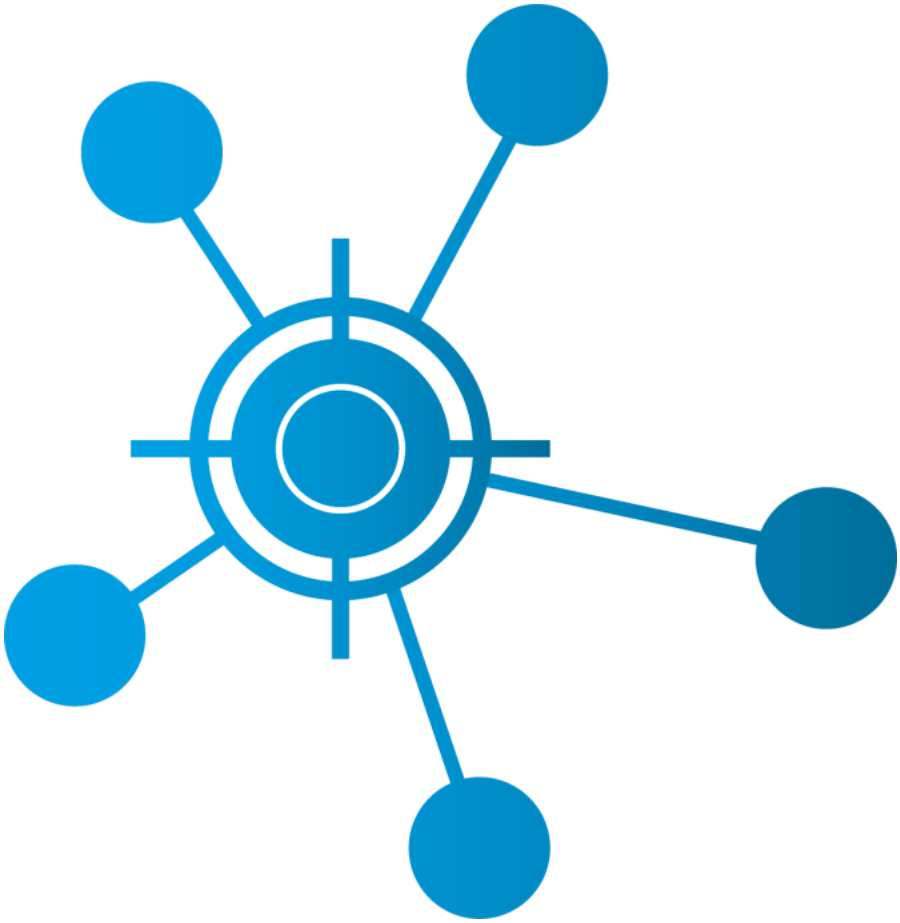
CCN-CERT IA-04/19

Informe Anual 2018
Dispositivos y comunicaciones móviles



Enero 2019

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.01.29 18:25:44 +01'00'

Fecha de Edición: enero de 2019

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 como uno de los objetivos principales de las ciberamenazas para el año 2019, 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 2018 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 2019.

3. EVOLUCIÓN DEL MERCADO DE DISPOSITIVOS MÓVILES EN 2018

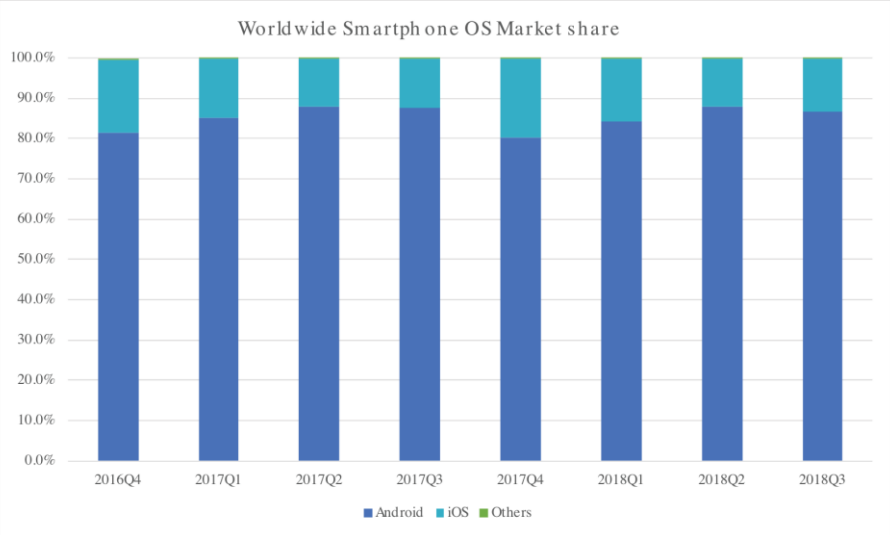
El año 2018 ha ratificado la disminución identificada (por primera vez en la historia) en el año 2017 relativa al volumen de distribución y venta de dispositivos móviles por parte de todos los fabricantes a nivel global respecto al año previo. En 2018 el declive observado fue cercano al 3,5%, con un total de 1,42 billones[1] de unidades vendidas en 2018, frente a los 1,47 billones de unidades de 2017, es decir, una media de 355 millones de unidades por trimestre en 2018 [Ref.- 1], según los estudios de IDC[2].

Algunos aspectos que han influido en este declive son la prohibición por parte de EEUU para la comercialización de dispositivos chinos de la marca ZTE, así como la lenta recuperación económica de China, junto a una ralentización en el ritmo de renovación de dispositivos móviles antiguos en los mercados ya consolidados.

La plataforma móvil Android mantiene la mayor cuota de mercado como líder indiscutible, ratificando los valores de años previos en torno al 85-87% de cuota de mercado global, seguido por iOS con una cuota entre un 13-15% (dependiendo del trimestre). Se confirma la definitiva desaparición de cualquier otra plataforma móvil existente en el pasado, como Windows Phone o Blackberry, que durante varios trimestres de 2018 aparecen reflejados en las estadísticas con un 0,0% de cuota.

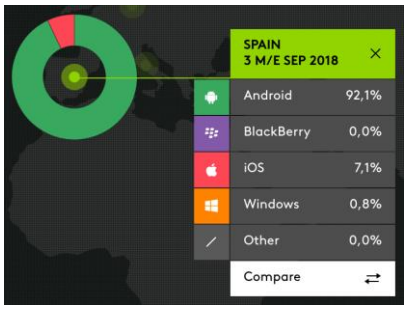
[1] Todas las referencias a billones en el presente informe corresponden a billones americanos, es decir, miles de millones de unidades.

[2] Datos obtenidos a mediados de enero de 2019, sin las estadísticas consolidadas del último trimestre de 2018 (Q4 2018), pero teniendo en cuenta las estimaciones de previsiones para ese trimestre de final del año 2018.



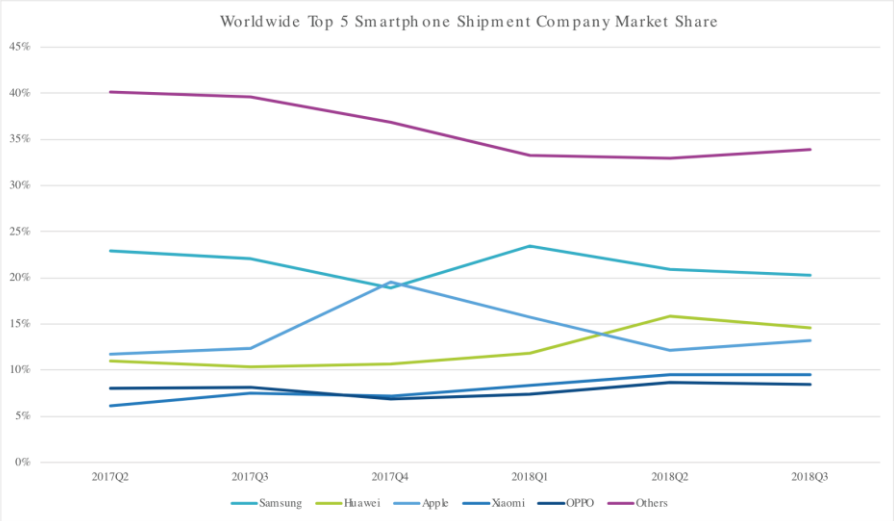
Quarter	2016Q4	2017Q1	2017Q2	2017Q3	2017Q4	2018Q1	2018Q2	2018Q3
Android	81,4%	85,0%	88,0%	87,6%	80,3%	84,3%	87,8%	86,8%
iOS	18,2%	14,7%	11,8%	12,4%	19,6%	15,7%	12,1%	13,2%
Others	0,4%	0,2%	0,2%	0,1%	0,1%	0,0%	0,1%	0,0%
TOTAL	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Por tanto, el presente informe sigue la evolución de los informes de años pasados, y se centra exclusivamente en las dos plataformas móviles relevantes a día de hoy, Android e iOS. Estas cifras globales se amplifican aún más con las estadísticas disponibles públicamente de manera específica para España, dónde en septiembre de 2018, la cuota de mercado de Android era de un 92% y la cuota de iOS de un 7% aproximadamente, aún con alguna presencia de Windows Phone (0,8%) respecto a los datos globales [Ref.- 3].



Pese al consolidado declive en el ritmo de adquisición de dispositivos móviles en la industria durante 2018, el crecimiento de ventas esperado por IDC en 2019 es más prometedor, con un ligero aumento entorno al 2,5% asociado a la demanda de terminales de más alta gama a la hora de renovar los dispositivos antiguos, interés en las pantallas flexibles (ver apartado "12. Tendencias para el año 2019") y la adopción de las tecnologías de comunicación móvil 5G (ver apartado "11. Comunicaciones móviles", aunque éstas puede que no se materialicen realmente hasta el año 2020 o

2021) [Ref.- 2]. Respecto a los fabricantes, cabe destacar que Samsung sigue liderando el mercado (con entre un 20-25% de cuota de mercado dependiendo del trimestre a lo largo de todo el 2018), y destaca cómo Huawei ha superado a Apple y se establece en el segundo puesto, con cifras cercanas al 15% y 13% respectivamente, seguidos por otros fabricantes de origen chino, como Xiaomi (que alcanza la cuarta posición, con una presencia relevante y creciente, especialmente en España[3]) y Oppo, con cuotas de mercado medias del 9,5% y 8,5% respectivamente.



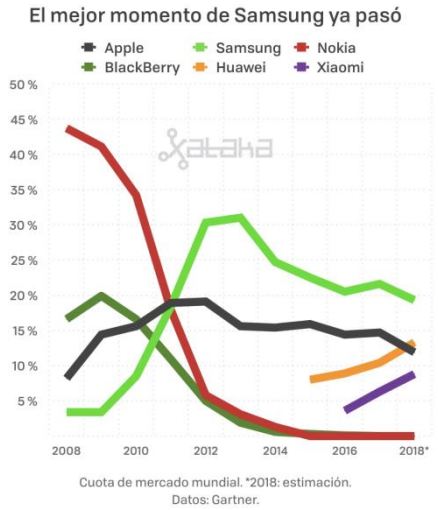
Quarter	2017Q1	2017Q2	2017Q3	2017Q4	2018Q1	2018Q2	2018Q3
Samsung	23,2%	22,9%	22,1%	18,9%	23,5%	21,0%	20,3%
Huawei	10,0%	11,0%	10,4%	10,7%	11,8%	15,9%	14,6%
Apple	14,7%	11,8%	12,4%	19,6%	15,7%	12,1%	13,2%
Xiaomi	4,3%	6,2%	7,5%	7,1%	8,4%	9,5%	9,5%
OPPO	7,5%	8,0%	8,1%	6,9%	7,4%	8,6%	8,4%
Others	40,2%	40,1%	39,6%	36,8%	33,2%	32,9%	33,9%
TOTAL	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Finalmente, respecto a la comercialización de los dispositivos móviles, cabe destacar el incremento notable en precio de los mismos, especialmente en los modelos de alta gama tanto de iOS como de Android, que ya se superan con creces la barrera de los mil euros durante 2018. Como consecuencia, la acción de Apple ya se vio afectada en noviembre de 2018 cuando la compañía anunció que no publicaría el número de unidades vendidas de sus dispositivos hardware en el futuro, asumiéndose un aumento de beneficios por el mayor precio de los dispositivos móviles, no por una mayor venta de unidades. Adicionalmente, el 3 de enero de 2019 la acción de Apple cayó un 10% (de $157,92 a $142,19), la mayor pérdida en 6 años, equivalente a un valor de mercado de 74 billones de dólares, tras anunciar oficialmente[4] una revisión a

[3] http://gs.statcounter.com/vendor-market-share/mobile/spain
[4] https://www.apple.com/newsroom/2019/01/letter-from-tim-cook-to-apple-investors/

la baja de las estimaciones en sus resultados financieros (algo que no ocurría desde 2002) y en el número de unidades vendidas de su producto estrella, el iPhone (en sus diferentes modelos). Los resultados se achacaron de nuevo a la situación económica en China (pero realmente también influye la reducida competitividad del iPhone frente a los dispositivos de fabricantes locales debido a su elevado precio, especialmente para el iPhone XS y XS Max, ampliamente criticado ya que ha crecido entre un 60-93% en los últimos 10 años [Ref.- 6]), a las tensiones entre China y EE.UU., a no cumplir las expectativas de ventas de su modelo ligeramente más económico, el iPhone XR, y a la ralentización global en el ritmo de renovación de dispositivos móviles antiguos, es decir, periodos más largos antes de que los usuarios renueven sus terminales. Este último punto ratifica la tendencia identificada en 2017 respecto a la madurez de la industria de los dispositivos móviles [Ref.- 11], siendo difícil superar la referencia de 220-230 millones de unidades vendidas por año del iPhone.

Es importante enfatizar cómo el impacto económico de una sola compañía, identificada principalmente por su dispositivo móvil estrella, el iPhone (que constituye más del 60% de los ingresos de la compañía [Ref.- 6]), tuvo un impacto más que significativo en la economía global, haciendo que cayeran todos los principales índices bursátiles (Dow Jones, Nasdaq y S&P 500) en casi un 3%[5], mostrando así la relevancia de la tecnología y de los dispositivos móviles en múltiples ámbitos de la sociedad a nivel mundial.



