas por cada uno de los Estados miembros, aunque

[54] http://www.mineco.gob.es/portal/site/mineco/menuitem.ac30f9268750bd56a0b0240e026041a0/?vgnextoid=32c-47faa9de6a610VgnVCM1000001d04140aRCRD&vgnextchannel=67f3a570b4ee3610VgnVCM1000001d04140aRCRD

[55] http://www.mineco.gob.es/portal/site/mineco/menuitem.ac30f9268750bd56a0b0240e026041a0/?vgnextoid=a8be-67b6ea69d610VgnVCM1000001d04140aRCRD&vgnextchannel=67f3a570b4ee3610VgnVCM1000001d04140aRCRD

[56] http://www.mineco.gob.es/portal/site/mineco/menuitem.609f3fe75b61c2edafb0240e026041a0/?vgnextoid=67f3a-570b4ee3610VgnVCM1000001d04140aRCRD&f1=1104534000000&f2=1735686000000

[57] Tal como demuestran los numerosos resultados que se obtienen al realizar una simple búsqueda por los términos "5g seguridad" (en español, o en inglés, "5g security"), a la que se anima realizar al lector.

se están coordinando conjuntamente sus líneas generales y definición: normativa, normalización, marco de control, contratación pública, financiación de la UE, etc. Estas recomendaciones se vieron ratificadas en la conferencia internacional de seguridad de Praga (Prague 5G Security Conference[58]) celebrada en mayo de 2019, reflejadas en una serie de propuestas y buenas prácticas.

Dejando a un lado los aspectos más estratégicos de la seguridad de las redes 5G, que requieren aglutinar y considerar múltiples aspectos y elementos en la ecuación de seguridad [Ref.- 102], a lo largo del 2019 y desde un punto de vista más técnico, se han publicado diferentes informes, estudios e investigaciones centrados en analizar e incrementar la seguridad de estas tecnologías. El elevado escrutinio de las tecnologías 5G durante el 2019 se refleja en el Hall of Fame oficial de la GSMA, reconociendo las contribuciones de seguridad de diferentes investigadores [Ref.- 103]; algunas de las más relevantes se describen a continuación.

Destaca el análisis de la propia GSMA [Ref.- 104], donde se reitera que debido a que las redes 5G de nueva generación siguen haciendo uso de tecnologías previas ya conocidas y vulnerables, como SS7 o Diameter, junto a la elevada flexibilidad (network slicing, para dar soporte a distintas subredes 5G virtuales) ofrecida por la tecnología 5G para los despliegues de sus redes (implicando a su vez mayor complejidad y más elementos a monitorizar), lo que potencialmente llevará a un mayor número de errores en su configuración, para poder proporcionar un nivel de seguridad adecuado será fundamental coordinar esfuerzos concertados entre los operadores de telecomunicaciones y los proveedores o fabricantes. Por ejemplo, debido a que las redes 5G NSA hacen uso de la infraestructura de las redes LTE, todas ellas son igualmente vulnerables a ataques de denegación de servicio (DoS) a través de la explotación de Diameter.

[58] https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/

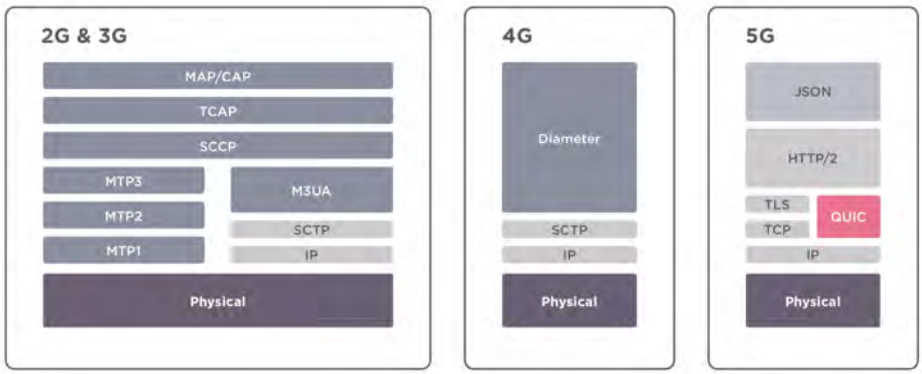


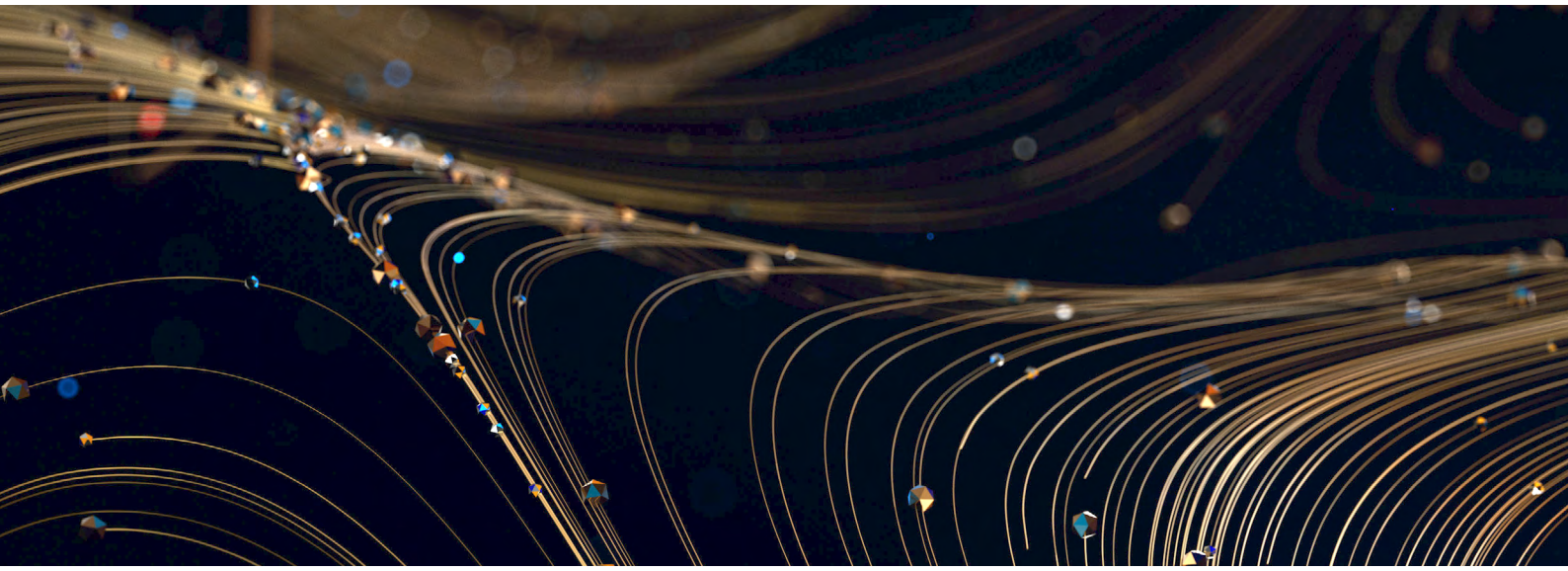
Figure 5. Evolution of network core signaling protocols

Por otro lado, al hacer las infraestructuras del núcleo de las redes 5G uso de soluciones con mayor orientación software y en la nube, como *Software-Defined Networking* (SDN) y *Network Function Virtualization* (NFV), tecnologías que hacen un uso extensivo de tecnologías web (HTTP y REST API), algunos de los futuros ataques a las redes 5G se convertirán realmente en ataques sobre las tecnologías web, para los que se dispone de un extenso conocimiento en la comunidad. A este riesgo se añade que el objetivo principal de las redes 5G no serán los dispositivos móviles, sino los dispositivos IoT, por lo que las redes 5G sufrirán los riesgos de disponer de billones de dispositivos potencialmente vulnerables conectados (*botnets*, DoS, etc.).

Con el objetivo de acomodar tanto la flexibilidad como la complejidad de las redes 5G desde una perspectiva de protección global, unificando su estudio desde el núcleo de la red hasta el borde de la red, e incluyendo tanto la capa física como la capa lógica (que habitualmente son analizadas desde el punto de vista de seguridad de manera independiente), se publicó en febrero de 2019 una propuesta para un *framework* automatizado de ataque y defensa para la seguridad de las redes 5G [Ref.- 105].