Este impacto económico no sólo afecta a Apple e iOS, ya que las previsiones de Samsung (recordemos el mayor fabricante de dispositivos móviles a nivel mundial) para 2019 en el mundo Android son similares [Ref.- 10], tras anunciar que tanto ingresos como beneficios caerían en el último trimestre de 2018 un 11% y 29% respectivamente, con una disminución de la distribución de dispositivos móviles del 7%

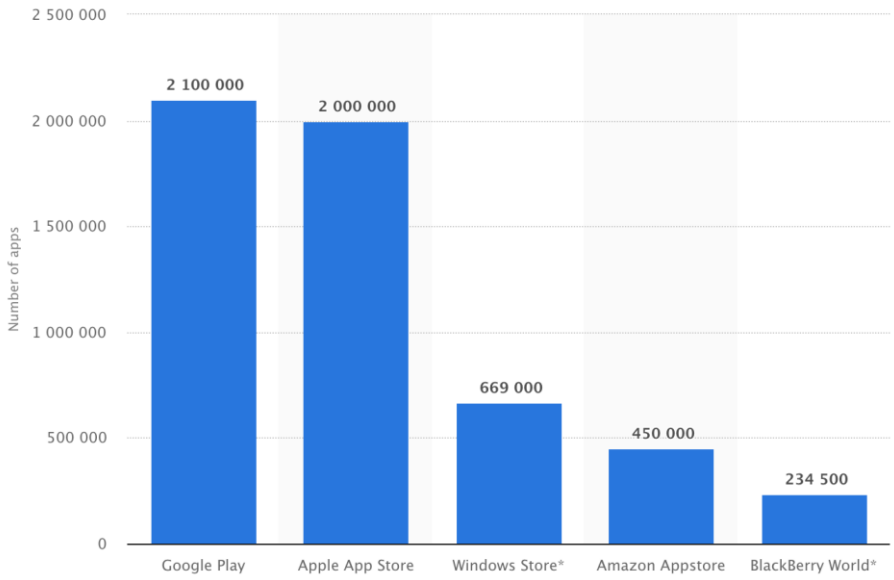
[5] https://www.cnbc.com/2019/01/03/tech-shares-dive-after-hours-after-apple-warning-nasdaq-etf-loses-nearly-2-percent.html & https://www.cnbc.com/2019/01/03/apple-stock-falls-after-cutting-q1-guidance-on-weak-iphone-sales.html

en el tercer trimestre de 2018 (comparado con el mismo trimestre de 2017[6]), ratificando así la desaceleración sufrida a lo largo de todo el 2018.

Por tanto, el 2018 y 2019 están marcando una época de madurez para el ecosistema global de dispositivos móviles, y dónde parece finalizar la hegemonía de los dos grandes fabricantes de dispositivos móviles de los últimos años (Samsung y Apple), y aparecen de forma consolidada nuevos actores, con mayores cuotas de mercado (también ratificadas por Gartner [Ref.- 10]).

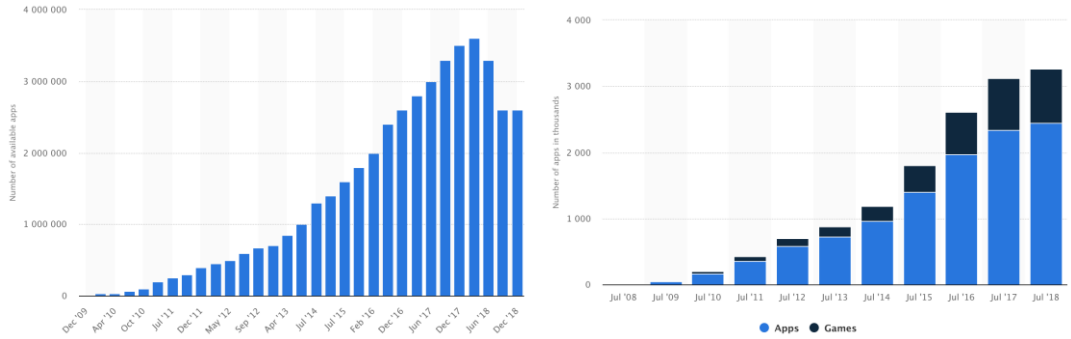
4. EVOLUCIÓN DE LOS MERCADOS OFICIALES DE APPS MÓVILES EN 2018

Las estadísticas del año 2018 consolidan el ya conocido interés, y la madurez, respecto al número total de aplicaciones móviles (en adelante, apps) disponibles en los mercados oficiales, dónde la Apple Store disponía de casi 2 millones de aplicaciones móviles en el tercer trimestre de 2018, y Google Play de 2,1 millones de apps [Ref.- 5].



Estas cifras (ligeramente variables según la fuente) reflejan cómo los mercados oficiales de apps también han madurado en 2018 con respecto al crecimiento consolidado de los últimos años, dado que se ha reducido el número de apps existentes (por primera vez en la historia) en comparación a periodos previos, dónde Google Play llegó a alcanzar los 3,6 millones de apps entre finales de 2017 y principios de 2018 [Ref.- 4], al igual que en la App Store, con un ligero descenso asociado a nuevos estándares para asegurar la calidad de las apps disponibles y su compatibilidad con las últimas versiones de iOS[7]. Estas variaciones, sin embargo, pueden ser temporales o inconsistentes, apreciándose de nuevo un crecimiento en el número total de apps en la App Store a lo largo de 2018 [Ref.- 9].

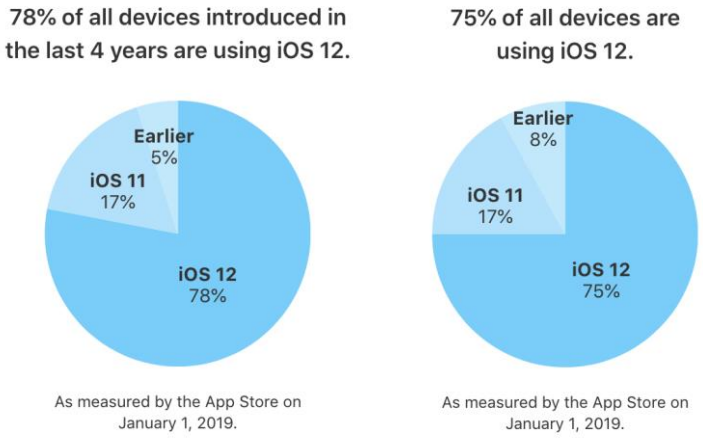
[6] https://www.marketwatch.com/story/samsung-electronics-warns-profit-will-tumble-29-2019-01-08
[7] https://www.lifewire.com/how-many-apps-in-app-store-2000252



5. ADOPCIÓN DE 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 como Apple y Google como para poder disponer de las últimas actualizaciones de seguridad frente a vulnerabilidades públicamente conocidas.

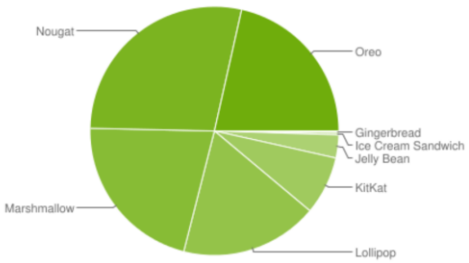
La última versión del sistema operativo iOS 12.x, publicada por Apple a mediados de septiembre de 2018, a fecha 1 de enero de 2019, es decir tres meses y medio después, estaba siendo utilizada por un 78% de usuarios con dispositivos móviles considerados recientes (es decir, comercializados en los últimos 4 años), y por un 75% de usuarios totales, en base a los datos oficiales obtenidos a través de la App Store por parte de Apple [Ref.- 8].



En el caso de Android, la última versión del sistema operativo publicada a principios de agosto de 2018, Android 9.x (Pie), está presentando un nivel de adopción muy lento con respecto a versiones previas de Android, incluso más lento que la adopción de Android 8.x en 2017. Tras más de 5 meses desde su publicación, las estadísticas oficiales de Google a mediados de enero de 2019 han quedado congeladas en el 26 de octubre de 2018, donde ni si quiera se refleja la existencia de la versión 9.0

de Android, indicando una adopción menor al 0,1% a nivel mundial (en aquel entonces, casi tres meses después de su publicación) [Ref.- 7]. En dichas estadísticas oficiales, Android 8.x (Oreo), un año y 2 meses después de su publicación, disponía de una cuota de mercado de un 21,5% (incluyendo 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 Android 9.x.

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.2%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.1%
4.2.x		17	1.5%
4.3		18	0.4%
4.4	KitKat	19	7.6%
5.0	Lollipop	21	3.5%
5.1		22	14.4%
6.0	Marshmallow	23	21.3%
7.0	Nougat	24	18.1%
7.1		25	10.1%
8.0	Oreo	26	14.0%
8.1		27	7.5%



Data collected during a 7-day period ending on October 26, 2018 (update coming soon: data feed under maintenance).
Any versions with less than 0.1% distribution are not shown.

Por tanto, las versiones de Android más comúnmente utilizadas en dicha fecha (26 de octubre de 2018) eran Android 7.x, 8.x, 6.x y, todavía, Android 5.x, con un 28,2%, 21,5%, 21,3% y 17,9% de cuota de mercado respectivamente. Este hecho ha incrementado aún más la fragmentación de Android ya conocida en años previos, al existir 4 versiones 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 es mucho peor de lo que se pensaba. Un estudio realizado a lo largo de los últimos dos años y presentado en 2018 por Security Research Labs ha desvelado como, no sólo los fabricantes de dispositivos móviles para esta plataforma fallan a la hora de proporcionar actualizaciones para sus dispositivos y usuarios, o cómo éstas se retrasan durante meses, sino cómo engañan al usuario intentado ocultar que realmente no se ha llevado a cabo la actualización por parte del fabricante, aunque el terminal indica que está completamente actualizado [Ref.- 24]. Tras hacer ingeniería inversa a cientos de dispositivos móviles Android (1.200 pertenecientes a más de una docena de fabricantes) se han encontrado diferentes escenarios, como que el terminal indica que dispone del nivel de actualizaciones hasta una fecha determinada, pero en realidad están ausentes numerosos parches de seguridad de ese periodo, haciendo que el dispositivo sea vulnerable. En casos peores, el fabricante simplemente cambia la fecha de actualización que es mostrada al usuario, sin aplicar ningún parche, creando una falsa sensación de seguridad. Por tanto, en algunos escenarios se trata de una ausencia por accidente, mientras que en otros casos se debe a una negligencia claramente intencionada. Como referencia, y de manera general, únicamente los dispositivos móviles Pixel de Google eran fieles al nivel de actualización mostrado, con ciertos fabricantes claramente ocultando la situación real de sus terminales. Por tanto, el nivel de inconsistencia identificado hace que realmente no sea posible conocer qué actualizaciones y parches han sido aplicados en un dispositivo móvil concreto.

MISSED PATCHES	0-1	1-3	3-4	4+
VENDORS	GOOGLE SONY SAMSUNG WIKO	XIAOMI ONEPLUS NOKIA	HTC HUAWEI LG MOTOROLA	TCL ZTE

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 y 2018 [Ref.- 11]), no han dado sus frutos. Será necesario esperar a los próximos años para comprobar realmente su efectividad.

En la misma línea, en 2018 Google ha comenzado a establecer requisitos más estrictos sobre los fabricantes de dispositivos móviles. Concretamente, estableciendo en los contratos que firman entre ambas partes que el fabricante se compromete (contractualmente) a ofrecer actualizaciones durante al menos 2 años para dispositivos "populares" [Ref.- 25], especificando adicionalmente que deben proporcionar al menos 4 actualizaciones de seguridad al año, es decir, trimestralmente (como mínimo). El concepto de dispositivo móvil "popular" parece que aplica a cualquier dispositivo comercializado a partir del 31 de enero de 2018 y que haya sido activado por más de 100.000 usuarios. Estos requisitos serán de aplicación a un mayor

número de dispositivos desde el 31 de julio de 2018, y a partir del 31 de enero de 2019. Google pretende que sea habitual la distribución regular de actualizaciones y parches de seguridad por parte de los fabricantes, y que, en el peor de los casos, solucionen los problemas y vulnerabilidades de seguridad de Android identificadas hace más de 90 días.

5.1 INSTALACIÓN DE UNA VERSIÓN PREVIA DEL SISTEMA OPERATIVO

Hay escenarios en los que, tras actualizar a la última versión disponible del sistema operativo móvil, podría requerirse instalar de nuevo una versión previa o más antigua, por ejemplo, por problemas de compatibilidad o de rendimiento del dispositivo móvil, o para poder realizar pruebas con versiones previas.

En iOS, desde prácticamente sus orígenes, Apple ha limitado la posibilidad de realizar un *downgrade*, es decir, llevar a cabo la instalación de una versión previa del sistema operativo, salvo durante un breve periodo o ventana de tiempo (que habitualmente está disponible justo tras la publicación de una nueva versión de iOS, para poder disponer de un margen de maniobra en el que poder solucionar posibles problemas con la nueva versión). El principal objetivo de esta medida de seguridad es evitar que cualquier usuario pueda volver atrás a una versión vulnerable de iOS, explotar una vulnerabilidad conocida, llevar a cabo el proceso de *jailbreak*, y disponer de control completo del dispositivo móvil, con las implicaciones de negocio que este escenario tendría para Apple y sus diferentes servicios de pago, como la App Store, iTunes Store, Apple Music, etc.

En el caso de Android, Google había permitido siempre la posibilidad de realizar un *downgrade* del sistema operativo. Sin embargo, en Android 8 (Oreo) se ha introducido una nueva funcionalidad, conocida como Android Rollback Protection, que no permite por defecto llevar a cabo la instalación de una versión previa del sistema operativo. De nuevo, el objetivo de esta medida de seguridad es evitar el uso de versiones antiguas de sistema operativo con vulnerabilidades que ya han sido solucionadas. Esta nueva medida de protección está vinculada a la versión 2.0 de Android Verified Boot (AVB)[8], el proceso de arranque seguro de Android disponible desde Android 8 [Ref.- 26].

La principal diferencia introducida en Android 9 (Pie) es que Google requiere que todos los dispositivos móviles que sean comercializados con Android 9 de fábrica implementen Android Verified Boot y, por tanto, Android Rollback Protection [Ref.- 27].

Por otro lado, la principal diferencia entre iOS y Android es que Apple no permite en ningún caso realizar el *downgrade*, y Google sí permite que los usuarios avanzados puedan llevarlo a cabo mediante el desbloqueo del gestor de arranque (acción que también conlleva otras implicaciones negativas desde el punto de vista de seguridad).

[8] https://android.googlesource.com/platform/external/avb/#Rollback-Protection

Asimismo, desde el punto de vista de la implementación, iOS lleva a cabo las verificaciones de actualización a través de operaciones criptográficas remotas con ciertos servidores de Apple, mientras que Android comprueba la integridad de las particiones del dispositivo móvil (boot, system, vendor, etc.) empleando índices almacenados localmente con la versión de Android actual y a instalar.

6. MECANISMOS DE AUTENTIFICACIÓN BIOMÉTRICA EN DISPOSITIVOS MÓVILES

Tal como se vaticinaba y detallaba minuciosamente en el informe de 2017 y 2018 [Ref.- 11], a lo largo de todo el año 2018 los mecanismos de autentificación biométrica se han consolidado como el elemento más habitual y solicitado para llevar a cabo el desbloqueo de los dispositivos móviles, tanto por su comodidad y facilidad de uso, y rapidez, como por su supuesta seguridad (dependiente de la implementación).

En particular, se consolidan los mecanismos de reconocimiento facial, tal como denota que todos los nuevos modelos de iPhone de Apple comercializados en 2018, como son el iPhone XR, XS y XS Max, así como los nuevos iPad Pro (de 11" y 12,9"), sólo disponen de Face ID, haciendo que el sensor de reconocimiento de la huella digital dactilar (Touch ID) forme parte del pasado (el último dispositivo móvil iOS con Touch ID es el iPad 2018 de 9.7", comercializado en marzo del pasado año).

En el caso de Android, la tendencia de los principales fabricantes de dispositivos móviles es la misma, consolidándose el uso de biometría en Android 9 (Pie) con una nueva API biométrica con soporte para el reconocimiento del iris, reconocimiento facial, y reconocimiento de la huella digital dactilar [Ref.- 28]. Un dispositivo móvil que ejemplifica el uso de estas capacidades es el Samsung Galaxy S9, ya que dispone de los tres tipos de reconocimiento biométrico [Ref.- 29][Ref.- 11]. Estas nuevas capacidades biométricas de Android 9 pretenden introducir un modelo de verificación de seguridad más avanzado, mediante la utilización de Machine Learning (ML), así como facilitar a los desarrolladores la utilización de las capacidades de autentificación biométricas dentro de sus apps.

El nuevo modelo fue introducido realmente en Android 8.1, empleándose dos nuevas métricas (denominadas Spoof Accept Rate (SAR) e Imposter Accept Rate (IAR)) para evaluar el factor de éxito y fracaso a la hora de reconocer satisfactoriamente al usuario legítimo, y no a otro usuario. Las nuevas métricas no sólo evalúan los ratios de aceptación y rechazo (tal como hacía las dos métricas existentes previamente, denominadas False Accept Rate (FAR) y False Reject Rate (FRR)), sino que también

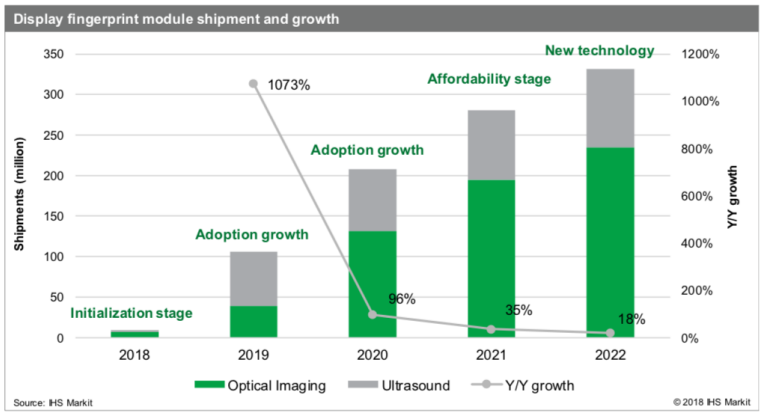
evalúan la facilidad para un potencial atacante a la hora de hacerse pasar por el usuario legítimo, mediante ataques de repetición (por ejemplo, reproduciendo una grabación de la voz o una imagen de la cara del usuario víctima) o ataques de suplantación (por ejemplo, imitando la voz o la apariencia del usuario víctima) [Ref.- 28]. Mediante estas nuevas métricas los diferentes mecanismos de autentificación biométrica son clasificados por Android como robustos o débiles. El modelo definido en Android requiere que los mecanismos más débiles estén complementados por otras medidas de seguridad como, por ejemplo, forzar a solicitar el código de acceso del dispositivo móvil después de una venta de tiempo de 4 horas sin actividad, o limitar su uso en escenarios más avanzados dentro de las apps, o para la confirmación de pagos.

Las nuevas funcionalidades disponibles para que los desarrolladores puedan emplear las capacidades de autentificación biométricas de Android dentro de sus apps se engloban en la BiometricPrompt API, ofreciendo únicamente los mecanismos biométricos considerados robustos, para ofrecer consistencia entre los múltiples dispositivos móviles en los que podría ejecutar una misma app. Independientemente de estas mejoras, otro elemento fundamental a tener en cuenta es que los desarrolladores de apps hagan un uso correcto de las librerías y APIs criptográficas proporcionadas por Google, ya que en el pasado se ha identificado un uso incorrecto de las mismas, dando lugar a la publicación de apps vulnerables que hacen uso de estas capacidades [Ref.- 30]. El estudio asociado reveló que casi un 54% de apps no realizan comprobaciones criptográficas para saber si el usuario realmente ha tocado el sensor de huella digital dactilar (pudiendo haberlo hecho un 80% de ellas), así como que menos de un 2% de las apps utilizaban las capacidades disponibles de la forma más segura posible.

La otra tendencia biométrica en el mundo Android también reflejada ya en el informe de 2017 y 2018 [Ref.- 11] era el uso de un lector de huella digital dactilar integrado en la propia pantalla del dispositivo móvil. Una de las principales ventajas de estos sensores es que son "invisibles", es decir, no consumen espacio de pantalla, tan valorado en los últimos modelos de smartphones dónde se busca disponer de pantallas sin bordes, ni con otros elementos (salvo el notch para las cámaras). En los sensores capacitivos tradicionales (basados en la medición de las cargas eléctricas) es necesario reservar un espacio dedicado al sensor de huella, únicamente para llevar a cabo el reconocimiento de la huella digital dactilar, salvo que esté situado en la parte trasera del dispositivo. El principal inconveniente de los nuevos sensores de huella digital dactilar bajo la pantalla es su compatibilidad con los protectores de pantalla tradicionales, por lo que será necesaria la comercialización de nuevos protectores fabricados con otros materiales y/o de distinto grosor. Dentro de las tecnologías empleadas para los sensores de huella digital dactilar se encuentras las capacitivas (ampliamente utilizadas actualmente), las basadas en un sensor de imagen CMOS, las que emplean un sensor óptico de imágenes, y las de ultrasonidos.

Las estimaciones de IHS Markit [Ref.- 31], publicadas en junio de 2018, vaticinan que unos 100 millones de smartphones en 2019 harán uso de sensores biométricos de

huella digital dactilar en la propia pantalla del dispositivo, año que se establece como el de adopción y mayor crecimiento de esta tecnología, con un crecimiento considerable estimado para años futuros. La mayor parte de las soluciones inicialmente harán uso de sensores de ultrasonido para posteriormente evolucionar (curiosamente, según se detalla a continuación) a sensores ópticos de imágenes.



Dentro de los modelos de dispositivo móvil disponibles a lo largo de 2018 con estas capacidades se encuentra el precursor móvil de Vivo, X20 Plus UD (mencionado en el informe de 2017 y 2018 [Ref.- 11]), con un sensor óptico de imágenes, el Oppo R17 (el sensor de Oppo es capaz de escanear un área mucho mayor que el de otros sensores actuales, *wider zone*[11]) o el Porsche Design Huawei Mate RS. Otros modelos anunciados a final de año que hacen uso de sensores ópticos son el Huawei Mate 20 Pro (junto al Honor Magic 2) y el OnePlus 6T, todos ellos empleando también sensores ópticos[9] [10]. Los sensores ópticos iluminan mediante luz el dedo del usuario, y una cámara diminuta bajo la pantalla obtiene una imagen de la huella, que es comparada con la imagen o representación de la huella previamente registrada. Este tipo de sensores sólo funcionan con pantallas OLED, a través de los huecos existentes entre los puntos de éstas, y no con pantallas LCD, ya que estas requieren disponer de una luz de fondo (backlight) que no permite al sensor de huella ver a través de la pantalla. Adicionalmente, la luz empleada por los sensores ópticos, con el paso del tiempo, podría llegar a degradar las pantallas[11]. Adicionalmente, el sensor del Mate 20 Pro dispone de 10 niveles de presión dinámica[11], lo que teóricamente mejora la velocidad de lectura de la huella y la precisión en las lecturas y, por tanto, su fiabilidad desde el punto de vista de seguridad.

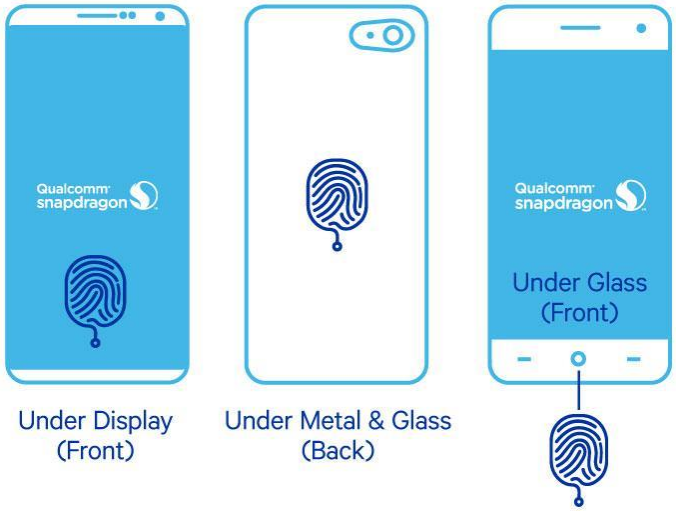
También a finales de 2018, Xiaomi ha comercializado el modelo Mi 8 Pro con un sensor óptico de Synaptics, denominado Clear ID. El sensor de Xiaomi también hace uso de un área de escaneo activa de 25x50 mm, mayor a la de otros fabricantes[12],

[9] https://www.xda-developers.com/oneplus-6t-optical-in-display-fingerprint-scanner/
[10] https://9to5google.com/2018/12/10/oneplus-6t-fingerprint-screen-unlock-tips/
[11] https://www.pocket-lint.com/phones/news/huawei/146063-in-display-fingerprint-readers-how-do-they-work
[12] https://www.theverge.com/circuitbreaker/2019/1/17/18187776/xiaomi-bigger-in-display-fingerprint-sensor

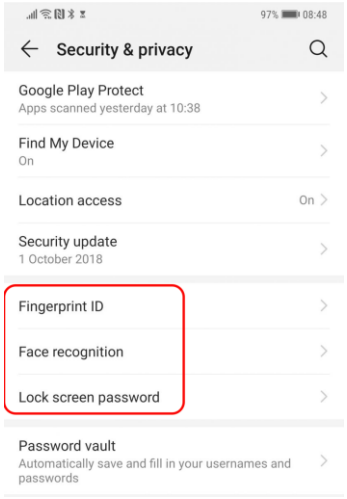
aumentando así su usabilidad. El concepto de Vivo Apex[13] en esa misma línea es disponer de la mitad, o un tercio, de la pantalla como área de trabajo del escáner óptico, aunque este tipo de alternativa puede reducir tanto la velocidad de respuesta como la fiabilidad del sensor, debiéndose evaluar de manera muy cuidadosa el equilibrio entre usabilidad y seguridad. La alternativa de Xiaomi también hace uso de un sensor de presión de muy alta sensibilidad complementario, asociado a la pantalla, lo que permite tanto agilizar el tiempo necesario para desbloquear la pantalla, así como detectar cuando se debe activar el sensor óptico y, por tanto, reducir significativamente el consumo de batería (al no tener que estar el sensor óptico constantemente escaneando la pantalla en busca de una huella, tal como ocurre con el precursor Vivo X20 UD)[14].

A finales de año, a su vez, se confirmó el uso de estas tecnologías en el futuro Samsung Galaxy S10, empleando (a diferencia de los modelos anteriores) el sensor o escáner de huella ultrasónico integrado en la pantalla de Qualcomm[15] (denominado 3D Sonic Sensor, en su tercera generación)[16] [17]. Este sensor no compara la huella contra un patrón bidimensional registrado previamente (tal como hacen los sensores ópticos), sino que crea un molde tridimensional de la huella del usuario mediante el envío de ondas de (ultra)sonido a través de la pantalla del dispositivo, con la posibilidad de capturar minuciosos detalles sobre los poros y rugosidades de la huella dactilar, siendo más similar a las representaciones tridimensionales empleadas en el reconocimiento facial, y supuestamente más fiable que los sensores de huella digital dactilar ópticos [Ref.- 32]. Los sensores ultrasónicos (de Qualcomm) son capaces de funcionar a través de superficies de pantallas OLED, cristal o metal (aluminio), con diferentes grosores según el tipo de material, e incluso dentro del agua (a diferencia de los sensores capacitivos actuales), pudiendo reconocer tanto gestos como obtener información sobre el ritmo cardiaco del usuario y detectar el flujo sanguíneo (información que potencialmente también podría ser empleada para el proceso de autentificación, combinada con los mecanismos biométricos ya existentes, aunque no paree que actualmente esté siendo utilizada).

[13] https://www.androidauthority.com/vivo-apex-hands-on-840339/
[14] https://www.gizmochina.com/2018/09/24/how-xiaomi-and-vivos-in-display-fingerprint-scanning-technology-differ/
[15] https://www.qualcomm.com/news/onq/2017/07/05/qualcomm-fingerprint-sensors-transform-device-authentication
[16] https://www.t3.com/news/samsung-galaxy-s10-in-display-ultrasonic-fingerprint-sensor-is-unmasked
[17] https://www.cnet.com/news/qualcomm-announces-first-ultrasonic-fingerprint-reader-headed-to-the-galaxy-s10/



Desde el punto de vista de seguridad, habrá que esperar aún para evaluar la efectividad de este nuevo tipo de sensores de huella digital dactilar integrados bajo la pantalla frente a los existentes actualmente, vaticinándose que investigaciones futuras los pondrán a prueba para identificar su ratio de error o la facilidad para suplantar al usuario legítimo. Supuestamente, los nuevos sensores ultrasónicos son más precisos que los ópticos, y no pueden ser engañados fácilmente con una simple imagen de la huella del usuario, riesgo que ya ha afectado a algunos sensores ópticos. Especialmente, queda pendiente evaluar el nivel de seguridad de estos sensores de huella digital dactilar en comparación a las soluciones basadas en el reconocimiento facial en tres dimensiones (3D), o la convivencia de ambos, tal como ocurre en algunos terminales Android actuales[18].



A principio de 2019 se publicó que en el CES de 2018 Google sembró la duda respecto a si los sensores ópticos de huella digital dactilar son suficientemente seguros como para ser empleados en los pagos móviles o apps bancarias (haciendo uso de los

[18] https://www.t3.com/reviews/huawei-mate-20-pro-review

mecanismos de autentificación de la TrustZone) [Ref.- 33]. Futuras investigaciones confirmarán el nivel de seguridad de estos y su integración finalmente en la nueva arquitectura de seguridad de Android 9. La decisión de Google tendrá un impacto directo en la industria y en el tipo de sensores utilizados en el futuro por los fabricantes de dispositivos móviles Android, dejando como única opción (al menos actualmente) los sensores ultrasónicos (más fiables y caros).