Las tecnologías 5G proporcionan mejoras de seguridad y privacidad respecto al seguimiento y/o la suplantación de usuarios, o de la red, cifrando más datos e identificadores (como el IMEI o el IMSI) que sus predecesoras [Ref.- 106]. Se debe tener en cuenta, sin embargo, que la seguridad de las redes 5G se verá realmente incrementada cuando no dependa de los requisitos de compatibilidad hacia atrás con tecnologías previas, tal como ocurre actualmente. Los investigadores de seguridad siguen destacando que el seguimiento de usuarios aún es posible, utilizando información que sigue sin estar cifrada y que permite el despliegue de estaciones base falsas, *stingrays* o IMSI *catchers* [Ref.- 107], eso sin tener en cuenta que, pese a que las especificaciones de seguridad de 5G sean robustas, será necesario evaluar la implementación llevada a cabo finalmente por los operadores, y que estos se adhieran a las mejoras prácticas de seguridad de la industria (aspecto en el que el FCC en EEUU y la UE pueden ayudar estableciendo regulaciones y normativas).

La investigación presentada en agosto de 2019 en BlackHat USA demuestra debilidades en 5G que permiten el despliegue de dispositivos de monitorización, como estaciones base falsas [Ref.- 107]. Cuando un dispositivo se registra en una nueva estación base (o torre de telefonía móvil) transmite ciertos datos identificativos que no están cifrados, tampoco en 5G, información que puede ser utilizada para el seguimiento de los usuarios. Estos datos permiten conocer el tipo de dispositivo, el fabricante, el modelo, sus componentes y sistema operativo, incluso su versión. Adicionalmente, y con un mayor impacto, esa filtración de datos permite realizar ataques de Man-in-the-Middle (MitM) y su manipulación.

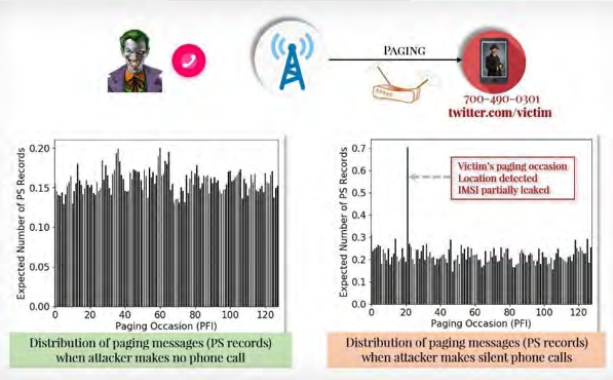


Se debe tener también en cuenta que debilidades en 5G aún permiten la realización de ataques de *downgrade*, hacía tecnologías 4G, 3G o 2G [Ref.- 107]. Los dispositivos celulares son clasificados en 12 categorías (1-12) en función de su naturaleza y complejidad, lo que permite a la red identificar a qué tipo de red (según sus necesidades y demandas de datos) se debe conectar cada tipo de dispositivo: 5G, 4G, 3G, 2G, etc. Mediante la manipulación de la categoría a la que pertenece un dispositivo (una vulnerabilidad en la implementación perpetuada durante años por los operadores; en el estudio, 21 de los 30 operadores analizados de Europa, EEUU y Asia eran vulnerables), por ejemplo, haciendo que un iPhone se identifique como un dispositivo IoT, es posible llevar a cabo ataques de *downgrade* en 5G, forzando a que el dispositivo víctima se conecte a un red más tradicional, donde los ataques clásicos y conocidos aun son viables. Es necesario que la red 5G, para solucionarlo, aplique los mecanismos de protección en una fase temprana del proceso de conexión de los abonados.

Complementariamente, la investigación descubrió que podían bloquear que los dispositivos entrasen en un estado de ahorro de energía (evitando que el mensaje que es enviado por la red a los dispositivos para este propósito, una vez disponen de una conexión estable, fuese entregado) y, como resultado, estuviesen constantemente escaneando en busca de conectividad de red para intentar reconectarse, consumiendo la batería del dispositivo víctima a un ritmo 5 veces superior al habitual. Este ataque es especialmente problemático de cara a la disponibilidad de sensores o controladores IoT, si dejan de estar operativos. En consecuencia, la GSMA se encuentra revisando de nuevo y mejorando la especificación de 5G para evitar o mitigar este tipo de ataques.

Estos descubrimientos se unían a investigaciones previas publicadas en febrero de 2019 que reflejaban la posibilidad de realizar el seguimiento de usuarios en redes 4G e incluso 5G [Ref.- 109], a través de un conjunto de vulnerabilidades y exploits denominado ToRPEDO (Tracking via Paging mEssage DistributiOn) que aprovecha debilidades en el protocolo de *paging* empleado para notificar a los dispositivos acerca de comunicaciones entrantes, llamadas o mensajes SMS [Ref.- 108]. ToRPEDO afectaba a los 4 operadores móviles principales de EEUU: AT&T, Verizon, Sprint y T-Mobile (junto a otras redes móviles en Europa y Asia). Los dispositivos comprueban a intervalos periódicos con las estaciones base si hay comunicaciones pendientes (optimizando el consumo de batería). Los investigadores descubrieron que mediante la realización de una serie de llamadas rápidas al dispositivo víctima en un breve espacio de tiempo, pueden dar lugar a un mensaje de *paging* sin alertar a la víctima (no se recibe la llamada entrante). Capturando y analizando las comunicaciones del protocolo de *paging*, podían determinar si el objetivo se encuentra en la zona, mediante la identificación de patrones. Complementariamente, ToRPEDO permite manipular el canal de *paging* para añadir o bloquear mensajes de *paging*, bloqueando por ejemplo la recepción de mensajes SMS o llamadas por parte de la víctima, o incluso permitiendo la inyección de ciertos mensajes.

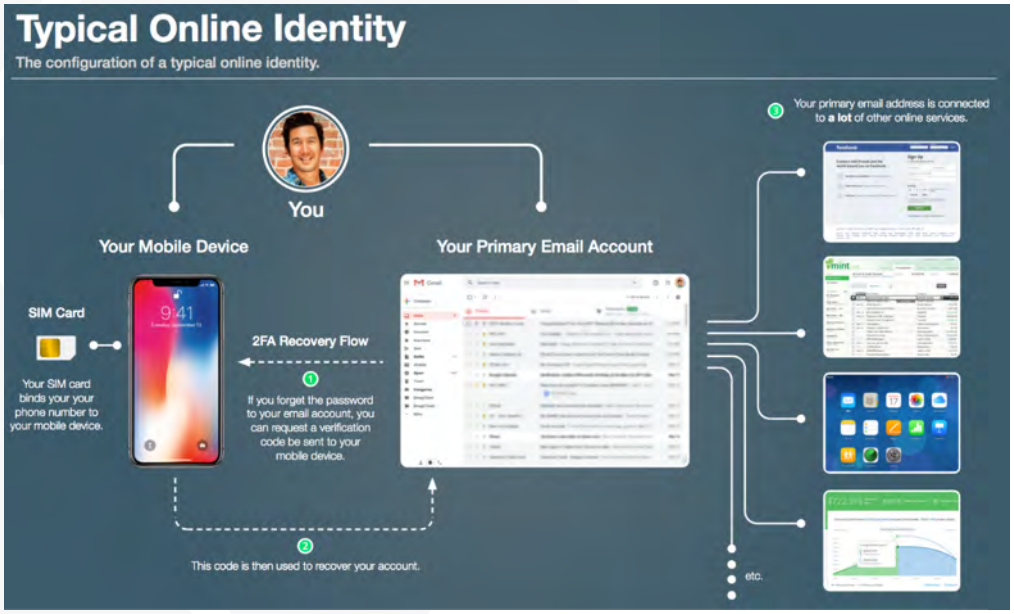
Por último, ToRPEDO permite también la realización de ataques de cracking sobre el IMSI del abonado (IMSI-Cracking, mediante técnicas de fuerza bruta), permitiendo su obtención en menos de 13 horas, con las consiguientes implicaciones frente al potencial seguimiento del usuario víctima. Este identificador, cifrado en redes 4G y 5G, no está convenientemente protegido en todos los escenarios, lo que permite ataques de fuerza bruta en redes 4G y 5G, o su obtención más directamente en 4G (en concreto, asociada a un ataque denominado Piercer contra la implementación de la red 4G de un operador móvil específico de EEUU, no desvelado).