En resumen, el futuro de la autentificación en iOS parece que se centra en el uso de mecanismos biométricos de reconocimiento facial (Face ID) por parte de Apple, mientras que en el mundo Android se dispone de numerosas alternativas biométricas, destacando principalmente los sensores de huella digital dactilar integrados en la pantalla del dispositivo móvil, junto a soluciones de reconocimiento facial (siendo el reconocimiento del iris una tecnología con menor adopción).

7. DESBLOQUEO DE DISPOSITIVOS MÓVILES Y EXTRACCIÓN FORENSE DE DATOS

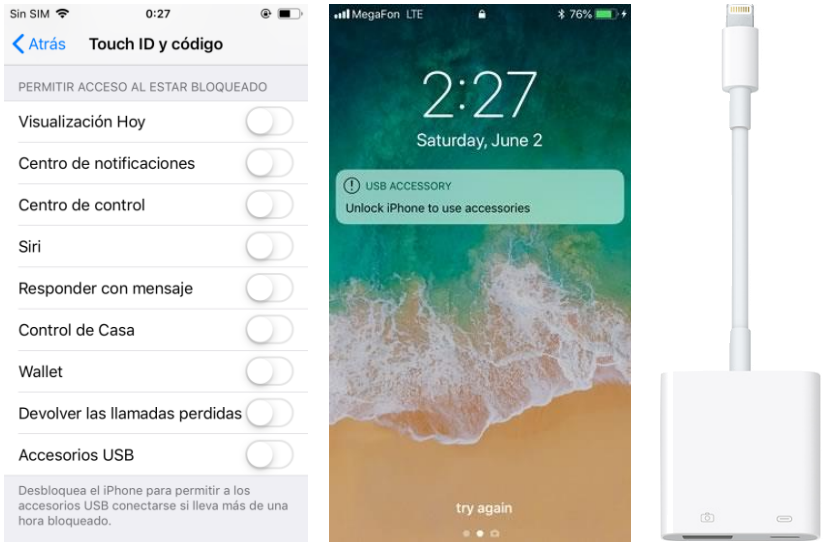
El informe anual de amenazas de 2017 y tendencias de 2018 de dispositivos y comunicaciones móviles publicado el pasado año por el CCN-CERT [Ref.- 11] ya reflejaba la relevancia que seguía tomando la posibilidad de evitar la pantalla de autentificación o bloqueo de los dispositivos móviles, junto a la 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. A este respecto, siempre es interesante comparar las capacidades de protección frente a este tipo de amenazas de las dos plataformas móviles principales, iOS y Android [Ref.- 13].

El año 2018 se ha caracterizado por los avances y modificaciones realizadas por Apple en las distintas versiones y subversiones de iOS con el objetivo de restringir los posibles accesos disponibles por parte de las soluciones comerciales de análisis forense de dispositivos móviles. Éstas ya fueron descritas en detalle en el informe de 2017 y 2018 [Ref.- 11], incluyendo los servicios avanzados de desbloqueo y extracción de datos de Cellebrite y el producto GrayKey de Grayshift.

Para contrarrestar estas capacidades ofensivas, Apple incluyó en iOS 11 una nueva funcionalidad conocida como modo restringido USB para accesorios. Esta característica de seguridad, disponible y habilitada por defecto desde iOS 11.4.1, deshabilita las capacidades de transmisión de datos del puerto USB, o conector Lightning, de los dispositivos móviles iOS tras transcurrir una hora[19] sin haberse desbloqueado el dispositivo móvil. Pasado ese tiempo desde el último evento de bloqueo, el dispositivo móvil no reconocerá ni establecerá ninguna conexión de datos con cualquier accesorio o periférico conectado a través del puerto o conector

[19] Inicialmente, en las versiones de iOS 11 beta previas, esta restricción era de aplicación tras 7 días, mucho menos restrictiva.

Lightning, como por ejemplo los empleados para la extracción de datos forenses sin autorización, salvo que el usuario proceda a desbloquear el dispositivo. Adicionalmente, la activación del modo de emergencia (o SOS) de iOS activa también el modo restringido USB [Ref.- 14], además de deshabilitar las capacidades biométricas (Touch ID o Face ID) de autentificación.



Se desconoce si Apple se ha visto forzado a introducir todas estas medidas de protección adicionales porque no dispone de todos los detalles acerca de las vulnerabilidades explotadas por las soluciones forenses comerciales de extracción de datos de iOS vía USB, o si se debe a que, pese a conocerlos, no es posible solucionar dichas vulnerabilidades sin afectar a la funcionalidad y/o compatibilidad hacia atrás de iOS, viéndose por tanto forzada simplemente a intentar mitigarlas [Ref.- 16]. La realidad es que, pese a todas las medidas descritas e introducidas por Apple en las últimas versiones de iOS, es todavía posible evitar las mismas mediante la conexión de un ordenador o un accesorio USB (incluso uno que no sea de confianza, es decir, no previamente conocido) al dispositivo móvil mientras aún no ha vencido el temporizador de una hora, es decir, en los 60 minutos posteriores al último evento de bloqueo del dispositivo móvil como, por ejemplo, el adaptador oficial de Lightning a USB o USB 3 para una cámara, o el adaptador de Lightning a HDMI (Digital AV) o VGA (que adicionalmente disponen de un conector de Lightning extra para permitir la carga simultánea del dispositivo móvil desde el propio adaptador).

Posteriormente, Apple introdujo mejoras en iOS 12 tal como se detalla en la guía práctica de seguridad de dispositivos móviles iPhone para iOS 12 del CCN-CERT [Ref.- 17]. Adicionalmente a la activación del modo restringido USB tras una hora desde el último desbloqueo del dispositivo, y/o una hora desde que el dispositivo móvil ha sido desconectado de un accesorio USB o un ordenador, en iOS 12 la conexión de datos vía USB también se deshabilitará 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, o si se han deshabilitado los mecanismos de autentificación biométrica y se requiere introducir el código de acceso [Ref.- 15].

Android 9 ha introducido un nuevo modo de bloqueo, conocido como Lockdown Mode (deshabilitado por defecto), similar al modo de emergencia (o SOS) de iOS, que permite que el usuario deshabilite de forma sencilla y rápida las capacidades de autentificación biométrica del dispositivo móvil, incluyendo la funcionalidad de Smart Lock, y ocultando todas las notificaciones [Ref.- 67]. Estos modos fuerzan a que sea necesario introducir el código de acceso para hacer uso del dispositivo.

Por otro lado, 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, permitiendo así el acceso a información parcial o total almacenada en los mismos, continua [Ref.- 12]. A lo largo del año 2018 se han publicado numerosas vulnerabilidades tanto para la versión 11 como la versión 12 de iOS, que permiten el acceso al identificador de Apple del usuario, deshabilitar las capacidades remotas de búsqueda del dispositivo, habilitar Siri (el asistente digital personal), o acceso al contenido de las notificaciones, contactos, fotos, conocer la última app utilizada, o compartir contenidos, 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).

8. MECANISMOS DE SEGURIDAD AVANZADOS EN DISPOSITIVOS MÓVILES

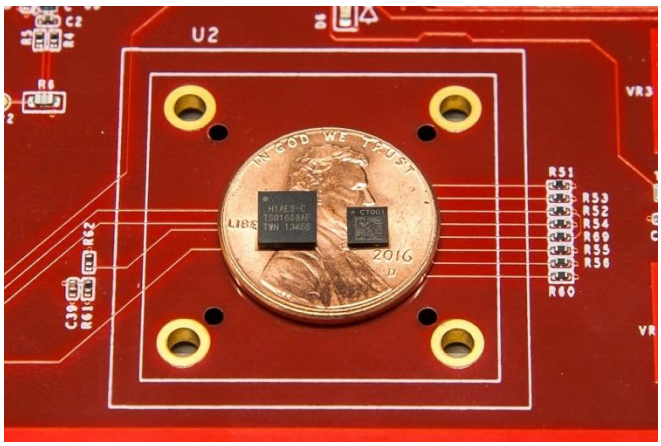
Con el objetivo de proteger los datos almacenados en los dispositivos móviles Android, especialmente cuando son transferidos a un ordenador local (fuera del alcance de la siguiente funcionalidad) o incluso a los servicios de almacenamiento en la nube de Google (Google Cloud Platform, o GCP), Android 9 introduce cambios relevantes. Pese a que las capacidades para cifrar las copias de seguridad (o backups) de Android existen desde hace años, estas eran opcionales y, además, en el caso de los backups en la nube, aunque estaban cifrados (según Google) no hacían uso del código de acceso del usuario. En Android 9, sin embargo, se cifran los backups por defecto, empleando una clave de cifrado protegida por el código de acceso [Ref.- 34], aunque esta funcionalidad puede ser deshabilitada por el usuario.

Estas capacidades están asociadas al nuevo servicio Cloud Key Vault (CKV) de Google Cloud, que hace uso de dispositivos hardware criptográficos de seguridad (como por ejemplo el chip o procesador Titan[20], diseñado por el propio Google) para almacenar claves criptográficas protegidas por el código de acceso del dispositivo móvil [Ref.- 34]. La clave criptográfica de cifrado (creada de manera aleatoria en el cliente) es protegida mediante cifrado con el código de acceso del usuario, y el resultado es almacenado en el chip Titan disponible en los servidores de Google. La misma sólo puede ser obtenida cuando se demuestra conocer el código de acceso, y el chip Titan adicionalmente implementa medidas para evitar ataques de fuerza bruta

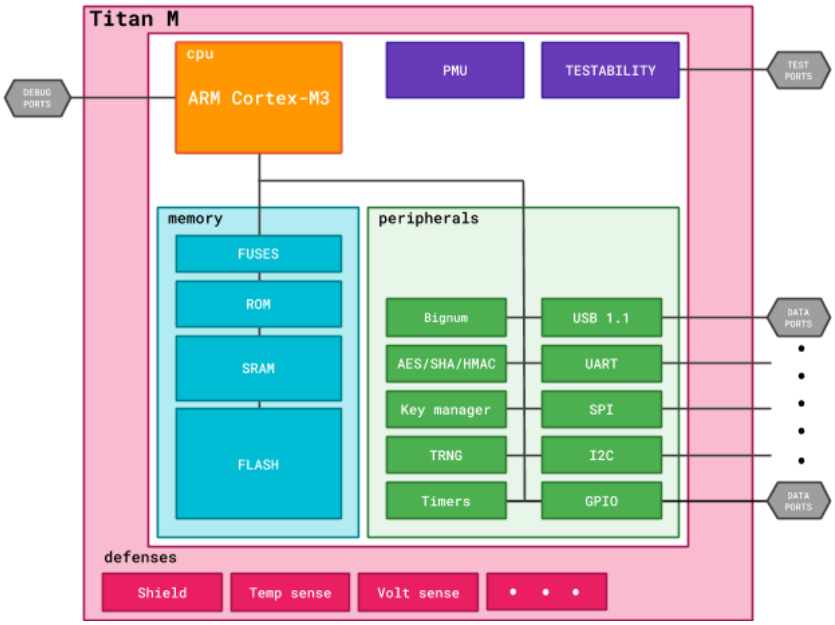
[20] https://cloud.google.com/blog/products/gcp/titan-in-depth-security-in-plaintext

contra este código [Ref.- 35]. En realidad, por tanto, el servicio actúa como un repositorio de claves en la nube, en este caso, empleado para cifrar los backups de Android 9.

Con la comercialización del Pixel 3 y Pixel 3 XL, Google ratificó no solo la utilización del chip criptográfico de seguridad Titan en sus servidores en la nube, sino también en sus dispositivos móviles más modernos [Ref.- 36][Ref.- 36], denominado Titan M (o Mobile)[21]. Titan M constituye una evolución del módulo de seguridad hardware ya introducido por Google en el Pixel 2 el año previo[22]. Dentro de las funciones de este chip criptográfico de seguridad hardware, separado físicamente del procesador principal y diseñado por Google, está dar soporte a múltiples características de seguridad de Android, como Verified Boot (por ejemplo, participando en la verificación de posibles ataques de *downgrade*, ver apartado "5.1. Instalación de una versión previa del sistema operativo"), el proceso de desbloqueo y cifrado del dispositivo móvil[22], y Protected Confirmación (descrito a continuación), el almacenamiento y posterior obtención de secretos mediante StrongBox[23] (un nuevo tipo de KeyStore), mecanismos seguros para la restauración del dispositivo móvil, evitar ciertos ataques de canales laterales (*side channel attacks*, como Rowhammer, Spectre y Meltdown), u ofrecer resistencia incluso a ataques internos, por ejemplo, en el propio proceso de actualización del firmware de Titan M[24]. Uno de los principales objetivos de Google con Titan M es establecer una plataforma de seguridad basada en la transparencia (en su diseño, código de arranque, firmware, modo de funcionamiento, etc.) y que sirva de referencia para innovaciones futuras en este campo (segundo factor de autentificación, dispositivos médicos, pagos entre usuarios, etc.).



[21] La imagen muestra el chip Titan a la izquierda, y el chip Titan M a la derecha, de menor tamaño.
[22] https://www.blog.google/products/android-enterprise/how-pixel-2s-security-module-delivers-enterprise-grade-security/
[23] https://android-developers.googleblog.com/2018/05/whats-new-in-android-p-beta.html
[24] https://android-developers.googleblog.com/2018/10/building-titan-better-security-through.html



Adicionalmente, Android 9 introdujo Android Protected Confirmation, un mecanismo para vincular las capacidades hardware de seguridad del dispositivo móvil (es decir, el Trusted Execution Environment, TEE) con el interfaz de usuario, empleando un interfaz de usuario confiable o seguro (Trusted UI), para la realización de transacciones críticas y sensibles (fuera del control del propio sistema operativo) [Ref.- 37]. Este sistema permite que el usuario tome decisiones de seguridad con confianza, por ejemplo, en apps bancarias, incluso pese a la existencia de apps fraudulentas o estar el sistema operativo comprometido. Para la implementación se hace uso de criptografía para firmar y verificar los mensajes de confirmación. Este sistema también puede ser utilizado en múltiples escenarios, como añadir confianza en los mecanismos de segundo factor de autentificación, intentando proteger que puedan aceptarse como válidos si han sido interceptados (por ejemplo, los SMS de confirmación de transferencias bancarias), o para la gestión de dispositivos médicos, y controlar, por ejemplo, la dosis de insulina que debe ser administrada.

Como resultado de todos estos avances, Google ha llevado a cabo en sus últimos dispositivos móviles de 2018 avances significativos desde el punto de vista de seguridad centrados en la integración del hardware y el software, en concreto del sistema operativo Android y chips criptográficos de seguridad hardware, similares a los proporcionados por Apple con el iPhone e iOS a través del Security Enclave Processor (SEP), al disponer ambos en 2018 de control de todo el ecosistema y plataforma móvil. Esta evolución de Android se refleja también en la publicación por parte de Google del "Android Enterprise Security White Paper" [Ref.- 38], centrado en las capacidades de seguridad empresariales de Android (complementando el nuevo programa de recomendaciones empresariales de Google[25]), similar a la guía oficial de seguridad para iOS de Apple [Ref.- 39], actualizada para cada nueva versión (o subversión relevante) de iOS. Desafortunadamente, en el momento de elaboración del presente informe,

[25] https://www.android.com/enterprise/recommended/

aún no se disponía del informe anual de seguridad del ecosistema Android para 2018 [Ref.- 38]("Android Security 2018 Year in Review"), siendo el último publicado por Google el del año 2017[26].

De manera similar, dentro de las capacidades de seguridad de bajo nivel más avanzadas de los dispositivos móviles, iOS 12 o, más concretamente, la última generación de dispositivos móviles de Apple, el iPhone XR, XS y XS Max incorporaron procesadores con la última versión de la arquitectura ARM, ARM v8.3, en su chip A12 Bionic[27]. Qualcomm ha incorporado en esta última versión de la arquitectura un nuevo mecanismo de seguridad de protección de la memoria, denominado Pointer Authentication Codes (PAC) [Ref.- 40], cuyo principal propósito es dificultar la explotación de vulnerabilidades asociadas a la corrupción de memoria, como por ejemplo buffer overflows, integer overflows, etc. De manera resumida, los PACs son códigos de autentificación e integridad criptográficos (MACs) empleados para identificar la manipulación de la dirección de memoria a la que apunta una instrucción concreta (denominado puntero), proporcionando por tanto integridad para los punteros a memoria. Por tanto, esta nueva protección dificultará supuestamente el proceso de explotación de iOS 12 y de generación de nuevos jailbreaks para los últimos dispositivos móviles iPhone de Apple. A lo largo del año 2018, se han liberado varios *jailbreaks* para diferentes versiones de iOS 11, tales como LiberiOS[28], Electra[29] o unc0ver[30], acompañados de todo el drama y el impacto mediático que rodea a este tipo de herramientas en los últimos años.

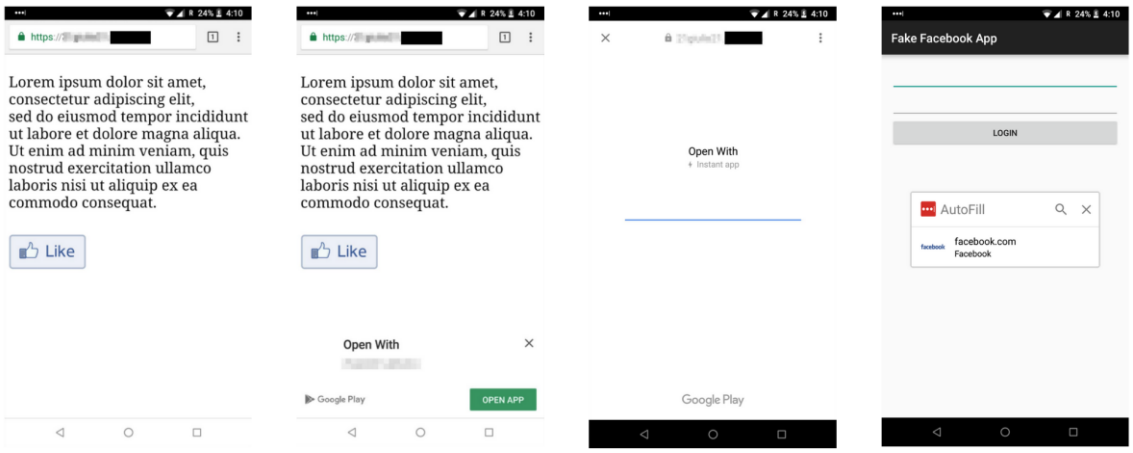
9. CÓDIGO DAÑINO PARA PLATAFORMAS MÓVILES

El informe anual de 2017 y 2018 [Ref.- 11] del pasado año confirmaba que las nuevas capacidades de Android para ejecutar apps instantáneamente, conocidas como Instant Apps, no habían dado lugar directamente a la distribución de especímenes de software malicioso que hicieran uso de esta funcionalidad. Sin embargo, en 2018 se publicó una investigación que detallaba como esta funcionalidad, junto a las nuevas capacidades asociadas a los gestores de contraseñas móviles (estudiando los 5 más comunes: Keeper, Dashlane, LastPass, 1Password y Google Smart Lock) pueden ser abusadas para ejecutar ataques de phishing de manera más sencilla y práctica que los que podían ser ejecutados hasta ahora [Ref.- 41].

El estudio detalla como los gestores de contraseñas de Android pueden ser engañados para auto desvelar las credenciales asociadas a sitios web elegidos por el atacante, así como también ser víctima de ataques centrados en el auto relleno de campos ocultos de contraseña, no visibles para el usuario, desvelando la contraseña del usuario. Asimismo, mediante el uso de Instant Apps, un atacante podría tomar

[26] https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf
[27] https://www.apple.com/lae/iphone-xs/a12-bionic/
[28] http://newosxbook.com/liberios/
[29] https://coolstar.org/electra/
[30] https://github.com/pwn20wndstuff/Undecimus

control completo del interfaz de usuario del dispositivo móvil y, abusando los gestores de contraseñas, lanzar un ataque de phishing completo únicamente con unas pocas pulsaciones por parte del usuario. Los gestores de contraseñas móviles no comprueban si una app es de tipo Instant o no, por lo que sugieren las credenciales que gestionan a ambos tipos de apps, facilitando los ataques de phishing vía Instant Apps.



El software malicioso, o malware móvil, para dispositivos móviles, especialmente para Android, sigue en constante evolución, identificándose numerosos especímenes a lo largo del año, tanto de malware como de spyware, para esta plataforma móvil. Los siguientes ejemplos detallados 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 los años previos, los dispositivos móviles son uno más de los objetivos de las amenazas y el malware, y así lo indican las predicciones de seguridad para 2019, donde Android sigue siendo el objetivo principal. En el caso de iOS, se hace necesaria habitualmente la concatenación de múltiples exploits para vulnerabilidades aún no publicadas (0-day), el uso de servidores falsos vinculados a soluciones MDM, o la utilización de la ingeniería social para convencer al usuario de que relaje el nivel de seguridad de su dispositivo, con objeto en todos los casos de instalar apps maliciosas. Está aún por ver si la filtración del código fuente del sistema de arranque de iOS que tuvo lugar a principio de 2018, aunque pertenecía a una versión no eminentemente reciente, puede facilitar la identificación de vulnerabilidades que sean puestas en práctica en ataques reales [Ref.- 42].

Dentro de las predicciones de 2019, en 2018 se puede concluir que la era del malware simple para Android ha finalizado, debido a su sofisticación, y unido al incremento de las medidas de seguridad en las últimas versiones de Android [Ref.- 43]. Algunas estadísticas reflejan un incremento del 40% al final del tercer trimestre de 2018 en el número de nuevos especímenes de malware móvil para Android con respecto al año previo, con unas estimaciones de 4 millones de nuevas apps maliciosas

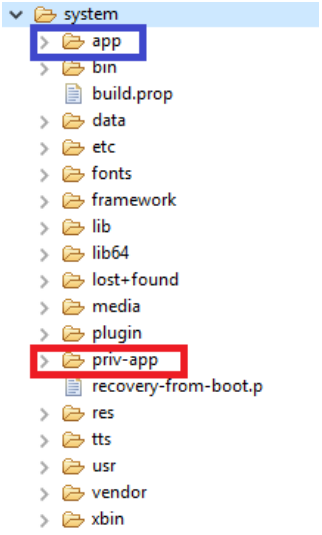
a lo largo de todo el año 2018. Estas negativas cifras record implican que aparecerían casi 11.000 nuevas apps maliciosas cada día, o una app cada menos de 8 segundos [Ref.- 44].

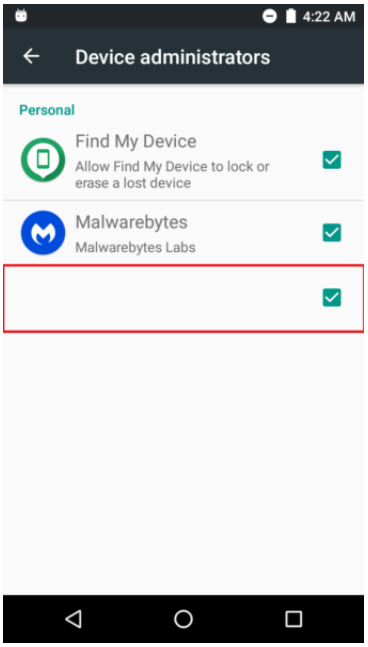
El informe anual de Sophos de finales de 2018 (denominado 2019) [Ref.- 45], también ratifica el crecimiento global de malware móvil, destacando algunas campañas como las de apps maliciosas que simplemente proporcionan una ventana de navegación web (WebView) para ataques de phishing (desarrolladas en sincronización con el sitio web de phishing), principalmente contra bancos online, evitando así ningún tipo de detección al ser distribuidas a través de la Play Store. Otros especímenes se han introducido en apps legítimas de fabricantes de dispositivos móviles, como Sound Recorder, tras vulnerar la cadena y el proceso de desarrollo de esta compañía o de uno de sus *partners*, ratificando la distribución de malware móvil preinstalado (tendencia descrita a continuación). Asimismo, se ha identificado un incremento en la distribución de código para minar criptomonedas dentro de otras apps, como juegos o utilidades. Dicho código puede ser ejecutado tanto cuando la app está siendo utilizada, como cuando no, y tiene un impacto directo en el consumo de batería del dispositivo móvil. Dado que este código no es inherentemente malicioso, es habitual que se permita su distribución a través de la Play Store. Por último, el fraude a través de anuncios constituye uno de los negocios más lucrativos actualmente, y su distribución a través de apps móviles juega un papel muy relevante y creciente. El coste estimado de anuncios fraudulentos (sobre los que supuestamente ha pulsado el usuario) a nivel global (no sólo móvil) es de 19 billones de dólares al año.

Una tendencia que podría materializarse a lo largo de 2019 aún más es la asociada a la existencia de malware móvil pre-instalado en algunos dispositivos, con las implicaciones que este escenario conlleva, ya que el malware forma parte, o es en sí mismo, una app de sistema (que no puede ser desinstalada, aunque sí deshabilitada o desactivada en algunos casos) [Ref.- 46]. Un primer ejemplo fue Adups, con variantes que han evolucionado a lo largo de 2016 y finales de 2017, una app preinstalada en dispositivos de fabricantes como BLU (Bold Like Us), como el modelo BLU Studio G2 HD, que no podía ser ni siquiera desactivada fácilmente desde el interfaz de usuario de Android, salvo a través de ADB y la línea de comandos a través del gestor de paquetes

(pm, package manager)[31] [Ref.- 47]. Adups dispone de un auto-instalador para instalar otros especímenes de malware.

El malware pre-instalado puede residir bajo "/system/app" o bajo "/system/priv-app", siendo esta última la ubicación oficial para las apps más relevantes en Android. Otro ejemplo de este tipo de malware es Riskware, descubierto en el modelo THL T9 Pro, embebido en la app System UI (en lugar de tratarse de una app independiente), app fundamental para el correcto uso de Android al implementar el interfaz de usuario [Ref.- 46]. Otro ejemplo es Monitor, descubierto en el modelo UTOK Q55, centrado en la recolección y envío de información sensible del usuario. En este caso, el malware se encontraba embebido en la app Settings, encargada de la gestión de los ajustes de configuración de Android. Estas infecciones, donde el código malicioso se ha embebido y, por tanto, ha troyanizado apps críticas de sistema, son complejas de remediar. En algunos casos se podría sustituir la app troyanizada por una versión legítima de la misma para la misma versión de Android.





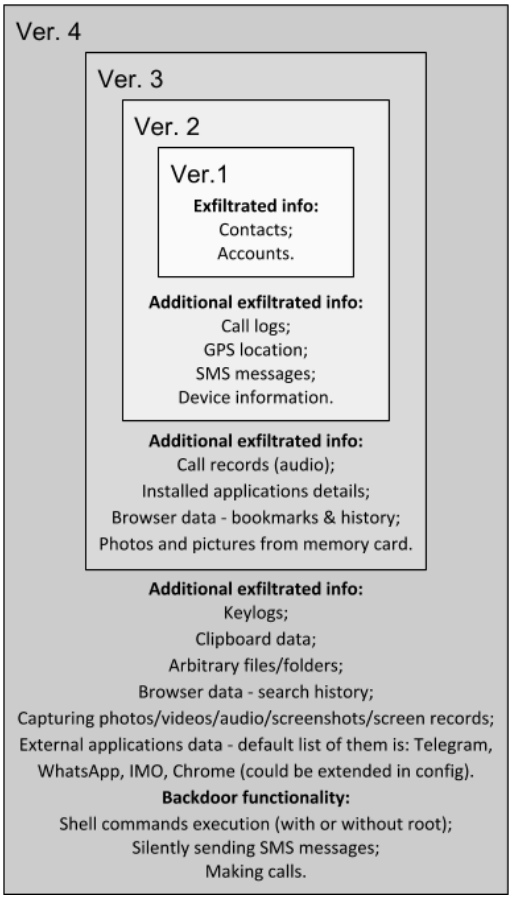
Complementariamente, dentro de las amenazas del malware móvil identificadas en 2018 sigue estando el ransomware móvil, bloqueando el dispositivo móvil o amenazando al usuario con multas y acciones legales por parte de los cuerpos y fuerzas de seguridad del estado, adware para la obtención de beneficios económicos a través de anuncios (como por ejemplo MobiDash, muy activo) y que en algunos casos se ha distribuido a través de la Play Store (como por ejemplo HiddenAds) o, como se ha descrito previamente, la existencia de malware preinstalado [Ref.- 47]. En muchos casos, el malware siempre intenta obtener permisos como administrador del dispositivo e implementa diferentes medidas para no perderlos una vez obtenidos, como ocultarse o dificultar su desinstalación (ver imagen superior derecha).