A su vez, los investigadores de Purdue University y de la universidad de Iowa publicaron el descubrimiento de un nuevo conjunto de 11 vulnerabilidades en noviembre de 2019 [Ref.- 110], que permiten desvelar la localización del usuario víctima, ataques de *downgrade* (de nuevo, evitando los nuevos mecanismos de cifrado de los identificadores en 5G), manipular la facturación de los servicios celulares (mediante ataques de *replay*, reenviando el mismo mensaje o comandos previos), o realizar el seguimiento de llamadas, mensajes SMS o navegación web, junto a otras vulnerabilidades de las redes 3G o 4G que se heredan en 5G, al haber adoptado ésta muchos mecanismos de seguridad de sus predecesores. La herramienta asociada a esta investigación y vulnerabilidades se acuñó como 5GReasoner [Ref.- 110].

Las redes móviles que intentan mitigar el seguimiento de sus suscriptores hacen uso de un identificador temporal (o TMSI, Temporary Mobile Subscriber Identity), que se va renovando periódicamente. El estudio identificó mecanismos para influenciar el periodo de renovación del TMSI, o correlar los valores de TMSI previos con los nuevos, para poder realizar el seguimiento de los abonados a través de herramientas SDR (Software Define Radio) de bajo coste.

Colateralmente a todo el análisis previo de la seguridad de las redes 5G, es importante concienciar sobre la dependencia que tienen actualmente muchos servicios digitales que hacen uso de un segundo factor de autentificación (2FA) en los mensajes SMS, una tecnología que adolece de múltiples problemas de seguridad, y el exceso de confianza que se deposita en el número de teléfono del usuario o abonado de cara a proteger su identidad online, incluso haciendo uso de medidas de seguridad más avanzadas como 2FA. Entre estos escenarios ofensivos, existe la posibilidad de llevar a cabo ataques de portabilidad de la tarjeta SIM (intercambio o secuestro de SIM, o SIM *swapping*), lo que permite al atacante tomar control completo sobre el número de teléfono del usuario víctima, y que éste pierda su número de teléfono, temporal o permanentemente. A lo largo de 2019 se han dado casos de incidentes de seguridad con un impacto económico alto en el que individuos han perdido miles, o incluso millones, de dólares en unas pocas horas (especialmente de carteras de criptomonedas), donde un atacante disponía de las credenciales de la víctima pero no de la capacidad de evitar el 2FA. Para ello, lleva a cabo la portabilidad fraudulenta del número de teléfono del usuario objetivo (habitualmente empleando técnicas de ingeniería social o explotando otras debilidades en los procesos de portabilidad de los operadores de telecomunicaciones), pudiendo así completar cualquier verificación de 2FA y disponer de acceso a las cuentas online de la víctima [Ref.- 111]. En otros escenarios, el atacante ni siquiera requiere disponer de las credenciales previamente, ya que puede resetear estas a través del número de teléfono del usuario.

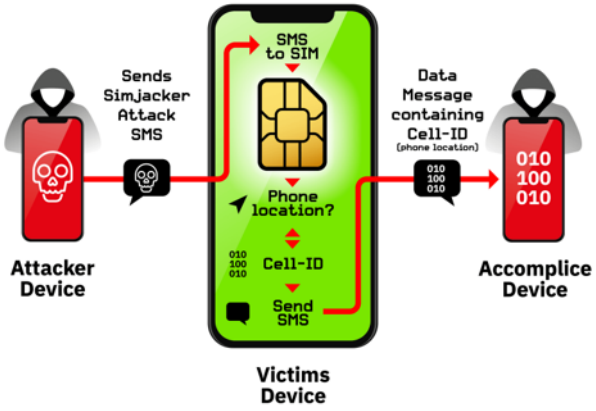


Como resultado, el atacante puede focalizarse en el servicio objetivo de sus actividades, la cuenta principal de correo electrónico (e-mail) del usuario víctima, que a su vez le permitirá resetear y/o cambiar las credenciales del resto de servicios online. Los últimos años han presentado un aumento en los casos de fraude por portabilidad de SIM, haciéndose públicas las primeras demandas por este tipo de incidentes, por ejemplo, contra el operador de telecomunicaciones americano AT&T[59].

En septiembre de 2019 se anunciaba una vulnerabilidad y los exploits asociados, denominada Simjacker [Ref.- 112], que había sido explotada durante los 2 últimos años por actores avanzados en múltiples países a través de las infrastructuras de los operadores de telecomunicaciones, con el objetivo de monitorizar a los usuarios víctima. El ataque hace uso de mensajes SMS especialmente formados para conseguir que la tarjeta SIM de la víctima tome control del dispositivo móvil y ejecute comandos sensibles. Los descubridores, AdaptiveMobile Security, afirman que ha sido desarrollado por una compañía privada que trabaja para gobiernos con el objetivo de monitorizar a usuarios individuales en múltiples países. Las víctimas de Simjacker también han sido atacadas a través de otras redes de los operadores de telecomunicaciones, como SS7, confirmándose que Simjacker actúa como un complemento, o un reemplazo, de ataques ya conocidos a través de las infraestructuras vulnerables de SS7. En los incidentes identificados se han visto ataques intentando monitorizar hasta 300 objetivos durante un mismo día, y objetivos que son monitorizados cientos de veces durante la misma semana, o un menor número de veces pero durante periodos más largos de tiempo, confirmando que se trata de operaciones dirigidas y no masivas.

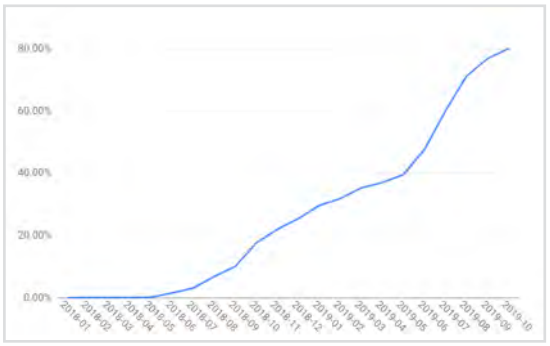
[59] https://www.xataka.com/seguridad/primera-demanda-sim-swapping-para-at-t-224-millones-dolares-despues-hackeo-robo-bitcoins

El mensaje SMS malicioso de Simjacker contiene instrucciones STK (SIM ToolKit), destinadas a la tarjeta SIM y, en concreto, al navegador S@T (SIMalliance Toolbox Browser) de la propia tarjeta SIM empleado como entorno de ejecución (demostrando la sofisticación y lo avanzado de este ataque), desde donde puede obtener la localización del dispositivo móvil y su identificador o IMEI. Estos datos son exfiltrados vía SMS a un número remoto gestionado por el atacante. Todas estas actividades ocurren de manera transparente para el usuario, no quedando constancia en el histórico de SMSs. La ventaja de este ataque es que para la mayoría de casos y acciones es independiente del dispositivo móvil, funcionando tanto en dispositivos móviles iOS como Android, incluyendo múltiples fabricantes, así como en dispositivos IoT (con una tarjeta SIM).



El navegador S@T no es ampliamente conocido, al tratarse de una tecnología antigua, cuyo propósito inicial era el de poder obtener el balance de la cuenta del usuario a través de la tarjeta SIM. Aunque en desuso (dependiendo del país; se ha identificado su utilización en unos 30 países de distintos continentes), sigue latente y disponible en las tarjetas SIM actuales. Las capacidades de este entorno de ejecución no permiten únicamente obtener la localización del usuario, sino que otras acciones como la obtención de información adicional, enviar mensajes SMS (para exfiltrar los datos), establecer llamadas (para fraude, espionaje actuando como un *bug* de escucha, etc.), enviar códigos USSD, abrir un navegador web, etc., también pueden ser ejecutadas.

Dentro de las comunicaciones de las plataformas móviles, no específicamente celulares, destaca la adopción a final de 2019 por parte de Android de TLS (Transport Layer Security) de manera mucho más global [Ref.- 113]. Con la incorporación del fichero de configuración de seguridad de red en 2016 a partir de Android 7 (API 24), se facilitó a los desarrolladores el uso de TLS en sus apps. Un cambio muy significativo fue introducido en Android 9 (API 28), forzando por defecto una política automática para no permitir (o bloquear) el tráfico no cifrado o en texto claro, lo que ha dado lugar a que el 90% de las apps que tienen como objetivo Android 9 cifren su tráfico en la actualidad (o un 80% de apps para Android, independientemente de su versión objetivo). Debido a que desde el 1 de noviembre de 2019 todas las nuevas apps, o las nuevas actualizaciones de apps existentes, a publicar en Google Play deben tener Android 9 como objetivo, se espera que estos porcentajes sigan creciendo.

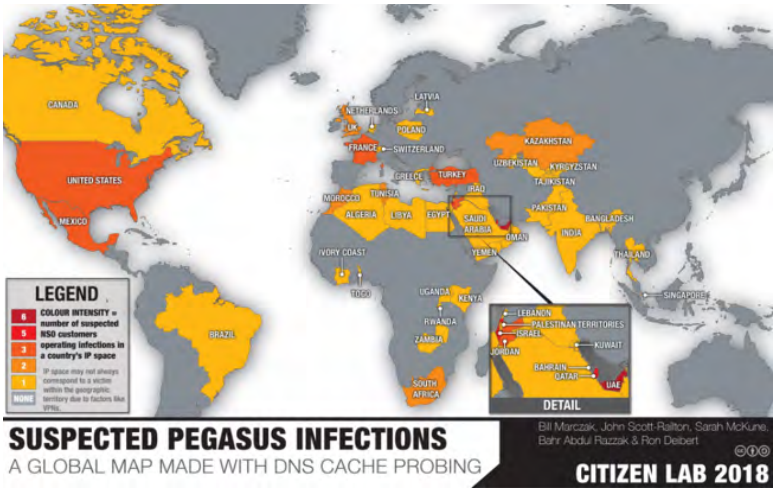


Dentro de las capacidades de comunicaciones móviles empleadas a nivel mundial por billones de usuarios destacan las aplicaciones de mensajería, como por ejemplo WhatsApp, que superó los 2 billones de usuarios en febrero de 2020[60]. A lo largo de 2019 WhatsApp ha sufrido algunas vulnerabilidades críticas, que fueron resueltas por Facebook, lo que enfatiza la necesidad por parte de los usuarios de mantener siempre actualizadas y al día las apps que utilizan. Dentro de estas, destaca la vulnerabilidad de desbordamiento de buffer en la pila de VoIP de la app, CVE-2019-3568 [Ref.- 114], publicada en mayo de 2019 que permitía la ejecución remota de código mediante una simple llamada de Voz sobre IP a través de la app (empleando paquetes SRTCP malformados), tanto en iOS como en Android, sin requerir ninguna interacción por parte del usuario, que no necesita ni siquiera responder dicha llamada para ser víctima del ataque. Por tanto, para explotar la vulnerabilidad sólo se requiere disponer del número de teléfono del usuario objetivo. La misma fue identificada en

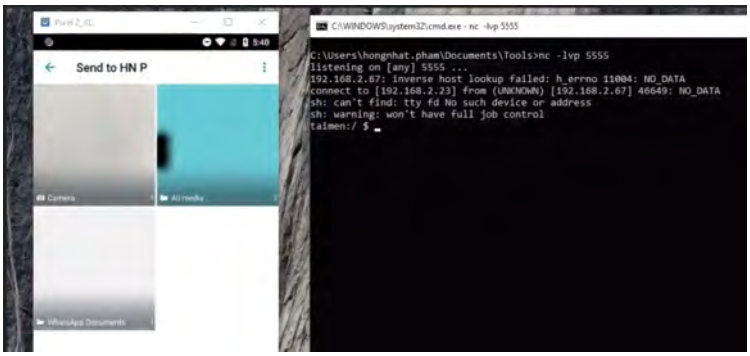
[60] https://blog.whatsapp.com/10000666/Dos-mil-millones-de-usuarios--Conectando-al-mundo-de-manera-privada (https://www.xataka.com/moviles/whatsapp-supera-2-000-millones-usuarios-todo-mundo-sigue-ganar-apenas-dinero)

ataques reales que tenían como objetivo la instalación de spyware en los dispositivos móviles de las víctimas, desarrollado por la compañía Israelí NSO Group dentro de su solución de espionaje Pegasus (conocida y utilizada en Oriente Medio, y otros países como Méjico), según el Financial Times [Ref.- 114]. Se dispone de referencias a posibles víctimas, como un abogado defensor de los derechos humanos de UK, que estaba colaborando con periodistas mejicanos, y un disidente de Arabia Saudí, así como miembros de Amnistía Internacional.

La utilización de Pegasus de NSO Group ha estado vinculada al operador KINGDOM, asociado a Arabia Saudí, en ataques dirigidos a disidentes Saudís, o a periodistas del New York Times durante los últimos años, especialmente en 2018, a través de mensajes SMS maliciosos [Ref.- 116]. Se dispone de más detalles respecto a otros incidentes móviles asociados a ataques dirigidos que han sido descubiertos a lo largo del año 2019, algunos de ellos también asociados a NSO Group [Ref.- 90].

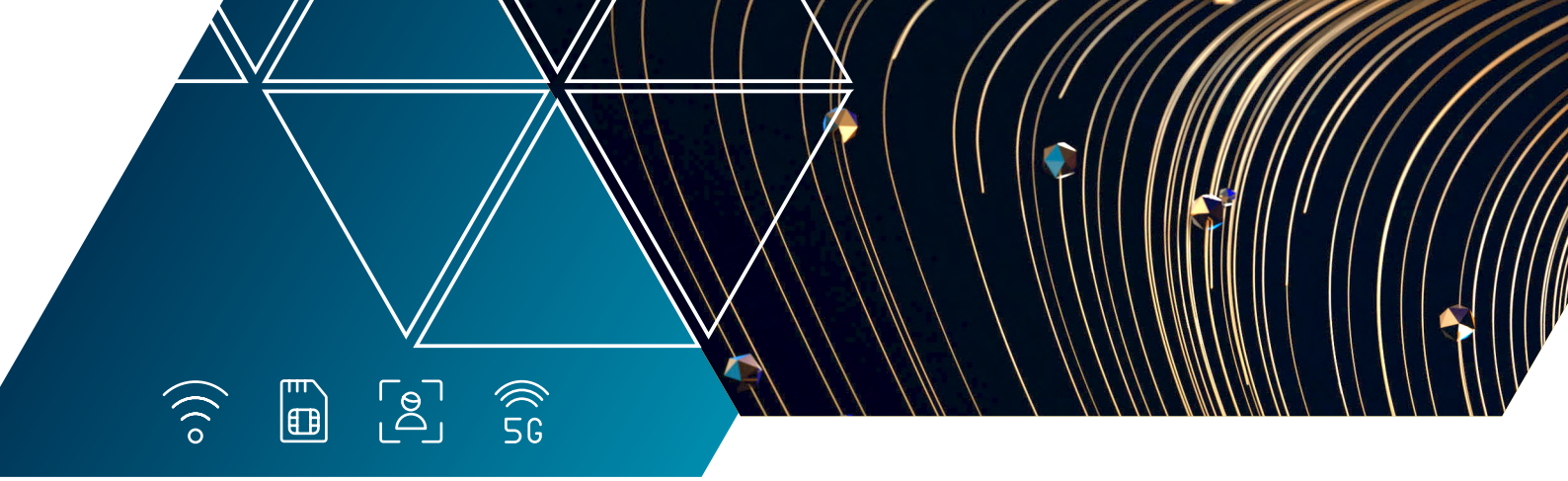


De manera similar, en octubre de 2019 Facebook solucionaba una nueva vulnerabilidad en WhatsApp, en este caso para Android, que también permitía la ejecución remota de código en Android 8.1 y 9.0, CVE-2019-11932 [Ref.- 115], en este caso explotable a través de una imagen GIF maliciosa compartida como documento a través de WhatsApp. Cuando el usuario víctima abre la Galería de Whatsapp, si esta contiene el GIF malicioso, aún sin abrirlo, la vulnerabilidad será explotada a través de la funcionalidad automática de previsualización de la galería. Esta vulnerabilidad fue descubierta por un investigador de seguridad y notificada responsablemente a Facebook para su resolución.



Uno de los casos más mediáticos en 2019 ha sido el (supuesto) ataque y compromiso del dispositivo móvil iPhone X de Jeff Bezzos, fundador y presidente de Amazon, por parte del gobierno de Arabia Saudí, con gran repercusión a nivel mundial y con acusaciones por parte, incluso, de Naciones Unidas. El ataque se llevó a cabo mediante el envío a Bezzos de un vídeo sospechoso a través de WhatsApp, vinculándolo con la vulnerabilidad descrita a continuación. Se han publicado diferentes informes y análisis (con referencias al proyecto CATO) desde su revelación inicial en marzo de 2019, hasta la fecha de publicación del presente informe, que confirman y desmienten dichas acusaciones. Sin profundizar más en dicho incidente, se proporcionan varias referencias para el lector interesado en su análisis [Ref.- 117] [Ref.- 118].