[31] https://forums.malwarebytes.com/topic/216616-removal-instructions-for-adups/

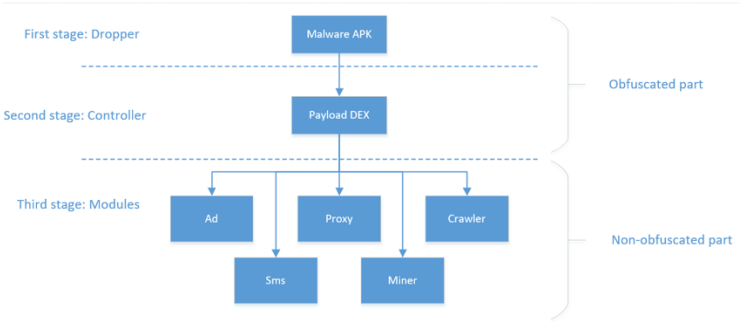
Como curiosidad, a principio de 2018 se publicó la referencia a la primera app maliciosa (malware móvil) que hacía uso del nuevo lenguaje de programación para Android, denominado Kotlin, e introducido por Google en mayo de 2017. Este malware registraba al usuario víctima en servicios SMS Premium, entre otras acciones (ejecución remota de comandos, redirecciones a sitios web, robo de información, etc.), aunque se hacía pasar por una app de limpieza del dispositivo móvil, denominada Swift Cleaner, que estaba disponible en la Play Store con entre 1.000 y 5.000 descargas [Ref.- 48].

En mayo de 2018, se publicaron los detalles de una operación de ciberespionaje denominada ZooPark, especialmente activa contra usuarios de Android en Oriente Medio (Egipto, Jordania, Marruecos, Líbano e Irán) durante varios años [Ref.- 49]. Esta campaña ha hecho uso de diferentes generaciones, o versiones, de una misma familia de malware, que ha ido evolucionando y añadiendo nuevas capacidades con cada versión (de v1 a v4), siendo v4 la más reciente, un spyware comercial complejo y muy sofisticado desplegado en 2017. La siguiente imagen resume la funcionalidad de cada versión, y sus capacidades.

ZooPark ha sido distribuido principalmente a través de canales de Telegram o de sitios web previamente comprometidos (*watering holes*) como, por ejemplo, sitios web de noticias.



En diciembre de 2018, Kaspersky publicó la existencia de un espécimen de malware móvil para Android, denominado Loapi (potencialmente vinculado a otro malware denominado Podec), que implementa una compleja arquitectura modular para llevar a cabo múltiples actividades ilícitas [Ref.- 50]. El malware incluye módulos para el minado agresivo de criptomonedas (como Monero), la distribución de anuncios, la ejecución de ataques de denegación de servicio distribuidos (DDoS), generación de tráfico web, subscripción del usuario víctima a servicios de pago, etc. Este malware se distribuye a través de campañas de anuncios y se oculta habitualmente tras apps de soluciones antivirus o de contenido para adultos. Uno de sus objetivos iniciales es obtener permisos como administrador del dispositivo (implementando diferentes medidas para no perderlos una vez obtenidos), y se ha descubierto que futuros módulos podrían aprovechar la ventaja de infectar dispositivos móviles ya rooteados (en función de las comprobaciones que realiza actualmente). Como novedad, este malware monitoriza la existencia o instalación de una serie de apps legítimas de protección del dispositivo (como soluciones de seguridad comerciales), para una vez detectadas, instar al usuario a su eliminación.



Ya en Android 8 (Oreo), con el objetivo de limitar el uso y abuso de los servicios de telefonía del dispositivo móvil por parte de apps maliciosas, Google introdujo permisos más granulares, ANSWER_PHONE_CALLS y READ_PHONE_NUMBERS, limitando que una app pudiera fácilmente obtener el número de teléfono del usuario y del llamante. Sin embargo, era posible evitar las restricciones asociadas a éstos mediante la utilización de los mensajes de broadcast PhoneStateListener, simplemente disponiendo del permiso READ_PHONE_STATE. Para mitigar esta debilidad, Android 9 (Pie) introduce un nuevo permiso, READ_CALL_LOG[32], necesario para poder acceder a los detalles de los mensajes de broadcast mencionados. De esta forma, una app deberá solicitar este nuevo permiso para poder acceder a la información personal de telefonía del usuario.

En Android 9, para proteger aún más la privacidad del usuario (aspecto también analizado, debido a su relevancia actual, en el apartado "10. Privacidad del usuario en las plataformas móviles"), se limita el acceso a los sensores por parte de apps de terceros que ejecutan en segundo plano o de fondo (*background*), de forma que no

[32] https://developer.android.com/about/versions/pie/android-9.0-changes-all#privacy-changes-all

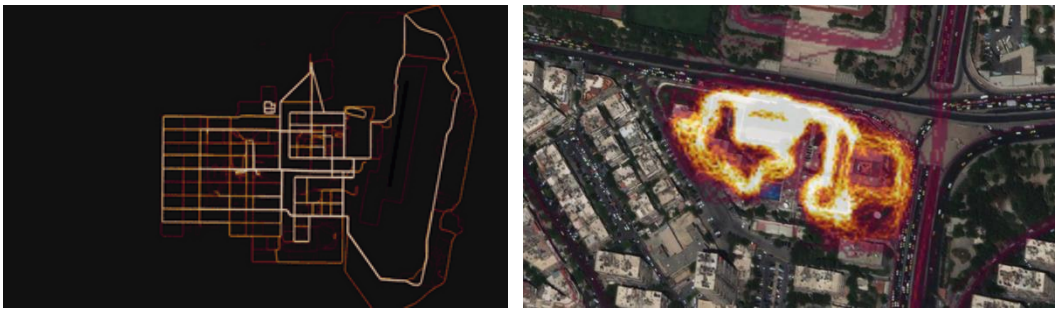
podrán acceder ni al micrófono, ni a la cámara, ni recibir eventos de sensores que operan de forma continua (como, por ejemplo, el acelerómetro o el giroscopio) [Ref.- 51]. Esta nueva medida de protección puede mitigar las acciones realizadas por el código dañino diseñado para Android y, en concreto, por numerosas apps y juegos (más de 250) que capturaban el audio del micrófono para saber que estaba escuchando el usuario, por ejemplo, durante espectáculos, programas y películas, y proporcionar así anuncios personalizados [Ref.- 52]. La precisión de la librería empleada, o plugin (perteneciente a una start-up denominada Alphonso), permite procesar el audio incluso cuando el dispositivo móvil está en el bolsillo o bolso del usuario.

10. PRIVACIDAD DEL USUARIO EN LAS PLATAFORMAS MÓVILES

Pese a no tratarse directamente de código dañino, pero teniendo en cuenta la relevancia que ha tomado en los últimos meses la protección de la privacidad y de la información personal de los usuarios, ratificada con la entrada en vigor de leyes y normativas a nivel europeo, y su trasposición a España, como la RGPD (Reglamento General de Protección de Datos), toman especial relevancia las numerosas capacidades de las que disponen los dispositivos móviles modernos para constantemente monitorizar, registrar y permitir disponer de un histórico, así como realizar un seguimiento, de todas las actividades de los usuarios, tanto en iOS como en Android. Los detalles reflejados por parte del CCN-CERT en las diferentes guías de seguridad publicadas a lo largo del 2018, asociadas a Android 6 [Ref.- 21], Android 7 [Ref.- 19], a los servicios de Google [Ref.- 20], iOS 11 [Ref.- 18] e iOS 12 [Ref.- 17], así como publicaciones de terceros sobre la privacidad de los dispositivos móviles, como ElcomSoft en la conferencia Hack In The Box (HitB) [Ref.- 22], permiten ser conscientes de las innumerables capacidades de las que disponen tanto Apple como Google, y las ingentes cantidades de datos personales, de todo tipo (credenciales y contraseñas de servicios y redes Wi-Fi, datos de actividad y salud, datos de pagos, llamadas telefónicas, mensajería, correo electrónico, documentos, ajustes de configuración, datos de navegación web, fotografías y vídeos, datos de geolocalización, etc.), que los dispositivos móviles recolectan y comparten con los servicios remotos en la nube de estos fabricantes. En resumen, Google (y por tanto, Android) recolecta significativamente más información (y por tanto, datos) que Apple (y por tanto, iOS) [Ref.- 22].

Los datos de geolocalización, obtenidos tanto por las plataformas móviles como por apps de terceros, siguen siendo un elemento muy preciado para múltiples propósitos, incluyendo los propios servicios que utiliza el usuario y sus funcionalidades extra (mapas, navegación, servicios en redes sociales, actividad física, fotografías, localización y estado de negocios cercanos, navegación en interiores, etc.), comercialización de anuncios personalizados y basados en la ubicación, comercialización de los propios datos de localización, etc. Uno de los casos más escandalosos del año 2018 relativos a la información de geolocalización fue el de la app de actividad física y deportiva Strava, que se vio expuesta y permitió identificar numerosas localizaciones sensibles, como las utilizadas por los servicios de inteligencia

y operativos militares en todo el mundo, incluyendo bases militares secretas[33] [Ref.-23].



Adicionalmente, en verano y otoño de 2018 se publicaron 3 vulnerabilidades que afectan a la privacidad de Android, y que han sido resueltas en Android 9 por Google, pero no en versiones previas de Android [Ref.- 53]. En la principal vulnerabilidad (CVE-2018-9489) se identificó que los mensajes de broadcast de la plataforma Android exponen información detallada de redes Wi-Fi (nombre de la red, dirección MAC del punto de acceso, direcciones IP locales, servidor DNS y dirección MAC) del dispositivo móvil a todas las apps ejecutando en el terminal. El acceso a esta información a través de los mecanismos habituales requeriría disponer de permisos concretos por parte de las apps, que se pueden evitar simplemente escuchando estos mensajes. La dirección MAC permite identificar unívocamente a un dispositivo móvil, y la dirección MAC del punto de acceso permite obtener información de geolocalización del dispositivo y del usuario. En resumen, cualquier app puede identificar al usuario y obtener información de localización, sin disponer de los permisos asociados.

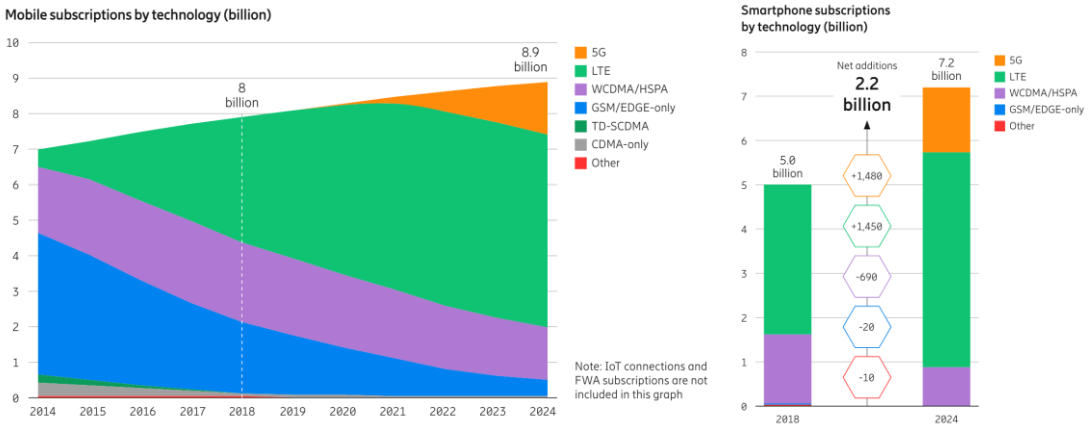
Con todos estos detalles, en la mayoría de ocasiones el dispositivo móvil sabe más de la vida del usuario que el propio usuario. Esta afirmación se ha agudizado aún más en 2018, debido a las nuevas capacidades para la recolección de datos y estadísticas de uso del propio dispositivo móvil tanto en Android 9 (Digital Wellbeing, para los dispositivos móviles Pixel y disponible en Google Play en versión beta) como en iOS 12 (Screen Time), accesibles por primera vez por el usuario, y categorizadas convenientemente, debido a la preocupación social creciente del excesivo uso que se realiza de este tipo de tecnologías y dispositivos. Los mismos recolectan detalles diarios y semanales de en qué apps, tipo de apps y tipo de actividades emplea más tiempo el usuario, o incluso del número de veces que se ha utilizado el dispositivo móvil al día, y por cuanto tiempo.

11.COMUNICACIONES MÓVILES

LTE (Long Term Evolution, o 4G) sigue siendo la tecnología principal empleada hoy en día por los dispositivos móviles (y numerosos otros dispositivos e

[33] https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

infraestructuras) para comunicarse a través de las redes de datos de los operadores móviles o de telecomunicaciones y, por tanto, juega un papel fundamental de cara a las capacidades de comunicación y seguridad de los propios dispositivos móviles y del intercambio de información. La omnipresencia de las redes móviles 4G se refleja en el número de suscripciones existentes a nivel mundial, con 3,3 billones[1] de suscripciones 4G a finales de 2018 (del total de 7,9 billones de suscripciones móviles) [Ref.- 54], según Ericsson. El tráfico de datos móvil creció un 79% entre el tercer trimestre de 2017 y el tercer trimestre de 2018, un crecimiento no experimentado desde el año 2013, reflejando la amplia utilización de estas infraestructuras como medio de comunicación en múltiples ámbitos.



La seguridad de las redes LTE o 4G es, por tanto, fundamental antes de que se lleve a cabo la implantación de la siguiente generación de redes móviles 5G, cuyas redes piloto están planificadas fundamentalmente para el año 2019 (incluyendo Europa). Tras varios años de investigación, estandarización y desarrollo, la comercialización inicial de las redes móviles 5G ha comenzado en 2018, consolidando la tendencia reflejada en el informe de 2017 y 2018 [Ref.- 11], con un nuevo servicio de acceso de banda ancha vía 5G desde el hogar comercializado en octubre de 2018 en cuatro ciudades de EEUU por parte de Verizon[34], basado en el estándar 5G TF (Technical Forum), precursor del 5G NR (New Radio) definitivo, que será empleado, por ejemplo, por AT&T[35]. AT&T ha empezado proporcionando la infraestructura y el servicio 5G en doce ciudades de EEUU[36] en diciembre de 2018 a través de un punto de acceso 5G/Wi-Fi (el Netgear Nighthawk). En el caso de España, Red.es lanzó en 2018 una convocatoria de ayudas para el desarrollo de proyectos piloto de tecnologías 5G, en el que ha participado la mayor parte del sector de las telecomunicaciones de nuestro país [Ref.- 55].

Se estima que la nueva tecnología 5G despegará realmente en el año 2021 y que en 2024 dispondrá de una cobertura mundial del 40% de la población, con una

[34] https://www.theverge.com/2018/10/1/17923072/verizon-5g-network-home-internet-service
[35] https://www.theverge.com/2018/10/24/18019256/att-5g-network-launch
[36] https://www.tomsguide.com/us/5g-release-date,review-5063.html & https://www.tomsguide.com/us/att-5g-launch,news-28886.html

estimación de 1,5 billones de suscripciones (un 17% aproximadamente, sin tener en cuenta los 4 billones de conexiones estimados para 2024 por parte de dispositivos y soluciones IoT, Internet of Things), lo que la constituiría en la generación de las diferentes tecnologías móviles de más rápida adopción a escala global [Ref.- 54]. Desde el punto de vista de los dispositivos móviles, se espera que en 2019 empiece la comercialización de los primeros terminales con soporte para 5G, por parte de fabricantes de la plataforma Android como Samsung, OnePlus, LG, Oppo, Xiaomi o Huawei, por ejemplo, basados en el chip Snapdragon 855 de Qualcomm, que incluye un módem X50 5G (junto al módem X24 de LTE), o mediante accesorios, como el 5G Moto Mod para el Motorola Moto Z3. Los nuevos dispositivos móviles con soporte para 5G serán anunciados previsiblemente en el Mobile World Congress (MWC) de febrero de 2019 en Barcelona. Apple, por otro lado, parece que esperará hasta el año 2020 para comercializar sus primeros dispositivos móviles con soporte para 5G (empleando chips de Intel), según Bloomberg[37], una vez que este estándar esté ampliamente disponible y más maduro.

Desde el punto de vista de seguridad y privacidad, consolidando las tendencias ya reflejadas en el informe de 2017 y 2018 [Ref.- 11], las tecnologías 5G han tenido en cuenta los aspectos de seguridad desde su fase de diseño, ratificándose estos con la publicación de la primera versión del estándar de seguridad 5G en marzo de 2018, conocido como 3GPP TS 33.501[38], por parte del grupo de trabajo de seguridad (SA W3G) del 3GPP (3rd Generation Partnership Project) [Ref.- 56], y basado en las propuestas de seguridad (TR 33.899) detalladas en el informe del pasado año [Ref.- 11]. Sin embargo, la evolución de los aspectos de seguridad de las tecnologías 5G no ha finalizado, ya que progresará junto a las nuevas capacidades emergentes de estas tecnologías como, por ejemplo, las comunicaciones entre vehículos y cualquier otro elemento (V2X, vehicle-to-everything), comunicaciones de voz sobre 5G (VoNR, Voice-over-NR, New Radio) o la coexistencia de 5G y 4G (o NR y LTE).

A mediados de 2018 se publicó un estudio de investigación centrado en el análisis formal de los mecanismos de autentificación del estándar 5G, protocolo conocido como 5G AKA (Authentication and Key Agreement), que identificaba que, aunque 5G mejora el nivel de seguridad de 3G y 4G (respecto a la protección de los datos y la utilización de IMSI catchers [Ref.- 11]), algunos de los objetivos de seguridad de 5G no eran proporcionados por este protocolo [Ref.- 57]. Dentro de estos objetivos se encuentra la autentificación mutua entre la red y el usuario, así como la confidencialidad de los datos intercambiados y la privacidad de la identidad y localización del usuario. Entre las vulnerabilidades identificadas, se descubrió que podría llegar a ser posible repercutir sobre un usuario los gastos de consumo de otro usuario, y se confirmó que un dispositivo móvil 5G, aunque no desvela su identidad completa, todavía revela su presencia en una zona vecina. Como parte del estudio, se

[37] https://www.bloomberg.com/news/articles/2018-12-03/apple-is-said-to-miss-rapid-5g-takeoff-sitting-out-tech-shift (https://www.tomsguide.com/us/apple-5g-iphone-launch,news-28743.html)
[38] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169 (http://www.3gpp.org/news-events/3gpp-news/1975-sec_5g)

proporcionaban recomendaciones para incluir en AKA ciertas propiedades de seguridad aún ausentes, y mitigar las vulnerabilidades y potenciales ataques identificados, que deberían ser incorporados en el estándar 5G, aunque su aplicación no es directa.

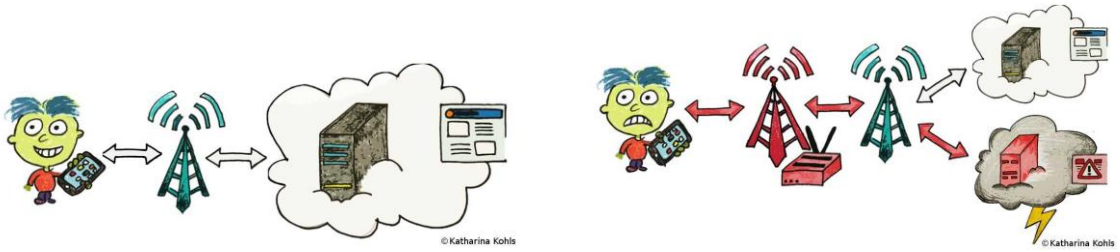
Adicionalmente, ENISA, la agencia de seguridad Europea, publicó un estudio en marzo de 2018 indicando que las vulnerabilidades de interceptación y suplantación de tráfico, denegación de servicio (DoS) e interceptación de datos de localización, ya conocidas en los mecanismos de señalización de las tecnologías 2G, 3G y 4G, y sus protocolos asociados, como SS7 (Signaling System 7) y Diameter, también podrían afectar a las redes 5G [Ref.- 58].

Dentro de las novedades de seguridad específicas que afectan a las comunicaciones móviles, en 2018 se pre-publicó (ya que la publicación académica se realizará en mayo de 2019) un nuevo tipo de ataque denominado aLTEr [Ref.- 59][Ref.- 59], que afecta (como su propio nombre indica) a las redes LTE o 4G. La investigación asociada revela tres nuevos vectores de ataque contra el protocolo LTE en la capa de enlace (capa 2). Investigaciones previas habían identificado vulnerabilidades de seguridad en LTE en las capas física (capa 1) y de red (capa 3). Dos de ellos son ataques pasivos, y permiten la identificación de la identidad de los usuarios conectados a una celda de radio y el reconocimiento de los sitios web que han sido accedidos por el usuario. El otro es un ataque criptográfico activo, el que realmente es conocido como aLTEr, que permite la redirección de conexiones de red mediante técnicas de suplantación de DNS (DNS spoofing) debido a una vulnerabilidad en el estándar LTE.

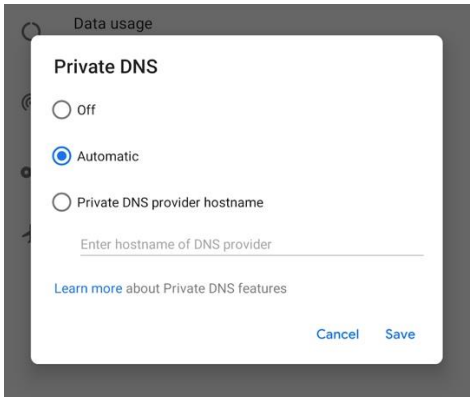
Más concretamente, aLTEr consiste en un ataque MitM (Man in the Middle) que permite secuestrar conexiones de red mediante la manipulación del tráfico de usuario intercambiado a través del protocolo LTE. En los ataques pasivos mencionados, el atacante simplemente captura el tráfico de usuario, lo que le permite a través de los metadatos incluidos en la capa de enlace de dichas comunicaciones, llegar a conocer con cierta probabilidad (un 89% en un entorno de laboratorio) mediante la información de consumo y uso, y la identificación de patrones, a qué sitios web se está conectando. En el ataque aLTEr activo, el atacante suplanta tanto a la red del operador móvil legítima de cara al usuario, como al usuario de cara a la red legítima, con el objetivo de interceptar todas las trasmisiones entre ambos.

LTE hace uso de mecanismos de autentificación mutua para identificar tanto usuarios como redes legítimas en las capas por encima de la capa de enlace, derivándose una clave compartida, que es empleada posteriormente para cifrar tanto el tráfico de control como de usuario. Sin embargo, la capa de enlace e inferiores no están protegidas y permiten el reenvío de mensajes de capas superiores. Adicionalmente, los datos de usuario no están protegido mediante mecanismos de integridad (mientras que los datos de control sí). Como resultado, el atacante puede modificar el contenido de un paquete conociendo el texto en claro original, aunque éste esté cifrado y, por ejemplo, modificar el tráfico DNS para cambiar el servidor DNS

destino y llevar a cabo ataques de redirección. En concreto, los datos de usuario se cifran con AES-CTR, lo que facilita este tipo de modificaciones del contenido cifrado. Una vez se dispone de estas capacidades, el servidor DNS malicioso es empleado para ataques de suplantación de DNS (DNS spoofing), pudiendo redirigir al usuario víctima a cualquier servicio o servidor.



Por otro lado, cabe destacar como Android 9 (Pie) desde agosto de 2018 introdujo soporte nativo para DNS over TLS (DoT), protocolo estandarizado mediante el RFC7858 (y RFC 8310) [Ref.- 60], protegiendo todo el tráfico DNS del dispositivo móvil, tanto en redes Wi-Fi como en redes móviles. La protección, principalmente abordada desde el punto de vista de la privacidad, de las comunicaciones asociadas al servicio DNS para la resolución de nombres en Internet, ha adquirido especial relevancia a lo largo del año 2018 [Ref.- 61], y se espera se materializará con un uso más generalizado de canales cifrados para proteger el tráfico DNS en el año 2019. Android ha sido la primera plataforma móvil con soporte nativo para este nuevo protocolo, cuyo objetivo principal es cifrar las comunicaciones DNS entre los clientes y los servidores DNS mediante TLS, de forma que un posible atacante situado entre éstos no pueda obtener o modificar los contenidos de las mismas, y conocer los diferentes servicios, servidores y dominios a los que el usuario está accediendo. Los ajustes avanzados de configuración de red de Android 9 permiten establecer un modo "DNS privado" (o "Private DNS") para hacer uso de DoT. Por defecto, el modo establecido es automático, es decir, se hará uso de DoT si el servidor DNS empleado actualmente (proporcionado por la red o configurado manualmente en los ajustes de red) lo soporta, o el servicio DNS tradicional en caso contrario. En el modo automático, Android hace uso de los servidores DNS públicos de Google (8.8.8.8). Si se desea hacer uso únicamente de DoT, es posible especificar manualmente el hostname del servidor DNS con soporte para DoT (ya sea público o propio), denominado por Android DNS privado, forzándose a que todo el tráfico generado por el dispositivo móvil sea cifrado y enviado a dicho servidor DNS resolver, o en caso de no poder contactar con el servidor, considerar que no se dispone de conexión a Internet.



Desafortunadamente, iOS 12 aún no dispone de soporte nativo para DNS over TLS (DoT), o para DNS over HTTPS (DoH), definido en el RFC 8484 [Ref.- 62], siendo necesario hacer uso de una app de terceros, como por ejemplo la app 1.1.1.1 de Cloudflare, que internamente hace uso de una VPN, si se desea hacer uso de estos protocolos de seguridad [Ref.- 63] (junto a su servicio DNS asociado, 1.1.1.1, que adicionalmente proporciona soporte para DNSSEC [Ref.- 63]; la app está disponible tanto para iOS como para Android, por ejemplo, para versiones previas a Android 9). Adicionalmente, los usuarios de versiones previas a Android 9 (desde Android 4.0) también disponen de la nueva app de Google denominada Intra [Ref.- 64], publicada en octubre de 2018, que permite proteger el tráfico DNS haciendo uso por defecto de los servidores DNS de Google (8.8.8.8), en este caso empleando el protocolo DNS over HTTPS (DoH) [Ref.- 62]para evitar posibles filtros o escenarios de censura online (al parecerse el tráfico DoH a tráfico web HTTPS ordinario) y, de nuevo, implementado mediante el uso de una VPN.

Finalmente, en junio del año 2018 se ratificó y publicó por parte de la Wi-Fi Alliance la nueva especificación de seguridad para redes Wi-Fi, conocida como WPA3 (Wireless Protected Access 3) [Ref.- 65], tras el anuncio inicial de enero de 2018 [Ref.- 66]. La especificación definitiva de WPA3 se ha dividido finalmente en tres diferentes estándares, cada uno de ellos con sus objetivos y alcance, que deberán ser implementados tanto por los puntos de acceso que proporcionan la red Wi-Fi, como por los clientes que se conectan a éstas, en caso de querer beneficiarse de todas las mejoras de seguridad introducidas respecto a WPA2:

- WPA3:
  - WPA3-Personal: Simultaneous Authentication of Equals (SAE): Un nuevo mecanismo de autentificación mediante contraseña más robusto que el disponible con WPA2-PSK (Pre-Shared Key).
  - WPA3-Enterprise: Un nuevo modo, o suite criptográfica, de 192 bits de seguridad (frente a los 128 bits previos) para proteger redes Wi-Fi con requisitos de seguridad más altos, como por ejemplo redes de gobiernos, ministerios de defensa o entornos industriales.
- Wi-Fi Enhanced OpenTM (OWE): Un nuevo mecanismo de seguridad para la protección de redes abiertas, sin autentificación, dónde se introduce la

opción de emplear cifrado (oportunista), mejorando la confidencialidad y privacidad de los usuarios frente a las redes Wi-Fi abiertas tradicionales.

- Wi-Fi Easy ConnectTM (DPP: Device Provisioning Protocol): Un nuevo conjunto de mecanismos de seguridad para facilitar y proteger el proceso de configuración e incorporación de nuevos clientes Wi-Fi a una red, especialmente de aquellos que no disponen de interfaz de usuario, o dónde éste es muy limitado.

A lo largo de 2018 y principio de 2019, el número de productos certificados por la Wi-Fi Alliance con soporte para WPA3 disponibles era muy reducido[39], incluyendo únicamente algunos puntos de acceso o routers de Aruba (Dell), y unidades sueltas de Synology, Ruckus, Ruijie, Netgear, Qualcomm y Marvell. Desde el punto de vista de los clientes la disponibilidad es aún más limitada, con la tarjeta Intel AC 9260, y más en concreto desde la perspectiva de los dispositivos móviles, el chip Snapdragon 835 de Qualcomm era el único disponible en la lista, de manera similar al chip 855 con soporte para 5G mencionado previamente. Sin embargo, desde mitad del año 2018, Qualcomm ya anunció que el chip Snapdragon 845 también dispondría de soporte para WPA3[40], con el objetivo de liderar la industria y de que éste se constituyera potencialmente en la referencia para WPA3 dentro del ecosistema móvil.

12.TENDENCIAS PARA EL AÑO 2019

Dentro de las principales tendencias esperadas para el año 2019, adicionalmente a las ya reflejadas en las nuevas capacidades de conexión a redes Wi-Fi con soporte para WPA3 y a redes móviles 5G (tal como se detalla en el apartado "11. Comunicaciones móviles"), con capacidades de seguridad superiores a sus predecesoras, destaca la utilización de pantallas flexibles o plegables, potencialmente extendiendo así su tamaño y resolución, y pudiendo dar lugar a dispositivos móviles híbridos (o *foldables*, plegables), del tamaño de un *smartphone* pero con posibilidad de convertirse temporalmente en tabletas. Aunque esta tendencia parecía que irrumpiría a lo largo de 2018, no ha sido hasta final de año, durante el CES 2018, cuando se ha visto el primer smartphone comercial con pantalla plegable, conocido como FlexPai de Royole[41], con pantalla de tipo AMOLED. Samsung también ha anunciado a finales de 2018 la comercialización de dispositivos móviles con esta característica durante 2019 (empleando el panel Infinity Flex Display) y Microsoft está adaptando Windows para dispositivos plegables o con pantalla duales[42], soporte que Google ya anunció, en

[39] https://www.wi-fi.org/product-finder-results?sort_by=certified&sort_order=desc&capabilities=16
[40] https://www.xda-developers.com/the-qualcomm-snapdragon-845-will-support-the-new-wpa3-wi-fi-security-standard/
[41] https://m.xataka.com/moviles/errores-flexpai-probamos-primer-smartphone-plegable-esto-que-deberian-evitar-quienes-vengan-despues
[42] https://m.xataka.com/moviles/microsoft-esta-preparando-windows-para-futuro-dispositivos-plegables-pantallas-duales

noviembre de 2018, estará disponible de forma nativa en futuras versiones de Android[43].