Posteriormente, en noviembre de 2019 Facebook solucionaba una nueva vulnerabilidad en WhatsApp, que afectaba a iOS, Android y Windows Phone, y que permitía la ejecución remota de código, CVE-2019-11931 [Ref.- 119], en este caso explotable a través de un vídeo, o fichero MP4, recibido por el usuario víctima a través de WhatsApp (potencialmente asociada al incidente de Jeff Bezzos mencionado).



12. TENDENCIAS PARA EL AÑO 2020

Dentro de las principales tendencias esperadas para el año 2020, adicionalmente a las ya reflejadas en las nuevas capacidades de conexión a redes Wi-Fi con soporte para WPA3 (que finalmente no se materializaron durante el año 2019 por la ausencia de soporte hasta Android 10 e iOS 13, y en éste último, sólo parcialmente) y a la inminente adopción de las redes móviles 5G, tanto las NSA como las SA que están por llegar (tal como se detalla en el apartado "11. Comunicaciones móviles"), sin duda las capacidades de comunicación inalámbrica serán un foco de atención, al igual que en 2019.

Respecto a los futuros avances y usos de los dispositivos móviles, más allá de Android 10, Google está analizando la posibilidad de poder emplear el móvil como identificador electrónico (ID) de cara a diferentes apps, de manera similar al carnet de conducir [Ref.- 41]. Las apps que hagan uso de este ID presentarán requisitos estrictos de seguridad, por lo que esta iniciativa requiere de su estandarización por organismos internacionales como ISO, capacidades criptográficas avanzadas, así como de una integración estrecha entre Android como plataforma, las librerías y frameworks proporcionados por Android de cara a las apps, la existencia de una capa de abstracción hardware (HAL) común, las apps cliente, el dispositivo que realice la lectura y verificación de la identidad del usuario, y los servidores o sistemas de backend de autorización empleados para la emisión, actualización y revocación de estos IDs digitales.

Ataques como Simjacker denotan la complejidad y lo poco que conocemos las tecnologías que están integradas hoy en día en un dispositivo móvil, especialmente las asociadas a las comunicaciones celulares móviles, la tarjeta SIM y los componentes de radio, que coexisten en paralelo con el sistema operativo y chips principales en Android e iOS, y para los que no se dispone de mecanismos avanzados y eficientes de monitorización y protección. El tiempo confirmará si los atacantes desarrollaran nuevos ataques sofisticados aprovechando esas capacidades ocultas, aún más cuando se despliegue toda la complejidad asociada a las nuevas redes móviles 5G.

Están aún por confirmarse también las posibles implicaciones de seguridad (y de muchos otros tipos) que podría introducir la existencia de un nuevo sistema operativo (y mercado) móvil en el ecosistema global, concretamente el asociado a los terminales Huawei, si finalmente el fabricante Chino no sigue haciendo uso de Android.

13. ANEXO A. REFERENCIAS

[Ref.- 1]	"Smartphone OS Market Share" (Updated: 25 Oct 2019). IDC. 2019. (Actualizado el 20 Jan 2020). URL: http://www.idc.com/promo/smartphone-market-share/os
[Ref.- 2]	"Smartphone Vendor Market Share" (Updated: 18 Jun 2019). IDC. 2019. (Actualizado el 20 Jan 2020). URL: https://www.idc.com/promo/smartphone-market-share/vendor
[Ref.- 3]	"Android vs. iOS. Smartphone OS sales market share evolution". Kantar Worldpanel. Sep 2019. URL: https://www.kantarworldpanel.com/global/smartphone-os-market-share/
[Ref.- 4]	"Number of available applications in the Google Play Store from December 2009 to December 2018". Statista. Q3 2018. URL: https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/
[Ref.- 5]	"Number of apps available in leading app stores as of 4th quarter 2019". Statista. Q4 2019.URL: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/
[Ref.- 6]	"Number of available applications in the Google Play Store from December 2009 to December 2019". Dec 2091. URL: https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/
[Ref.- 7]	"Android Dashboards. Platform Versions". Android Developers. URL: https://developer.android.com/about/dashboards/index.html
[Ref.- 8]	"Support - App Store". Apple Developer. URL: https://developer.apple.com/support/app-store/
[Ref.- 9]	"Number of available apps in the Apple App Store from 2008 to 2019 (in 1,000s)". Statista. July 2019. URL: https://www.statista.com/statistics/268251/number-of-apps-in-the-itunes-app-store-since-2008/
[Ref.- 10]	"CCN-CERT IA-04/19: Informe Anual 2018 - Dispositivos y comunicaciones móviles". CCN-CERT. Enero 2019. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3464-ccn-cert-ia-04-19-informe-anual-2018-dispositivos-moviles/file.html
[Ref.- 11]	"CCN-CERT IA-10/18: Informe Anual 2017 - Dispositivos y comunicaciones móviles". CCN-CERT. Mayo 2018. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2826-ccn-cert-ia-10-18-informe-ciberamenazas-2017-y-tendencias-2018-dispositivos-moviles-dispositivos-y-comunicaciones-moviles/file.html
[Ref.- 12]	"Bypassing iOS Lock Screens: A Comprehensive Arsenal of Vulns". DinoSec. Jan 2019. URL: http://blog.dinosec.com/2014/09/bypassing-ios-lock-screens.html

[Ref.- 13]	"Apple Platform Security - Fall 2019". Apple. Dec 2019. URL: https://support.apple.com/en-gb/guide/security/welcome/web URL: https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf
[Ref.- 14]	"Apple informa de resultados récord en el primer trimestre de su año fiscal". Apple Newsroom. Enero 2020. URL: https://www.apple.com/es/newsroom/2020/01/apple-reports-record-first-quarter-results/
[Ref.- 15]	"iOS 12 Enhances USB Restricted Mode". ElcomSoft. Sep 2018. URL: https://blog.elcomsoft.com/2018/09/ios-12-enhances-usb-restricted-mode/
[Ref.- 16]	"USB Restricted Mode in iOS 13: Apple vs. GrayKey, Round Two". ElcomSoft. Sep 2019. URL: https://blog.elcomsoft.com/2019/09/usb-restricted-mode-in-ios-13-apple-vs-graykey-round-two/ URL: https://blog.elcomsoft.com/tag/usb-restricted-mode/
[Ref.- 17]	"Guía práctica de seguridad en dispositivos móviles: iPhone (iOS 12.x)". CCN-STIC 455D. CCN-CERT. Oct 2018. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3158-ccn-stic-455d-guia-practica-de-seguridad-en-dispostivos-moviles-iphone-ios-12/file.html URL: https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/7175-guias-practicas-de-seguridad-en-dispositivos-moviles-iphone-ios-11-x-y-ios-12-x.html
[Ref.- 18]	"Guía práctica de seguridad en dispositivos móviles: iPhone (iOS 13.x)". CCN-STIC 455E. CCN-CERT. Feb 2020. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/4569-ccn-stic-455e-configuracion-segura-de-ios-13.html
[Ref.- 19]	"Exclusive: Google suspends some business with Huawei after Trump blacklist - source". Reuters. May 19, 2019. URL: https://www.reuters.com/article/us-huawei-tech-alphabet-exclusive/exclusive-google-suspends-some-business-with-huawei-after-trump-blacklist-source-idUSKCN1SP0NB
[Ref.- 20]	"Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android ". CCN-STIC 456. CCN-CERT. Sep 2018. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3043-ccn-stic-456-cuenta-de-usuario-servicios-aplicaciones-google-para-dispositivos-moviles-android.html URL: https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/7018-dos-nuevas-guias-de-seguridad-sobre-dispositivos-moviles-android-y-su-cuenta-de-usuarios-de-google.html
[Ref.- 21]	"Huawei Launches New Distributed Operating System, HarmonyOS". Huawei. Aug 2019. URL: https://consumer.huawei.com/en/press/news/2019/huawei-launches-harmonyos/ URL: https://www.theverge.com/2019/8/9/20798251/huawei-harmonyos-hongmengos-smartphones-internet-of-things-operating-system-android URL: https://www.techradar.com/news/harmonyos
[Ref.- 22]	"Así es iPadOS, el nuevo sistema operativo para el iPad nacido de las entrañas de iOS". Xataka Móvil. Junio 2019. URL: https://www.xatakamovil.com/apple/asi-ipados-nuevo-sistema-operativo-para-ipad-nacido-entranas-ios URL: https://www.xataka.com/tablets/ipados-sistema-operativo-exclusivo-ipad-para-transformarlo-alternativa-brutal-al-portatil
[Ref.- 23]	"EPIC JAILBREAK: Introducing checkm8 (read "checkmate")". axi0mX. Sep 2019. URL: https://twitter.com/axi0mX/status/1177542201670168576
[Ref.- 24]	checkra1n. 2019. URL: https://checkra.in URL: https://github.com/axi0mX/ipwndfu

[Ref.- 25]	checkra1n 0.9.8. Feb 2020. URL: https://checkra.in/releases/0.9.8-beta
[Ref.- 26]	Apple vs. Corellium. 2019. URL: https://corellium.com/statement-dmca/ URL: https://docs.google.com/document/d/1NSAJpv1FI-JpoLUwVGtIzux8bj-sumTdJXLxJBnKoOc/view URL: https://corellium.com/statement/
[Ref.- 27]	"Behind the scenes of iOS and Mac Security". Ivan Krstic. BlackHat USA: Aug 2019. URL: https://www.blackhat.com/us-19/briefings/schedule/index.html#behind-the-scenes-of-ios-and-mac-security-17220 URL: http://i.blackhat.com/USA-19/Thursday/us-19-Krstic-Behind-The-Scenes-Of-IOS-And-Mas-Security.pdf URL: https://www.youtube.com/watch?v=3byNNUReyvE
[Ref.- 28]	"It Seemed Like a Popular Chat App. It's Secretly a Spy Tool. (ToTok)". NY Times. Dec 2019. URL: https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html URL: https://twitter.com/patrickwardle/status/1210742545451323392
[Ref.- 29]	"Apple Security Bounty". Apple. URL: https://developer.apple.com/security-bounty/
[Ref.- 30]	"Google is starting to reveal the secrets of its experimental Fuchsia OS". The Verge. May 2019. URL: https://www.theverge.com/2019/5/9/18563521/google-fuchsia-os-android-chrome-hiroshi-lockheimer-secrets-revealed URL: https://www.techradar.com/news/google-fuchsia URL: https://fuchsia.dev
[Ref.- 31]	"Exclusive: China's mobile giants to take on Google's Play store - sources". Reuters. Feb 2020. URL: https://www.reuters.com/article/us-china-mobile-exclusive-idUSKBN20018H URL: https://www.xataka.com/moviles/huawei-prepara-alianza-xiaomi-oppo-vivo-para-crear-alternativa-a-play-store-google-reuters
[Ref.- 32]	"El Parlamento Europeo lo tiene claro y vota 582-40 a favor de un cargador único para smartphones a pesar de las protestas de Apple". Xataka. Ene 2020. URL: https://www.xataka.com/moviles/parlamento-europeo-tiene-claro-vota-582-40-a-favor-cargador-unico-para-smartphones-a-pesar-protestas-apple URL: https://www.xataka.com/moviles/apple-se-opone-al-puerto-universal-comision-europea-alegan-que-ahoga-innovacion URL: https://www.xataka.com/moviles/30-puertos-carga-para-moviles-2009-a-solo-uno-comision-europea-insiste-puerto-universal
[Ref.- 33]	"iOS Device Acquisition with checkra1n Jailbreak". Elcomsoft. Nov 2019. URL: https://blog.elcomsoft.com/2019/11/ios-device-acquisition-with-checkra1n-jailbreak/
[Ref.- 34]	"BFU Extraction: Forensic Analysis of Locked and Disabled iPhones". Elcomsoft. Dec 2019. URL: https://blog.elcomsoft.com/2019/12/bfu-extraction-forensic-analysis-of-locked-and-disabled-iphones/
[Ref.- 35]	"Checkra1n Era - Ep 1-5 - Before First Unlock (aka "…")". Mattia Epifani Dec 2019. URL: https://blog.digital-forensics.it/2019/12/checkra1n-era-ep-1-before-first-unlock.html URL: https://blog.digital-forensics.it/2019/12/checkra1n-era-ep-2-extracting-data.html URL: https://blog.digital-forensics.it/2019/12/checkra1n-era-ep-3-automating.html URL: https://blog.digital-forensics.it/2019/12/checkra1n-era-ep-4-analyzing.html URL: https://blog.digital-forensics.it/2019/12/checkra1n-era-ep-5-automating.html

[Ref.- 36]	"Introducing Adiantum: Encryption for the Next Billion Users". Google Security Blog. Feb 2019. URL: https://security.googleblog.com/2019/02/introducing-adiantum-encryption-for.html URL: https://blog.google/technology/safety-security/adiantum-encryption-safer-devices/ URL: https://source.android.com/security/encryption/adiantum
[Ref.- 37]	"The Android Platform Security Model". Google Security Blog. Apr 2019. URL: https://security.googleblog.com/2019/04/the-android-platform-security-model.html URL: https://arxiv.org/abs/1904.05572
[Ref.- 38]	"Android Enterprise Security White Paper". Android. Jan 2020. URL: https://source.android.com/security/overview/reports URL:https://static.googleusercontent.com/media/www.android.com/en//static/2016/pdfs/enterprise/Android_Enterprise_Security_White_Paper_2019.pdf
[Ref.- 39]	"Android Security & Privacy 2018 Year in Review". Android. Mar 2019. URL: https://source.android.com/security/reports/Google_Android_Security_2018_Report_Final.pdf URL: https://source.android.com/security/overview/reports
[Ref.- 40]	"Giving users more control over their location data". Android Developers Blog. Mar 2019. URL: https://android-developers.googleblog.com/2019/03/giving-users-more-control-over-their.html
[Ref.- 41]	"What's New in Android Q Security". Google Security Blog. May 2019. URL: https://security.googleblog.com/2019/05/whats-new-in-android-q-security.html
[Ref.- 42]	"Queue the Hardening Enhancements". Google Security Blog. May 2019. URL: https://security.googleblog.com/2019/05/queue-hardening-enhancements.html
[Ref.- 43]	"Expanding bug bounties on Google Play". Google Security Blog. Aug 2019. URL: https://security.googleblog.com/2019/08/expanding-bug-bounties-on-google-play.html
[Ref.- 44]	"Have an iPhone? Use it to protect your Google Account with the Advanced Protection Program". Google Security Blog. Jan 2020. URL: https://security.googleblog.com/2020/01/have-iphone-use-it-to-protect-your.html URL: https://landing.google.com/advancedprotection/
[Ref.- 45]	"The ultimate account security is now in your pocket". Google. Apr 2019. URL: https://www.blog.google/technology/safety-security/your-android-phone-is-a-security-key/
[Ref.- 46]	"Use your Android phone's built-in security key to verify sign-in on iOS devices". Google Security Blog. Jun 2019. URL: https://security.googleblog.com/2019/06/use-your-android-phones-built-in.html
[Ref.- 47]	"Making authentication even easier with FIDO2-based local user verification for Google Accounts". Google Security Blog. Aug 2019. URL: https://security.googleblog.com/2019/08/making-authentication-even-easier-with_12.html
[Ref.- 48]	"Fresher OS with Projects Treble and Mainline". Android Developers Blog. May 2019. URL: https://android-developers.googleblog.com/2019/05/fresher-os-with-projects-treble-and-mainline.html