Están aún por confirmarse las posibles implicaciones de seguridad que podrá introducir esta nueva tecnología pero, el soporte nativo anunciado por parte de Google para Android, al menos, mitigará una posible nueva fragmentación donde cada fabricante podría acabar implantando su propia implementación, tanto hardware como software, y donde (una vez más) se dificultaría y ralentizaría la distribución de las actualizaciones del sistema operativo Android, por problemas de compatibilidad o de intereses de negocio por parte de los fabricantes de los dispositivos móviles.

[43] https://www.xataka.com/moviles/android-tendra-soporte-oficial-para-dispositivos-plegables-arma-secreta-google-para-anticiparse-a-todos

13. ANEXO A. REFERENCIAS

[Ref.- 1] "Smartphone OS Market Share, 2018 Q3". IDC. 2019.
URL: http://www.idc.com/promo/smartphone-market-share/os

[Ref.- 2] "Smartphone Vendor Market Share, 2018 Q3". IDC. 2019.
URL: https://www.idc.com/promo/smartphone-market-share/vendor

[Ref.- 3] "Android vs. iOS. Smartphone OS sales market share evolution". Kantar Worldpanel. 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 3rd quarter 2018". Statista. Q3 2018.
URL: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

[Ref.- 6] "La madurez de la industria del smartphone se le atraganta a Apple". Xataka. 3 de enero de 2019.
URL: https://www.xataka.com/empresas-y-economia/madurez-industria-smartphone-se-le-atraganta-a-apple

[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 2018 (in 1,000s)". Statista. July 2018
URL: https://www.statista.com/statistics/268251/number-of-apps-in-the-itunes-app-store-since-2008/

[Ref.- 10] "Samsung también se ve afectada por China y la madurez del mercado de smartphones". Xataka. 8 de enero de 2019. URL: https://www.xataka.com/empresas-y-economia/china-madurez-mercado-smartphones-empanan-futuro-samsung

[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] "iOS vs. Android: Physical Data Extraction and Data Protection Compared". ElcomSoft. Oct 2017.
URL: https://blog.elcomsoft.com/2017/10/ios-vs-android-physical-data-extraction-and-data-protection-compared/

[Ref.- 14] "iOS 11.4.1 Beta: USB Restricted Mode Has Arrived". ElcomSoft. Jun 2018.
URL: https://blog.elcomsoft.com/2018/05/ios-11-4-to-disable-usb-port-after-7-days-what-it-means-for-mobile-forensics/
URL: https://blog.elcomsoft.com/2018/06/ios-11-4-1-beta-usb-restricted-mode-has-arrived/
URL: https://blog.elcomsoft.com/2018/06/ios-11-4-1-second-beta-extends-usb-restricted-mode-with-manual-activation/

[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] "This $39 Device Can Defeat iOS USB Restricted Mode". ElcomSoft. Jul 2018.
URL: https://blog.elcomsoft.com/2018/07/this-9-device-can-defeat-ios-usb-restricted-mode/
URL: https://blog.elcomsoft.com/2018/07/usb-restricted-mode-inside-out/

[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 11.x)". CCN-STIC 455C. CCN-CERT. Oct 2018. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3161-ccn-stic-455c-guia-practica-de-seguridad-en-dispositivos-moviles-iphone-ios-11x-1/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.- 19] "Seguridad de dispositivos móviles: Android 7.x". CCN-STIC 453E. CCN-CERT. Sep 2018.
URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3040-ccn-stic-453e-seguridad-de-dispositivos-moviles-android-7-x/file.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.- 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/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3043-ccn-stic-456-cuenta-de-usuario-servicios-aplicaciones-google-para-dispositivos-moviles-android/file.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] "Seguridad de dispositivos móviles: Android 6.x". CCN-STIC 453D. CCN-CERT. Jun 2018.
URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2901-ccn-stic-453d-seguridad-de-dispositivos-moviles-android-6-x/file.html

[Ref.- 22] "Smartphone Privacy: How Your Smartphone Tracks Your Entire Life". ElcomSoft. HitB. Nov 2018.
URL: https://conference.hitb.org/hitbsecconf2018pek/materials/D2T2%20-%20How%20Your%20Smartphone%20Tracks%20Your%20Entire%20Life%20-%20Vladimir%20Katalov.pdf

[Ref.- 23] "Why Strava's Fitness Tracking Should Really Worry You". Forbes. Jan 2018.
URL: https://www.forbes.com/sites/thomasbrewster/2018/01/29/strava-fitness-data-location-privacy-scare/

[Ref.- 24] "How Android Phones Hide Missed Security Updates From You". Wired. Apr 2018.
URL: https://www.wired.com/story/android-phones-hide-missed-security-updates-from-you/

[Ref.- 25] "Google mandates two years of security updates for popular phones in new Android contract". The Verge. Oct 2018. URL: https://www.theverge.com/2018/10/24/18019356/android-security-update-mandate-google-contract

[Ref.- 26] "Android Oreo's Rollback Protection Will Block OS Downgrades, but it can be Disabled". XDA Developers. Sep 2017. URL: https://www.xda-developers.com/android-oreo-rollback-protection/

[Ref.- 27] "Android Oreo's rollback protection required on phones launching with Android Pie". XDA Developers. Aug 2018.
URL: https://www.xda-developers.com/android-pie-rollback-protection/

[Ref.- 28] "Better Biometrics in Android P". Android Developers Blog. Jun 2018.
URL: https://android-developers.googleblog.com/2018/06/better-biometrics-in-android-p.html

[Ref.- 29] "Android P adds new Biometrics API that supports iris, face, and fingerprint scanning". XDA Developers. May 2018. URL: https://www.xda-developers.com/android-p-new-biometrics-api/

[Ref.- 30] "Broken Fingers: On the Usage of the Fingerprint API in Android". EURECOM. Feb 2018. URL: http://www.s3.eurecom.fr/~yanick/publications/2018_ndss_fingerprint.pdf

[Ref.- 31] "Display Fingerprint Technology & Market Report - 2018". IHS Markit. June 2018. URL: https://technology.ihs.com/598645/display-fingerprint-technology-market-report-2018

[Ref.- 32] "Qualcomm Fingerprint Sensors transform device authentication [video]". Qualcomm. Jul 2017. URL: https://www.qualcomm.com/news/onq/2017/07/05/qualcomm-fingerprint-sensors-transform-device-authentication

[Ref.- 33] "Google not sure if current fingerprint sensors are secure enough for mobile payments". Phandroid. Jan 2019. URL: https://phandroid.com/2019/01/15/google-not-sure-if-current-fingerprint-sensors-are-secure-enough-for-mobile-payments/

[Ref.- 34] "Android 9 features and APIs - Android backups". Android. URL: https://developer.android.com/about/versions/pie/android-9.0#android-backups URL: https://developer.android.com/about/versions/pie/security/ckv-whitepaper

[Ref.- 35] "Google and Android have your back by protecting your backups". Google Security Blog. Oct 2018. URL: https://security.googleblog.com/2018/10/google-and-android-have-your-back-by.html URL: https://www.nccgroup.trust/us/our-research/android-cloud-backuprestore/?research=Public+Reports

[Ref.- 36] "Building a Titan: Better security through a tiny chip". Android Developers Blog. Oct 2018. URL: https://android-developers.googleblog.com/2018/10/building-titan-better-security-through.html

[Ref.- 37] "Android Protected Confirmation: Taking transaction security to the next level". Android Developers Blog. Oct 2018. URL: https://android-developers.googleblog.com/2018/10/android-protected-confirmation.html

[Ref.- 38] "Android Enterprise Security White Paper". Android. Sep 2018. URL: https://source.android.com/security/overview/reports URL:https://source.android.com/security/reports/Google_Android_Enterprise_Security_Whitepaper_2018.pdf

[Ref.- 39] "iOS Security" (Guide). Apple. Nov 2018 (iOS 12.1). URL: https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf

[Ref.- 40] "What do Pointer Authentication Codes mean for iOS jailbreaking?". Ivan R Blog. Sep 2018. URL: https://ivrodriguez.com/pointer-authentication-on-armv8-3/ URL: https://www.qualcomm.com/documents/whitepaper-pointer-authentication-armv83

[Ref.- 41] "Phishing Attacks on Modern Android". University of Genova & EURECOM. Oct 2018. URL: http://www.s3.eurecom.fr/projects/modern-android-phishing/

[Ref.- 42] "Kaspersky Security Bulletin 2018. Threat Predictions for 2019". Kaspersky. Nov 2018. URL: https://securelist.com/kaspersky-security-bulletin-threat-predictions-for-2019/88878/ URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/11/27082929/KSB_Predictions-2019_General-APT.pdf

[Ref.- 43] "Predictions 2019: "The era of simple Android malware is over"". G Data. Dec 2018. URL: https://www.gdatasoftware.com/blog/2018/12/31380-preview-2019-the-time-of-simple-android-malware-is-passing

[Ref.- 44] "Cyber attacks on Android devices on the rise". G Data. Nov 2018. URL: https://www.gdatasoftware.com/blog/2018/11/31255-cyber-attacks-on-android-devices-on-the-rise

[Ref.- 45] "SophosLabs 2019 Threat Report". Sophos. Nov 2018.
URL: https://www.sophos.com/en-us/press-office/press-releases/2018/11/sophos-2019-threat-report.aspx
URL: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf

[Ref.- 46] "The new landscape of pre-installed mobile malware: malicious code within". Malwarebytes Labs. Jan 2019. URL: https://blog.malwarebytes.com/cybercrime/2019/01/the-new-landscape-of-preinstalled-mobile-malware-malicious-code-within/

[Ref.- 47] "Mobile Menace Monday: top five scariest mobile threats". Malwarebytes Labs. Oct 2018. URL: https://blog.malwarebytes.com/cybercrime/2018/10/mobile-menace-monday-top-five-scariest-mobile-threats/

[Ref.- 48] "First Kotlin-Developed Malicious App Signs Users Up for Premium SMS Services". Trend Micro. Jan 2018. URL: https://blog.trendmicro.com/trendlabs-security-intelligence/first-kotlin-developed-malicious-app-signs-users-premium-sms-services/

[Ref.- 49] "Who's who in the Zoo". Kaspersky. May 2018.
URL: https://securelist.com/whos-who-in-the-zoo/85394/

[Ref.- 50] "Jack of all trades". Kaspersky. Dec 2018.
URL: https://securelist.com/jack-of-all-trades/83470/

[Ref.- 51] "Android P will also Prevent Idle Background Apps from Recording you via Microphone". XDA Developers. Feb 2018. URL: https://www.xda-developers.com/android-p-audio-recording-limitations-privacy/

[Ref.- 52] "More than 250 Android Games Use Your Mic to Track What You're Watching". XDA Developers. Dec 2017. URL: https://www.xda-developers.com/android-apps-tracking-mic-always-listening/

[Ref.- 53] "Android Privacy Bugs (CVE-2018-9489, CVE-2018-9581 and CVE-2018-15835)". Nightwatch Cybersecurity. Nov 2018.
URL: https://wwws.nightwatchcybersecurity.com/2018/11/05/speaking-bsidesde-this-friday-on-android-privacy-bugs-cve-2018-9489-cve-2018-9581-and-cve-2018-15835/
URL: https://wwws.nightwatchcybersecurity.com/2018/08/29/sensitive-data-exposure-via-wifi-broadcasts-in-android-os-cve-2018-9489/

[Ref.- 54] "Ericsson Mobility Report". Ericsson. Nov 2018.
URL: https://www.ericsson.com/en/mobility-report
URL: https://www.ericsson.com/en/mobility-report/reports/november-2018

[Ref.- 55] "La mayor parte del sector de las telecomunicaciones participa en la convocatoria de ayudas para el desarrollo de proyectos pilotos 5G". Red.es. Ene 2019.
URL: https://red.es/redes/es/actualidad/magazin-en-red/la-mayor-parte-del-sector-de-las-telecomunicaciones-participa-en-la
URL: https://www.red.es/redes/es/que-hacemos/pilotos-5g

[Ref.- 56] "With 5G, security is top of mind from the start". Ericsson. Mar 2018.
URL: https://www.ericsson.com/en/news/2018/3/5g-security
URL: https://www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system

[Ref.- 57] "A Formal Analysis of 5G Authentication". ETH. arXiv. Jun 2018.
URL: https://arxiv.org/abs/1806.10360

[Ref.- 58] "Signalling Security in Telecom SS7/Diameter/5G". ENISA.
URL: https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g

[Ref.- 59] "Breaking LTE on Layer Two". Ruhr-Universität Bochum & New York University Abu Dhabi. May 2019. URL: https://alter-attack.net URL: https://alter-attack.net/#paper

[Ref.- 60] "DNS over TLS support in Android P Developer Preview". Android Developers Blog. April 2018. URL: https://android-developers.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html
URL: https://tools.ietf.org/html/rfc7858 (RFC 7858 - May 2016)

[Ref.- 61] "To Sec or Not To Sec: DNS Question". CCN-CERT - DinoSec. Dic 2018.
URL: https://www.dinosec.com/en/lab.html#JornadasCCN-CERT2018

[Ref.- 62] "RFC 8484: DNS Queries over HTTPS (DoH)". IETF. Oct 2018.
URL: https://tools.ietf.org/html/rfc8484

[Ref.- 63] "1 Thing You Can Do To Make Your Internet Safer And Faster". Cloudflare. Nov 2018.
URL: https://blog.cloudflare.com/1-thing-you-can-do-to-make-your-internet-safer-and-faster/

[Ref.- 64] "Intra". Google. Oct 2018. URL: https://getintra.org
URL: https://github.com/Jigsaw-Code/intra

[Ref.- 65] "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.- 66] "Wi-Fi Alliance® introduces security enhancements". Wi-Fi Alliance. Jan 2018.
URL: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements

[Ref.- 67] "Android Pie Lockdown Option: a Match for iOS SOS Mode?". ElcomSoft. Aug 2018.
URL: https://blog.elcomsoft.com/2018/08/android-pie-lockdown-option-a-match-for-ios-sos-mode/