[Ref.- 49]	"Mobile OSs and Device Security: A Comparison of Platforms". Gartner. May 2019. URL: https://bayton.org/docs/enterprise-mobility/android/gartner-comparison-of-security-controls-for-mobile-devices-2019/ URL: https://www.gartner.com/en/documents/3913286 URL: https://security.googleblog.com/2019/05/quantifying-measurable-security.html
[Ref.- 50]	"An Analysis of Pre-installed Android Software". May 2019. URL: https://arxiv.org/pdf/1905.02713.pdf
[Ref.- 51]	"How we fought bad apps and malicious developers in 2019". Android Developers Blog. Feb 2020. URL: https://android-developers.googleblog.com/2020/02/how-we-fought-bad-apps-and-malicious.html
[Ref.- 52]	"Committed to a safer Google Play for Families". Android Developers Blog. Aug 2019. URL: https://android-developers.googleblog.com/2019/08/committed-to-safer-google-play-for.html URL: https://android-developers.googleblog.com/2019/05/building-safer-google-play-for-kids.html
[Ref.- 53]	"Improving the update process with your feedback". Android Developers Blog. Apr 2019. URL: https://android-developers.googleblog.com/2019/04/improving-update-process-with-your.html#my_anchor
[Ref.- 54]	"The App Defense Alliance: Bringing the security industry together to fight bad apps". Google Security Blog. Nov 2019. URL: https://security.googleblog.com/2019/11/the-app-defense-alliance-bringing.html URL: https://developers.google.com/android/play-protect/app-defense-alliance
[Ref.- 55]	"PHA Family Highlights: Zen and its cousins". Google Security Blog. Jan 2019. URL: https://security.googleblog.com/2019/01/pha-family-highlights-zen-and-its.html
[Ref.- 56]	"PHA Family Highlights: Triada". Google Security Blog. Jun 2019. URL: https://security.googleblog.com/2019/06/pha-family-highlights-triada.html
[Ref.- 57]	"PHA Family Highlights: Bread (and Friends)". Google Security Blog. Jan 2020. URL: https://security.googleblog.com/2020/01/pha-family-highlights-bread-and-friends.html
[Ref.- 58]	"Bad Binder: Android In-The-Wild Exploit". Google Project Zero. Nov 2019. URL: https://googleprojectzero.blogspot.com/2019/11/bad-binder-android-in-wild-exploit.html URL: https://bugs.chromium.org/p/project-zero/issues/detail?id=1942
[Ref.- 59]	"UAE Used Cyber Super-Weapon To Spy on iPhones of Foes". Jan 2019. URL: https://www.reuters.com/investigates/special-report/usa-spying-karma/ URL: https://www.reuters.com/investigates/special-report/usa-spying-raven/ URL: https://darknetdiaries.com/episode/47/
[Ref.- 60]	"Google researchers disclose vulnerabilities for 'interactionless' iOS attacks". ZDNet. July 2019. URL: https://www.zdnet.com/article/google-researchers-disclose-vulnerabilities-for-interactionless-ios-attacks/
[Ref.- 61]	"About the security content of iOS 12.4". Apple. July 2019. URL: https://support.apple.com/en-us/HT210346
[Ref.- 62]	"Look, No Hands! -- The Remote, Interaction-less Attack Surface of the iPhone". Natalie Silvanovich. Black Hat USA. Aug 2019. URL: https://www.blackhat.com/us-19/briefings/schedule/#look-no-hands----the-remote-interaction-less-attack-surface-of-the-iphone-15203

[Ref.- 63]	"The Fully Remote Attack Surface of the iPhone". Natalie Silvanovich. Google Project Zero. Aug 2019. URL: https://googleprojectzero.blogspot.com/2019/08/the-fully-remote-attack-surface-of.html
[Ref.- 64]	"The Many Possibilities of CVE-2019-8646". Natalie Silvanovich. Google Project Zero. Aug 2019. URL: https://googleprojectzero.blogspot.com/2019/08/the-many-possibilities-of-cve-2019-8646.html URL: https://youtu.be/br2xCvtVFn4
[Ref.- 65]	"Android Messaging: A Few Bugs Short of a Chain". Natalie Silvanovich. Google Project Zero. Mar 2019. URL: https://googleprojectzero.blogspot.com/2019/03/android-messaging-few-bugs-short-of.html
[Ref.- 66]	"Wi-Fi Alliance® introduces Wi-Fi CERTIFIED WPA3™ security". Wi-Fi Alliance. June 2018. URL: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security
[Ref.- 67]	"A very deep dive into iOS Exploit chains found in the wild". Google Project Zero. Aug 2019. URL: https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html
[Ref.- 68]	"Twelve Million Phones, One Dataset, Zero Privacy". Times Opinion. NY Times. Dec 2019. URL: https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html
[Ref.- 69]	"Amazon's Ring Is a Perfect Storm of Privacy Threats". EFF. Aug 2019. URL: https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats URL: https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats URL: https://www.eff.org/deeplinks/2019/08/five-concerns-about-amazon-rings-deals-police
[Ref.- 70]	"Everything You Need to Know About Ring, Amazon's Surveillance Camera Company". Motherboard. Jul & Aug 2019. URL: https://www.vice.com/en_us/article/qvg48d/everything-you-need-to-know-about-ring-amazons-surveillance-camera-company URL: https://www.vice.com/en_us/article/bjwmem/ring-has-given-active-camera-maps-of-its-customers-to-police URL: https://www.vice.com/en_us/article/j5wyjy/amazon-told-police-it-has-partnered-with-200-law-enforcement-agencies URL: https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement
[Ref.- 71]	"Ring Doorbell App Packed with Third-Party Trackers". EFF. Jan 2020. URL: https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers
[Ref.- 72]	"Guía Práctica de Seguridad de Servicios de Apple". CCN-CERT. *Publicación prevista durante el año 2020*.
[Ref.- 73]	"A Billion Open Interfaces for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link". Technical University of Darmstadt & Northeastern University. Aug 2019. URL: https://news.northeastern.edu/2019/08/19/airdrop-is-making-your-iphone-vulnerable-to-attackers/ URL: https://www.usenix.org/conference/usenixsecurity19/presentation/stute
[Ref.- 74]	"Privacy, Discovery, and Authentication for the Internet of Things". Standford University & Google. Feb 2017. URL: https://arxiv.org/pdf/1604.06959.pdf

[Ref.- 75]	"Handoff All Your Privacy – A Review of Apple's Bluetooth Low Energy Continuity Protocol". Jeremy Martin et. al. Jun 2019. URL: https://arxiv.org/pdf/1904.10600.pdf
[Ref.- 76]	"Open Wireless Link (OWL)". Technical University of Darmstadt. 2019. URL: https://owlink.org URL: https://owlink.org/publications/
[Ref.- 77]	"Apple Bleee: Everyone Knows What Happens on your iPhone". Hexway. Oct 2019. URL: https://hexway.io/research/apple-bleee/
[Ref.- 78]	"AirDrop Crazy". Telefónica. Nov 2019. URL: https://github.com/ElevenPaths/Airdrop-Crazy URL: https://empresas.blogthinkbig.com/airdrop-crazy-herramienta-para-recopilar-informacion-de-dispositivos-apple-adyacentes/
[Ref.- 79]	"AirDoS". Kishan Bagaria. Dec 2019. URL: https://kishanbagaria.com/airdos/
[Ref.- 80]	"Designing for Privacy". Apple WWDC 2019. URL: https://developer.apple.com/videos/play/wwdc2019/708/?time=1919
[Ref.- 81]	"The Clever Cryptography Behind Apple's 'Find My' Feature". Wired. May 2019. URL: https://www.wired.com/story/apple-find-my-cryptography-bluetooth/
[Ref.- 82]	"KNOB Attack". USENIX. Aug 2019. URL: https://knobattack.com URL: https://www.usenix.org/conference/usenixsecurity19/presentation/antonioli URL: https://greatscottgadgets.com/2019/08-16-tools-of-the-knob-attack/
[Ref.- 83]	"¡Póngame otras 3! Whisky, Pacharán y Anís". Raúl Siles. DinoSec. Navaja Negra. Oct 2019. URL: https://www.dinosec.com/en/lab.html#NNED9R
[Ref.- 84]	"Android 10 features and APIs". Android Developers. URL: https://developer.android.com/about/versions/10/features
[Ref.- 85]	"WPA3 and Wi-Fi Enhanced Open". Android Developers. URL: https://source.android.com/devices/tech/connect/wifi-wpa3-owe
[Ref.- 86]	"New features available with iOS 13". Apple. URL: https://www.apple.com/ios/ios-13/features/
[Ref.- 87]	"Critical Bluetooth Vulnerability in Android (CVE-2020-0022) – BlueFrag". ERNW. Feb 2020. URL: https://insinuator.net/2020/02/critical-bluetooth-vulnerability-in-android-cve-2020-0022/
[Ref.- 88]	"Test Results for Mobile Device Acquisition". DHS Science and Technology. 2019. URL: https://www.dhs.gov/publication/st-mobile-device-acquisition
[Ref.- 89]	"Lookout Phishing AI Blog". Lookout. 2019. URL: https://blog.lookout.com/topics#/researchers
[Ref.- 90]	"Targeted Threats". The Citizen Lab. 2019. URL: https://citizenlab.ca/category/research/targeted-threats/
[Ref.- 91]	"CrowdStrike Mobile Threat Report Offers Trends and Recommendations for Securing Your Organization". CrowdStrike. Jul 2019. URL: https://www.crowdstrike.com/blog/mobile-threat-report-2019-trends-and-recommendations/
[Ref.- 92]	"Vulnerabilities and threats in mobile applications, 2019". Positive Technologies. Jun 2019. URL: https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/

[Ref.- 93]	"McAfee Mobile Threat Report". McAfee. Q1 2019. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf
[Ref.- 94]	"Zimperium's "State of Enterprise Mobile Security" Report Says Every Enterprise has Mobile Security Threats and Attacks". Zimperium. Jul 2109. URL: https://blog.zimperium.com/the-state-of-mobile-device-threats-2019-h1-mobile-threat-report/ URL: https://blog.zimperium.com/zimperiums-state-of-enterprise-mobile-security-report-says-every-enterprise-has-mobile-security-threats-and-attacks/
[Ref.- 95]	"Understanding the mobile threat landscape". Wandera. 2019. URL:https://citrixready.citrix.com/content/dam/ready/partners/wa/wandera/mobilethreatlandscape-2019-brochures.pdf
[Ref.- 96]	"Ring's new setting to opt out of sharing video with your community or police is rolling out now (Updated)". Android Police. Feb 2020. URL: https://www.androidpolice.com/2020/02/03/ring-to-add-new-control-center-to-its-app-claims-to-offer-more-privacy-and-security-controls-in-wake-of-concerns/ URL: https://www.businesswire.com/news/home/20200106005267/en/
[Ref.- 97]	"¿Qué significa que existan dos tipos de 5G? Diferencias y compatibilidades entre 5G NSA y 5G SA". Xataka. Aug 2019. URL: https://www.xataka.com/moviles/que-significa-que-existan-dos-tipos-5g-diferencias-compatibilidades-5g-nsa-5g-sa
[Ref.- 98]	"Leaked documents reveal Huawei's secret operations to build North Korea's wireless network". The Washington Post. Jul 2019. URL: https://www.washingtonpost.com/world/national-security/leaked-documents-reveal-huaweis-secret-operations-to-build-north-koreas-wireless-network/2019/07/22/583430fe-8d12-11e9-adf3-f70f78c156e8_story.html
[Ref.- 99]	"Los Estados miembros de la UE publican un informe acerca de la seguridad de las redes 5G". CCN-CERT. Oct 2019. URL: https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/8821-los-estados-miembros-de-la-ue-publican-un-informe-acerca-de-la-seguridad-de-las-redes-5g.html URL: https://www.dsn.gob.es/en/actualidad/sala-prensa/seguridad-redes-5g URL: https://europa.eu/rapid/press-release_IP-19-6049_es.htm
[Ref.- 100]	"RECOMENDACIÓN (UE) 2019/534 DE LA COMISIÓN, de 26 de marzo de 2019, Ciberseguridad de las redes 5G". BOE. Mar 2019. URL: https://www.boe.es/doue/2019/088/L00042-00047.pdf URL: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks
[Ref.- 101]	"Seguridad de las redes 5G: la Comisión aprueba el conjunto de instrumentos de la UE y define las próximas etapas". Comisión Europea. Ene 2020. URL: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures URL: https://ec.europa.eu/commission/presscorner/detail/es/ip_20_123
[Ref.- 102]	"5G Security". Bruce Schneier. Jan 2020. URL: https://www.schneier.com/blog/archives/2020/01/china_isnt_the_.html
[Ref.- 103]	"GSMA Mobile Security Hall of Fame". GSMA. 2019. URL: https://www.gsma.com/security/gsma-mobile-security-hall-of-fame/
[Ref.- 104]	"Positive Technologies: 5G security issues". GSMA. Nov 2019. URL: https://www.gsma.com/membership/resources/positive-technologies-5g-security-issues/

[Ref.- 105]	"Automated Attack and Defense Framework for 5G Security on Physical and Logical Layers". arXiv. Feb 2019. URL: https://arxiv.org/abs/1902.04009
[Ref.- 106]	"5G Is More Secure Than 4G and 3G—Except When It's Not". Wired. Dec 2019. URL: https://www.wired.com/story/5g-more-secure-4g-except-when-not/ URL: https://www.wired.com/story/wired-guide-5g/
[Ref.- 107]	"New Vulnerabilities in 5G Networks". Ravishankar Borgaonkar. BlackHat USA 2019. Aug 2019. URL: https://www.blackhat.com/us-19/briefings/schedule/#new-vulnerabilities-in-g-networks-15279 URL: https://www.wired.com/story/5g-security-stingray-surveillance/
[Ref.- 108]	"Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information". Purdue University & University of Iowa. Feb 2019. URL: http://homepage.divms.uiowa.edu/~comarhaider/publications/LTE-torpedo-NDSS19.pdf
[Ref.- 109]	"Holes in 4G and 5G Networks Could Let Hackers Track Your Location ". Wired. Feb 2019. URL: https://www.wired.com/story/torpedo-4g-5g-network-attack-stingray/ URL: https://techcrunch.com/2019/02/24/new-4g-5g-security-flaws/
[Ref.- 110]	"5GReasoner: A Property-Directed Security And Privacy Analysis Framework For 5G Cellular Network Protocol". Purdue University & University of Iowa. Nov 2019. URL: https://relentless-warrior.github.io/wp-content/uploads/2019/10/5GReasoner.pdf URL: https://relentless-warrior.github.io/index.php/publications/5greasoner-a-property-directed-security-and-privacy-analysis-framework-for-5g-cellular-network-protocol/ URL: https://www.wired.com/story/5g-vulnerabilities-downgrade-attacks/
[Ref.- 111]	"The Most Expensive Lesson Of My Life: Details of SIM port hack". Sean Coonce. May 2019. URL: https://medium.com/coinmonks/the-most-expensive-lesson-of-my-life-details-of-sim-port-hack-35de11517124
[Ref.- 112]	"Simjacker". AdaptiveMobile Security. Sep 2019. URL: https://simjacker.com URL:https://simjacker.com/downloads/technicalpapers/AdaptiveMobile_Security_Simjacker_Technical_Paper_v1.01.pdf URL: https://www.adaptivemobile.com/blog/simjacker-next-generation-spying-over-mobile
[Ref.- 113]	"An Update on Android TLS Adoption". Google Security Blog. Dec 2019. URL: https://security.googleblog.com/2019/12/an-update-on-android-tls-adoption.html
[Ref.- 114]	"CVE-2019-3568". Facebook. May 2019. URL: https://www.facebook.com/security/advisories/cve-2019-3568 URL: https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab URL: https://research.checkpoint.com/2019/the-nso-whatsapp-vulnerability-this-is-how-it-happened/
[Ref.- 115]	"How a double-free bug in WhatsApp turns to RCE". Awakened. Oct 2019. URL: https://awakened1712.github.io/hacking/hacking-whatsapp-gif-rce/ URL: https://www.facebook.com/security/advisories/cve-2019-11932
[Ref.- 116]	"New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator". CitizenLab. Jan 2020. URL: https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/

[Ref.- 117]	"Saudis hacked Amazon chief Jeff Bezos's phone, says company's security adviser". The Guardian. Mar 2019. URL: https://www.theguardian.com/technology/2019/mar/31/saudis-hacked-amazons-jeff-bezos-phone-claims-security-chief-jamal-khashoggi-mohammed-bin-salman URL: https://www.documentcloud.org/documents/6668313-FTI-Report-into-Jeff-Bezos-Phone-Hack.html URL: https://www.ohchr.org/Documents/Issues/Expression/SRsSumexFreedexAnnexes.pdf
[Ref.- 118]	"There's no evidence the Saudis hacked Jeff Bezos's iPhone". Errata Security. Jan 2020. URL: https://blog.erratasec.com/2020/01/theres-no-evidence-saudis-hacked-jeff.html URL: https://blog.erratasec.com/2020/01/how-to-decrypt-whatsapp-end-to-end.html
[Ref.- 119]	"CVE-2019-11931". Facebook. Nov 2019. URL: https://www.facebook.com/security/advisories/cve-2019-11931
[Ref.- 120]	"El Mobile World Congress ha sido cancelado: la GSMA no celebrará el mayor evento de telefonía del mundo por el coronavirus". Xataka. Feb 2020. URL: https://www.xataka.com/eventos/mobile-world-congress-ha-sido-cancelado-gsma-no-celebrara-mayor-evento-telefonia-mundo-coronavirus URL: https://www.gsma.com/newsroom/press-release/gsma-statement-on-mwc-barcelona-2020/ URL: https://www.youtube.com/watch?v=wFoOD9SdUZE

CCN
centro criptológico nacional

2654: 5 - Qualified Certificate: AAPP
2.5.4.97=VATES-S2800155J, o=CENTRO
CRIPTOLÓGICO NACIONAL, c=ES
2020.05.13 13:53:55 +01'00'

CCN
centro criptológico nacional

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA