# INFORME ANUAL 2020


# DISPOSITIVOS Y COMUNICACIONES MÓVILES

## CCN-CERT IA-18/21

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


CCN-CERT centro criptológico nacional

CCN centro criptológico nacional

MAYO **2020**


Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA



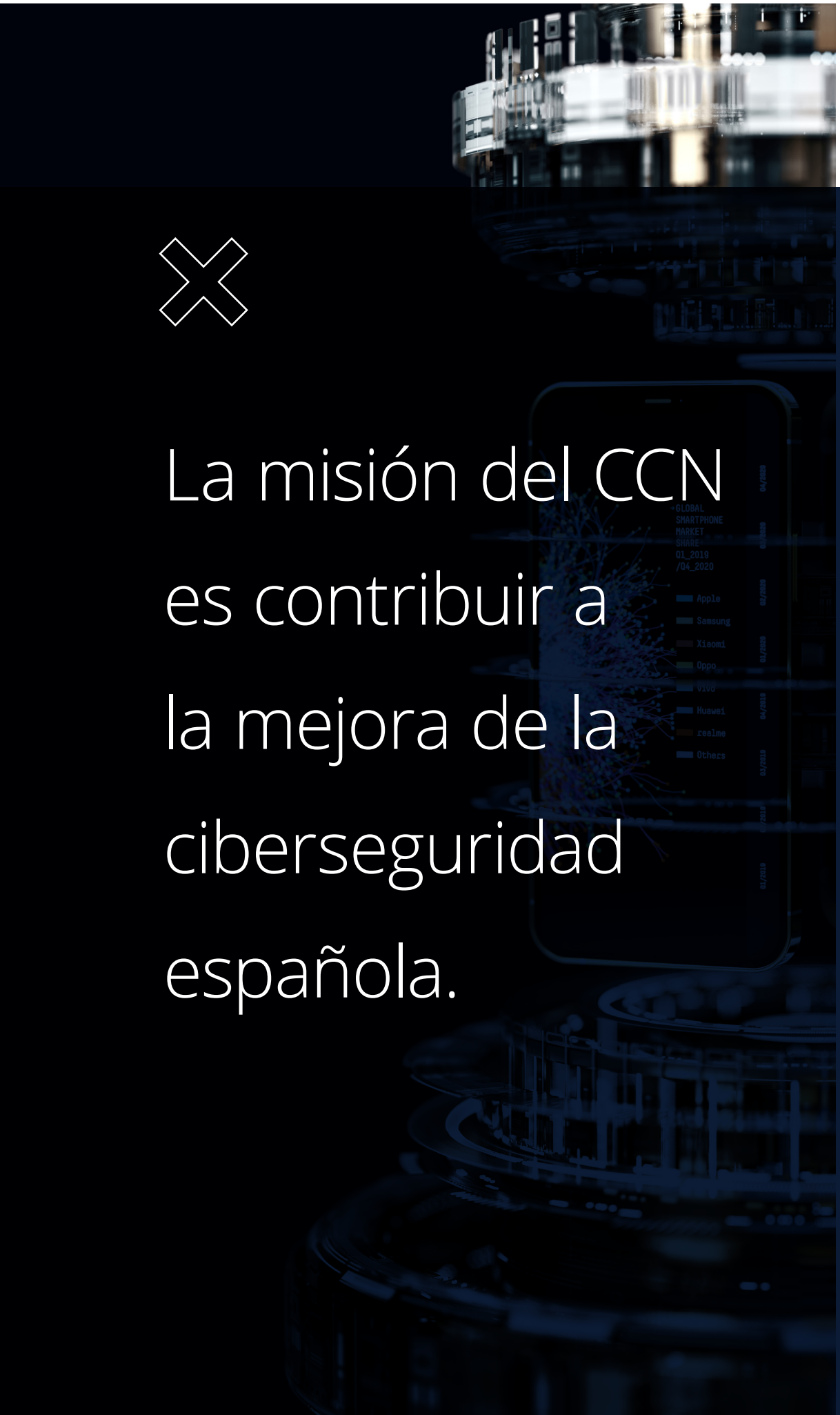
Fecha de Edición: mayo de 2021

**LIMITACIÓN DE RESPONSABILIDAD**

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

**AVISO LEGAL**

# Índice




# La misión del CCN es contribuir a la mejora de la ciberseguridad española.

# 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 consolidado su nivel de madurez y estabilidad en 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 ratifica a los dispositivos móviles y a sus capacidades de comunicación inalámbricas, tanto en redes Wi-Fi y conexiones Bluetooth como en redes móviles (2/3/4/5G), como uno de los objetivos principales de las ciberamenazas para el año 2021, consolidándose la tendencia de los últimos años.

En este informe se presentan algunas de las principales amenazas de seguridad y vulnerabilidades descubiertas a lo largo del año 2020 en los entornos de comunicaciones y dispositivos móviles, así como los avances y las tendencias más relevantes identificadas en este tipo de tecnologías para el año 2021.

# 3. Evolución del mercado de dispositivos móviles en 2020

El año 2020, especialmente durante los dos primeros trimestres y con un declive total en la economía mundial debido a la pandemia sanitaria, confirmaba la disminución ya identificada en los años previos relativa al volumen global de negocio, distribución y venta de dispositivos móviles, pero amplificada notablemente.

En el total del año 2020 el declive observado fue del 6,7%, con un volumen de ventas totales en 2020 de 1.280 billones[1] de unidades, en comparación a los 1.373 billones de 2019[2,3], el mayor declive de la historia, según los estudios de IDC[4]. Sin embargo, el tercer trimestre de 2020 (Q32020) mostró ligeros signos de recuperación, que se materializaron también en el cuarto trimestre (Q42020), lo que hace que las expectativas de crecimiento para el año 2021 aumenten en un 5,5%, durante el proceso de recuperación de la pandemia e impulsado también por la llegada al mercado de nuevos terminales con capacidades 5G. El crecimiento esperado por IDC a medio y largo plazo es de un total de 1.526 billones de unidades en el año 2025.

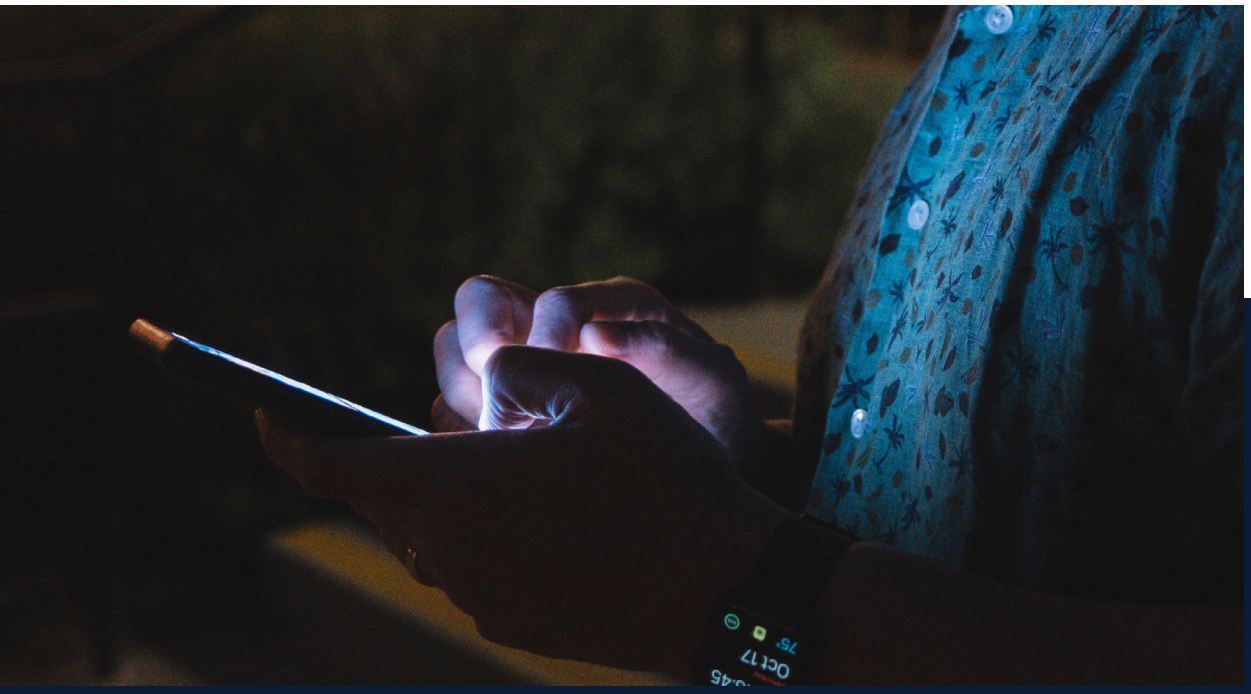
---

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

**2.** "Smartphone Market Share: OS Data Overview" (Updated: 8 Apr 2021). IDC. 2021. URL: http://www.idc.com/promo/smartphone-market-share/os

**3.** "Smartphone Market Share: Vendor Data Overview" (Updated: 8 Apr 2021). IDC. 2021. URL: https://www.idc.com/promo/smartphone-market-share/vendor

**4.** Datos obtenidos a finales de abril de 2021, disponiendo ya de las estadísticas consolidadas del último trimestre de 2020 (Q42020) y, por tanto, de la visión global del año, en lugar de en base a estimaciones de previsiones, como ocurría en algunos de los informes anuales de años previos.

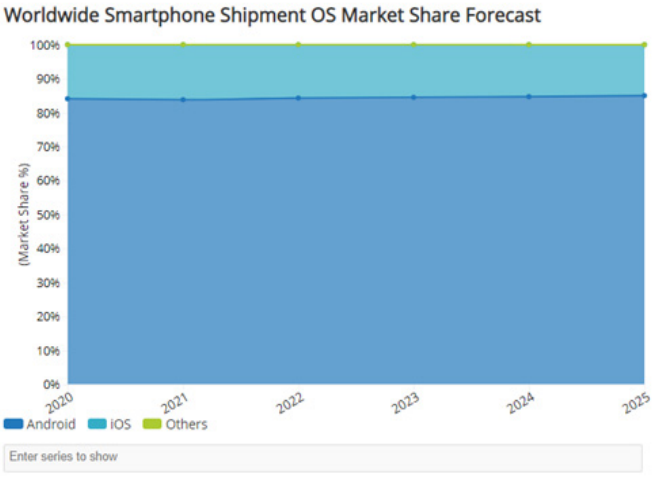


El principal aspecto que ha influido en este declive ha sido la pandemia de la COVID-19, quedando ya atrás las disputas por el mercado entre EEUU y China.

Pese a ello, la digitalización repentina de gran parte de la sociedad ha mantenido una fuerte demanda de dispositivos móviles. Parece sin duda que el principal factor dinamizador de la industria es el 5G, llegando por primera vez a los iPhone 12. IDC espera que más del 40% de ventas en 2021 estén asociadas a terminales 5G, creciendo hasta casi un 70% en 2025. Continuando con la tendencia e importancia del precio como factor decisorio en la compra de dispositivos móviles, se identifica una caída en los terminales 5G con la llegada de fabricantes chinos, hasta los $404 a finales de 2025 (con un precio medio global estimado de $261 para los terminales en 2021).

La plataforma móvil Android consolida su hegemonía de cuota de mercado como líder indiscutible, con en torno al 84% de cuota de mercado global, con un ligero descenso asociado a los retrasos en la distribución de los dispositivos móviles más altos de gama con soporte para 5G debido a la pandemia, y a la presencia en el mercado del iPhone SE de 2ª generación (modelo 2020) durante la primera mitad del año, un dispositivo de gama media con un precio muy atractivo, competencia de muchos terminales Android. Por otro lado, iOS incrementa su cuota de mercado a un 16%, superando las previsiones de años previos en tres puntos porcentuales. Durante 2020 las ventas de iOS aumentaron un 6.5% respecto al año pasado (YoY, Year over Year), alcanzando 203,4 millones, con una buena aceptación del iPhone 11 y del iPhone 12, que con su soporte para 5G ha ayudado a mantener las ventas y la progresión de crecimiento de Apple a pesar de la pandemia a final del año 2020. Se espera que este crecimiento se mantenga durante 2021. No quedan en el mercado otras plataformas móviles que compitan con estas dos. Por tanto, hay ligeras novedades en la evolución respecto a años previos con ese crecimiento de iOS, aunque no extremadamente significativas. El presente informe se centra exclusivamente en las dos plataformas móviles relevantes a día de hoy, Android e iOS[5].

**5.** La mayoría de referencias a iOS en el presente informe hacen referencia igualmente a iPadOS.




| Year | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | |
|---|---|---|---|---|---|---|---|
| Android | 84.1% | 83.8% | 84.3% | 84.5% | 84.7% | 85.0% | |
| iOS | 15.9% | 16.2% | 15.7% | 15.5% | 15.3% | 15.0% | |
| Others | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% |
| TOTAL | 100.0% | 100.0% | 100.0% | 100.0% | 100.0% | 100.0% | 100.0% |

Figura 1

Se confirma finalmente la duda pendiente del pasado año, al haber incorporado Apple soporte para 5G en sus nuevos modelos de finales de 2020 (iPhone 12 y similares). Estas cifras globales se ratifican con las estadísticas disponibles públicamente de manera específica para España, dónde en marzo de 2021, igualmente, se mantienen las cuotas de mercado globales del 84% para Android y del 16% para iOS, dirigiendo las decisiones de compra las capacidades 5G y la duración de la batería de los terminales[6].

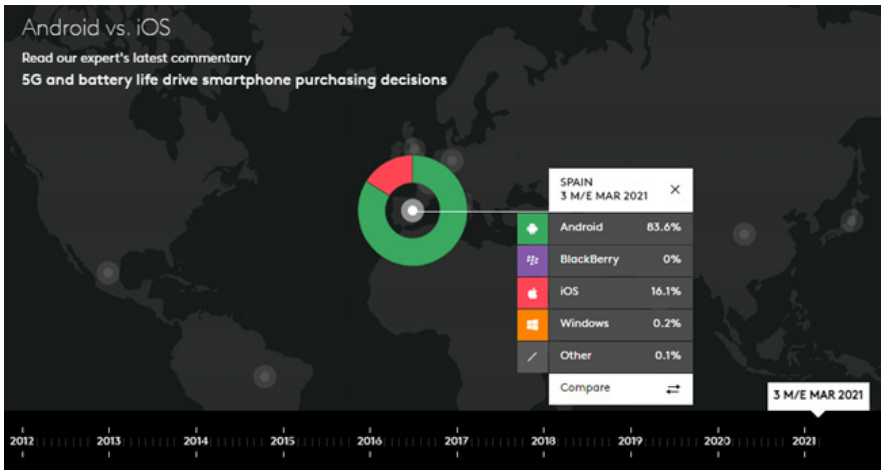
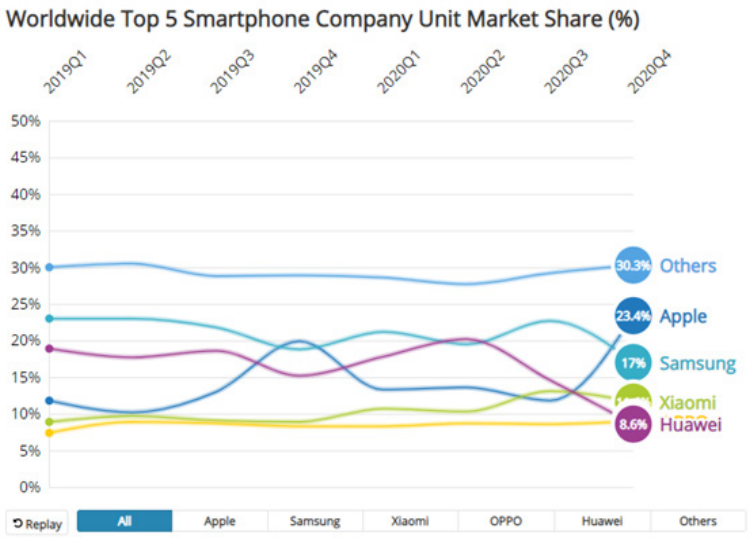



Figura 2

**6.** "Android vs. iOS. Smartphone OS sales market share evolution". Kantar Worldpanel. Sep 2019. URL: https://www.kantarworldpanel.com/global/smartphone-os-market-share/

Respecto a los fabricantes, se distribuyeron un total de 374 millones de unidades en el último trimestre de 2020 (Q42020), con un crecimiento del 1,1% (YoY), debido a la demanda de final de año y a la recuperación de la cadena de suministro y de componentes electrónicos, qué comenzó en el tercer trimestre (Q32020). Cabe destacar cómo Apple ha vuelto a liderar el mercado en este último trimestre, superando el 23%, por delante de Samsung, gracias a la llegada de la familia de iPhone 12 y su soporte para 5G, y a su crecimiento en China. Estas cifras suponen un crecimiento 18,6% YoY. Samsung sigue liderando el mercado de dispositivos móviles Android, con un 17% de cuota de mercado (pero con una caída relevante YoY del 8%), y destaca cómo Xiaomi alcanza por primera vez en la historia el tercer puesto global con un 11,6% y un crecimiento del 32% YoY (pese a controversias asociadas a la privacidad que se detallan en el presente informe[7]).

Como en años previos, la cuota de mercado de Samsung en España[8] es del 28%, seguida de Xiaomi con un 25% y de Apple con un 19%, manteniendo Huawei el 15% de cuota de mercado.




| Quarter | 2019Q1 | 2019Q2 | 2019Q3 | 2019Q4 | 2020Q1 | 2020Q2 | 2020Q3 | 2020Q4 |
|---|---|---|---|---|---|---|---|---|
| Apple | 11.8% | 10.2% | 13.0% | 19.9% | 13.3% | 13.6% | 11.8% | 23.4% |
| Samsung | 23.0% | 23.0% | 21.8% | 18.8% | 21.2% | 19.5% | 22.7% | 17.0% |
| Xiaomi | 8.9% | 9.7% | 9.1% | 8.9% | 10.7% | 10.3% | 13.1% | 11.6% |
| OPPO | 7.4% | 8.9% | 8.7% | 8.3% | 8.3% | 8.7% | 8.6% | 9.0% |
| Huawei | 18.9% | 17.7% | 18.6% | 15.2% | 17.8% | 20.2% | 14.6% | 8.6% |
| Others | 30.0% | 30.5% | 28.8% | 28.9% | 28.6% | 27.7% | 29.2% | 30.3% |
| **TOTAL** | **100.0%** | **100.0%** | **100.0%** | **100.0%** | **100.0%** | **100.0%** | **100.0%** | **100.0%** |

Figura 3

**7.** Exclusive: Warning Over Chinese Mobile Giant Xiaomi Recording Millions Of People's 'Private' Web And Phone Use". Forbes. Apr 2020. URL: https://www.forbes.com/sites/thomasbrewster/2020/04/30/exclusive-warning-over-chinese-mobile-giant-xiaomi-recording-millions-of-peoples-private-web-and-phone-use/#40395cd71b2a URL: https://blog.mi.com/en/2020/05/02/live-post-evidence-and-statement-in-response-to-media-coverage-on-our-privacy-policy/

**8.** http://gs.statcounter.com/vendor-market-share/mobile/spain

Como se mencionaba en el informe anual de 2019[9], Huawei comercializaba en septiembre de 2019 la versión 1.0 de HarmonyOS con la Honor TV, y en diciembre de 2020 liberaba la versión beta para dispositivos móviles de la versión 2.0 de HarmonyOS (conocido en China como HongmengOS)[10], basada en Android 10, y disponible para algunos modelos como el P40 (Pro) y Mate 30 (Pro). En abril de 2021 la lista de potenciales dispositivos compatibles se ha ampliado, como modelos como el Mate 40 (Pro) o el Mate X2, y con la expectación de que la versión 2.0 estará disponible para smartphones en abril de 2021, pudiendo ser el Mate 40 Pro 4G el primer modelo que disponga de esta versión preinstalada de fábrica[11], con estimaciones de que a final de 2021 esté en 200 millones de dispositivos[12].

Actualmente, la versión 2.0 beta de HarmonyOS sólo está disponible en China, para obtenerla (por ejemplo, como desarrollador) es necesario pasar un proceso de verificación personal muy exhaustivo, y los primeros datos parecen indicar que no se trata de un nuevo sistema operativo móvil diseñado e implementado por Huawei, sino de una variante basada en Android 10 (con referencias incluso a la versión 10 y no a la versión 2.0), que adicionalmente mantiene la capa de interfaz de usuario EMUI característica de los dispositivos móviles de Huawei[13].

---

**9.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html

**10.** "Huawei releases HarmonyOS 2.0 beta for select phones, still lets you roll back to EMUI 11". GSM Arena. Dec 2020. URL: https://www.gsmarena.com/huawei_releases_harmonyos_20_beta_for_select_phones_those_who_install_can_roll_back_to_emui_11-news-46772.php

**11.** https://www.gizchina.com/2021/04/28/all-new-huawei-smartphones-will-pre-install-harmonyos/

**12.** "HarmonyOS 2.0: Eligible Devices, Beta, Rollout Date, Leaks and more". Huawei Central. Apr 2021. URL: https://www.huaweicentral.com/huawei-harmonyos-2-7/ URL: https://www.huaweicentral.com/harmonyos-eligible-devices/

**13.** "Huawei's HarmonyOS: "Fake it till you make it" meets OS development". Ars Technica. Feb 2021. URL: https://arstechnica.com/gadgets/2021/02/harmonyos-hands-on-huaweis-android-killer-is-just-android/

# 4. Evolución de los mercados oficiales de apps móviles en 2020

Respecto al número total de aplicaciones móviles (en adelante, apps) disponibles en los mercados oficiales, en el año 2020 se aprecia una diferencia notable entre Google Play (Android) y la App Store (iOS), dónde Google Play supera los tres (3) millones de apps y la App Store se encuentra ligeramente por encima de dos (2) millones[14].

Se debe tener en cuenta que el número de apps fluctúa significativamente en un mismo día, mucho más dentro de una semana o mes, por lo que los números proporcionados son estimativos, pero permiten corroborar su crecimiento a lo largo del tiempo.

---

**14.** "Number of apps available in leading app stores as of 4th quarter 2020". Statista. Feb 25, 2021. URL: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

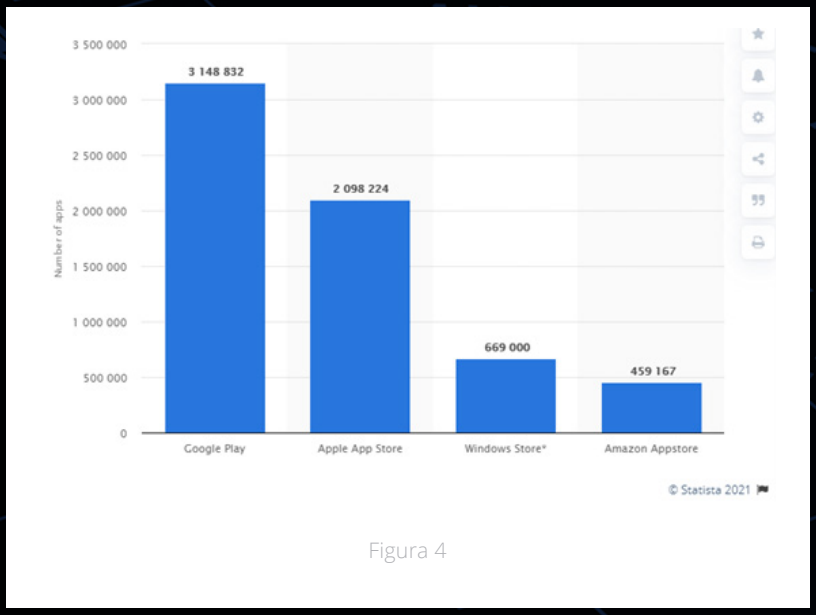



Figura 4

Concretamente, la App Store en julio de 2020 disponía de 3,4 millones de apps, y de casi un millón de juegos (la categoría más popular de apps, con aproximadamente un 22%). Como se puede confirmar, aunque los datos provienen de la misma fuente, existen incongruencias entre el análisis global de los mercados de apps previos, y el específico de la App Store[15].

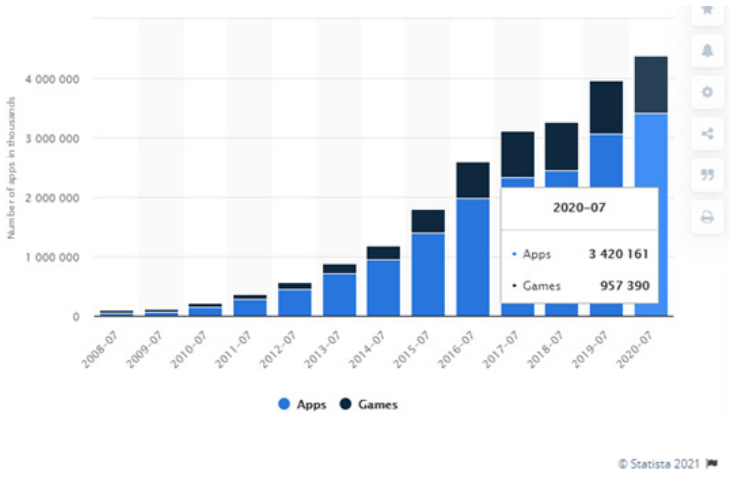



Figura 5

**15.** "Number of available apps in the Apple App Store from 2008 to 2020". Statista. Feb 4, 2021. URL: https://www.statista.com/statistics/268251/number-of-apps-in-the-itunes-app-store-since-2008/

Las estadísticas del año 2020 respecto a las apps disponibles en Google Play han sido finalmente actualizadas por parte de Statista, y presentan un incremento progresivo a lo largo de todo el año 2019 y 2020, tras la brusca disminución que se produjo a finales de 2017 y principios de 2018. El número total de apps en Google Play ronda los 3 millones a finales de 2020[16].

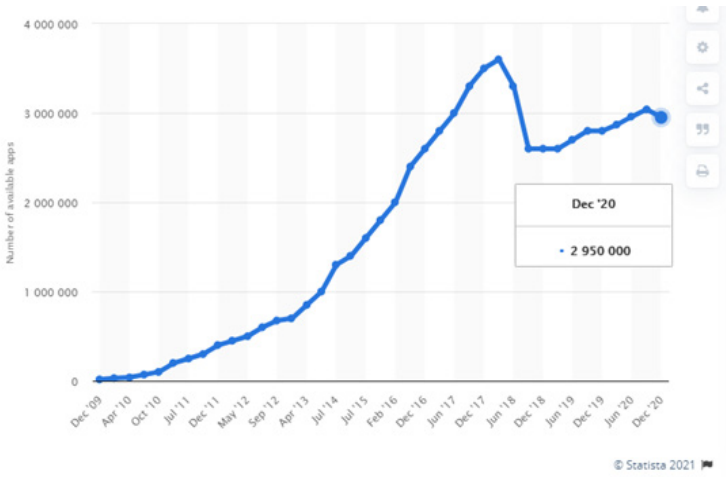
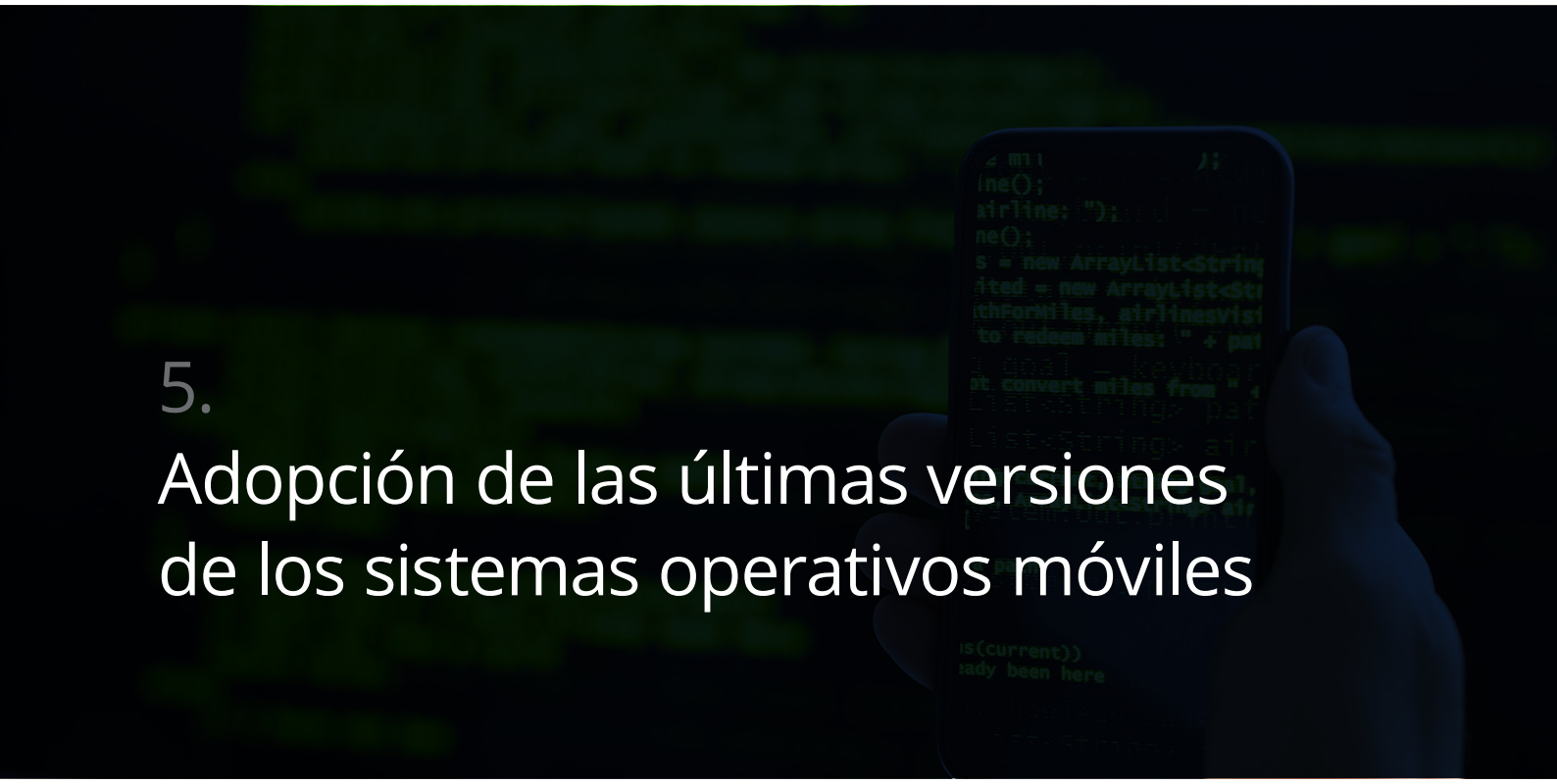



Figura 6

**16.** "Number of available applications in the Google Play Store from December 2009 to December 2020". Statista. Feb 4, 2021. URL: https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

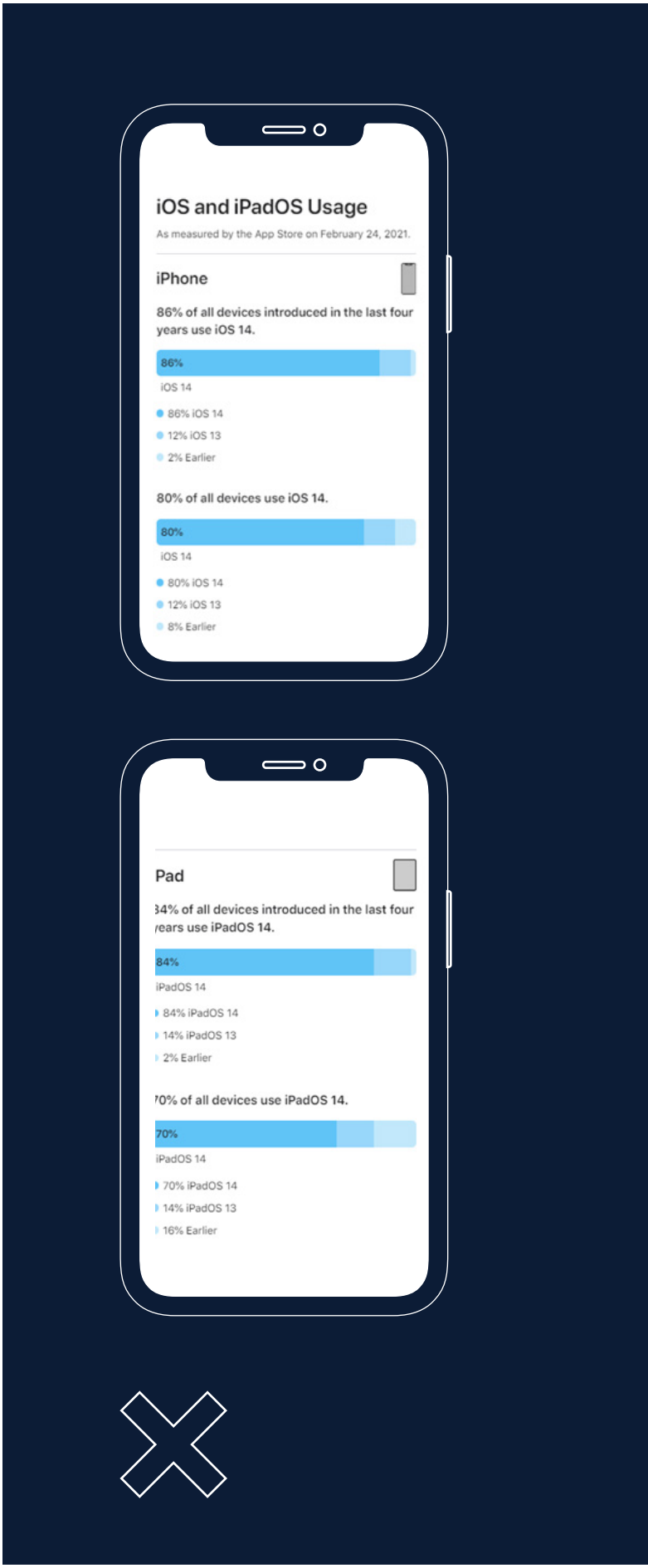


# 5. Adopción de las últimas versiones de los sistemas operativos móviles

La adopción de las nuevas versiones disponibles de los sistemas operativos móviles, iOS y Android, es crítica desde el punto de vista de seguridad, tanto para hacer uso de las nuevas funcionalidades y capacidades de protección introducidas por los fabricantes, Apple y Google, como para poder disponer de las últimas actualizaciones de seguridad que corrigen las vulnerabilidades públicamente conocidas y que, cada vez con más asiduidad, están asociadas a vulnerabilidades *zero-day* (o 0-day) que son explotadas de manera activa en el mundo real, como se muestra en varios ejemplos del presente informe.

Apple liberó, en septiembre de 2020, las últimas versiones del sistema operativo iOS 14.x para iPhone y iPadOS 14.x para iPad. A finales de febrero de 2021, es decir unos 5 meses después, estaban siendo utilizadas por un 86% y un 84% respectivamente de usuarios con dispositivos móviles considerados recientes (es decir, comercializados en los últimos 4 añ Apple liberó, en septiembre de 2020, las últimas versiones del sistema operativo iOS 14.x para iPhone y iPadOS 14.x para iPad. A finales de febrero de 2021, es decir unos 5 meses después, estaban siendo utilizadas por un 86% y un 84% respectivamente de usuarios con dispositivos móviles considerados recientes (es decir, comercializados en los últimos 4 años), y por un 80% y un 70% de usuarios totales, en base a los datos oficiales obtenidos a través de la App Store por parte de Apple [Ref.- 8]. os), y por un 80% y un 70% de usuarios totales, en base a los datos oficiales obtenidos a través de la App Store por parte de Apple[17].

Durante el proceso de elaboración de la presente guía, Apple actualizó las estadísticas de adopción de iOS 13 (ver imagen superior derecha), lo que permite ver la evolución en el tiempo desde la fase inicial de comercialización hasta cuatro (4) meses después, 27 de enero de 2020. En ese momento, iOS y iPadOS 13 estaban siendo utilizadas por un 77% y un 79% respectivamente de usuarios con dispositivos móviles recientes, y por un 70% y un 57% de usuarios totales[18].



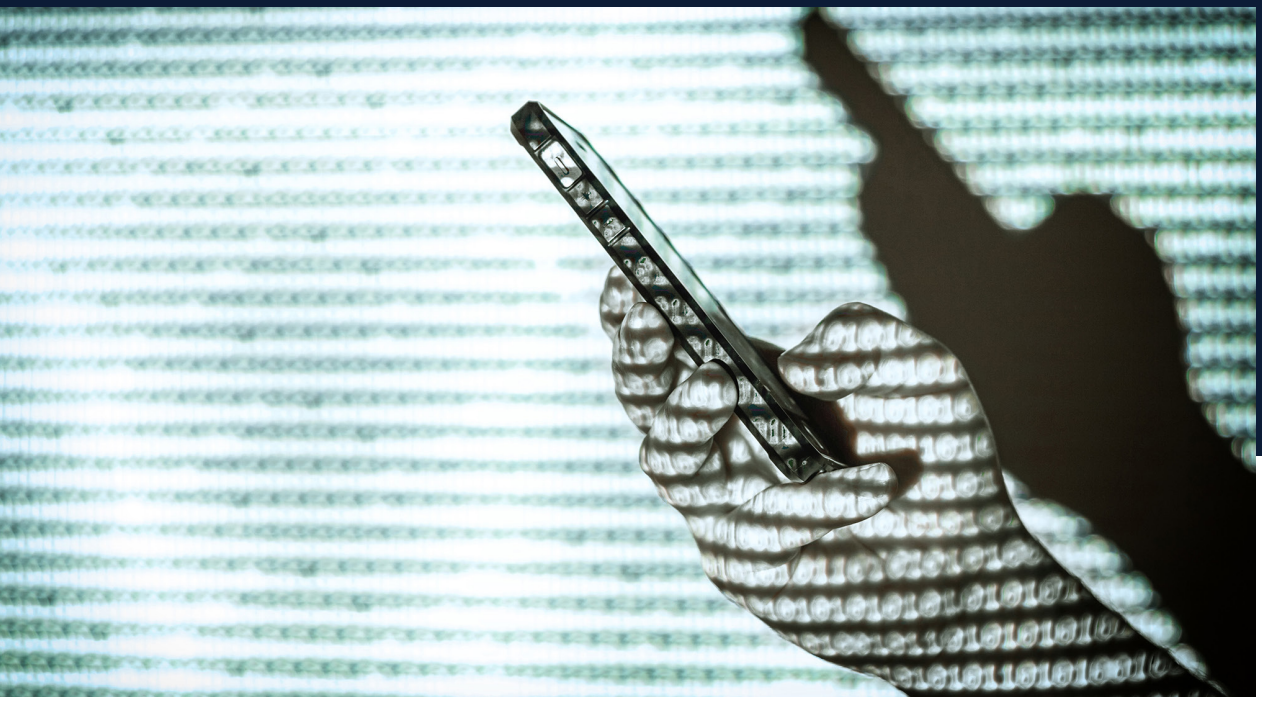

**17,18.** "Support - App Store". Apple Developer. URL: https://developer.apple.com/support/app-store/

En el caso de Android, la última versión del sistema operativo publicada a principios de septiembre de 2020, Android 11 (sin nombre en código), está presentando un nivel de adopción muy lento, en la línea de otras versiones previas de Android, como Android 9 o 10. Tras seis (6) meses desde su publicación, las estadísticas oficiales de Google a finales de abril de 2021 todavía no reflejan la existencia de la versión 11 de Android, lo que indica teóricamente una adopción menor al 0,1% a nivel mundial. Se debe tener en cuenta que estos detalles ya no están disponibles públicamente en las Android Dashboards[19].

| ANDROID PLATFORM VERSION | API LEVEL | CUMULATIVE DISTRIBUTION |
|---|---|---|
| 4.0 Ice Cream Sandwich | 15 | |
| 4.1 Jelly Bean | 16 | 99.8% |
| 4.2 Jelly Bean | 17 | 99.2% |
| 4.3 Jelly Bean | 18 | 98.4% |
| 4.4 KitKat | 19 | 98.1% |
| 5.0 Lollipop | 21 | 94.1% |
| 5.1 Lollipop | 22 | 92.3% |
| 6.0 Marshmallow | 23 | 84.9% |
| 7.0 Nougat | 24 | 73.7% |
| 7.1 Nougat | 25 | 66.2% |
| 8.0 Oreo | 26 | 60.8% |
| 8.1 Oreo | 27 | 53.5% |
| 9.0 Pie | 28 | 39.5% |
| 10. Android 10 | 29 | 8.2% |

Figura 7

Las estadísticas oficiales de Google muestran cómo un 8,2% de dispositivos móviles dispone de Android 10 frente a Android 9.x (Pie) con un 31% de cuota de mercado, Android 8.x (Oreo) con un 14% para Android 8.1 y un 7,3% para Android 8.0 (entre ambos un 21%), o Android 7.0 y 7.1 con casi un 13% conjuntamente. Android 6 sigue manteniendo un 11,2% de cuota, una cifra nada despreciable. Esta situación impide, una vez más, que los usuarios de Android puedan beneficiarse de todas las mejoras de seguridad introducidas en las últimas versiones de Android, siendo a comienzo de 2021 la versión 9 la más ampliamente utilizada.



**19.** "Android Dashboards. Platform Versions". Android Developers. URL: https://developer.android.com/about/dashboards/index.html

Este hecho mantiene la fragmentación de Android ya conocida en años previos, al seguir existiendo cinco versiones distintas con porcentajes muy significativos, lo que tiene un impacto directo en la prevalencia de vulnerabilidades y en la limitada disponibilidad de actualizaciones de seguridad para esta plataforma para muchos usuarios. Cabe recordar que Google sigue proporcionando ciertas actualizaciones de seguridad para la plataforma Android a través de la actualización automática de otros componentes, como Google Play Services (GPS) o del proyecto Mainline (descrito en el informe anual de 2019[20]), aunque las mismas no conlleven ningún incremento de la versión del sistema operativo del dispositivo móvil.

Con el objetivo de disponer de una comparativa de referencia en base a una clasificación y puntuación asociada, y de poder realizar el seguimiento de los dispositivos móviles Android y los fabricantes asociados que proporcionan actualizaciones de seguridad de forma activa y frecuente y especialmente con agilidad, Android Police publica el "Android security update tracker"[21]. En la edición de marzo de 2021 destacan, como habitualmente, los dispositivos Pixel 4/4a/5 de Google, junto a modelos recientes de otros fabricantes como el Samsung Galaxy S20 y Note 20, y con más retrasos, el Sony Xperia 1 II o el LG Velvet 5G. El retraso medio (a lo largo de varios meses) en días a la hora de liberar una nueva actualización de Android cada mes en el caso de muchos fabricantes y modelos de dispositivos móviles modernos se alarga por encima de 20 días (ver siguiente imagen derecha).

**20.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html

**21.** "Android security update tracker, March 2021: Rankings for popular smartphones". Android Police. Mar 2021. URL: https://www.androidpolice.com/2021/03/03/android-phone-security-update-tracker/

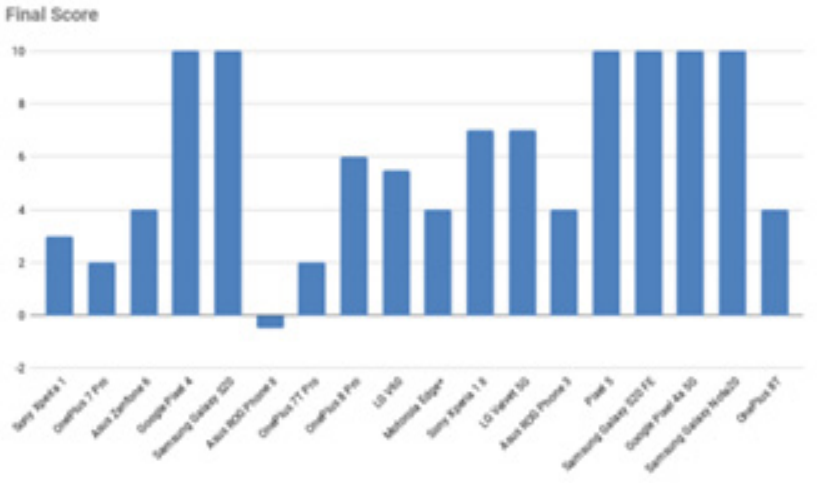



Figura 8

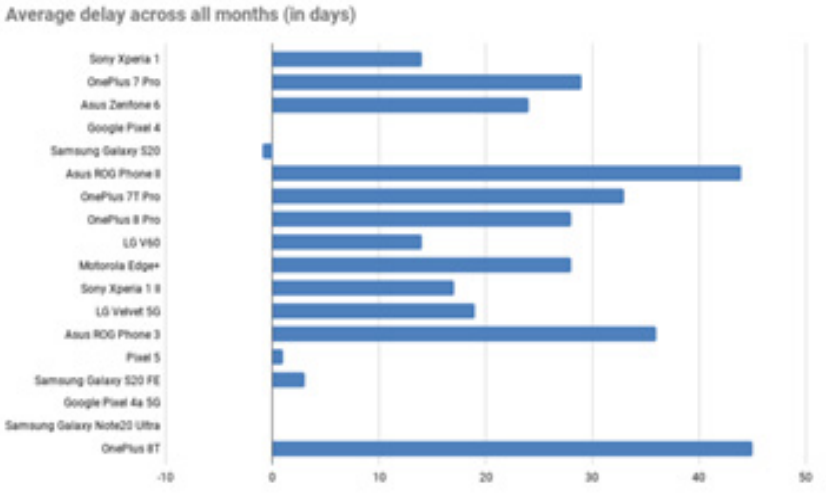
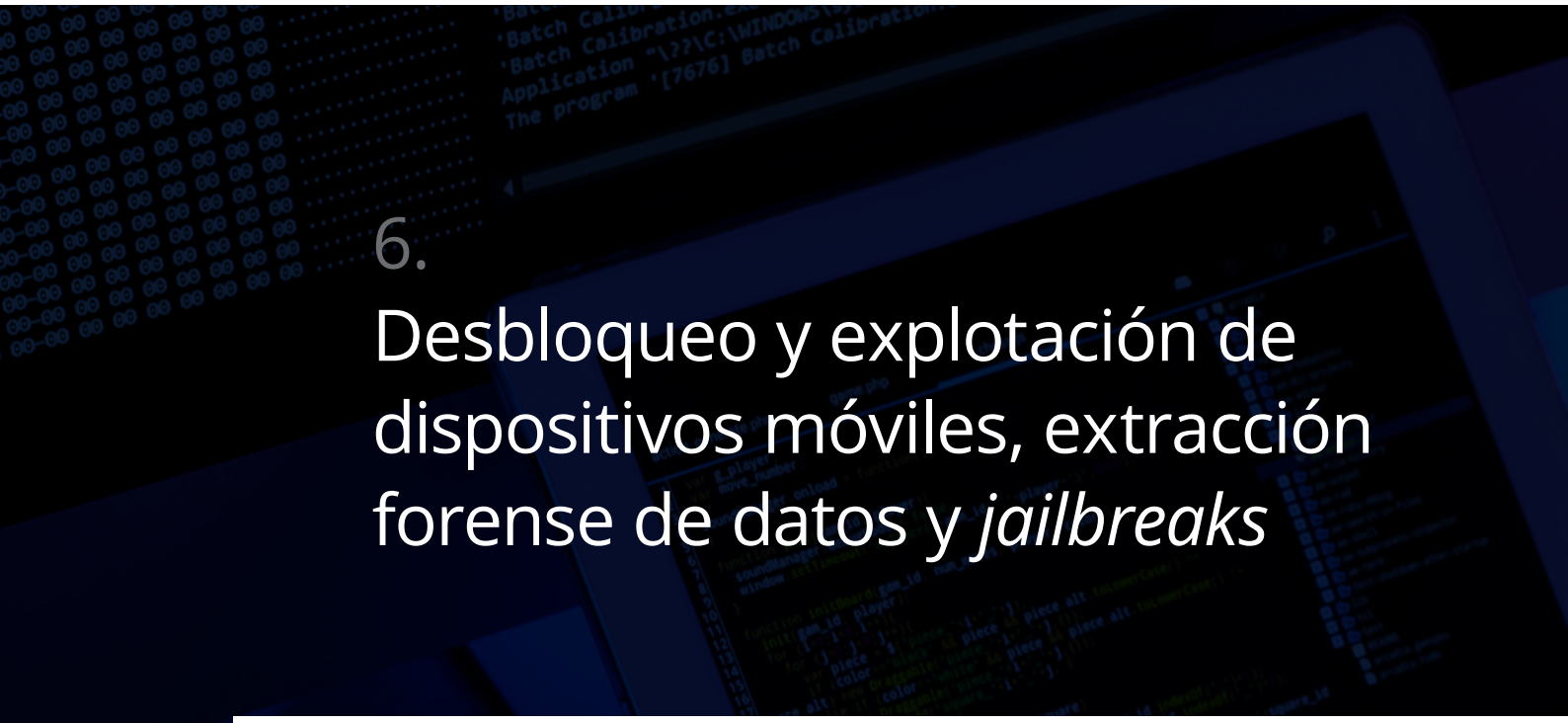



Figura 9



# 6. Desbloqueo y explotación de dispositivos móviles, extracción forense de datos y *jailbreaks*

Los informes anuales de amenazas y tendencias de dispositivos y comunicaciones móviles publicados por el CCN-CERT en los tres últimos años (2017-2029)[22, 23, 24] ya enfatizaban la relevancia que tiene, incluso a día de hoy, 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.

---

**22.** "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

**23.** "CCN-CERT IA-04/19: Informe Anual 2018 - Dispositivos y comunicaciones móviles". CCN-CERT. Enero 2019. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3464-ccn-cert-ia-04-19-informe-anual-2018-dispositivos-moviles/file.html

**24.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html

Continuando con la tendencia de los últimos años, donde los dispositivos móviles basados en iOS han presentado numerosas vulnerabilidades que han permitido evitar la pantalla de desbloqueo sin disponer del código de acceso[25], iOS 14 ya acumula un total de tres (3) vulnerabilidades hasta la versión 14.4.2, reduciendo ligeramente su número respecto a iOS 12 o iOS 13. Estas vulnerabilidades permiten el acceso al contenido de notificaciones y de contactos. Este tipo de amenaza refleja los riesgos asociados a accesos físicos no autorizados, temporales, durante un breve espacio de tiempo, o permanentes, como en la pérdida o robo de los dispositivos móviles, siendo imprescindible tomar medidas de protección frente a estos escenarios de ataque.

El año 2020 se ha caracterizado una vez más por los avances ofensivos de las soluciones comerciales de análisis forense de dispositivos móviles y las restricciones impuestas por Apple, con el objetivo de restringir los posibles accesos no autorizados a través del puerto USB. Las últimas mejoras disponibles en versiones previas de iOS, incluyendo las capacidades del modo restringido USB de iOS 13 (dispositivos USB de confianza previamente emparejados) ya mencionadas en detalle en el informe anual de 2019[26] y en la guía práctica de seguridad de dispositivos móviles iOS 13 del CCN-CERT[27], pueden ser todavía evitadas mediante el modo de diagnóstico de iOS[28] (referenciado a continuación), introducido en iOS 10.3 (también denominado CheckerBoard, y utilizado por el servicio de soporte en tiendas Apple).

**25.** "Bypassing iOS Lock Screens: A Comprehensive Arsenal of Vulns". DinoSec. Mar 2021. URL: http://blog.dinosec.com/2014/09/bypassing-ios-lock-screens.html

**26.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html

**27.** "Guía práctica de seguridad en dispositivos móviles: iOS 13.x". CCN-STIC 455E. CCN-CERT. Feb 2020. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/4569-ccn-stic-455e-configuracion-segura-de-ios-13/file.html

**28.** "Working Around the iPhone USB Restricted Mode". Elcomsoft. May 2020. URL: https://blog.elcomsoft.com/2020/05/iphone-usb-restricted-mode-workaround/ - URL: https://blog.elcomsoft.com/2020/05/ios-acquisition-reloaded/

En el proceso de adquisición física y extracción forense de datos de un dispositivo móvil hay un escenario muy común denominado BFU (Before First Unlock), que fue presentado en el informe de 2019[29], es decir, qué datos parciales están disponibles antes del primer desbloqueo del dispositivo, o lo que es equivalente, al arrancar el dispositivo en modo normal y no disponer del código de acceso.

Alternativamente, los dispositivos iOS pueden ser arrancados en modo DFU (Device Firmware Update) para obtener información limitada, como el modelo y número de serie. En modo DFU es posible aprovecharse del *jailbreak* checkra1n[30], desde el iPhone 5S al iPhone X, para llevar a cabo una adquisición completa del sistema de ficheros y la potencial extracción de la keychain (especialmente si se conoce el código de acceso). Si las restricciones USB están activas, es posible arrancar en modo DFU. Sin embargo, e independientemente de su estado previo, las nuevas versiones de checkra1n (con soporte para iOS 13.4 y versiones superiores) activan estas restricciones USB.

Por tanto, para poder completar el proceso de *jailbreak* e instalar checkra1n es necesario deshabilitar estas restricciones USB, para lo que se debe conocer el código de acceso (un requisito innecesario si se desea llevar a cabo una extracción BFU). Aunque podría pensarse que, por tanto, las restricciones USB son efectivas frente a las nuevas versiones de checkra1n, a través de la herramienta minaUSB[31](disponible para macOS) es posible engañar al modo restringido USB mediante el modo de diagnóstico de iOS (mencionado previamente) e instalar checkra1n (incluso sin conocer el código de acceso del dispositivo). minaUSB parchea y deshabilita el estado de las restricciones USB y permite completar la adquisición BFU. Versiones posteriores de checkra1n evolucionaron para permitir la extracción de datos desde el modo DFU en un escenario BFU sin necesidad de utilizar herramientas adicionales[32].

Desde un punto de vista defensivo, existen numerosas recomendaciones y opciones de configuración que pueden ser aplicadas en los dispositivos móviles iOS para evitar ser víctima de estas técnicas de análisis forense[33]. De manera resumida, se recomienda siempre disponer de la última versión de iOS estable pública, hacer uso de un código de acceso y de una contraseña para los backups robustos, establecer un código de Tiempo de Uso (ver siguiente párrafo), habilitar los mecanismos de autobloqueo de la pantalla, restringir la funcionalidad existente en la pantalla de bloqueo[34], prestar atención a las conexiones USB que se establecen desde el dispositivo (incluyendo los cables empleados y el cargador o dispositivo al que se conecta el móvil), y más concretamente al establecimiento de relaciones de confianza, aprender cómo activar el modo de emergencia (o SOS) o evaluar el uso de iCloud, entre muchas otras buenas prácticas.

**29.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html
**30.** checkra1n. 2020-2021. URL: https://checkra.in URL: https://github.com/axi0mX/ipwndfu
**31.** "Working Around the iPhone USB Restricted Mode". Elcomsoft. May 2020. URL: https://blog.elcomsoft.com/2020/05/iphone-usb-restricted-mode-workaround/ - URL: https://blog.elcomsoft.com/2020/05/ios-acquisition-reloaded/
**32.** "checkra1n, USB Restrictions and Breaking Into Locked iPhones". Elcomsoft. July 2020. URL: https://blog.elcomsoft.com/2020/07/checkra1n-usb-restrictions-and-breaking-into-locked-iphones/ - URL: https://blog.elcomsoft.com/2020/07/checkra1n-installation-tips-tricks/
**33.** "Playing devil's advocate: iPhone anti-forensics". Elcomsoft. Sep 2020. URL: https://blog.elcomsoft.com/2020/09/playing-devils-advocate-iphone-anti-forensics/
**34.** "Bypassing iOS Lock Screens: A Comprehensive Arsenal of Vulns". DinoSec. Mar 2021. URL: http://blog.dinosec.com/2014/09/bypassing-ios-lock-screens.html

Desde iOS 11, Apple redujo el nivel de seguridad de los dispositivos móviles al añadir la posibilidad de resetear la contraseña de los backups locales cifrados, tal como se detallaba en el informe anual de 2017[35], opción que no estaba disponible en versiones previas de iOS. Esta funcionalidad sigue presente en iOS 13 e iOS 14, pero en el año 2020 se descubrió que al establecer un código de Tiempo de Uso (o Screen Time), compuesto por un PIN de 4 dígitos, se impide que la contraseña de los backups pueda ser reseteada[36]. Las capacidades asociadas al Tiempo de Uso, aunque no directamente relacionadas con la seguridad y privacidad, proporcionan mecanismos avanzados para la protección de dispositivos móviles iOS en caso de que un tercero no autorizado disponga de acceso físico temporal al dispositivo, tal como se detalla en la guía práctica de seguridad de dispositivos móviles iOS 13 del CCN-CERT[37]. Debe tenerse en cuenta que el código de Tiempo de Uso se almacena localmente en el dispositivo móvil y en versiones recientes de iOS (iOS 13) puede ser obtenido mediante el proceso de jailbreak, a diferencia de en versiones previas de iOS, y en el caso de iOS 14 a través de iCloud en ciertos casos concretos[38].

Desde el punto de vista del estado del arte de los jailbreaks, aunque checkra1n fue ya analizado en el informe de 2019[39], junto al exploit checkm8 tras su publicación inicial, este jailbreak ha evolucionado significativamente en el año 2020 y comienzos de 2021 para proporcionar soporte a las nuevas versiones de iOS.

Debido a que se trata de una nueva vulnerabilidad de BootROM, todos los dispositivos móviles vulnerables (desde el iPhone 5s al X, dispositivos con un SoC <= A11), seguirán siendo potencialmente vulnerables por el resto de sus días, independientemente de la versión de iOS de la que dispongan.

Para intentar mitigar este escenario de ataque, en iOS 14 Apple introdujo nuevas restricciones en dispositivos móviles con un SoC A10 o superior, es decir, el iPhone 7 o modelos posteriores. Las mitigaciones de iOS 14 hacen que si un dispositivo arranca en modo DFU (requisito imprescindible para poder explotar la vulnerabilidad del BootROM vía checkra1n), si el Secure Enclave recibe una petición para descifrar los datos de usuario, se aborta la ejecución. Por tanto, las nuevas versiones de checkra1n sólo funcionaban inicialmente en iOS 14 hasta el iPhone 6S o SE (SoC A9)[40]. Para permitir el proceso de jailbreak en estos modelos, checkra1n[41] implementó el nuevo exploit asociado a la vulnerabilidad blackbird del Secure Enclave, lo que permite deshabilitar la nueva mitigación. Como resultado, versiones posteriores de checkra1n publicadas a lo largo de 2020 y principios de 2021 permiten de nuevo realizar el proceso de jailbreak en todos los dispositivos móviles hardware afectados, desde el iPhone 5s al X (en dispositivos con el SoC A11, iPhone 8 o posterior, debe de eliminarse el código de acceso).

---

**35.** "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

**36, 38.** "Using Screen Time Password to Protect iPhone Local Backups". Elcomsoft. Sep 2020. URL: https://blog.elcomsoft.com/2020/09/using-screen-time-password-to-protect-iphone-local-backups/

**37.** "Guía práctica de seguridad en dispositivos móviles: iOS 13.x". CCN-STIC 455E. CCN-CERT. Feb 2020. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/4569-ccn-stic-455e-configuracion-segura-de-ios-13/file.html

**39.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html

**40.** "The state of checkra1n on iOS 14". checkra1n. URL: https://checkra.in/news/2020/09/iOS-14-announcement

**41.** checkra1n. 2020-2021. URL: https://checkra.in URL: https://github.com/axi0mX/ipwndfu

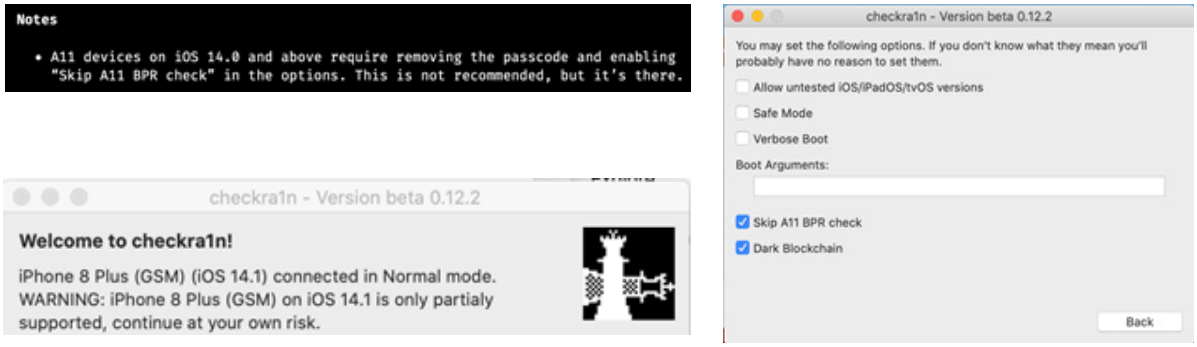



Figura 10

Adicionalmente, la comunidad de *jailbreak* durante el año 2020 y comienzo de 2021 ha evolucionado también hacia iOS 14 mediante nuevas versiones de **unc0ver**[42], como la versión 6.0.0 publicada el 28 de febrero de 2021, que implementa el exploit cicuta_virosa de escalada local de privilegios (LPE) en el kernel de iOS 14, y proporciona soporte hasta iOS 14.3 (frente al soporte de la versión 5.0.0 desde iOS 11.0 hasta iOS 13.5 existente previamente, y disponible desde mayo de 2020, al ser solucionada la vulnerabilidad de kernel con CVE-2020-9859 en iOS 13.5.1). Este *jailbreak* supone de nuevo un avance significativo al permitir aplicar el proceso a cualquier dispositivo con iOS 14.3 o inferior, incluyendo los últimos modelos de iPhones y iPads.

Tal como se mencionaba en el informe anual de 2019[43] la comunidad de *jailbreaks* estuvo rodeada de gran controversia debido a las disputas legales de Apple contra Corellium, y su plataforma de virtualización de iOS, que salieron a la luz públicamente a finales de diciembre de 2019. A finales de 2020, un año después, se conocía que Corellium había ganado la batalla legal, al menos inicialmente, respecto a la demanda interpuesta por Apple, en base a la sentencia de un juez federal en Florida[44], lo que le permite continuar con sus actividades de negocio y evolucionando su producto ampliamente utilizado por investigadores a nivel comercial.

Igualmente, y en relación con el nuevo programa de recompensas (*bug bounty*) para investigadores de seguridad de Apple, Apple Security Bounty, finalmente en el año 2020 Apple publicaba y distribuía los nuevos dispositivos móviles iOS oficiales de investigación de Apple, con acceso de bajo nivel como root y capacidades de depuración. Concretamente, los nuevos dispositivos de investigación en seguridad, o Apple Security Research Devices (SRDs), se anunciaban en julio de 2020[45] como parte de un programa privado para ciertos investigadores de seguridad (España incluida), a los que se les "prestan" los dispositivos durante un periodo de 12 meses para realizar sus tareas de investigación y de descubrimiento de vulnerabilidades en iOS.

---

**42.** unc0ver. 2020-2021. URL: https://unc0ver.dev URL: https://github.com/pwn20wndstuff/Undecimus
**43.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html
**44.** "Apple loses copyright battle against security start-up Corellium". The Washington Post. Dec 2020. URL: https://www.washingtonpost.com/technology/2020/12/29/apple-corellium-lawsuit/
**45.** "Apple Security Research Device Program". Apple. URL: https://developer.apple.com/programs/security-research-device/ - URL: https://developer.apple.com/security-bounty/

A finales de marzo de 2021, Apple publicaba la versión 14.4.2 de iOS y iPadOS para corregir únicamente una vulnerabilidad de WebKit (CVE-2021-1879)[46], que permitía explotar un Cross-Site Scripting (XSS) universal. Es decir, que un sitio web malicioso pudiera ejecutar código JavaScript en cualquier otro sitio web u origen. Apple tenía constancia de que esta vulnerabilidad estaba siendo activamente explotada, por lo que no le quedó más remedio que sacar una nueva versión de iOS/iPadOS para solucionarla.

**46.** https://support.apple.com/en-us/HT212256

# 7. Mecanismos de seguridad avanzados en dispositivos móviles

Con el objetivo de mitigar las amenazas asociadas a la pantalla de bloqueo (mencionadas en el apartado previo, "6. Desbloqueo y explotación de dispositivos móviles, extracción forense de datos y *jailbreaks*"), especialmente al identificarse la importancia de los dispositivos móviles como una extensión directa de la vida e identidad digital y real de sus usuarios, Android 11 introdujo mejoras significativas en la pantalla de bloqueo (lockscreen) y en los mecanismos de autentificación[47], concretamente, en los relacionados con la biometría y la interacción con el entorno.

**47.** "Lockscreen and Authentication Improvements in Android 11". Google Security Blog. Sep 2020. URL: https://security.googleblog.com/2020/09/lockscreen-and-authentication.html

Android clasifica los mecanismos de autentificación mediante un modelo de autentificación por capas, compuesto por tres capas: primaria (qué conoces - basada en datos conocidos), secundaria (qué eres - basada en biometría) y terciaria (qué tienes - basada en el entorno). Estas capas evolucionan de mayor a menor seguridad, y de un menor a un mayor número de restricciones impuestas sobre el usuario, construyéndose unas sobre las otras.

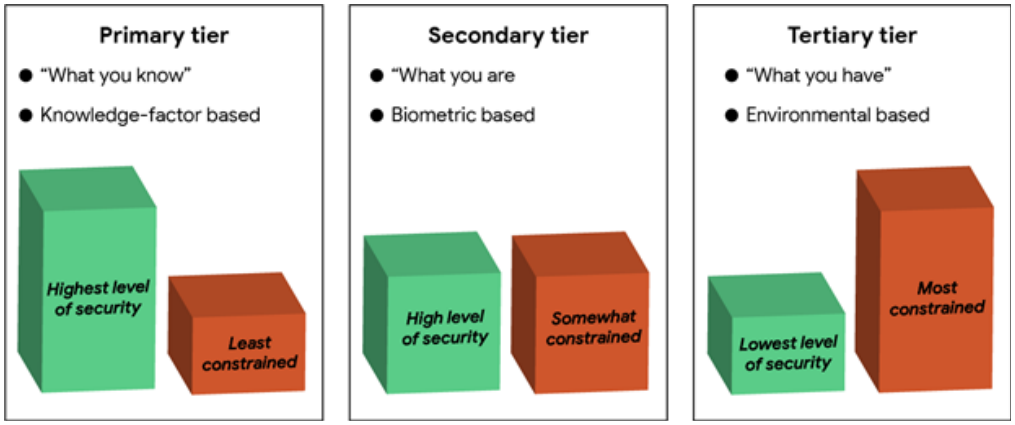



Figura 11

La primera capa autentifica al usuario en base a algo que conoce, un PIN, código de acceso o contraseña, donde la entropía es un factor fundamental (contraseñas suficientemente robustas y no predecibles). La segunda capa autentifica al usuario en base a algo que es, biometría, con identificación facial o de la huella dactilar digital, métodos más cómodos, pero potencialmente menos seguros. La tercera capa autentifica al usuario en base a algo que tiene, un token físico, un dispositivo Bluetooth (o dispositivo de confianza), o mediante el entorno que le rodea, como una ubicación de confianza (como su hogar u oficina).

Esta última capa, todavía más cómoda, ofrece niveles de seguridad más débiles que las anteriores, al ser más manipulables. Por este motivo, ya en Android 10 la capa terciaria no permite desbloquear el dispositivo móvil, sino mantener el estado de desbloqueo a lo largo del tiempo (una vez el dispositivo ha sido desbloqueado mediante algún mecanismo de la capa primaria o secundaria), hasta un máximo de 4 horas.

Desde el punto de vista biométrico, Android clasifica los mecanismos de autentificación y su implementación en base a dos factores: la seguridad de su arquitectura, que mide el impacto asociado en caso de que el kernel o la plataforma sea comprometida, y un indicador o métrica conocido como SAR (Spoof Acceptable Rate)[48], introducida en Android 9 (realmente en 8.1) y en el informe anual de 2018[49], que mide la posibilidad de suplantación del usuario legítimo o cómo de robusto es el mecanismo de autentificación biométrico frente a un atacante dedicado. En base a estos dos factores, las soluciones biométricas se clasifican en tres clases (3, 2 o 1) de mayor a menor nivel de seguridad. Google proporciona una tabla de clasificación en estas tres (3) clase[50].

Los mecanismos de autentificación biométricos (como mecanismos o capa secundaria), tan ampliamente utilizados hoy en día en los dispositivos móviles, y con un alto nivel de adopción en los últimos 3-4 años, buscan encontrar un equilibrio entre proporcionar un nivel de seguridad elevado y un alto nivel de usabilidad. Por ejemplo, su adopción ayuda a que los usuarios establezcan mecanismos en la capa primaria más robustos, como códigos de acceso o contraseñas más largas y/o complejas, beneficiándose de las protecciones de la pantalla de bloqueo, y de los mecanismos de cifrado del dispositivo móvil y de las copias de seguridad en la nube. Sin embargo, siempre debe tenerse en cuenta que potencialmente los mecanismos biométricos pueden ser engañados.

Una vez más, en Android 11, como en versiones de Android anteriores (9 y 10), se actualizan y mejoran las capacidades de la API BiometricPrompt para permitir a los desarrolladores de apps restringir los mecanismos biométricos permitidos por la app[51], en función de las tres clases mencionadas previamente (3, 2 o 1), así como conocer qué mecanismo ha sido utilizado en cada intento de autentificación exitoso[52]. Adicionalmente, se mejora el soporte para claves autentificadas o *auth-per-use*, es decir, claves criptográficas almacenadas en la Android KeyStore (mediante protección hardware vía el TEE o Strongbox) y protegidas por biometría, siendo necesario que el usuario se autentifique para poder hacer uso de los datos protegidos por estas claves por parte de la app. El usuario por tanto debe demostrar su presencia y su identidad.

**48.** https://source.android.com/security/biometric/measure
**49.** "CCN-CERT IA-04/19: Informe Anual 2018 - Dispositivos y comunicaciones móviles". CCN-CERT. Enero 2019. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3464-ccn-cert-ia-04-19-informe-anual-2018-dispositivos-moviles/file.html
**50, 52.** "Lockscreen and Authentication Improvements in Android 11". Google Security Blog. Sep 2020. URL: https://security.googleblog.com/2020/09/lockscreen-and-authentication.html
**51.** https://source.android.com/security/biometric

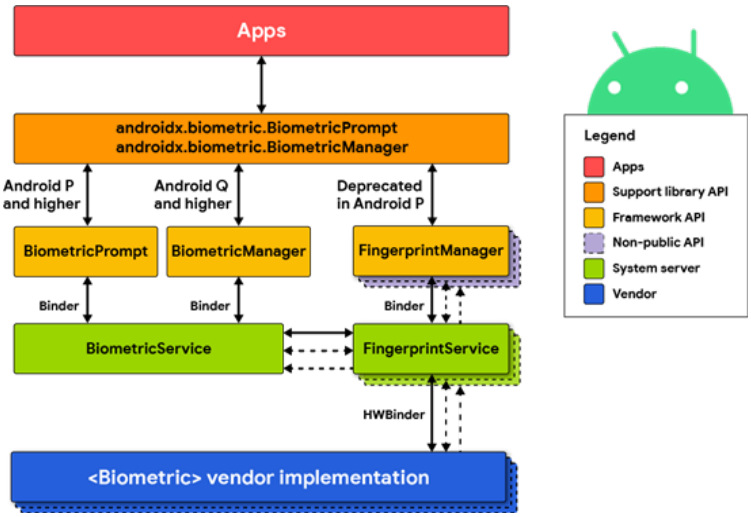



Figura 12

Estas capacidades de protección avanzadas, integrando los mecanismos criptográficos y biométricos[53], son empleadas habitualmente por parte de apps críticas, por ejemplo, en el sector financiero, sanitario, gubernamental o empresarial. Dentro de las capacidades disponibles está tanto el cifrado de datos, como la verificación de integridad y autentificación, o la generación de firmas digitales.

Complementando las capacidades biométricas de Android, en el caso de la implementación biométrica de iOS, mediante TouchID o FaceID, en agosto de 2020 se desvelaba una vulnerabilidad que ponía en riesgo las cuentas de iCloud de los usuarios[54]. En iOS 13 Apple añadió la posibilidad de autentificarse en los sitios web del propio Apple mediante biometría empleando Safari, tanto en iOS como en macOS, en dispositivos con sensores biométricos, y sin requerir 2FA. El proceso de autentificación en los sitios web de Apple se basa en OAuth2, pero al hacerse uso de TouchID/FaceID, se utiliza de forma diferente y la implementación (en concreto del servidor "gsa.apple.com") permitía potencialmente acceder a las cuentas de iCloud de otros usuarios, ya que no se verificaba correctamente la relación entre la redirect_uri y el client_id empleados por OAuth2.

En ese proceso de evolución anual continuo de la seguridad de las plataformas móviles, Android 11 introduce nuevos ajustes por defecto más seguros, hace uso de un gestor de memoria más protegido (denominado Scudo), y añade comprobaciones y mitigaciones adicionales en el compilador[55]. Android 11 mejora el proceso de inicialización de memoria, tanto en espacio de usuario como de kernel, para evitar ciertos exploits de memoria no inicializada comunes en C/C++. Las mitigaciones del compilador incluyen sanitizadores de enteros y de límites en librerías críticas que aún no los implementaban, como por ejemplo en la pila NFC.

**53.** "Using BiometricPrompt with CryptoObject: how and why". Android Developers. Feb 2020. URL: https://medium.com/androiddevelopers/using-biometricprompt-with-cryptoobject-how-and-why-aace500ccdb7
**54.** "Vulnerability in new TouchID feature put iCloud accounts at risk of being breached". Computest. Aug 2020. URL: https://www.computest.nl/en/knowledge-platform/blog/vulnerability-new-touchid-feature-iCloud-accounts-at-risk-breached/
**55.** "System hardening in Android 11". Google Security Blog. Jun 2020. URL: https://security.googleblog.com/2020/06/system-hardening-in-android-11.html

Adicionalmente, se extiende el uso de CFI, Control Flow Integrity, a nuevos componentes como el demonio de red o el cliente (o resolver) DNS. Las contramedidas previas tomadas en Android 10 respecto al sandbox para la ejecución de los codecs multimedia parecen haber sido efectivas, al no haberse identificado ninguna vulnerabilidad crítica en los *media frameworks* en Android 10, por primera vez desde Android 5.0. Adicionalmente, Android 11 incorpora nuevas mejoras para proteger, no sólo la seguridad, sino también la privacidad del usuario[56].

En la fecha final de elaboración del presente informe (abril de 2021) Google no ha publicado una actualización de su guía "Android Enterprise Security White Paper"[57], siendo la última actualización existente la publicada a principios de 2020 ya comentada en el informe anual del pasado año[58].

Por el contrario, a lo largo del año 2020 y en 2021 Apple ha continuado actualizando su guía técnica oficial de seguridad ("Apple Platform Security")[59], unificada en un único documento desde 2019, que aglutina en sus casi 200 páginas todos los aspectos de seguridad de sus diferentes plataformas y dispositivos, incluyendo tanto equipos tradicionales como móviles, y todos los sistemas operativos iOS, iPadOS, watchOS, tvOS y macOS. Adicionalmente a la última versión de macOS BigSur, y las nuevas tecnologías ARM para portátiles (Apple Silicon y el procesador M1), la última versión de la guía incluye las novedades de iOS 14 y watchOS 7, con actualizaciones[60] en el Security Enclave (SE), la desconexión hardware del micrófono, seguridad de Apple Cash y del Activation Lock, privacidad de Wi-Fi, y mejoras en la protección de memoria de iBoot, los nuevos dispositivos de investigación en seguridad (mencionados en el apartado "6. Desbloqueo y explotación de dispositivos móviles, extracción forense de datos y *jailbreaks*"), o innovaciones como la seguridad de llaves de coche en iOS.

---

**56.** https://security.googleblog.com/2020/06/11-weeks-of-android-privacy-and-security_29.html
**57.** "Android Enterprise Security White Paper". Android. Jan 2020. (no actualizada en 2021) URL: https://source.android.com/security/overview/reports - URL: https://static.googleusercontent.com/media/www.android.com/en//static/2016/pdfs/enterprise/Android_Enterprise_Security_White_Paper_2019.pdf
**58.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html
**59.** "Apple Platform Security - February 2021". Apple. Feb 2021. URL: https://support.apple.com/guide/security/welcome/web - URL: https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf
**60.** https://9to5mac.com/2021/02/18/2021-apple-platform-security-guide-available/

La versión de febrero de 2021 de la guía, sin embargo, no hace mención al nuevo sistema de seguridad BlastDoor para iMessage en iOS 14 (y macOS BigSur), pese a existir una sección específica en la guía dedicada a la seguridad de iMessage. BlastDoor es un sandbox que protege iOS frente al procesamiento de mensajes entrantes a través de la app de mensajería de Apple, y aísla esta del resto del sistema iOS[61]. El nombre ha sido acuñado en base al nombre del servicio, desarrollado en Swift, e identificado mediante ingeniería inversa (ver siguiente imagen). Su propósito es mitigar el impacto de potenciales mensajes maliciosos recibidos, a la hora de desempaquetarlos y procesar sus contenidos, por parte del resto del sistema, ya que, como se ha detallado en los informes anuales de años previos, en varias ocasiones el envío de mensajes maliciosos ha sido empleado para llevar a cabo ataques dirigidos contra usuarios relevantes concretos explotando vulnerabilidades en iOS. Estas vulnerabilidades han permitido incluso la ejecución de código remoto (RCE) y, por tanto, tomar el control de un dispositivo móvil iOS remotamente únicamente mediante el envío de un mensaje conociendo el número de móvil del usuario objetivo.

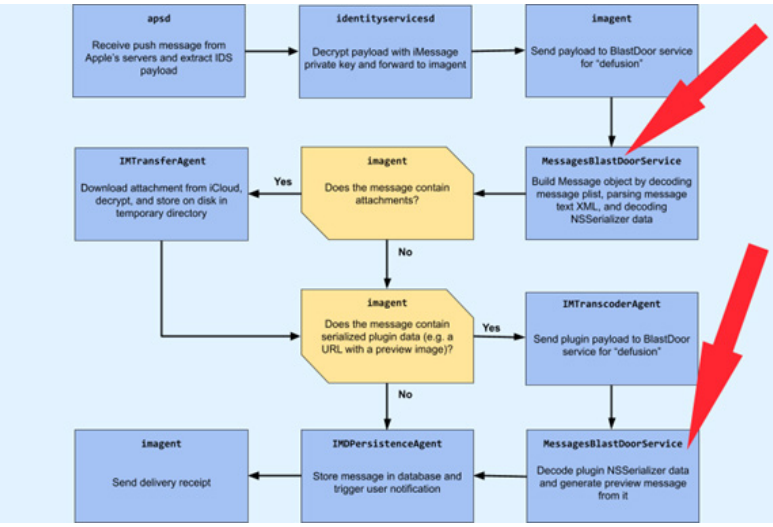



Figura 13

Más específicamente, el informe anual de 2019[62] detallaba un conjunto de vulnerabilidades que afectaron a iMessage e iOS y que fueron descubiertas por investigadores del Proyecto Zero de Google, al igual que la existencia de BlastDoo[63], concretamente por Samuel Groß.

En enero de 2020, estos extendían sus investigaciones y profundizaban más en detalle en la explotación remota de los iPhone a través de iMessage sin la intervención del usuario, a través de una serie de publicaciones técnicas en su blog[64].

---

**61.** "Google researcher discovers new iOS security system". ZDNet. Jan 2021. URL: https://www.zdnet.com/article/google-researcher-discovers-new-ios-security-system/ - "Apple adopts new 'BlastDoor' security system on iOS 14 to reinforce iMessage integrity". 9to5Mac. Jan 2021. URL: https://9to5mac.com/2021/01/28/apple-adopts-new-blastdoor-security-system-on-ios-14-to-reinforce-imessage-integrity/

**62.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html

**63.** "A Look at iMessage in iOS 14". Google Project Zero. Jan 2021. URL: https://googleprojectzero.blogspot.com/2021/01/a-look-at-imessage-in-ios-14.html

**64.** "Remote iPhone Exploitation Part 1: Poking Memory via iMessage and CVE-2019-8641". Google Project Zero. Jan 2020. URL: https://googleprojectzero.blogspot.com/2020/01/remote-iphone-exploitation-part-1.html - "Remote iPhone Exploitation Part 2: Bringing Light into the Darkness -- a Remote ASLR Bypass". Google Project Zero. Jan 2020. URL: https://googleprojectzero.blogspot.com/2020/01/remote-iphone-exploitation-part-2.html - "Remote iPhone Exploitation Part 3: From Memory Corruption to JavaScript and Back -- Gaining Code Execution". Google Project Zero. Jan 2020. URL: https://googleprojectzero.blogspot.com/2020/01/remote-iphone-exploitation-part-3.html


Un caso real de este tipo de vulnerabilidades y exploits, acontecido a mediados de 2020, se detalla en el apartado "11. Comunicaciones móviles" bajo el nombre de "The Great iPwn", publicado por Citizen Lab[65], donde se detallaba que los exploits no parecían ser efectivos contra iOS 14 debido a las nuevas protecciones de seguridad implementadas, es decir, BlastDoor.

Complementando la guía técnica oficial, Apple ha publicado un nuevo portal y una guía asociada relacionada, "Security Certifications and Compliance Center" (SCCC), con las certificaciones de seguridad y cumplimiento del hardware, sistemas operativos, software y apps, y servicios de Apple[66], reflejando la importancia creciente por parte de los fabricantes en ratificar la seguridad de sus productos mediante referencias reconocidas en la industria.

Adicionalmente, en diciembre de 2020 Apple actualizó su sitio web oficial de privacidad[67], argumentando que se trata de un derecho humano fundamental, y detallando las protecciones de privacidad implementadas en diferentes apps de Apple existentes por defecto en iOS, y en iOS 14. Asimismo, la política de privacidad incluye numerosos detalles acerca de qué se consideran datos personales y cómo se procesan. Adicionalmente, Apple publicó las etiquetas de privacidad (Privacy Labels) en la App Store, un sistema para identificar de forma sencilla y transparente las prácticas de privacidad de las apps[68].

Desde principio de diciembre, Apple solicitó a los desarrolladores proporcionar información de privacidad para sus apps a través de la App Store. A finales de mes, los usuarios podían ver las etiquetas en la App Store y entender de manera global como una app procesará sus datos en tres categorías: datos utilizados para seguirte, datos asociados a ti y datos no asociados a ti. Los desarrolladores que abogan por la privacidad pueden informar a los usuarios acerca de qué tipos de datos recopila su app, si los datos son compartidos con terceros, y cómo el usuario puede optar para que sus datos no sean procesados.

---

**65.** "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit". Citizen Lab. Dec 2020. URL: https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/

**66.** "Security Certifications and Compliance Center". Apple. Feb 2021. URL: https://support.apple.com/guide/sccc/ URL: https://manuals.info.apple.com/MANUALS/1000/MA1997/en_US/security-certifications-compliance-center.pdf

**67.** "Privacy". Apple. URL: https://www.apple.com/privacy/ URL: https://www.apple.com/legal/privacy/en-ww/

**68.** "New 'App Privacy' labels now live in the App Store, offering detailed overviews of app data practices". 9to5 Mac. Dec 2020. URL: https://9to5mac.com/2020/12/14/app-privacy-labels-app-store/ URL: https://www.apple.com/privacy/labels/

Los detalles de privacidad de las propias apps de Apple también están disponibles en la web oficial de privacidad[69].

Dentro de la tendencia generalizada existente en la industria de ciberseguridad hacia la certificación de productos y servicios que permitan proporcionar confianza y fiabilidad en los mismos, tal como denota la guía previa de certificación y cumplimiento de Apple o los avances a nivel europeo en la certificación de ciberseguridad de tecnologías 5G (ver apartado "11. Comunicaciones móviles"), cabe también destacar cómo el Pixel 4a, en agosto de 2020, fue el primer dispositivo móvil en obtener la certificación de ioXt en su lanzamiento al mercado[70], junto al Pixel 4/4XL que ya se habían comercializado previamente. La Internet of Secure Things Alliance (ioXt), una organización internacional de la que Google es miembro junto a muchas otras empresas de la industria, dispone de un programa de cumplimiento y certificación para dispositivos del Internet de las Cosas (IoT, Internet of Things), incluyendo dispositivos móviles a través del perfil de certificación de Android, que permite evaluar la postura de seguridad de los dispositivos móviles Android frente a un conjunto de requisitos base.

Complementariamente, y teniendo presente el principio de seguridad por defecto (Security by Default)[71], Google llevó a cabo un análisis junto a expertos académicos para disponer de una fórmula que permite evaluar el nivel de riesgo de un dispositivo móvil Android, en base a todos los elementos pre-cargados existentes en el mismo, incluyendo apps de sistema, permisos de apps pre-instaladas, apps que no hacen uso de tráfico cifrado, etc. Como resultado publicaron en el Android Security Symposium en julio de 2020 el proyecto Android-Device-Security.org (o Android Device Security Database)[72], con una serie de atributos definidos que permiten clasificar el nivel de seguridad de un dispositivo móvil Android en base a ciertas métricas, creando una base de datos para poder comparar los dispositivos entre sí. La herramienta de código abierto Uraniborg permite recopilar estos atributos para obtener una puntuación para un dispositivo móvil objetivo.

En el informe anual de 2019[73] se detallaba cómo Google había publicado a comienzos de 2020 una serie de recomendaciones para la protección avanzada de la cuenta de usuario de Google[74], mediante el Advanced Protection Program. Nueve meses después, en septiembre, Google anunciaba protecciones adicionales frente al malware para los usuarios que se estaban beneficiando de este programa[75]. Las nuevas mejoras están asociadas al navegador web Chrome, y al proceso de escaneo de descargas, y permiten al usuario remitir ficheros sospechosos al sistema de análisis de Google Safe Browsing antes de abrirlos, complementando las protecciones frente a phishing ya existentes.

---

**60.** "Privacy". Apple. URL: https://www.apple.com/privacy/ URL: https://www.apple.com/legal/privacy/en-ww/
**70, 71.** "Pixel 4a is the first device to go through ioXt at launch". Google Security Blog. Aug 2020. URL: https://security.googleblog.com/2020/08/pixel-4a-is-first-device-to-go-through.html
**72.** "Android Device Security Database". Various. URL: https://www.android-device-security.org - URL: https://www.youtube.com/watch?v=zxkbyyl-9b8&t=865s - URL: https://github.com/android/security-certification-resources/tree/master/ioXt/uraniborg
**73.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html
**74.** "Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android ". CCN-STIC 456. CCN-CERT. Sep 2018. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3043-ccn-stic-456-cuenta-de-usuario-servicios-aplicaciones-google-para-dispositivos-moviles-android.html - URL: https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/7018-dos-nuevas-guias-de-seguridad-sobre-dispositivos-moviles-android-y-su-cuenta-de-usuarios-de-google.html
**75.** "Improved malware protection for users in the Advanced Protection Program". Google Security Blog. Sep 2020. URL: https://security.googleblog.com/2020/09/improved-malware-protection-for-users.html

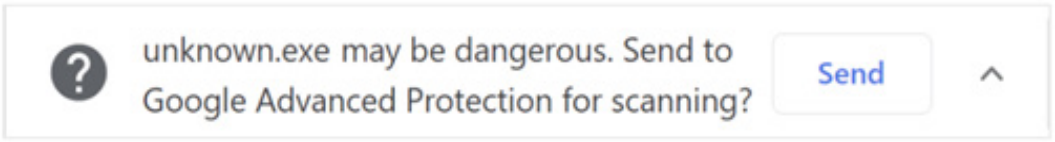



Figura 14

En octubre de 2020, Google anunció el lanzamiento de un nuevo programa o iniciativa para la gestión de vulnerabilidades de seguridad que afectan específicamente a los fabricantes (u OEMs) de dispositivos móviles Android, denominado APVI: Android Partner Vulnerability Initiative[76]. Esta iniciativa permite la notificación responsable, y la posterior difusión, de vulnerabilidades de seguridad asociadas a componentes propietarios y código propio de los fabricantes, complementando los programas de gestión de vulnerabilidades en el sistema operativo Android, Android Security Rewards Program (ASR), o en las apps móviles de terceros a través del Google Play Security Rewards Program (GPSRP), que ya fue ampliado en 2019 (ver el informe asociado[77]).

A través de ASR, y de los boletines de seguridad oficiales publicados mensualmente, Android Security Bulletins (ASB), Google gestiona todas las vulnerabilidades de Android vinculadas a su código fuente en el AOSP (Android Open Source Project), que afectan normalmente a todos los dispositivos móviles que ejecutan Android. Sin embargo, hasta ahora, no se disponía de mecanismos para gestionar vulnerabilidades que solo afectan a un subconjunto de dispositivo móviles, debido a que están ocasionadas por componentes muy específicos de ciertos fabricantes, y por código que no mantiene o distribuye Google propiamente.

APVI, por tanto, añade una capa de seguridad adicional, que ya ha permitido solventar algunas vulnerabilidades como, por ejemplo, una que permitía disponer de permisos a través de un servicio de sistema pre-instalado de una solución de actualizaciones OTA (Over-the-Air). Los fabricantes afectados proporcionaban dicho acceso a través de una contraseña fijada en el código fuente del servicio, y se permitía la instalación o desinstalación silenciosa de apps, habilitar o deshabilitar permisos en las apps, etc.

En otros casos se ha identificado un navegador web pre-instalado, con capacidades de gestor de contraseñas, que estaban expuestas a las WebViews vía JavaScript en cualquier página web, permitiendo a cualquier sitio web malicioso acceder a todo el repositorio de contraseñas del usuario, que estaban cifradas con DES (un algoritmo obsoleto) y con una clave fija disponible, de nuevo, en el código de la app. Las vulnerabilidades asociadas a APVI serán publicadas a través de la siguiente URL, existiendo ya más de una docena sólo dentro del año 2020, y con varios fabricantes afectados: **https://bugs.chromium.org/p/apvi/**.

**76.** "Announcing the launch of the Android Partner Vulnerability Initiative". Google Security Blog. Oct 2020. URL: https://security.googleblog.com/2020/10/announcing-launch-of-android-partner.html
**77.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html

Las conclusiones del informe del pasado año 2019[78] planteaban la posible evolución futura de los dispositivos móviles para ser empleados como identificador electrónico (ID) oficial, como el carnet de conducir. En USA, este carnet no sólo permite conducir un vehículo, sino que también es empleado como identificador personal en otros ámbitos, al no disponerse de un identificador nacional oficial como el DNI o NIF en España. En octubre de 2020, Google describía las mejoras de privacidad introducidas por el estándar ISO 18013-5, "Mobile driving licence (mDL) application" (que a fecha de elaboración del presente informe aún no ha sido ratificado y se encuentra en desarrollo).

El objetivo es disponer de apps móviles mDL que el usuario pueda tener instaladas en su dispositivo móvil sin necesidad de disponer del carnet físico, y que puede emplear para identificarse oficialmente.

Como se indicaba el pasado año, esta iniciativa requiere de su estandarización por parte de organismos internacionales como ISO, de ahí la referencia ISO 18013-5 previa, empleando capacidades criptográficas avanzadas que preserven la privacidad, mecanismos conocidos en inglés como "privacy-preserving".

Estos mecanismos también fueron introducidos en Android 11 en el año 2020 en el teclado GBoard, para predecir lo que quiere escribir el usuario tratando de no exponer su privacidad[79], e independizando el procesamiento de datos sensibles entre la plataforma Android y GBoard.

Este ejemplo del carnet de conducir o mDL, que sin duda abre la puerta a nuevos ámbitos de aplicación y uso futuro de los dispositivos y apps móviles, requiere de una integración estrecha entre Android como plataforma y las apps mDL (u otro tipo de apps de identificación futuras, como carnets de biblioteca, tarjetas de fidelización, pasaportes, etc.).

Android 11 introdujo nuevas capacidades en esta dirección, como la API Identity Credential HAL, con un interfaz o capa de abstracción hardware (HAL) para implementar el soporte de credenciales e identidad en elementos hardware seguros. Estas capacidades podrán potencialmente emplearse en el futuro para identificar a los usuarios a través de los mecanismos de autentificación biométrica del dispositivo móvil, y no mediante la coincidencia de entre la foto y el usuario que la presenta (un área en el que se está trabajando).


Figura 15

**78.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html

**79.** https://security.googleblog.com/2020/10/privacy-preserving-smart-input-with.html

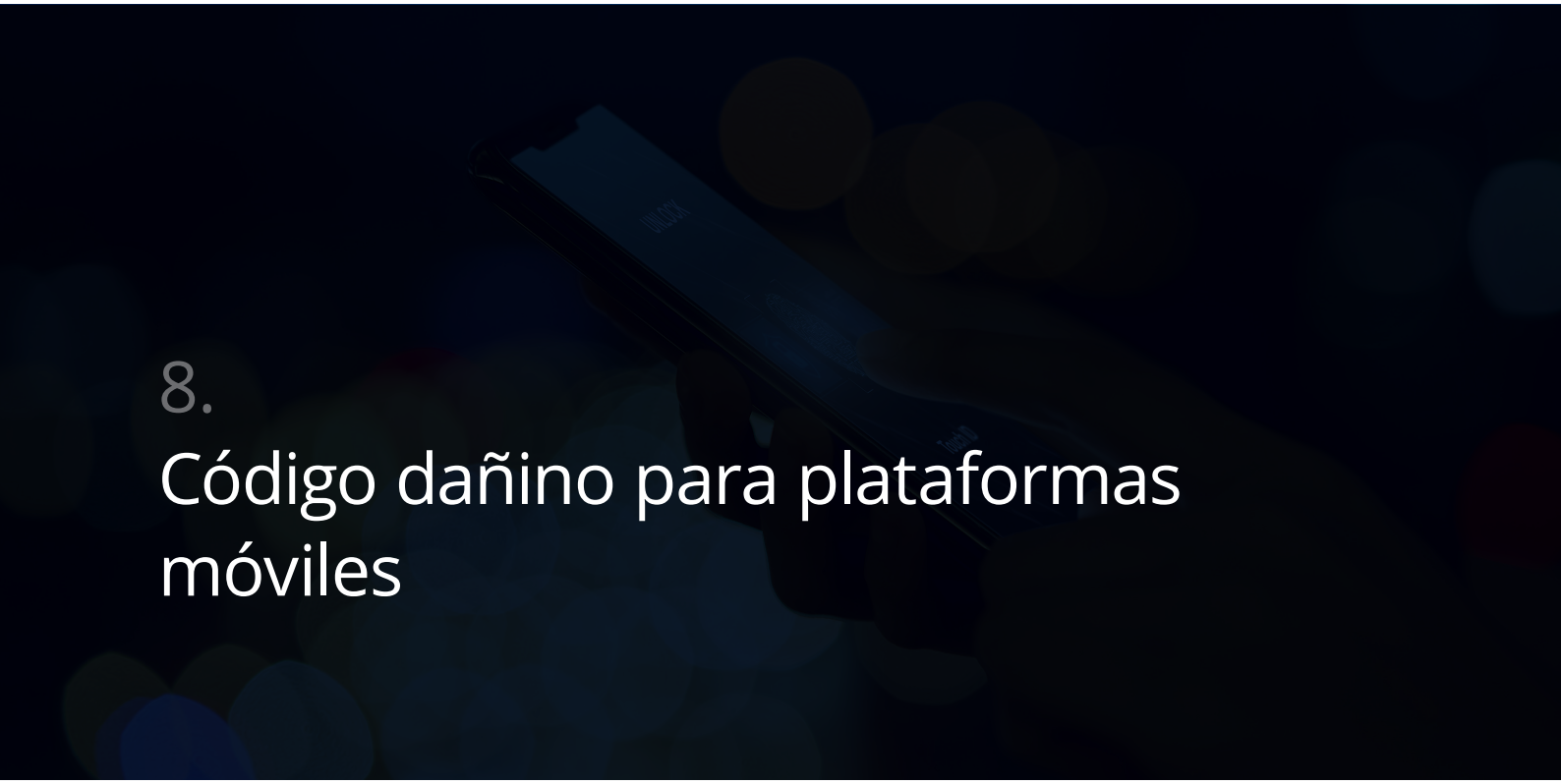
Por otro lado, estas capacidades de identificación podrían estar disponibles (en nuevos dispositivos móviles) vía NFC incluso cuando el dispositivo móvil no tiene batería suficiente ni para arrancar.

El proceso de verificación del carnet de conducir digital o mDL se basaría en el siguiente proceso, en el que el usuario abre la app asociada, y la persona que debe verificar su identidad, a su vez, abre otra app de lectura de mDLs. Mediante el escaneo de un código QR o la lectura de una etiqueta NFC, el lector puede obtener una clave pública criptográfica efímera de la app mDL, es decir, de uso temporal, y una dirección hardware a la que conectarse.

El lector de mDL genera su propio par de claves efímeras y establece una conexión cifrada y autentificada, a través de un canal inalámbrico seguro punto a punto (ya sea vía BLE, Wi-Fi Aware o NFC) con la dirección proporcionada previamente por el usuario.

A través de dicho canal, el lector puede obtener los datos del usuario, como la foto o la categoría del carnet de conducir, que indica los tipos de vehículos que puede conducir el usuario. Estas capacidades podrían ser empleadas incluso para obtener detalles a preguntas más abstractas, como si el usuario es mayor de edad, es decir, si tiene más de 18 años. Estas capacidades permiten hacer un uso más granular y selectivo de qué información se desvela al lector.

El modelo puede incorporar mecanismos de autorización adicionales, que consulten al usuario qué datos quiere desvelar al lector, e incluso autentificar al usuario a través de su dispositivo móvil, mediante biometría o el código de acceso, para confirmar que es realmente el usuario legítimo el que proporciona dicha autorización.



# 8. Código dañino para plataformas móviles

El software malicioso para dispositivos móviles, o malware móvil, evoluciona como en años anteriores para adecuarse a las nuevas restricciones impuestas por las nuevas versiones de los sistemas operativos de las plataformas móviles iOS y Android, identificándose nuevos especímenes y muestras a lo largo de cada año, tanto de malware como de spyware o ransomware, aumentando su complejidad y sofisticación.

Como en informes de años previos, los ejemplos y referencias detallados a continuación sólo constituyen una reducida muestra del amplio abanico de especímenes que son descubiertos cada año en campañas y operaciones activas para infectar a los usuarios. Los dispositivos móviles siguen siendo uno de los objetivos del malware, identificándose campañas específicas tanto para Android como para iOS.

La principal novedad respecto a años previos reside en que parece que se consolidan los estudios de inteligencia y de análisis de la industria, por lo que se dispone de numerosos informes con datos relativos al malware móvil del pasado año, provenientes de múltiples fuentes y empresas de ciberseguridad, cada uno de ellos con sus propios datos y estadísticas. Muchos de estos informes no están públicamente disponibles, siendo necesario registrarse para obtenerlos. A continuación, se reflejan algunos casos más concretos acontecidos en 2020, y varios resúmenes asociados a estos informes. De cara a limitar la extensión del presente informe, se insta al lector a profundizar en ellos, compararlos, e identificar discrepancias entre las distintas visiones obtenidas por parte de los diferentes actores de la industria de ciberseguridad móvil.

Como ocurría el pasado año, a finales de abril de 2021, etapa final de elaboración del presente informe, Google no había publicado el informe anual de seguridad del ecosistema Android para 2020, pero tampoco había publicado el correspondiente al año 2019, interrumpiéndose así la publicación de este informe durante los 5 años previos (2014-2018), siendo el último publicado por Google el del año 2018, "Android Security & Privacy 2018 Year in Review"[80].

Alternativamente, Google sí publicaba recientemente cómo ha librado la lucha frente a los desarrolladores de apps maliciosas a lo largo del año 2020[81], detallando cómo Google Play Protect escaneó más de 100 billones de apps instaladas cada día, a lo largo de billones de dispositivos móviles de sus usuarios. Debido a la pandemia sanitaria, Google introdujo requisitos específicos en Google Play para las apps asociadas a la COVID-19 (el apartado "10. Comunicaciones inalámbricas y apps de la COVID-19" analiza en detalle las apps oficiales de la COVID-19), como el respaldo oficial de las autoridades sanitarias de un país, o el asegurar que se siguen muy altos estándares respecto a la protección de privacidad de los datos del usuario.

Con el objetivo de evitar las noticias falsas y la desinformación, Google instauró una nueva política para las apps de publicación de noticias (clasificadas dentro de la categoría "News"), promoviendo la transparencia y la identificación de los desarrolladores detrás de estas apps. Aunque las apps móviles no son empleadas aún en la actualidad para votar directamente, si proporcionan información a los votantes en relación a los candidatos, permiten registrarse para votar (dependiendo del país) o encontrar los lugares en los que ejercer el voto, proporcionando soporte para algunas actividades complementarias durante las elecciones[82].

No sólo Google afirma que su infraestructura de detección basada en Machine Learning evitó la publicación de casi un millón de apps que violaban las políticas de publicación de Google Play, sino que permitió bloquear más de cien mil cuentas vinculadas a desarrolladores maliciosos[83].

**80.** "Android AOSP Security Reports". Android. Apr 2021. URL: https://source.android.com/security/overview/reports
**80, 83.** "How we fought bad apps and developers in 2020". Google Security Blog. Apr 2021. URL: https://security.googleblog.com/2021/04/how-we-fought-bad-apps-and-developers.html
**82.** https://blog.google/outreach-initiatives/civics/google-play-helping-safeguard-elections/

Uno de los objetivos de Android es reducir el acceso y abuso por parte de los desarrolladores de apps a datos sensibles del usuario, motivo por el que en febrero de 2020 se anunció una nueva política que gobernase la obtención de información de geolocalización cuando una app está ejecutando de fondo (no está en primer plano), asegurándose de que este permiso es solicitado por apps que realmente lo requieren[84] (en caso contrario la app podría ser eliminada de Google Play). En Android 10 ya se introdujo este permiso, y en Android 11 se añadió la capacidad para que el usuario sólo permita el acceso a los servicios de ubicación a una app en una única ocasión, muy puntualmente. Con el objetivo de proteger a los más jóvenes, Google introdujo también una nueva clasificación para las apps de Android en Google Play denominada "Teacher approved", que permite confirmar que una app ha sido validada por expertos académicos, al identificarse como valiosa para el aprendizaje y la educación.

En agosto de 2020 Snyk, conocidos por sus análisis de dependencias en software, descubrieron comportamientos maliciosos en un kit de desarrollo, librería o SDK de anuncios, denominado Mintegral SDK (un proveedor chino), y utilizado por más de 1.200 apps de iOS publicadas en la App Store, con más de 200 millones de descargas al mes en global.

Estos comportamientos maliciosos fueron referenciados como SourMint[85], y permitían espiar a los usuarios registrando las peticiones web realizadas a través de las apps que hacía uso de esta librería de anuncios. La información capturada incluía la URL completa, las cabeceras HTTP, estos dos potencialmente con detalles de autentificación o de la sesión del usuario, en qué lugar de la app se producía la petición, e identificadores del dispositivo. Los datos se remiten a un servidor remoto y podrían incluir información personal y sensible del usuario. El SDK implementa numerosas protecciones anti-análisis intencionadamente (como detecciones de simuladores, root, proxies, etc., herramientas comunes en el proceso de análisis e investigación), para dificultar el descubrimiento de su comportamiento real, modificando su comportamiento malicioso y presentando un comportamiento benigno en caso de estar siendo analizado.

Adicionalmente, el SDK interceptaba las actividades de navegación y clicks o pulsaciones sobre los anuncios, para atribuirlas a su propia infraestructura de anuncios y cobrar por ellas, en lugar de ser reportadas a través de la infraestructura de anuncios legítimamente empleada por el desarrollador, cometiendo fraude. Los mecanismos implementados en el SDK podían ser, a su vez, controlados desde los servidores de Mintegral, activando o desactivando sus capacidades avanzadas a discreción.


**84.** https://android-developers.googleblog.com/2020/02/safer-location-access.html
**85.** "SourMint: malicious code, ad fraud, and data leak in iOS". Snyk. Aug 2020. URL: https://snyk.io/blog/sourmint-malicious-code-ad-fraud-and-data-leak-in-ios/

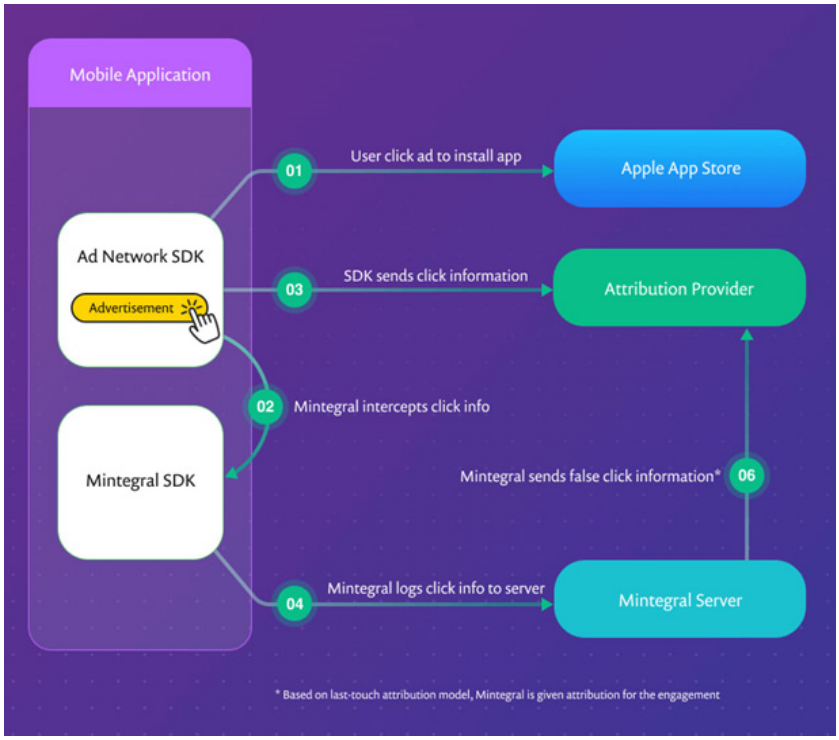



Figura 16

Reiteradamente, en octubre de 2020, se descubrieron nuevas vulnerabilidades en el SDK tanto para iOS como para Android[86], confirmándose la posibilidad de ejecución de código remota vía el SDK, así como capacidades de seguimiento de descargas en la versión de Android del SDK, cuyas actividades como la realización descargas desde dominios de Google, incluyendo APKs, documentos y otros recursos, eran reportadas a Mintegral sin el conocimiento del usuario o desarrollador de la app.

Destaca asimismo uno de los escándalos más relevantes de privacidad acontecidos a lo largo del año 2020, el asociado a la app y servicio TikTok (propiedad del gigante Chino ByteDance), masivamente utilizado por unos 800 millones de usuarios a nivel mundial, y que atentaba directamente contra la privacidad de estos, recopilando cantidades ingentes de información y convirtiéndose en une herramienta de vigilancia masiva digital[87].

Sin duda, el año 2020 ha sido el año de TikTok, popularizándose aún más con la generalización y uso de servicios digitales durante la pandemia. Anteriormente, en julio de 2020, se descubría, gracias a las nuevas capacidades de privacidad de iOS 14 (incluso en su versión beta), cómo la app de TikTok recopilaba detalles de otras apps y del dispositivo móvil a través del portapapeles compartido de iOS, denominado Pasteboard. A esta mala práctica se unía el descubrimiento asociado a la app de Linked-In o de Reddit posteriormente, reflejando una mala práctica de la industria más generalizada de lo que se creía y por parte de proveedores de servicios de referencia. La app de TikTok recopila y almacena información de sus usuarios, incluso de aquellos que no se han registrado y no tienen una cuenta[88].

**86.** "SourMint: iOS remote code execution, Android findings, and community response". Snyk. Oct 2020. URL: https://snyk.io/blog/remote-code-execution-rce-sourmint/
**87.** "TikTok and the privacy perils of China's first international social media platform". Protonmail. July 2020. URL: https://protonmail.com/blog/tiktok-privacy/
**88.** https://www.vice.com/en/article/jgqbmk/tiktok-data-collection

Profundizando en el informe de inteligencia y amenazas de Nokia de 2020[89] destaca la distribución de malware en redes móviles y fijas, con una temática significativa en torno a la COVID-19 (no sólo en el mundo móvil, sino también en Windows), con variantes como CoViper o COVIDLock, enmascaradas como apps legítimas que proporcionan información de la evolución de la pandemia, y con un crecimiento del 30% en los meses de febrero y marzo de 2020, al comienzo de la epidemia.

Este crecimiento en el cibercrimen asociado a la COVID-19, no sólo en el ecosistema móvil, también ha sido confirmado por otros informes, como el de INTERPOL de agosto de 2020[90]. Destaca cómo Android constituye uno de los objetivos más comunes del malware, con casi un 27% de las víctimas entre todas las plataformas tecnológicas (con casi un 2% en el caso de iOS), aunque desciende respecto a 2019 (47%), en comparación con entornos tradicionales como Windows, o entornos IoT.

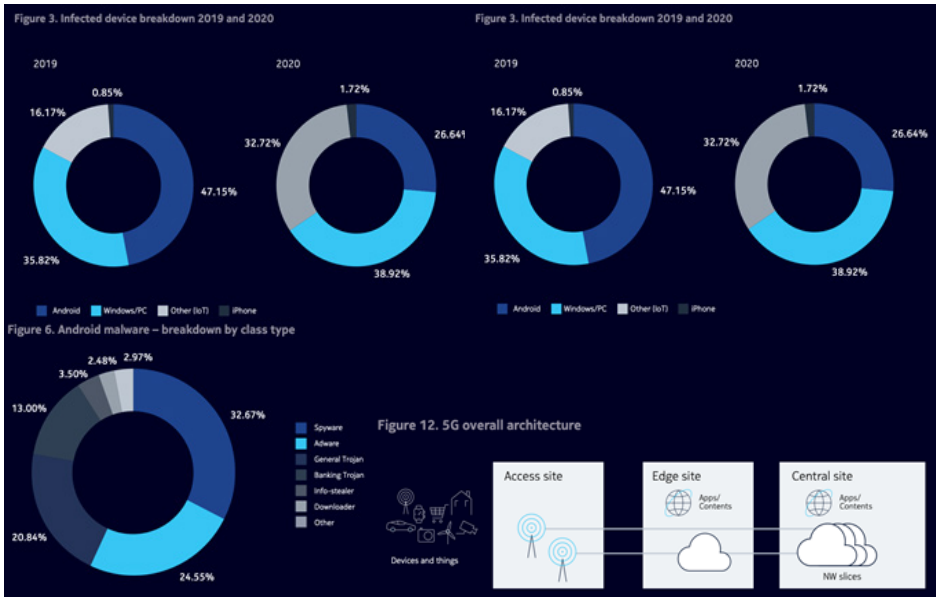
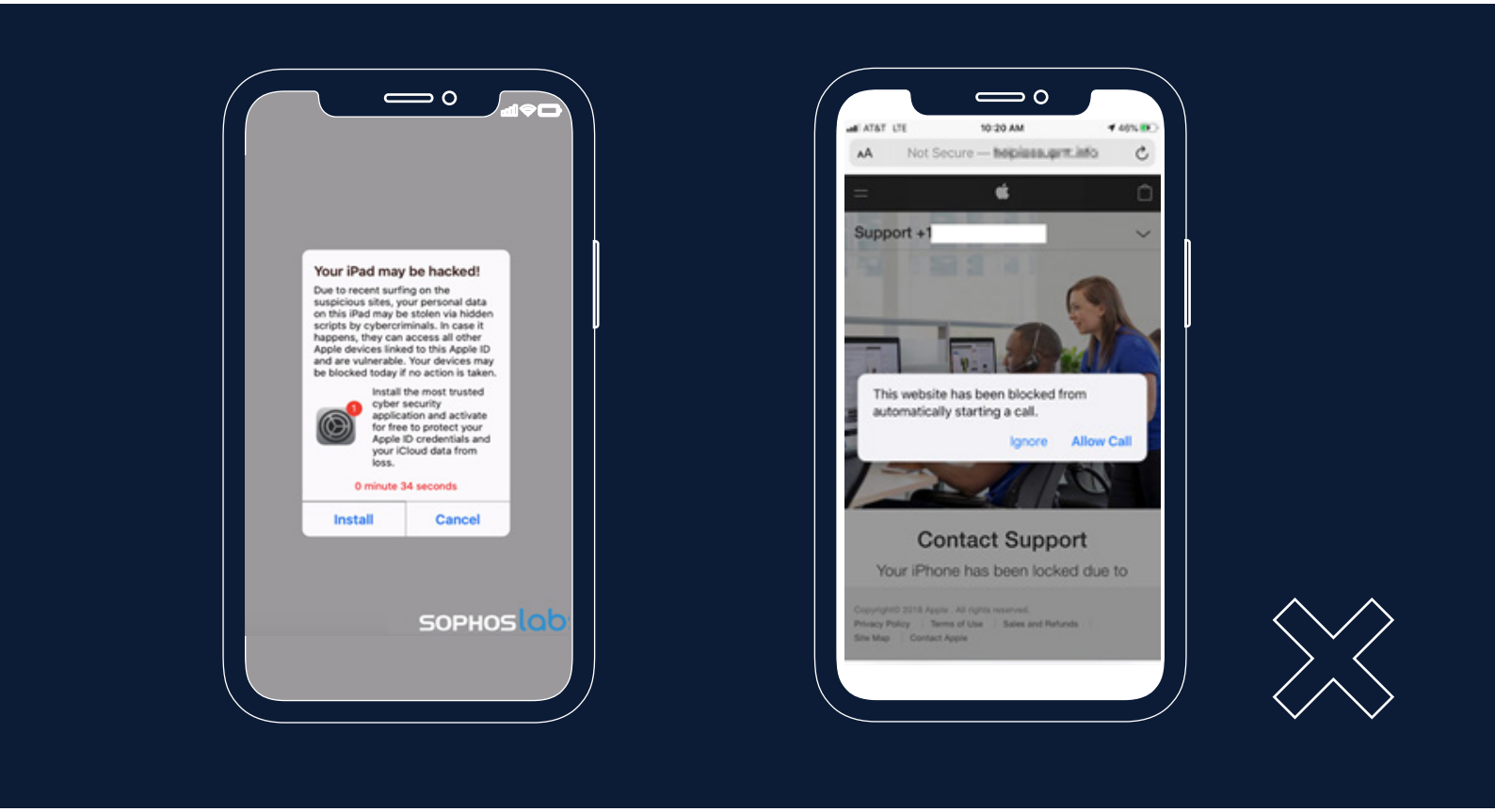



Figura 17

Asociado al malware de Android, donde continúa creciendo el número de muestras, destacan los especímenes centrados en robar información y de spyware, con casi un 36% de las infecciones. El informe igualmente se centra en la necesidad de evolucionar y monitorizar la seguridad de los nuevos entornos de comunicaciones y arquitecturas de las redes 5G.

Basándonos en el informe de amenazas de Sophos de 2021[91], el crecimiento en el volumen del malware Joker para Android, también conocido como Bread, una app de fraude en la facturación y envío de SMS, continúa progresando y evadiendo los mecanismos de detección de Google Play por sus capacidades avanzadas de ofuscación. No parece que esta tendencia vaya a disminuir en 2021. Sophos también destaca la existencia de apps falsas maliciosas de anuncios (denominadas *malvertising*) y de bloqueo de páginas web, ambos tipos generando popups con los que se insta a interactuar al usuario.

**89.** "Nokia Threat Intelligence Report 2020". Nokia. 2020. URL: https://onestore.nokia.com/asset/210088
**90.** https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
**91.** "Sophos 2021 Threat Report". Sophos. Nov 2020. URL: https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf




Los detalles del informe de McAfee de abril de 2021[92], de los dos últimos trimestres de 2020 (Q3 y Q4 2020), reflejan un crecimiento del 118% del malware móvil entre el Q3 y el Q4 (en color marrón claro, tras las gamas verdes), debido a la familia de malware SMSReg.


Figura 18

Otro informe, como el de Kaspersky sobre la evolución del malware móvil en 2020, destaca numerosas variantes de troyanos bancarios y de ransomware móvil, así como el uso de ingeniería social para distribuir una app como si fuera realmente otra legítima, con una alta demanda, como por ejemplo las asociadas a la COVID-19, término empleado por multitud de apps móviles maliciosas en 2020[93] en su nombre, nombre de paquete, interfaz de usuario, descripción, etc., como por ejemplo, el troyano bancario Cebruser, simplemente denominado Coronavirus. Sin embargo, las cifras obtenidas demuestran que la media de ataques sobre los usuarios móviles en 2020 disminuyó ligeramente con respecto a 2019, especialmente en los primeros meses de la pandemia, donde los cibercriminales también se vieron forzados a suspender parte de sus actividades, hasta que se estabilizó la situación global.

---

**92.** "McAfee Labs Threats Report: April 2021". McAfee. Apr 2021. URL: https://www.mcafee.com/enterprise/en-us/lp/threats-reports/apr-2021.html - URL: https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/reports.html
**93.** "Mobile malware evolution 2020". Securelist by Kaspersky. Mar 2021. URL: https://securelist.com/mobile-malware-evolution-2020/101029/

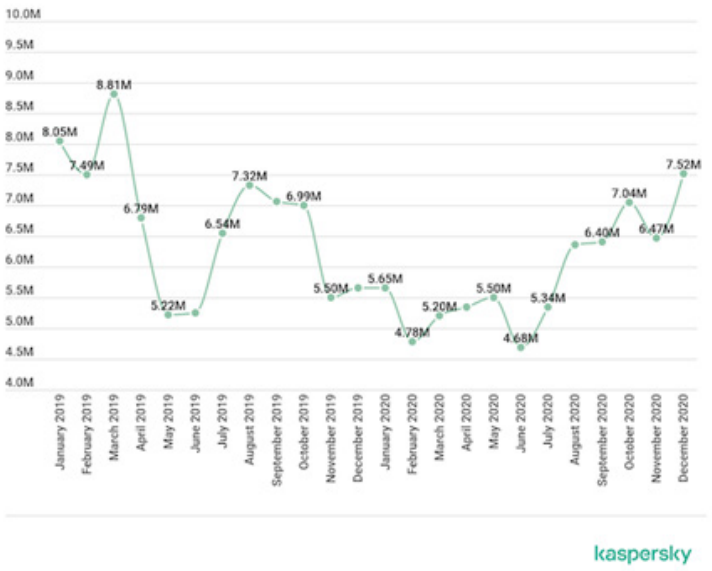



Figura 19

La obtención de los datos y actividades del usuario son el objetivo del malware para Android, donde se mantiene el número de ataques asociados a esquemas de anuncios o adware con respecto a 2019, y aparecen troyanos de sistemas financieros como Ghimob, o de robo de cookies de sesión como Cookiethief[94]. En el caso de iOS, destaca el troyano LightSpy, con un diseño modular. Por otro lado, el *dropper* Hqwar, malware que se centra en la descarga e instalación de otros componentes, habitualmente troyanos bancarios (cuyo número se ha duplicado respecto a 2019), también ha estado muy activo en 2020, ocupando España el tercer puesto en infecciones, con más de 15 mil usuarios atacados, según Kaspersky.

Octubre de 2020 fue el mes de publicación de los detalles de un nuevo ransomware para Android, MalLocker.B, que en lugar de cifrar los ficheros del usuario, se centra en emplear varias técnicas para hacer que el dispositivo móvil no sea usable, y forzar al usuario a pagar el rescate[95], convirtiéndose en una de las variantes más avanzadas vistas hasta la fecha.

Esta es la última variante de una familia de malware en constante evolución, que muestra una notificación al usuario que ocupa la totalidad de la pantalla del dispositivo móvil, imposibilitando la utilización del resto de apps, e informa al usuario acerca de cómo proceder a pagar el rescate. La notificación está habitualmente asociada a una nota de la policía falsa o al descubrimiento de imágenes sexuales con contenido explícito supuestamente encontradas en el dispositivo móvil de la víctima.

Profundizando en este ransomware móvil, descubierto por los investigadores de Microsoft, detallaban que su distribución se lleva a cabo a través de sitios web arbitrarios o foros, empleando técnicas de ingeniería social, haciéndose pasar por apps populares, juegos crackeados y gratuitos, o reproductores de vídeos[96]. La nueva variante evita la mayoría de protecciones existentes y sólo es detectada por un reducido número de soluciones de seguridad.

---

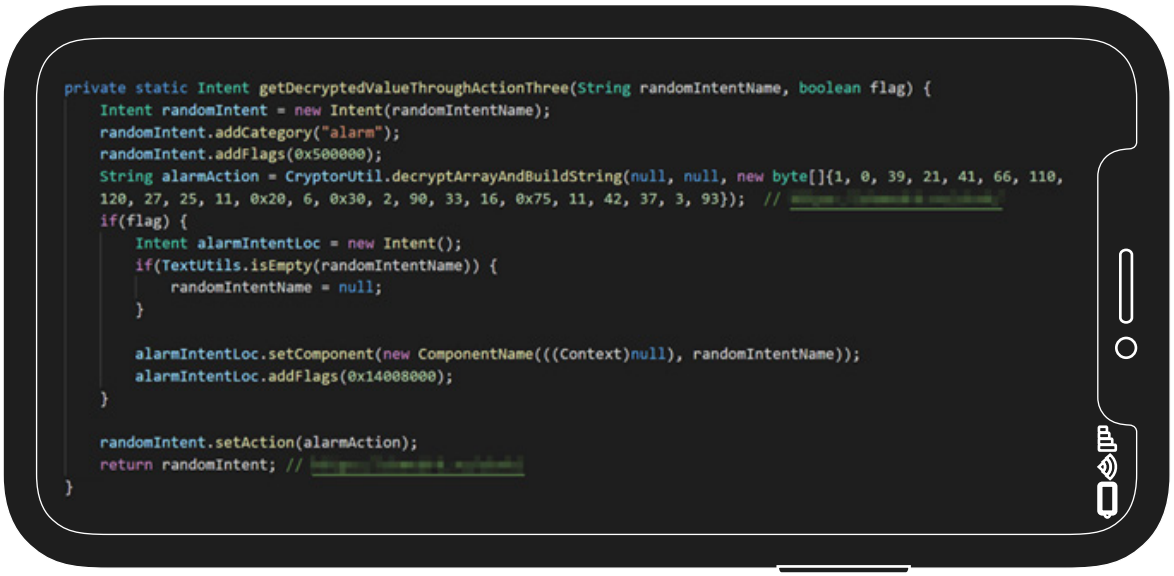
**94.** "Mobile malware evolution 2020". Securelist by Kaspersky. Mar 2021. URL: https://securelist.com/mobile-malware-evolution-2020/101029/

**95.** "What You Need to Know about the MalLocker.B Mobile Ransomware". WASM. Nov 2020. URL: https://wamsinc.com/2020/11/27/what-you-need-to-know-about-the-mallocker-b-mobile-ransomware/

**96.** "Sophisticated new Android malware marks the latest evolution of mobile ransomware". Microsoft. Oct 2020. URL: https://www.microsoft.com/security/blog/2020/10/08/sophisticated-new-android-malware-marks-the-latest-evolution-of-mobile-ransomware/

Dentro de las técnicas de ofuscación empleadas, no parece disponer del código asociado a las clases definidas o declaradas en el fichero *manifest* de Android, disponiendo el fichero DEX de la app de tan sólo dos clases: la utilizada en el arranque de la app, y una clase que hace uso de mecanismos de cifrado y descifrado propietarios. Esta segunda clase se utiliza para acceder al código cifrado de la app disponible en la carpeta "Assets" y referenciado desde el fichero *manifest*.

Dentro del código a descifrar, se incluyen fragmentos falsos para dificultar el análisis. El proceso de descifrado del código que será ejecutado realmente por la app se lleva a cabo a través de *intents* de Android, empleando el parámetro *action* para obtener el contenido descifrado con el código, correspondiente a un fichero ejecutable DEX. La app adicionalmente obtiene del servidor malicioso la configuración correspondiente a la notificación a mostrar, y al rescate para una víctima concreta.



```
private static Intent getDecryptedValueThroughActionThree(String randomIntentName, boolean flag) {
    Intent randomIntent = new Intent(randomIntentName);
    randomIntent.addCategory("alarm");
    randomIntent.addFlags(0x500000);
    String alarmAction = CryptorUtil.decryptArrayAndBuildString(null, null, new byte[]{1, 0, 39, 21, 41, 66, 110,
    120, 27, 25, 11, 0x20, 6, 0x30, 2, 90, 33, 16, 0x75, 11, 42, 37, 3, 93});  //
    if(flag) {
        Intent alarmIntentLoc = new Intent();
        if(TextUtils.isEmpty(randomIntentName)) {
            randomIntentName = null;
        }

        alarmIntentLoc.setComponent(new ComponentName(((Context)null), randomIntentName));
        alarmIntentLoc.addFlags(0x14008000);
    }

    randomIntent.setAction(alarmAction);
    return randomIntent; //
}
```

Figura 20

En versiones pasadas (que comparten fragmentos de su código entre sí) se empleaba la ventana de alerta del sistema (mediante el permiso "SYSTEM_ALERT_WINDOW") para superponer la venta de notificación (una técnica conocida como *ovelay*) pero, una vez Google mitigó este vector de ataque en Android 10 (ya desde Andorid 8 Google tomó medidas para la potencial desactivación de ventanas de alerta de sistema), comenzaron a emplear los servicios de accesibilidad de Android que requieren la aceptación de múltiples permisos de Android por parte del usuario, aunque no son tan efectivos (ver siguiente imagen con las diferentes variantes de esta familia de malware).

Otras familias de ransomware muestran infinidad de ventanas superpuestas, aunque existe la posibilidad de evitar alguna de ellas y desinstalar la app maliciosa desde los ajustes del dispositivo móvil. La última variante, en un ejercicio de innovación no visto previamente, hace uso de un tipo de notificaciones de llamada ("call") en Android, que requiere la atención inmediata del usuario, combinada con una función de callback ("onUserLeaveHint()") de las actividades o pantallas de las apps en Android, que hace que cuando la app o pantalla vaya a pasar a su ejecución en segundo plano, se invoque y tome una acción, mostrando la notificación de rescate en pantalla completa.

Como resultado, se consigue una cadena de eventos continua, mostrando la notificación automáticamente, sin requerir mostrar decenas de pantallas.

Adicionalmente, esta variante incluye un motor de código abierto de Machine Learning (ML), tinyML, para acomodar el contenido de la pantalla de notificación de pago del rescate y, específicamente, ajustar automáticamente las imágenes en función del tamaño de la pantalla del dispositivo móvil. Esto le permite al malware acomodar la ventana de notificación a los diferentes dispositivos móviles víctima, de manera profesional y sin distorsiones. Aunque este motor no está siendo utilizado por las versiones actuales, deja entrever su futura utilización.

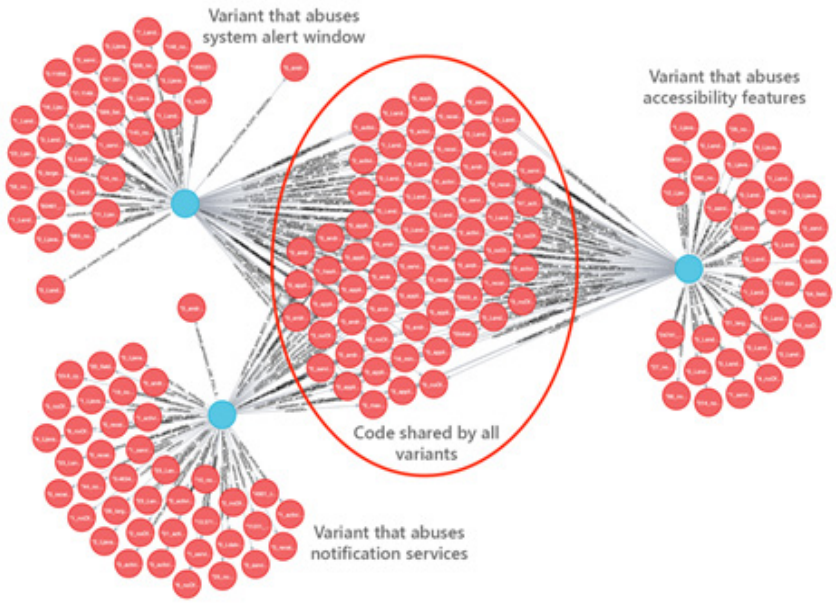



*Figure 4. Knowledge graph of techniques used by ransomware family*

Figura 21

Zimperium publicaba en septiembre de 2020 una línea temporal interactiva resumiendo los incidentes, compromisos de seguridad (*breaches*), filtraciones de información (*leaks*) y vulnerabilidades más relevantes en la industria móvil en lo que se llevaba de año, superando antes del último trimestre lo acontecido en el año previo[97].

**97.** "2020 Mobile App Breaches, Failures, and Data Leaks". Zimperium. Sep 2020. URL: https://blog.zimperium.com/mobile-app-breaches-and-leaks/

El año comenzaba con la vulnerabilidad de mail en iOS descrita en el presente informe, casos de spyware a nivel internacional, filtraciones de la app móvil de Walgreens, un incremento del 50% en el fraude en apps móviles (con respecto a navegadores web móviles) en el primer trimestre de 2020, la exposición de datos de apps de mensajería privadas, como Whisper, campañas de espionaje móvil en Irán de víctimas de la COVID-19, un incidente con la app de la COVID-19 en Corea del Sur, con la app de casinos Clubillion, con la app de pagos BHIM de la India y con la app bancaria Dave.

Posteriormente, con la app de Telegram; diferentes malware para Android como Eventbot, WolfRAT, Wroba, Joker (con múltiples variantes inundando el ecosistema Android en septiembre) y Blackrock, el troyano bancario Cerberus (cuyo código fuente era publicado en septiembre de 2020), el troyano bancario Alien Android o la existencia de malware en apps de la COVID-19 (o de variantes de apps falsas como Aarogya Setu, en la India); el filtrado de datos muy sensibles por parte de más de 4 mil apps de Android que hacían uso de Google Firebase como base de datos en la nube, y de otras apps que hacían uso de buckets S3 de Amazon, destacando errores de seguridad en la integración de apps móviles con servicios en la nube, junto al filtrado de datos de usuarios por otras apps como Wishbone, vulnerabilidades como Standhogg; malas prácticas en los mecanismos de actualización de la app para Android del fabricante chino de drones DJI, evitando Google Play, o la operación policial Encrochat; así como numerosas referencias adicionales a eventos acontecidos a lo largo de 2020. Como se puede ver, el número y la gravedad de los eventos de seguridad y privacidad en el ecosistema móvil aumenta cada año.

Figura 22

Respecto a las vulnerabilidades asociadas a las apps móviles en iOS, en abril de 2020 se publicaba un 0-day que permitía a una app escapar de su sandbox, o espacio de ejecución restringido, e interactuar con otras apps, simplemente mediante la modificación de su fichero XML de derechos o entitlements[98]. Algo tan simple y sencillo que hacía que esta vulnerabilidad, solucionada por Apple en iOS 13.5, pudiera ser utilizada por cualquier app maliciosa para acceder al sandbox de otras apps y, por ejemplo, robar la base de datos de mensajes SMS e iMessage.


Figura 23

Independientemente y como era de esperar, a lo largo del año 2020, se identificaron múltiples apps maliciosas y falsas (el estudio mencionado a continuación hace referencia a 12 apps) de rastreo de contactos para la COVID-19 que se hacían pasar por apps oficiales de COVID-19 con el objetivo de distribuir malware en los dispositivos de las víctimas[99].

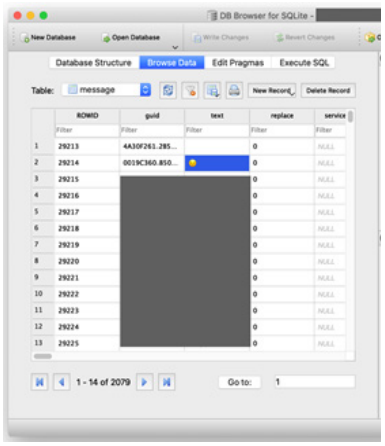



Figura 24

*Table 1 - Malicious Applications*

| Government Tracing App | Official Package Name | Malicious Package Name | Detection Name |
|---|---|---|---|
| Armenia | am.gov.covid19 | am.ac19.health | *Trojan |
| Arrogyasetu (India) | nic.goi.aarogyasetu | com.android.tester | Spynote |
| Brazil | br.gov.datasus.guardioes | wocwvy.czyxoxmbauu.slsa | Anubis |
| Chhattisgarh | com.mobcoder.govcth | cmf0.c3b5bm90zq.patch | *Trojan |
| Columbia | co.gov.ins.guardianes | qmkeasedjeumxmgb.czmofiuouafiuwt.mwonw.eeepqsunrbflk | *Trojan |
| Indonesia | com.telkom.tracencare | cmf0.c3b5bm90zq.patch | Spynote |
| Iran | ir.covidapp.android | co.health.covid | *Trojan |
| Italy (impersonating INPS) | certificati.farma.droid | ynhsumknjtd.hphsefyntauykl.hauqklysedjjnukso | *Trojan |
| Kyrgyzstan | kg.cdt.stopcovid19 | kg.cdt.stopcovid19 | *Adware |
| Russia - EMERCOM | com.minsvyaz.gosuslugi.stopcorona | anubis.bot.myapplication | Anubis |
| Singapore | sg.gov.tech.bluetrace | iiyyxasgfmaeph.jyefwosxdajh.ubempzgulrqdkcmjaplqrxeq | *Trojan |
| Singapore | sg.gov.tech.bluetrace | zfhxmtepnxyljw.wqnszljeb.bkolzgalth | *Trojan |

*Unnamed or generic malware

Figura 25

Particularizando, dentro de las apps identificadas se encontraban múltiples familias de malware, como troyanos bancarios, Anubis y SpyNote, con capacidades de espionaje, robo de credenciales bancarias e información personal. Las víctimas de estas apps eran ciudadanos de múltiples países, al imitarse las apps de la COVID-19 oficiales (ninguna de ellas centrada en la app de España; ver siguiente imagen), y la posible confianza de los usuarios en estas apps. Las apps maliciosas no correspondían a una campaña coordinada, sino a diferentes incidentes centrados en un tema común que facilite la distribución de las mismas por parte de potenciales víctimas.

**98.** "Psychic Paper". Siguza. May 2020. URL: https://siguza.github.io/psychicpaper/ URL: https://twitter.com/s1guza/status/1255641164885131268 URL: https://wojciechregula.blog/post/stealing-your-sms-messages-with-ios-0day/

**99.** "Anomali Threat Research Identifies Fake COVID-19 Contact Tracing Apps Used to Download Malware that Monitors Devices, Steals Personal Data". Anomali (ATR). Jun 2020. URL: https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data


9.

# Seguridad y privacidad del usuario en las plataformas móviles

Continuando con la tendencia de años previos, las innumerables capacidades disponibles en las plataformas móviles y en los servicios ampliamente utilizados por los usuarios abren la puerta a la posibilidad de monitorizar las actividades de estos, y a la recopilación masiva de datos personales, vulnerando su privacidad.

A lo largo del año 2020 y comienzos de 2021 se han producido nuevos escándalos e incidentes de seguridad, desvelados públicamente, que han afectado severamente a la privacidad de los usuarios.

Desde el punto de vista de seguridad, uno de los casos más relevantes del pasado año, que tuvo un muy alto impacto en el mes de abril de 2020, fueron las vulnerabilidades 0-day críticas publicadas por ZecOps el día 20, y que afectaban a la app por defecto nativa de Mail disponible en dispositivos móviles iOS y iPadOS de Apple[100]. Estas se acuñaron como "MailDemon". Las mismas permitían a un potencial atacante enviar un e-mail malicioso a un usuario víctima y como resultado, consumir una cantidad significativa de memoria, y obtener capacidades de ejecución de código remoto en el dispositivo móvil. Si estas capacidades se combinaban con una vulnerabilidad de kernel para llevar a cabo una escalada de privilegios, podía ser posible tomar control completo del dispositivo víctima.

Se evaluó que la explotación de esta vulnerabilidad podría haberse estado llevando a cabo de manera silenciosa desde el año 2018 (posteriormente se encontraron evidencias desde octubre de 2010), con todas las implicaciones asociadas y de desconocimiento por parte de las víctimas, y/o pudiéndose desinstalar temporalmente la app de Mail vulnerable.

Para su explotación no era necesaria la intervención del usuario, en el caso de iOS 13 (versión más reciente de iOS en aquel momento; en el caso de iOS 12, el usuario simplemente tenía que abrir el e-mail recibido), y su ejecución podía pasar inadvertida. Debido a que la app de Mail puede realizar la comprobación de si hay nuevos e-mails disponibles en la cuenta del usuario automáticamente, no era suficiente con no hacer uso de la app, siendo necesario desactivar las cuentas de e-mail del usuario en el dispositivo móvil.

**100.** "You've Got (0-click) Mail!". ZecOps. Apr 2020. URL: https://blog.zecops.com/research/youve-got-0-click-mail/ URL: https://blog.zecops.com/research/seeing-maildemons-technique-triggers-and-a-bounty/

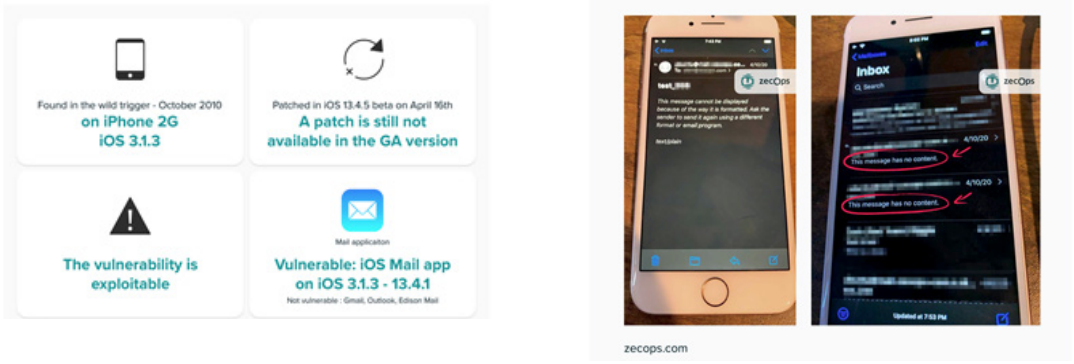



Figura 26

Todas las versiones de iOS, desde la versión 6 (del año 2015, posteriormente se confirmó que iOS 3.1.3 también era vulnerable) hasta las últimas versiones de iOS 13 (13.4.1) estaban afectadas. Debido al amplio uso de este tipo de dispositivos móviles por parte de numerosos usuarios y a la utilización de la app nativa de Mail para gestionar el correo electrónico por muchos de ellos (independientemente de la infraestructura de e-mail empleada: MS Exchange, Office 365, Gmail, etc.), fue necesaria la publicación de avisos urgentes y de recomendaciones para mitigar la misma, mientras Apple publicaba una solución a través de una actualización del sistema operativo, como los avisos y posterior "Abstract" publicados por el CCN-CERT en abril de 2020[101]. Este tipo de vulnerabilidad resaltó la importancia de contar con apps alternativas, en este caso clientes de e-mail, que permitiesen a los usuarios seguir disponiendo de acceso al servicio de correo electrónico sin estar expuestos. No fue hasta un mes después, el 20 de mayo de 2020, que Apple no publicó la versión 13.5 de iOS que resolvía finalmente estas vulnerabilidades, identificadas con las CVEs CVE-2020-9818 y CVE-2020-9819.

Recientemente, en abril de 2021 saltaba a la opinión pública un nuevo escándalo asociado a un incidente de seguridad que afectaba a Facebook, datado en el año 2019, filtrándose en foros online[102] los datos de 533 millones de usuarios de todo el mundo (106/107 países)[103] (incidente identificado con el hashtag #FacebookLeak). Concretamente, casi 11 millones de estos usuarios estaban asociados a España, y la información filtrada incluía numerosos datos personales (dependiendo del caso, números de teléfono, identificadores de Facebook, fecha de creación de la cuenta, nombre completo, fecha de cumpleaños, ubicación, estado civil, biografía, direcciones de e-mail, sólo 2.5 millones de usuarios para este último dato), incluso de personalidades públicamente conocidas, como el número de teléfono del propio Mark Zuckerberg, CEO de la compañía[104].

**101.** "CCN-CERT AV 40/20 Análisis de la vulnerabilidad en iOS Mail. Recomendaciones y buenas prácticas". CCN-CERT. Abr 2020. URL: https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/10007-ccn-cert-av-34-20-vulnerabilidades-zero-day-en-ios-2.html URL: https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/10049-ccn-cert-av-40-20-analisis-de-la-vulnerabilidad-en-ios-mail-recomendaciones-y-buenas-practicas.html URL: https://www.ccn-cert.cni.es/informes/abstracts/4892-analisis-de-la-vulnerabilidad-en-ios-mail-recomendaciones-y-buenas-practicas/file.html
**102.** https://twitter.com/UnderTheBreach/status/1378314424239460352
**103.** "533 million Facebook users' phone numbers and personal data have been leaked online". Business Insider. April 3 2021. URL: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4
**104.** https://nypost.com/2021/04/03/mark-zuckerbergs-cellphone-number-goes-online-after-facebook-hack/

Con anterioridad, en enero de 2021, ya se publicitó y comercializó desde dichos foros un bot de Telegram que proporcionaba los números de teléfono de millones de usuarios, mediante créditos (pagados en dólares), empleando esta base de datos[105]. El bot permitía obtener el número de teléfono en base al identificador de usuario de Facebook, incluso para usuarios que mantienen este dato como privado en el servicio, o viceversa.

La vulnerabilidad, solucionada en 2019, permitió recorrer y enumerar de manera automatizada la información accesible en el perfil de los usuarios (con técnicas conocidas como *scrapping*) mediante la funcionalidad de importación de contactos de Facebook, que facilitaba a los usuarios encontrar a sus amigos para conectar en el servicio mediante su lista de contactos.

Los atacantes emplearon estas capacidades para remitir listas de números de teléfono de gran tamaño, y obtener los datos asociados de los usuarios en el servicio.

Aunque este incidente desde un punto de vista técnico fue posible debido a esta vulnerabilidad, su relación y principal impacto con los dispositivos móviles (objeto del presente informe) radica específicamente en la filtración de los números de teléfono móvil de los usuarios, con las implicaciones de seguridad asociadas. Teniendo en cuenta la relevancia del número de teléfono móvil en numerosos mecanismos de seguridad, empleados como segundo factor de autentificación (2FA), disponer de la asociación entre el número de teléfono y otros datos personales de un usuario puede ser empleado por parte de potenciales intrusos para llevar a cabo ataques de ingeniería social, de suplantación, o de fraude.

Asimismo, es importante tener en cuenta que, aunque los datos obtenidos no son completamente actuales, en la mayoría de los casos siguen siendo válidos, ya que los usuarios no cambian frecuentemente de número de teléfono móvil por todas las implicaciones que este cambio tiene asociadas, tanto desde el punto de vista funcional como de seguridad.

**105.** "Bot Lets Hackers Easily Look Up Facebook Users' Phone Numbers". Motherboard. Jan 2021. URL: https://www.vice.com/en/article/xgz7bd/facebook-phone-numbers-bot-telegram

En otros incidentes de seguridad similares, la recomendación principal a las víctimas es que modifiquen su contraseña, acción que sólo requiere de unos minutos para ser completada. El cambio de número de teléfono tiene muchas más implicaciones. Tras una filtración como esta, numerosos usuarios se verán potencialmente forzados a cambiar de número de móvil, hecho que de nuevo puede ser usado como ventaja por parte de potenciales atacantes, anticipándose a dicho proceso de cambio forzado.

Este incidente es una buena oportunidad para reflexionar sobre posibles incidentes de seguridad futuros que también expongan el número de teléfono de las víctimas, y sobre las acciones que deberían llevarse a cabo para mitigar y reducir el impacto asociado. Por ejemplo, puede ser más conveniente hacer uso de mecanismos de segundo factor de autentificación (2FA) que no requieran de la identificación personal del usuario, como TOTP, basado en una semilla aleatoria, haciendo uso de una app de autentificación en el dispositivo móvil, en lugar de empleando el número de teléfono y mensajes SMS, mecanismo que por otro lado es más inseguro, como ya se detalló en los ataques de intercambio o secuestro de SIM, o SIM *swapping*, del informe anual de 2019[106].

Debe tenerse en cuenta que la información de todos esos millones de usuarios fue obtenida hace 2 años, tiempo durante el cual estos ataques han podido tener lugar sin el conocimiento de la filtración por parte de las víctimas, ya que Facebook no desveló detalles públicamente de este volcado, pese a haber detectado la vulnerabilidad, su uso abusivo, y haberla resuelto en agosto de 2019[107]. Como resultado, la compañía está siendo investigada a nivel europeo en relación con el RGPD y las posibles sanciones millonarias asociadas, y todas las implicaciones legales están siendo evaluadas, y que han llevado, por ejemplo, a cerrar servicios asociados en Italia que permitían a los usuarios confirmar si habían sido afectados por el incidente, sin disponer del volcado completo filtrado, como "https://haveibeenfacebooked.com" (similar al servicio Have I Been Pwned, que ya ha incorporado esta base de datos en relación a los e-mails[108]).

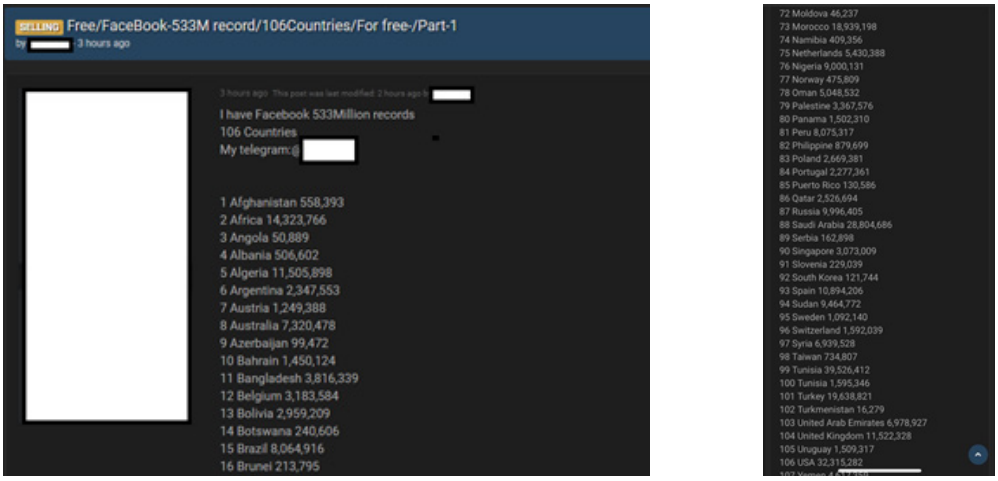



Figura 27

**106.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html

**107.** "The Facts on News Reports About Facebook Data". Facebook. Apr 2021. URL: https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/amp/

**108.** https://haveibeenpwned.com/PwnedWebsites#Facebook

Figura 28

Tan sólo unos días después en la misma semana del mes de abril de 2021, de otra filtración que también afecta a los datos personales de más de 500 millones de usuarios de Linked-In, aunque en este caso las bases de datos filtradas no se han distribuido públicamente en foros online[109]. Para ratificar la existencia de la filtración, los atacantes publicaron 2 millones de registros públicamente, manejándose para la venta cifras de más de 4 dígitos. Las técnicas empleadas para obtener los datos han sido las mismas que en el caso de Facebook (*scrapping*), tal como confirmaba brevemente la propia compañía.

Dentro de los datos filtrados se incluyen el nombre completo, los identificadores de usuario y de perfil en el servicio, direcciones de e-mail, enlaces de perfil en otras redes sociales, género, información del lugar de trabajo, y, de nuevo, los números de teléfono de las víctimas. Pese a que estos incidentes no incluyen datos bancarios, de tarjetas de crédito o de pago, ni de las contraseñas de las víctimas (dos de los elementos considerados más críticos en este tipo de filtraciones), aun así, es fácil identificar el alto impacto de la información filtrada.

Posteriormente, otro actor publicaba en los foros online otra filtración que añadía 327 millones de potenciales registros a los 500 millones previos[110]. Pese a que todavía no se dispone de todos los detalles asociados a este incidente para poder evaluar minuciosamente su impacto, ya se dispone de herramientas online[110] (Personal Data Leak Check) para comprobar si los usuarios están entre las víctimas afectadas de ese primer conjunto de datos publicado, con casi 800 mil direcciones de e-mail vinculadas a Linked-In[112].

Dentro de los incidentes asociados a la revelación de información personal técnica de los usuarios, como números de teléfono o registros de actividad de sus comunicaciones, en ocasiones referida como "customer proprietary network information (CPNI)" por los operadores de telecomunicaciones, T-Mobile sufrió dos incidentes, a finales de 2020 y en marzo de 2020 (con un mayor impacto), al igual que Sprint (compañía asociada) en mayo y julio de 2020[113].

---

**109, 110.** "Scraped data of 500 million LinkedIn users being sold online, 2 million records leaked as proof". Cybernews. Apr 6 2021. URL: https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2/

**111.** https://cybernews.com/personal-data-leak-check/

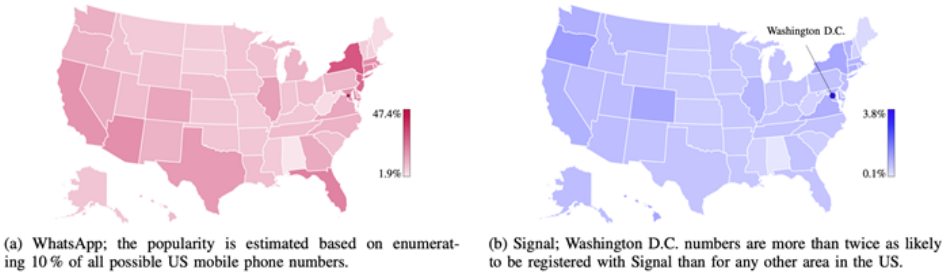
**112.** "An update on report of scraped data". Linked-In. Apr 2021. URL: https://news.linkedin.com/2021/april/an-update-from-linkedin

**113.** "Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE". USENIX 29th. Aug 2020. URL: https://www.usenix.org/conference/usenixsecurity20/presentation/rupprecht - URL: www.revolte-attack.net

Este ejemplo demuestra cómo los operadores de telefonía son uno de los principales objetivos, debido a los millones de suscriptores que tienen vinculados.

Parece por tanto que las filtraciones, incidentes de seguridad y ataques de enumeración asociados a la información de perfil de los usuarios y de sus contactos en múltiples servicios o aplicaciones está copando la actualidad de las noticias de la industria de ciberseguridad durante los primeros meses del año 2021, aunque algunos ataques se materializasen años o meses antes.

Esta afirmación se corrobora con la publicación de un nuevo estudio publicado en el NDSS Symposium en febrero de 2021, que demuestra cómo es posible aprovechar la funcionalidad para el descubrimiento de contactos existente en las aplicaciones y servicios de mensajería instantánea, permitiendo vulnerar su privacidad. Como resultado, el análisis muestra cómo una base de datos de prefijos válidos y números de teléfonos móviles permite ataques de obtención de contactos a gran escala en tres (3) apps de mensajería ampliamente utilizadas como WhatsApp, Signal y Telegram. El estudio ha permitido realizar un muestreo para un 10% de los números de teléfono de USA de WhatsApp, un 100% de Signal y la posibilidad de obtener información sensible a través de la API de Telegram, incluso para números no registrados en este servicio. Este tipo de análisis también permite conocer cuántos usuarios tienen cuenta en varios de los servicios de mensajería y en cuáles concretamente, así como estudios de utilización por estado (en el caso de USA).




(a) WhatsApp; the popularity is estimated based on enumerating 10 % of all possible US mobile phone numbers.

(b) Signal; Washington D.C. numbers are more than twice as likely to be registered with Signal than for any other area in the US.

Figura 29. Número de cuentas de WhatsApp y Signal registradas en los estados de EE.UU. y Washington D.C. en relación con su población.

El análisis estudia problemas de privacidad en los métodos de descubrimiento de los contactos de las tres apps objetivo desde la perspectiva del propio proveedor del servicio o app, o de un usuario malicioso, empleando dos escenarios. El primero de ellos permite hacer uso de grandes bases de datos de números de teléfonos, incluso en el caso de Signal, que hace uso de hashes derivados del número de teléfono de un usuario para referenciar a los contactos (en lugar de usar los números en claro como WhatsApp o Telegram).

Es posible revertir el proceso de obtención del hash y conocer el número de teléfono a partir del hash mediante la generación de bases de datos de gran tamaño de hashes empleadas para realizar búsquedas inversas, por la baja entropía de los números de teléfono, ya que el formato internacional de los números de teléfono es conocido (formado por el código de país, un conjunto de prefijos válidos para números de teléfonos móviles asignados por cada país y/o estado o región, y el número del abonado). Es posible obtener el número asociado a un hash buscando en la base de datos cargada en memoria (con un muy bajo tiempo de búsqueda), empleando *rainbowtables* optimizadas, o mediante fuerza bruta.

El segundo escenario automatiza las consultas a los servicios de descubrimiento de las apps, registrando nuevas cuentas de usuario, y simulando el proceso de sincronización inicial de contactos, iterando a lo largo del tiempo entre distintas direcciones IP origen y dispositivos móviles, para enumerar contactos y evitar las restricciones y contramedidas de los servicios frente a consultas masivas por parte de un mismo usuario y ataques de *scrapping* (previamente mencionados en los incidentes de Facebook y Linked-In).

Como resultado[114], se demostró la posibilidad de obtener los números de teléfono de usuarios válidos en las apps de mensajería en un tiempo razonable disponiendo de suficientes recursos de computación, y se demostró el impacto de las capacidades actuales de descubrimiento o sincronización de contactos en las apps, lo que hace necesario una evolución de los métodos actuales, empleando mecanismos con esquemas incrementales de descubrimiento de contactos, que limiten el número de peticiones posibles (*rate limiting*), que preserven la privacidad de los usuarios y, preferiblemente, que no almacenen la información de contactos en el servidor (como en el caso de Signal), como la propuesta *incremental contact discovery*.

Aunque los ataques de descubrimiento de contactos no pueden ser prevenidos completamente, debido a que es necesario disponer de la funcionalidad asociada por parte de los usuarios de las apps de mensajería, sí se pueden implementar contramedidas para mitigar su abuso y la obtención masiva de datos de usuarios.

Es asimismo relevante conocer qué información del usuario es accesible a través del servicio de descubrimiento de contactos, por defecto o tras restringir el usuario el acceso a su perfi[l115]. WhatsApp por ejemplo permite establecer si la imagen de perfil del usuario (o avatar), la descripción del perfil y la última vez que se ha conectado estarán disponibles, para todo el mundo, sólo para los contactos, o para nadie.

Signal, más centrado en la privacidad, no expone información de los usuarios a través de este servicio. Únicamente se puede obtener la imagen de perfil del usuario y su nombre en formato cifrado, pudiendo sólo ser descifrados si el usuario objetivo da su consentimiento a la petición de contacto y establece una conversación con el usuario que le contacta.

Telegram expone numerosos datos de los usuarios, incluyendo nombre y apellidos, nombre de usuario, identificador de Telegram, descripción, la última vez que se ha conectado, todas las imágenes de perfil del usuario (hasta 100), y el número de grupos comunes, pudiendo restringirse esta información tan solo a los contactos. El servicio almacena adicionalmente cuántos usuarios registrados disponen de un número de teléfono en su lista de contactos, concretamente cuando dicho número no está registrado en Telegram (o proporciona el valor 0 para números registrados). Esta información se actualiza dinámicamente en función de los cambios en la lista de contactos de los usuarios, lo que constituye una fuente de metadatos muy relevante.

Las conclusiones obtenidas en el estudio respecto a los mecanismos de mitigación de los servicios de mensajería ante peticiones masivas por parte de un usuario confirman diferentes aproximaciones[116]. WhatsApp parece disponer de un límite de consultas (puntual) cercano a los 120 mil contactos, sin restricciones para un mismo usuario a lo largo del tiempo, pudiendo comprobar millones de diferentes números de teléfono objetivo.

En Signal el límite de consultas es de 50 mil contactos, pudiéndose obtener unos 200 mil contactos al día, y no dispone de una limitación global en el máximo número de contactos que pueden ser consultados, ya que el servidor no almacena los contactos de un usuario, por lo que es necesario llevar a cabo la comprobación por parte de los clientes en cada sincronización (el servidor no puede compararlos con números previamente sincronizados, a diferencia de WhatsApp o Telegram, ya que sus servidores sí almacenan los contactos).

**114, 115, 116.** "All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers". University of Würzburg, TU Darmstadt. NDSS Symposium. Feb 2021. URL: https://www.ndss-symposium.org/ndss-paper/all-the-numbers-are-us-large-scale-abuse-of-contact-discovery-in-mobile-messengers/ URL: https://contact-discovery.github.io

Telegram sólo permite a un usuario tener 5 mil contactos, y añadir posteriormente 100 al día, aplicándose reglas de bloqueo a los usuarios que intentan abusar del servicio de descubrimiento de contactos (a diferencia de Signal o WhatsApp), lo que ha limitado significativamente su análisis masivo durante el estudio. Los diferentes proveedores han tomado medidas adicionales como resultado del estudio para mitigar este tipo de ataques.

En relación con la privacidad del usuario y las apps móviles de la COVID-19, analizadas en gran nivel de detalle en el siguiente apartado por su amplia utilización de las comunicaciones inalámbricas Bluetooth y BLE, en abril de 2021 se publicaba un estudio que reflejaba cómo un fallo de privacidad de Android podía haber expuesto los logs de las apps de rastreo de contactos, incluyendo si el usuario ha estado en contacto de proximidad con otro usuario diagnosticado positivo, a otras apps móviles pre-instaladas en el dispositivo móvil del usuario[117].

El fallo de implementación en Android reside en que, aunque los datos, registros y logs de rastreo de contactos se almacenan en el área privada de memoria del sistema (no accesible para apps estándar), concretamente en los logs del sistema (logcat), las apps pre-instaladas en los dispositivos móviles por parte de sus fabricantes o de los operadores de telefonía que los comercializan con personalizaciones, disponen de privilegios de sistema para poder acceder a esos logs del sistema (específicamente, mediante el permiso de Android READ_LOGS)[118]. Aunque no se tiene constancia de apps que hayan sacado provecho de esta vulnerabilidad, el informe anual de 2018[119] ya desvelaba una tendencia en el mundo Android asociada a los abusos llevados a cabo por apps pre-instaladas de múltiples fabricantes. Esta tendencia se materializaba de nuevo a finales de marzo y en mayo de 2019 con el descubrimiento de todo un ecosistema que estaba poniendo en riesgo la seguridad de Android, detallado en profundidad en el informe anual de 2019[120].

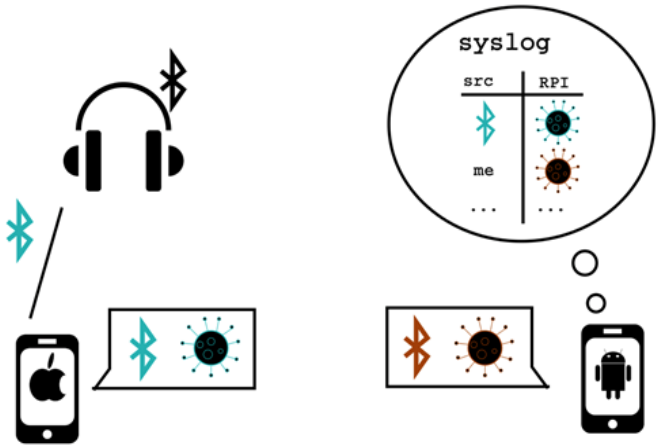
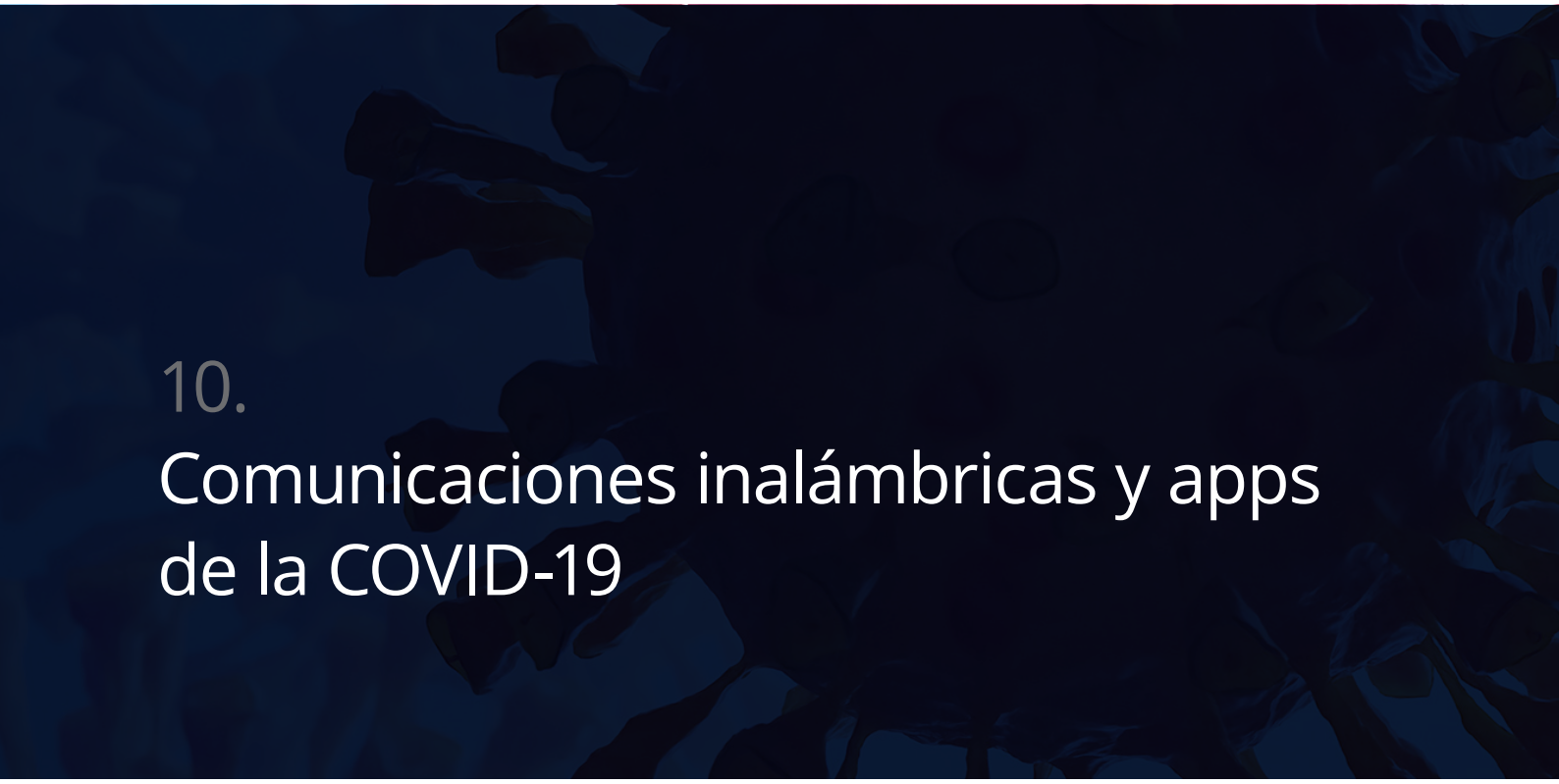



Figura 30. El sistema GAEN en la práctica. Un dispositivo Apple y otro Android transmiten RPI junto con sus direcciones MAC Bluetooth (actuales). Los dispositivos también pueden transmitir sus direcciones MAC Bluetooth en otros contextos, por ejemplo, porque el Bluetooth está activado o se está utilizando. El dispositivo Android almacena todas las MACs+RPIs observadas en su registro del sistema, junto con sus propios RPIs. Ten en cuenta que, por diseño, Android no permite que las aplicaciones aprendan sus propias direcciones MAC.

**117.** "Android bug exposed COVID-19 contact tracing logs to preinstalled apps". The Verge. Apr 2021. URL: https://www.theverge.com/2021/4/27/22405425/android-google-contact-tracing-bug-privacy
**118.** "Why Google Should Stop Logging Contact-Tracing Data". AppCensus Blog. Apr 2021. URL: https://blog.appcensus.io/2021/04/27/why-google-should-stop-logging-contact-tracing-data/
**119.** "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
**120.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html



# 10. Comunicaciones inalámbricas y apps de la COVID-19

En abril de 2020 se publicaba una investigación que mostraba tanto las capacidades proporcionadas por "Find My" (o el uso de nuevos sistemas basados en este esquema de comunicación distribuido) para exfiltrar información confidencial de forma anónima a través de diferentes modelos y escenarios de uso, así como algunas debilidades asociadas a "Find My" que podían afectar al anonimato de los usuarios.

Complementariamente, en marzo de 2021 (mucho más recientemente), una investigación desvelaba que las capacidades de "Offline Finding" de Apple podrían ser empleadas de manera no autorizada para localizar el dispositivo y las localizaciones más comunes de un usuario con una precisión de 10 metros, a través de un análisis de seguridad y privacidad detallado y de técnicas de ingeniería inversas sobre los protocolos propietarios de Apple[121].

La existencia de dos errores de diseño e implementación permiten realizar ataques de correlación para obtener datos del histórico de ubicaciones de un usuario durante los últimos 7 días, desanonimizando a los usuarios.

El estudio fue realizado por investigadores alemanes del proyecto OWL (Open Wireless Link), referenciado en el informe anual del pasado año 2019[122], y sus conclusiones fueron notificadas a Apple en el mes de julio de 2020.

Potencialmente, Apple podría crear un diagrama social de las ubicaciones de dispositivos perdidos reportadas por los mismos dispositivos, lo que permitiría su correlación. Un atacante podría sacar provecho de las debilidades a través de la instalación de una aplicación maliciosa en el ordenador macOS de la víctima, que extrajese las claves criptográficas empleadas para las notificaciones de ubicación de su dispositivo móvil.

---

**121.** "Who Can Find My Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System". arXiv. Mar 2021. URL: https://arxiv.org/abs/2103.02282

**122.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html

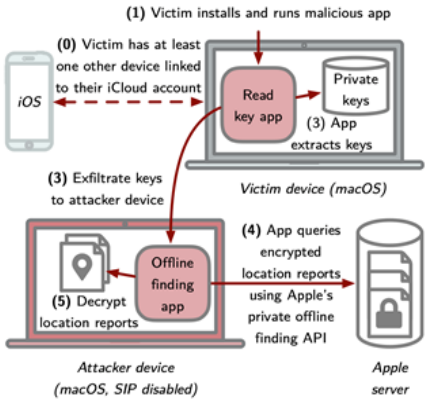



Figura 31. Flujo de ataque que obtiene acceso al historial de localización de la víctima. Los componentes controlados por el atacante están marcados en rojo.

Estas capacidades de "Find My" tienen relación directa con una tecnología derivada que ha sido de especial relevancia a lo largo del año 2020 en relación a la COVID-19: la infraestructura o tecnologías para el rastreo de contactos de la COVID-19, o en su denominación en inglés, Privacy-Preserving Contact Tracing. Esta fue desarrollada conjuntamente (en una colaboración sin precedente en la industria de telefonía móvil) entre Apple y Google, con la colaboración de autoridades públicas sanitarias, universidades y otras organizaciones, y es de aplicación tanto para dispositivos móviles iOS como Android, asegurando su interoperabilidad, es decir, con cobertura para la práctica totalidad de usuarios de dispositivos móviles a nivel mundial (ver las cuotas de mercado reflejadas al principio del presente informe).

Esta tecnología se basa en el uso de las comunicaciones Bluetooth y BLE para detectar y rastrear la proximidad entre personas (realmente, entre sus dispositivos móviles), con el objeto de ayudar a gobiernos y agencias de salud a reducir la propagación del virus, respetando la privacidad y seguridad de los usuarios.

Desde el inicio se identificó como un elemento clave disponer de la confianza de los usuarios para que realmente hiciesen uso de las apps asociadas, y lograr así una adopción significativa (necesaria para que la tecnología fuese realmente efectiva), lo que conllevaba estrictos estándares centrados en asegurar su privacidad y la anonimización de todos los intercambios de información.

Desde un punto de vista técnico, muy brevemente, los dispositivos móviles con la app móvil instalada generan identificadores aleatorios (en realidad se hace uso de claves criptográficas efímeras que permiten generar estos identificadores) cada 10-20 minutos, para evitar el seguimiento de un usuario. Estos identificadores, que preservan la privacidad del usuario, se propagan o difunden (mediante un mecanismo de *broadcast*) a través de Bluetooth (BLE, para minimizar el consumo de batería) para que otros dispositivos móviles cercanos puedan identificar la presencia del usuario.

De igual manera, el usuario recibe los identificadores de otros usuarios próximos vía Bluetooth, identificando también su presencia. Los dispositivos móviles almacenan localmente los identificadores del resto de usuarios que han estado en un área próxima durante días. Este intercambio se lleva a cabo incluso sin tener la app en ejecución en primer plano. Cuando un usuario es diagnosticado como positivo, puede (mediante un código asociado) reportar su caso a través de la app, lo que será notificado al servidor, y desde este, al resto de usuarios de la app.

Las apps periódicamente (habitualmente un par de veces al día, pero depende de la app y del país) obtienen o descargan desde el servidor los identificadores asociados a todos los casos positivos reportados por otros usuarios, y los comparan con su base de datos local, que habitualmente contiene los identificadores de contactos de proximidad recibidos vía BLE, junto a la fecha y hora, durante un periodo de dos semanas (14 días). La verificación se realiza localmente para no desvelar la identidad del usuario a un tercero. Si se encuentra una coincidencia entre el identificador de un caso positivo reportado por otro usuario, y el identificador de un usuario que fue recibido vía Bluetooth en ese periodo, se sabe que un posible contacto de proximidad del usuario se ha infectado y, por tanto, el usuario ha podido estar expuesto al virus. Como consecuencia, la app notifica al usuario de este posible riesgo, con instrucciones de cómo proceder. El usuario decide si, y cuándo, activa el sistema de notificaciones de exposición, así como si quiere reportar su caso positivo[123].

Las primeras especificaciones técnicas de esta solución se anunciaron en abril de 2020[124, 125], con el objetivo de disponer de su implementación inicial operativa en junio de 2020, por ejemplo, en Europa[126]. A principios de junio se publicaba Immuni, la app de rastreo de contactos de Italia como la primera app oficial europea basada en el sistema de notificación de exposiciones a la COVID-19 de Apple y Google[127]. Posteriormente, en el caso de España, se llevó a cabo un piloto en la Gomera en el mes de julio[128], y finalmente se comenzó a desplegar la infraestructura a nivel nacional en el mes de septiembre[129] (previamente, en agosto, y posteriormente, en octubre, según la Comunidad Autónoma[130]).

Finalmente, a mediados del mes de octubre se llevó a cabo la integración de Radar COVID con otras apps e infraestructuras de rastreo de la COVID-19 de diferentes países europeos, a través de un nodo o plataforma de interoperabilidad de la Comisión Europea[131], con el objetivo de detectar la exposición incluso entre ciudadanos extranjeros, y no únicamente entre ciudadanos del mismo país, independientemente de la app de rastreo (asociada a cada país) que estén utilizando[132]. Con posterioridad se fueron incorporando a la integración otros países europeos, como España a finales del mes de octubre (en el segundo grupo de países en unirse a la iniciativa).


**123.** https://ncase.me/contact-tracing/
**124.** "Apple and Google partner on COVID-19 contact tracing technology". Google. Apr 10, 2020. URL: https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/
**125.** "Apple and Google partner on COVID-19 contact tracing technology". Apple. Apr 10, 2020. URL: https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/
**126.** "National COVID-19 contact tracing apps". Briefing. European Parliament. May 2020. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI(2020)652711_EN.pdf
**127.** "Probamos Immuni, la primera app oficial europea de seguimiento de contactos basada en el sistema de Apple y Google". Xataka. Jun 2020. URL: https://www.xataka.com/aplicaciones/probamos-immuni-primera-app-oficial-europea-seguimiento-contactos-basada-sistema-apple-google - URL: https://github.com/immuni-app/immuni-app-android
**128.** https://www.lagomera.es/la-gomera-habilita-desde-hoy-cuatro-puntos-de-informacion-para-la-descarga-de-la-app-radar-covid/
**129.** https://www.rtve.es/noticias/20200803/radar-covid-aplicacion-rastreo-probada-gomera-duplica-contactos-detectados-manera-manual/2036587.shtml
**130.** https://www.xataka.com/medicina-y-salud/radar-covid-esta-disponible-puedes-instalarla-android-e-ios-no-funcionara-que-cc-aa-activen#c1544683
**131.** https://ec.europa.eu/commission/presscorner/detail/es/ip_20_1904
**132.** "Radar COVID ya es interoperable con las aplicaciones de rastreo de COVID-19 de otros países europeos". Xataka. Oct 2020. URL: https://www.xataka.com/aplicaciones/radar-covid-interoperable-aplicaciones-rastreo-covid-19-otros-paises-europeos

El acuerdo entre Apple y Google se anunció en abril de 2020, y se materializó en mayo[133] con la publicación de la API o *framework* para desarrolladores, y se puso a disposición de las autoridades sanitarias públicas a nivel internacional. El nombre interno de este proyecto fue "Bubble" en el caso de Google y "Apollo" en el caso de Apple. Posteriormente, en junio ambas compañías proporcionaron la infraestructura con la que se comunican los dispositivos móviles de los usuarios y que les conecta con las plataformas específicas de cada app y país.

A lo largo del proceso de implantación y despliegue, se han realizado actualizaciones y mejoras del sistema y de la tecnología asociada. Por ejemplo, se introdujeron mejoras en la calibración de la detección de dispositivos cercanos mediante Bluetooth, y sobre la obtención de detalles de intensidad de señal, para que cada autoridad sanitaria pudiese evaluar y personalizar el riesgo de exposición en base a detalles técnicos de la API, como el nivel de señal Bluetooth detectado, y, por tanto, la distancia estimada entre usuarios.

Cabe destacar también la funcionalidad introducida para permitir la interoperabilidad entre países, la posibilidad de activar o desactivar la funcionalidad de rastreo con un único botón por parte del usuario (proporcionándole más control sobre estas capacidades) o la inclusión de notificaciones y recordatorios periódicos para que el usuario sepa que la funcionalidad sigue estando activa.

Tanto Apple[134, 135] como Google[136] publicaron sus sitios webs oficiales específicos del sistema de rastreo de contactos (Privacy-Preserving Contact Tracing), exposición y notificaciones (Exposure Notification), con información general para usuarios y organizaciones sanitarias, así como con todos los detalles técnicos y especificaciones (tanto de Bluetooth como criptográficas) para desarrolladores (incluyendo APIs y *frameworks*[137]) y para otros profesionales involucrados en la creación y despliegue de soluciones de rastreo de contactos.

Inicialmente las especificaciones se publicaron como borrador, para que fueran revisadas por la comunidad, confirmándose finalmente la versión final que se emplearía en las implementaciones reales. En un ejercicio de transparencia sin precedente a nivel internacional, debido a la sensibilidad de la información gestionada, concretamente de geolocalización, de contactos y de salud, Google y Apple, publicaron la documentación de referencia de la API o *framework* para facilitar el desarrollo de apps en iOS[138] y Android[139] por parte de los diferentes países, las especificaciones y preguntas frecuentes (FAQ)[140] y el código fuente, tanto de la implementación de referencia de Apple[141] como de Google[142].

Al igual que en el caso de "Find My", en las tecnologías para el rastreo de contactos de la COVID-19 se hace uso de comunicaciones BLE empleando identificadores dinámicos y de mecanismos criptográficos avanzados, en concreto claves públicas efímeras (de curva

**133.** "Apple and Google partner on COVID-19 contact tracing technology". Google. Apr 10, 2020. URL: https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/
**134, 141.** "Exposure Notification". Apple. URL: https://developer.apple.com/exposure-notification/
**135, 140.** "Privacy-Preserving Contact Tracing". Apple. URL: https://covid19.apple.com/contacttracing
135. "Exposure Notifications: Using technology to help public health authorities fight COVID-19". Google. URL: https://www.google.com/covid19/ URL: https://www.google.com/covid19/exposurenotifications/
**137, 138.** "Exposure Notification System (ES) o API". Apple Developer. URL: https://developer.apple.com/documentation/exposurenotification
**139.** "Exposure Notifications API". Google Developer. URL: https://developers.google.com/android/exposure-notifications/exposure-notifications-api
**142.** "Exposure Notifications API: Android Reference Design". Google. URL: https://github.com/google/exposure-notifications-android

elíptica) que cambian o rotan a lo largo del tiempo, al igual que los identificadores que se derivan de estas claves (aproximadamente cada 15 minutos), y que son difundidos por los dispositivos móviles de los usuarios para identificar la presencia o cercanía de otros dispositivos y, por tanto, de sus usuarios. En este caso, incluso, el nivel de intensidad de la señal de Bluetooth puede permitir (con limitaciones en su precisión) estimar el rango aproximado de la distancia o cercanía entre usuarios. En base a la distancia estimada, y a la cantidad de tiempo que dos usuarios han estado cerca del otro, se puede estimar el nivel de riesgo o exposición al virus en caso de que uno de ellos sea diagnosticado como positivo posteriormente.

Teniendo como objetivo identificar la propagación de infecciones asociadas a la pandemia y crisis sanitaria a nivel mundial de la COVID-19, esta infraestructura está también asociada a la API o *framework* de notificaciones de exposición (en inglés, Exposure Notification System, ENS[143] o Exposure Notification API)[144], desarrollada por Apple y Google (algunas referencias emplean el término GAEN, Google-Apple Exposure Notifications[145]), ya que su propósito es doble, de ahí su nombre: por un lado, tal y como se ha descrito previamente, identificar y realizar el rastreo y seguimiento de aquellos usuarios que han estado potencialmente en contacto, por su proximidad física, y por tanto potencialmente expuestos al virus; y por otro lado, proporcionarles posteriormente notificaciones respecto a esa posible exposición al virus, es decir, alertas de contactos de riesgo por la COVID-19, para ponerlo en su conocimiento y que lleven a cabo las comprobaciones y acciones oportunas.

Esta tecnología de "traceo (o seguimiento) automático" complementa la labor inicial de los rastreadores manuales para identificar posibles contactos de riesgo y anticiparse a potenciales contagios.

---

**143.** No relacionado con el Esquema Nacional de Seguridad (ENS).
**144.** "Exposure Notification". Apple. URL: https://developer.apple.com/exposure-notification/
**145.** "Why Google Should Stop Logging Contact-Tracing Data". AppCensus Blog. Apr 2021. URL: https://blog.appcensus.io/2021/04/27/why-google-should-stop-logging-contact-tracing-data/

Independientemente de toda la tecnología involucrada en la solución, y de los mecanismos de privacidad y seguridad implementados, existen muchos otros aspectos, tanto sociológicos como vinculados a los medios, procesos y procedimientos facilitados por los sistemas sanitarios de cada país, y más concretamente de cada Comunidad Autónoma, región o ciudad en España, que deben ser tenidos en cuenta para corroborar que se trata de una tecnología y herramienta realmente valiosa y efectiva para evitar o reducir la propagación del virus.

Con el objeto de proporcionar los datos precisos existentes en la fase final de la elaboración del presente informe (abril de 2021), según la propia app Radar COVID, la misma se ha descargado más de 7 millones de veces, con 59 mil casos positivos declarados desde el 19/08/2020 y con un total de 16 países europeos conectados. Es posible obtener más estadísticas diarias (proporcionadas por terceros) a través del proyecto Radar STATS[146].

Esta tecnología es de uso voluntario, no identifica con quién ha estado una persona, ni hace uso de las capacidades de geolocalización, pese a que la arquitectura e implementación de Android en el uso de Bluetooth, en concreto para realizar escaneos mediante BLE, imponía inicialmente como requisito disponer de los servicios de localización activos (por simplificar, el GPS, y el resto de servicios asociados), debido a cómo hacía Android uso de las capacidades de Bluetooth a nivel del sistema operativo[147], condicionado por la existencia de dispositivos de (micro)geolocalización Bluetooth conocidos como *beacons* BLE.

El argumento de Google ya en 2015 para hacer uso de esta implementación fue precisamente ese, evitar desde el punto de vista de privacidad que una app pudiera geolocalizar al usuario mediante Bluetooth a través de este tipo de *beacons*, por ejemplo, en una tienda, incluso cuando el usuario no tiene los servicios de localización o ajustes de ubicación activos[148]. Pese a este requisito, de manera general, las apps de rastreo que hacen uso del ENS no obtenían detalles de localización de los usuarios, y Google y Apple implementaron medidas compensatorias para este tipo de apps.

**146.** https://twitter.com/RadarCOVIDSTATS
**147.** "Por qué Radar Covid no funciona sin el GPS activo en Android pero sí lo hace en los iPhone". Ago 2020. Xataka. URL: https://www.xataka.com/aplicaciones/que-radar-covid-no-funciona-gps-activo-android-hace-iphone
**148.** "An update on Exposure Notifications". Google Blog. Jul 2020. URL: https://blog.google/inside-google/company-announcements/update-exposure-notifications/

La controversia generada forzó a que Google cambiase este modo de funcionamiento, disponible desde el año 2015 en la versión 6.0 de Android, para que no se requiera tener activos los servicios de localización por parte de las apps que hacen uso del ENS en Android 11[149, 150].

Google dispone de un artículo descriptivo clarificando la diferencia en el comportamiento entre Android 10 (y versiones previas) y Android 11[151] aunque, como siempre, el principal inconveniente es que muchos usuarios no dispondrán de la capacidad de actualizar sus dispositivos móviles a la versión 11 de Android (un elemento clave de seguridad que debería siempre ser tenido en cuenta a medio y largo plazo a la hora de adquirir un nuevo dispositivo móvil Android).

Desde un punto de vista técnico, muchas soluciones y apps de rastreo de contactos se basan en un proyecto descentralizado conocido como DP-3T[152]. Fue en el repositorio de GitHub de dicho proyecto, entre otros, en el que se incidía en la necesidad de desvincular el requisito de disponer de los servicios de localización activos para poder hacer uso de los escaneos BLE y, en consecuencia, de las apps frente a la COVID-19[153], tomando como ejemplo la app de Suiza, SwissCovid[154]. Esta preocupación se reflejaba igualmente en la gestión de mejoras e *issues* de Google para Android, con mención explícita a Radar COVID en agosto de 2020[155] (ver imágenes superiores de ambas apps).

En el caso de iOS, la implementación para llevar a cabo el escaneo de dispositivos Bluetooth es completamente diferente y no hace uso de los servicios de localización. Sus capacidades previas cambiaban si la app está disponible en primer plano, pudiendo escanear cualquier dispositivo, o está ejecutando en segundo plano, sólo pudiendo escanear dispositivos Bluetooth ya conocidos.


Figura 32

**149.** "Por qué Radar Covid no funciona sin el GPS activo en Android pero sí lo hace en los iPhone". Ago 2020. Xataka. URL: https://www.xataka.com/aplicaciones/que-radar-covid-no-funciona-gps-activo-android-hace-iphone
**150.** "An update on Exposure Notifications". Google Blog. Jul 2020. URL: https://blog.google/inside-google/company-announcements/update-exposure-notifications/
**151.** "Acerca del sistema de notificaciones de exposición y los ajustes de ubicación de Android". Ayuda de Android. Google. URL: https://support.google.com/android/answer/9930236?hl=es
**152.** "DP-3T: Decentralized Privacy-Preserving Proximity Tracing". GitHub. URL: https://github.com/DP-3T
**153.** "Location / Bluetooth Permissions". GitHub DP-3T. May 2020. URL: https://github.com/DP-3T/dp3t-app-android-ch/issues/61
**154.** https://www.nytimes.com/2020/07/20/technology/google-covid-tracker-app.html
**155.** "BluetoothLeScanner.startScan require Location Service" (148429135). Google Android IssueTracker. Ago 2020. URL: https://issuetracker.google.com/issues/148429135#comment7

Este fue uno de los motivos principales, inicialmente, para que Apple tuviese que implementar una nueva funcionalidad y API, Exposure Notifications, que modificase el comportamiento existente previamente y permitiese escanear dispositivos Bluetooth incluso estando la app en segundo plano, minimizando así también el consumo de batería por parte de las apps de rastreo de contactos[156]. El cambio fue necesario ya que la idea en todo momento por parte de Google y Apple era que la gente confiase en este sistema de rastreo de contactos para usarlo masivamente y así ayudar a mitigar la pandemia a nivel mundial.

A lo largo de los meses numerosas noticas, polémicas y vulnerabilidades de seguridad y privacidad han estado rodeando la publicación de las diferentes apps móviles de rastreo de contactos en las tiendas o mercados oficiales de apps. Empezando por países que optaron por no hacer uso de la solución descentralizada de Apple y Google previamente descrita, y decidieron hacer uso de una solución centralizada controlada por las autoridades sanitarias del país, con el riesgo de ataques y del compromiso de toda la información de contagios de todos sus ciudadanos. Uno de los ejemplos más conocidos fue la app del NHS (National Health Service)[157], el servicio sanitario de UK (aunque posteriormente una nueva versión de la app adoptó el modelo descentralizado[158]).

En aras de promover esa transparencia y confianza previamente mencionadas, muchas de las apps móviles de la COVID-19 se pusieron a disposición de la comunidad como proyectos de código abierto.

Las capacidades de detección y notificación de posibles exposiciones a otros ciudadanos infectados con la COVID-19, existentes a través de las apps móviles creadas por los diferentes países para sus ciudadanos, fueron extendidas posteriormente por Apple, en la versión 13.7 de iOS[159], con el sistema de notificaciones de exposición exprés (Exposure Notifications Express)[160], que permite configurar la infraestructura de notificaciones de cada país para notificar a los ciudadanos de potenciales exposiciones a la COVID-19 incluso si no disponen de una app de rastreo de contactos instalada en su dispositivo móvil, es decir, directamente a través del sistema operativo iOS. Esta mejora facilita que la tecnología llegue a un mayor número de usuarios, incluso si estos activamente no han descargado e instalado la app de rastreo de la COVID-19 de su país.

En el caso de España la app oficial, disponible para Android[161] e iOS[162], se denomina Radar COVID[163] y ha sido difundida y promovida activamente a lo largo de todo el año 2020 por el Ministerio de Asuntos Económicos y Transformación Digital[164], y más concretamente por la S.E. (Secretaría de Estado) de Digitalización e Inteligencia Artificial (IA)[165], especialmente en Twitter (@SEDIAgob[166]).

---

**156.** "Por qué Radar Covid no funciona sin el GPS activo en Android pero sí lo hace en los iPhone". Ago 2020. Xataka. URL: https://www.xataka.com/aplicaciones/que-radar-covid-no-funciona-gps-activo-android-hace-iphone
**157.** https://www.zdnet.com/article/contact-tracing-apps-why-the-nhs-said-no-to-apple-and-googles-plan/
**158.** https://www.theguardian.com/world/2020/sep/21/covid-coronavirus-contact-tracing-app-hampered-lack-trust
**159.** https://support.apple.com/en-us/HT210393#137
**160.** "Supporting Exposure Notifications Express" . Apple Developer. URL: https://developer.apple.com/documentation/exposurenotification/supporting_exposure_notifications_express
**161.** "Radar COVID: Android". Google Play. URL: https://play.google.com/store/apps/details?id=es.gob.radarcovid
**162.** "Radar COVID: iOS". App Store. URL: https://apps.apple.com/es/app/radar-covid/id1520443509
**163.** "Radar COVID". Ministerio de Asuntos Economicos y Transformacion Digital. URL: https://radarcovid.gob.es URL: https://github.com/RadarCOVID
**164.** https://portal.mineco.gob.es/es-es/Paginas/default.aspx
**165.** https://avancedigital.mineco.gob.es/es-es/Paginas/index.aspx
**166.** https://twitter.com/sediagob

En un ejercicio de transparencia, de nuevo, sin precedente a nivel nacional, el código fuente de algunos componentes de la solución empleada en España fueron publicados en GitHub para su potencial análisis por parte de cualquier ciudadano o usuario[167].

Es posible identificar las apps de rastreo de contactos de los diferentes países a través de los recursos facilitados por Google[168] y Apple[169] a este efecto.

El año 2020 adicionalmente ha presentado nuevas investigaciones y descubrimientos relevantes de seguridad asociados a las tecnologías Bluetooth y BLE, descritas a continuación.


Figura 33

**167.** "Radar COVID". Ministerio de Asuntos Economicos y Transformacion Digital. URL: https://radarcovid.gob.es URL: https://github.com/RadarCOVID
**168.** "COVID-19 Android Apps". Google. URL: http://g.co/ENS URL: https://www.google.com/covid19/exposurenotifications/select/
**169.** "COVID-19 iOS Apps". Apple. URL: https://apps.apple.com/story/id1527477499

Aparte de en KNOB, Key Negotiation of Bluetooth Attack (CVE-2019-9506)[170], el framework InternalBlue[171] ha sido utilizado para el descubrimiento de nuevas vulnerabilidades y ataques Bluetooth, como BIAS[172] en el caso de mensajes LMP y SweynTooth[173] en el caso de mensajes LCP, ambas descritas a continuación. Adicionalmente, permitió en mayo de 2020 identificar una vulnerabilidad (CVE-2020-6616) en la incorrecta generación de números aleatorios por parte de ciertos chips de Broadcom (ej. BCM4361), que hacen uso de un PRNG (Pseudo Random Number Generator) con muy baja entropía, en lugar de un HRNG (Hardware Random Number Generator)[174]. Esta vulnerabilidad afectó al Samsung Galaxy S8, S8+ y Note 8 (con la vulnerabilidad de Samsung identificada como SVE-2020-16882), y también a macOS[175].

BIAS[176], Bluetooth Impersonation AttackS, es una vulnerabilidad en el proceso de autentificación de Bluetooth (no de BLE, en este caso) con la que un atacante puede realizar ataques de MitM (Man-in-the-Middle), rebajando la autentificación mutua a una autentificación en un solo sentido, y suplantar al dispositivo maestro o esclavo de una comunicación Bluetooth. De este modo el dispositivo Bluetooth víctima se autentifica con el atacante, pero el atacante (suplantando al dispositivo destino de la comunicación) no requiere autentificarse contra el dispositivo víctima.

---

**170.** "KNOB Attack". USENIX. Aug 2019. URL: https://knobattack.com - URL: https://www.usenix.org/conference/usenixsecurity19/presentation/antonioli - URL: https://greatscottgadgets.com/2019/08-16-tools-of-the-knob-attack/

**171.** "InternalBlue". SEEMOO. 2021. URL: https://github.com/seemoo-lab/internalblue

**172.176.** "BIAS: Bluetooth Impersonation AttackS". Daniele Antonioli, Nils Ole Tippenhauer, Kasper Rasmussen. May 2020. URL: https://francozappa.github.io/about-bias/

**173.** "SweynTooth: Unleashing Mayhem over Bluetooth Low Energy". Matheus E. Garbelini, Chundong Wang, Sudipta Chattopadhyay, Sumei Sun, and Ernest Kurniawan. ASSET SUTD. Feb/Jul 2020. URL: https://asset-group.github.io/disclosures/sweyntooth/

**174.** "Finding Eastereggs in Broadcom's Bluetooth Random Number Generator". Jiska. CCC. URL: https://vulmon.com/vulnerabilitydetails?qid=CVE-2020-6616 URL: https://media.ccc.de/v/DiVOC-6-finding_eastereggs_in_broadcom_s_bluetooth_random_number_generator

**175.** https://support.apple.com/en-us/HT211100


Figura 34. Resumen de los ataques de suplantación de identidad por Bluetooth (BIAS)

El proceso de autentificación de Bluetooth se emplea durante el proceso de emparejamiento inicial y durante el proceso de establecimiento de conexiones seguras, empleando claves criptográficas a largo plazo (Long Term Keys, LTK). Existen dos modos de autentificación, el modo *legacy* y el modo seguro (más moderno), denominados Legacy Secure Connections (LSC) y Secure Connections (SC) respectivamente. La especificación no obliga al uso de autentificación mutua, es decir, permite el paso del modo Secure al modo Legacy Secure (mediante un ataque de *downgrade* del primero al segundo), especialmente al hacer uso del mecanismo de intercambio de roles (role switching) de maestro a esclavo, o viceversa.

La investigación plantea cuatro tipos de ataques, al modo de autentificación LSC o SC, y suplantando al maestro (MI, Master Impersonation) o al esclavo (SI, Slave Impersonation). Esta vulnerabilidad fue descubierta por los mismos autores de KNOB. Debido a que la vulnerabilidad está presente en la especificación del protocolo Bluetooth, potencialmente cualquier dispositivo podría ser vulnerable. Sorprende que a estas alturas todavía sean descubiertas vulnerabilidades en las especificaciones de protocolos ampliamente utilizados, como Bluetooth, y que afectan a numerosas versiones del protocolo (ver siguiente imagen).

Las cuatro (4) causas raíz de BIAS incluyen el hecho de que el establecimiento de conexiones seguras no esté protegido por mecanismos de integridad, lo que permite modificar el soporte de SC; que el modo LSC no requiere autentificación mutua, lo que permite al atacante no tener que autentificarse ante la víctima (actuando tan solo de verificador o *verifier*); que el intercambio de rol se puede realizar en cualquier momento, algo problemático unido a la no obligatoriedad de la autentificación mutua previa, ya que el atacante puede iniciar el proceso de conexión y pasar a ser el verificador, sin tener que autentificarse; y que Bluetooth no fuerza el uso de SC, por lo que dos dispositivos que se emparejaron con SC pueden usar LSC para el establecimiento de conexiones futuras, lo que es aprovechado por el atacante para hacer un *downgrade* de SC a LSC.

La investigación evaluó 30 dispositivos diferentes, que hacían uso de 28 chips Bluetooth distintos, confirmándose como vulnerables todos ellos a alguna o varias de las cuatro vulnerabilidades o ataques descritos, incluyendo chips y dispositivos móviles como los iPhone 8, 7 Plus, 6 y 5s, iPad 2018, Nokia 7 y X6, Pixel 2 y 3, Nexus 5, OnePlus 6, Samsung Galaxy J5, J3 y S5 mini, Lumia 530, LG K4, Motorola G3, etc. Estos ataques además pasan inadvertidos ya que Bluetooth no notifica al usuario del resultado del proceso de autentificación, si no se usa la opción segura (frente a la *legacy*), o acerca de la ausencia de autentificación mutua.

| | | LSC | | SC | |
|---|---|---|---|---|---|
| Chip | Device(s) | MI | SI | MI | SI |
| *Bluetooth v5.0* | | | | | |
| Apple 339S00397 | iPhone 8 | ● | ● | ● | ● |
| CYW20819 | CYW920819EVB-02 | ● | ● | ● | ● |
| Intel 9560 | ThinkPad L390 | ● | ● | ● | ● |
| Snapdragon 630 | Nokia 7 | ● | ● | ● | ● |
| Snapdragon 636 | Nokia X6 | ● | ● | ● | ● |
| Snapdragon 835 | Pixel 2 | ● | ● | ● | ● |
| Snapdragon 845 | Pixel 3, OnePlus 6 | ● | ● | ● | ● |
| *Bluetooth v4.2* | | | | | |
| Apple 339S00056 | MacBookPro 2017 | ● | ● | ● | ● |
| Apple 339S00199 | iPhone 7plus | ● | ● | ● | ● |
| Apple 339S00448 | iPad 2018 | ● | ● | ● | ● |
| CSR 11393 | Sennheiser PXC 550 | ● | ● | - | - |
| Exynos 7570 | Galaxy J3 2017 | ● | ● | - | - |
| Intel 7265 | ThinkPad X1 3rd | ● | ● | - | - |
| Intel 8260 | HP ProBook 430 G3 | ● | ● | - | - |
| *Bluetooth v4.1* | | | | | |
| CYW4334 | iPhone 5s | ● | ● | - | - |
| CYW4339 | Nexus 5, iPhone 6 | ● | ● | - | - |
| CYW43438 | RPi 3B+ | ● | ● | ● | ● |
| Snapdragon 210 | LG K4 | ● | ● | ● | ● |
| Snapdragon 410 | Motorola G3, Galaxy J5 | ● | ● | ● | ● |
| *Bluetooth v≤ 4.0* | | | | | |
| BCM20730 | ThinkPad 41U5008 | ● | ○ | - | - |
| BCM4329B1 | iPad MC349LL | ● | ● | - | - |
| CSR 6530 | PLT BB903+ | ● | ● | - | - |
| CSR 8648 | Philips SHB7250 | ● | ● | - | - |
| Exynos 3470 | Galaxy S5 mini | ● | ● | - | - |
| Exynos 3475 | Galaxy J3 2016 | ● | ● | - | - |
| Intel 1280 | Lenovo U430 | ● | ● | - | - |
| Intel 6205 | ThinkPad X230 | ● | ● | - | - |
| Snapdragon 200 | Lumia 530 | ● | ● | - | - |

TABLE III: BIAS evaluation results. For each of the 28 Bluetooth chips tested, the table shows if the chip is vulnerable (●)

Figura 35

SweynTooth[177] es una familia de doce (12) vulnerabilidades en implementaciones de Bluetooth, concretamente BLE, que fue publicada en febrero de 2020, y que afectaban a los System-on-Chip (SoC) de múltiples fabricantes de la industria, ampliamente utilizados en dispositivos IoT (Internet of Things) y/o periféricos utilizados por dispositivos móviles. Posteriormente, en julio de 2020 se publicó la segunda ola de vulnerabilidades de SweynTooth, que incluía cinco (5) nuevas vulnerabilidades que permiten evitar el proceso de autentificación, DoS, corrupción de memoria, etc.

Otras vulnerabilidades de Bluetooth publicadas a lo largo del año 2020 y que también afectan a dispositivos móviles incluyen BlueRepli[178] (analizada a continuación), y vulnerabilidades de BLE, incluso de ejecución remota de código (RCE), en firmwares de chips Bluetooth de diferentes fabricantes empleados habitualmente en periféricos a los que se conectan los dispositivos móviles, al analizar el comportamiento por debajo de la capa HCI (Host Controller Interface) de Bluetooth, similares a vulnerabilidades previas como BleedingBit[179], ambas presentadas en la conferencia Black Hat USA en agosto de 2020.

**177.** "SweynTooth: Unleashing Mayhem over Bluetooth Low Energy". Matheus E. Garbelini, Chundong Wang, Sudipta Chattopadhyay, Sumei Sun, and Ernest Kurniawan. ASSET SUTD. Feb/Jul 2020. URL: https://asset-group.github.io/disclosures/sweyntooth/

**178.** "Stealthily Access Your Android Phones: Bypass the Bluetooth Authentication". BlackHat USA 2020. URL: https://www.blackhat.com/us-20/briefings/schedule/#stealthily-access-your-android-phones-bypass-the-bluetooth-authentication-19993 URL: https://www.youtube.com/watch?v=6J3weqoiads

**179.** "Finding New Bluetooth Low Energy Exploits via Reverse Engineering Multiple Vendors' Firmwares". BlackHat USA 2020. URL: https://www.blackhat.com/us-20/briefings/schedule/#finding-new-bluetooth-low-energy-exploits-via-reverse-engineering-multiple-vendors-firmwares-19655 URL: https://www.youtube.com/watch?v=vdEoQgTP0H4

BlueRepli (o Bluetooth Replicant) permite explotar en Android dos nuevas formas de evitar los mecanismos de autorización de Bluetooth (incluyendo un 0-day que afectaba a un fabricante conocido con potencialmente 100 millones de dispositivos móviles afectados) para disponer de acceso a los perfiles más sensibles, como PBAP, MAP o SAP. Como resultado, es posible explotar las vulnerabilidades a través de una única interacción con el dispositivo móvil Android víctima para robar información de los contactos del usuario, histórico de llamadas, códigos SMS de 2FA, o incluso realizar el envío de SMS suplantándolo.

Técnicamente el ataque se centra en manipular el proceso de emparejamiento de Bluetooth, para que no se muestre la petición de PIN al usuario, y el proceso de petición de autorización al usuario para el acceso a un perfil.

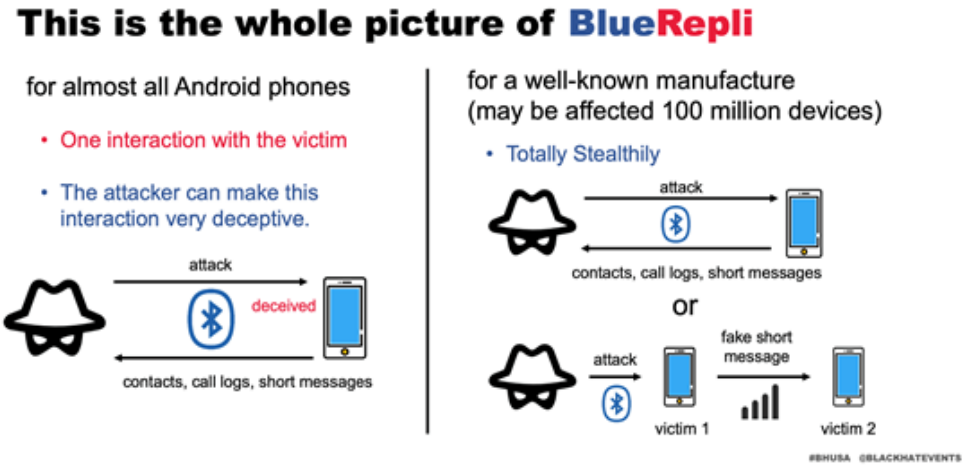
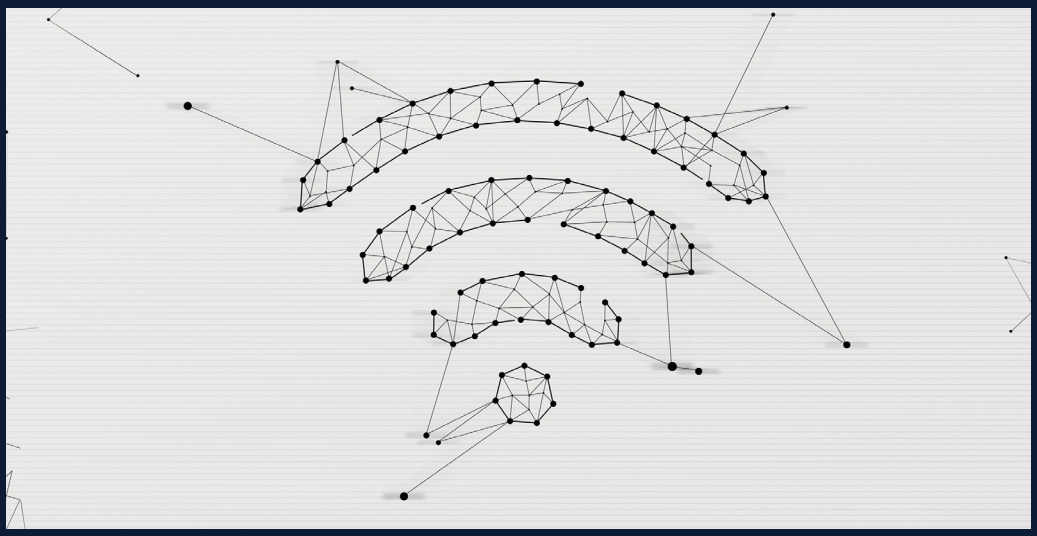



Figura 36

Estas se unen a vulnerabilidades previas publicadas en el NDSS Symposium en febrero de 2019 y no mencionadas en informes anuales anteriores, debido al ingente número de fallos de seguridad tecnológicos reportados cada año, como BadBluetooth[180]. BadBluetooth permite evitar los mecanismos de seguridad de Android a través de periféricos Bluetooth maliciosos, como un teclado o ratón o manos libres, que al cambiar su perfil de Bluetooth (de manera similar a ataques pasados como DirtyTooth en iOS) se le asignan mecanismos de autentificación y autorización diferentes, o establece relaciones de confianza sin que se notifique al usuario del cambio. El estudio mostraba tres (3) tipos de ataques contra múltiples versiones de Android, desde Android 5.1 hasta 8.1, que permitían evitar las protecciones de permiso y aislamiento de Android, ejecutar ataques de MitM, controlar las apps del usuario víctima, exfiltrar información, etc.

**180.** "BadBluetooth: Breaking Android Security Mechanisms via Malicious Bluetooth Peripherals" University of Hong Kong. NDSS Symposium. Feb 2019. URL: https://www.ndss-symposium.org/ndss-paper/badbluetooth-breaking-android-security-mechanisms-via-malicious-bluetooth-peripherals/



Desde el punto de vista de las tecnologías inalámbricas Wi-Fi, durante el año 2020 el mercado de productos y dispositivos con soporte para WPA3 (Wireless Protected Access 3) se ha consolidado, disponiéndose de soporte ampliado para WPA3 dentro del ecosistema móvil, más concretamente, en Android 11 e iOS 14. Aunque el estándar de seguridad de referencia más moderno sigue siendo WPA3, desde el año 2018, la Wi-Fi Alliance continúa evolucionando el mismo, y ampliando la planificación o *roadmap* de actualizaciones de seguridad, anunciado en diciembre de 2020, con una larga lista de nuevas capacidades[181], destacando la introducción de la validación de certificados en los métodos de autentificación EAP (SCV, Server Certificate Validation) de 2019[182], o un nuevo método de autentificación SAE Public Key (SAE-PK) en 2020, entre muchas otras novedades futuras. Las nuevas tecnologías Wi-Fi con mayor ancho de banda, como Wi-Fi 6 (802.11ax) o 6E (6 GHz) deberán hacer uso de las últimas capacidades de seguridad de WPA3 y Wi-Fi Enhanced Open, sin modos de transición a mecanismos de seguridad antiguos y más inseguros.

Wi-Fi 6 está soportado por numerosos dispositivos móviles[183] Android actualmente, como el Huawei P40 Pro, One Plus 8(Pro) o los Samsung Galaxy S10, Note 10, S20 y S21 (y variantes), y en iOS a partir del iPhone 11 (y variantes) en adelante, y el iPhone SE de 2ª generación (2020). Sin embargo, los dispositivos Pixel 5 y Pixel 4a 5G de Google. anunciados en octubre de 2020, no disponen de soporte para Wi-Fi 6. Adicionalmente, Samsung ha sido el primer fabricante en comercializar un dispositivo móvil en enero de 2021 con soporte para Wi-Fi 6E, empleando el rango de 6 GHz, el Samsung Galaxy S21 Ultra[184], basado en un chip de Broadcom.

Android 11 (al igual que Android 10) proporciona soporte para WPA3 personal (SAE, Simultaneous Authentication of Equals) y empresarial (modo 192 bits) y para Wi-Fi Enhanced Open (OWE, Opportunistic Wireless Encryption), incluyendo el modo de transición de WPA2 a WPA3 y de redes abiertas a OWE[185].

---

**181.** "Wi-Fi Alliance® Wi-Fi® Security Roadmap and WPA3TM Updates". Wi-Fi Alliance. Dec 2020. URL: https://www.wi-fi.org/download.php?file=/sites/default/files/private/202012_Wi-Fi_Security_Roadmap_and_WPA3_Updates.pdf

**182.** "Why iOS (Android & others) Fail inexplicably". Raúl Siles. DinoSec. RootedCON. 2013. URL: https://www.dinosec.com/en/lab.html#Rooted2013WiFi

**183.** https://www.techietech.tech/wi-fi-6-compatible-smartphones/

**184.** https://wifinowglobal.com/news-and-blog/wi-fi-6e-era-begins-samsung-releases-worlds-first-6-ghz-wi-fi-smartphone/

**185.** https://source.android.com/devices/tech/connect/wifi-wpa3-owe

Adicionalmente, Google, en Android 11 y con la actualización de seguridad de diciembre de 2020 (al menos para los Pixels), realizó un cambio en las capacidades de conexión a redes Wi-Fi empresariales, WPA2 o WPA3[186]. La opción insegura existente con anterioridad en los perfiles Wi-Fi empresariales de Android que permitía no validar el certificado del servidor RADIUS ha sido eliminada y, en consecuencia, todos los dispositivos móviles que hacían uso de redes Wi-Fi empresariales con certificados digitales no válidos no podrán conectarse a estas[187].

Con respecto al soporte de WPA3, los dispositivos móviles de Apple siguen sin proporcionar soporte para Wi-Fi Enhanced Open en iOS 14 (al igual que en iOS 13), y se dispone de soporte para WPA3 personal y empresarial desde el iPhone 7 y el iPad de 5ª generación. Los nuevos dispositivos a partir del iPhone 11 (y variantes) también proporcionan soporte para WPA3 empresarial de 192 bits de seguridad[188].

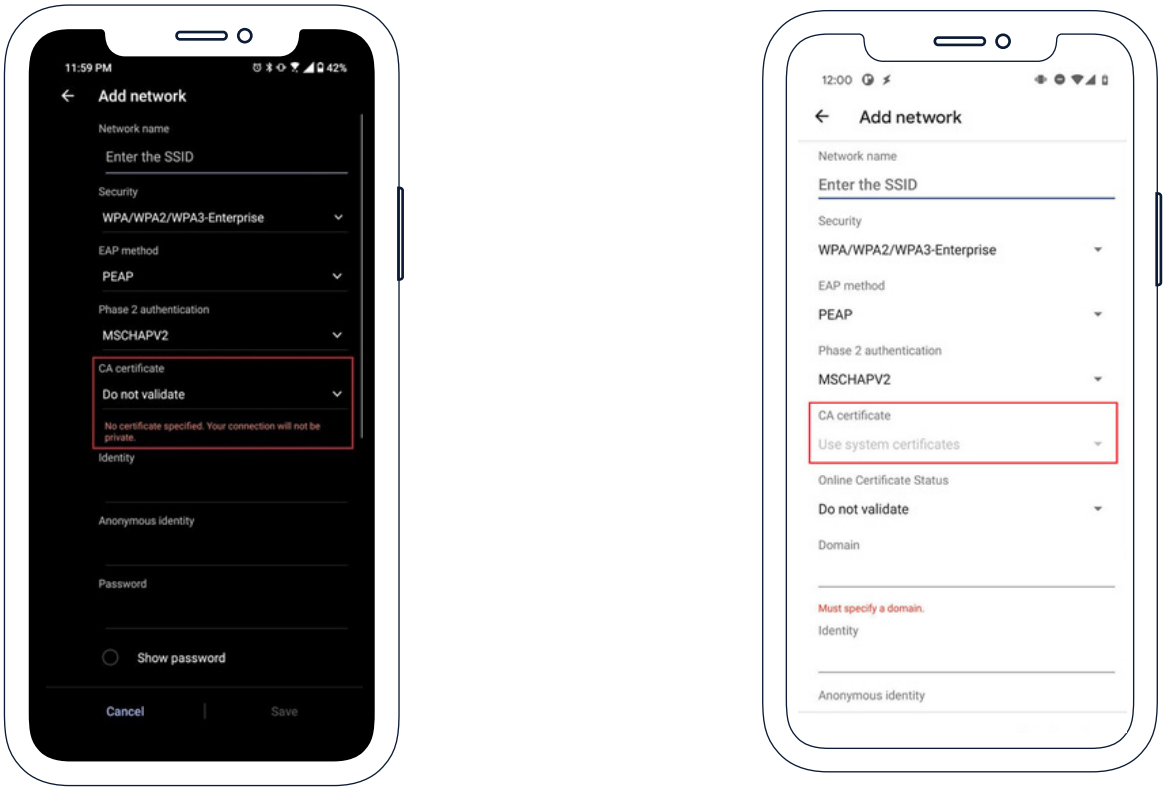



Figura 37

**186.** "PSA: Android 11 will no longer let you insecurely connect to enterprise WiFi networks". XDA Developers. Jan 2021. URL: https://www.xda-developers.com/android-11-break-enterprise-wifi-connection/ URL: https://www.securew2.com/blog/android-11-server-certificate-validation-error-solution/

**187.** "Wi-Fi Alliance® Wi-Fi® Security Roadmap and WPA3TM Updates". Wi-Fi Alliance. Dec 2020. URL: https://www.wi-fi.org/download.php?file=/sites/default/files/private/202012_Wi-Fi_Security_Roadmap_and_WPA3_Updates.pdf

**188.** "Protocol Security". Apple Platform Security. Apple. Feb 2021. URL: https://support.apple.com/guide/security/protocol-security-sec8a67fa93d/web

Adicionalmente, iOS 14 es más estricto desde el punto de vista de la seguridad Wi-Fi y refleja algunas redes Wi-Fi con "Weak Security", o seguridad débil, al confirmar que hacen uso de protocolos de seguridad antiguos, como WPA/WPA2-TKIP. Asimismo, en iOS/iPadOS 14 y watchOS 7 se dispone de una nueva característica de privacidad Wi-Fi en la que los dispositivos móviles hacen uso por defecto de una dirección MAC aleatoria diferente cada vez que se conectan a una nueva red Wi-Fi[189], no únicamente en las actividades de escaneo en busca de redes Wi-Fi[190]. Para evitar el potencial seguimiento de los usuarios (*tracking*), en lugar de usar la misma dirección MAC para conectarse a todas las redes Wi-Fi, iOS 14 emplea una dirección MAC diferente (estática y privada) para cada red Wi-Fi. Esta funcionalidad puede ser deshabilitada por el usuario para hacer uso de la dirección MAC real del interfaz Wi-Fi del dispositivo móvil.


En febrero de 2020, durante la conferencia RSA, se publicó la vulnerabilidad conocida como kr00k por parte de ESE[191], identificada por el CVE-2019-15126, que afectaba a los chipsets Wi-Fi de Broadcom y Cypress, por lo que aplicaba a ciertos dispositivos móviles iOS y iPadOS de Apple, Nexus de Google, Galaxy de Samsung, Redmi de Xiaomi, etc., y permitía descifrar parte del tráfico protegido por WPA2/CCMP.


Figura 38

Por ejemplo, en el caso de iOS y iPadOS la vulnerabilidad fue resuelta en la versión 13.2 de iOS. En cierto sentido, esta vulnerabilidad tenía relación con la vulnerabilidad de KRACK (Key Reinstallation Attacks) descubierta en 2017, ya que el forzar una desasociación de la red Wi-Fi de los dispositivos vulnerables, hace que estos hagan uso de una clave criptográfica con valor cero, lo que permite a un atacante descifrar el tráfico intercambiado por la víctima con tan solo capturar la señal Wi-Fi asociada al mismo.

**189.** "Apple Platform Security - February 2021". Apple. Feb 2021. URL: https://support.apple.com/guide/security/welcome/web URL: https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf
**190.** "Use private Wi-Fi addresses in iOS 14, iPadOS 14, and watchOS 7". Apple. URL: https://support.apple.com/en-us/HT211227
**191.** "Kr00K". ESET. Feb 2020. URL: https://www.eset.com/afr/kr00k/ URL: https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf

Al desasociar el dispositivo de la red se elimina el valor de la clave de sesión que estaba siendo utilizada (medida intencionada para proteger el valor previo), pero el problema reside en que si aún existían tramas por intercambiar en el buffer de transmisión del chip estas son enviadas con la nueva clave conocida, es decir, una clave con valor cero.

Posteriormente, en agosto de 2020 durante la conferencia Black Hat USA, se confirmó que vulnerabilidades similares afectaban a más chips y fabricantes de los identificados inicialmente, incluyendo Qualcomm y MediaTek[192].

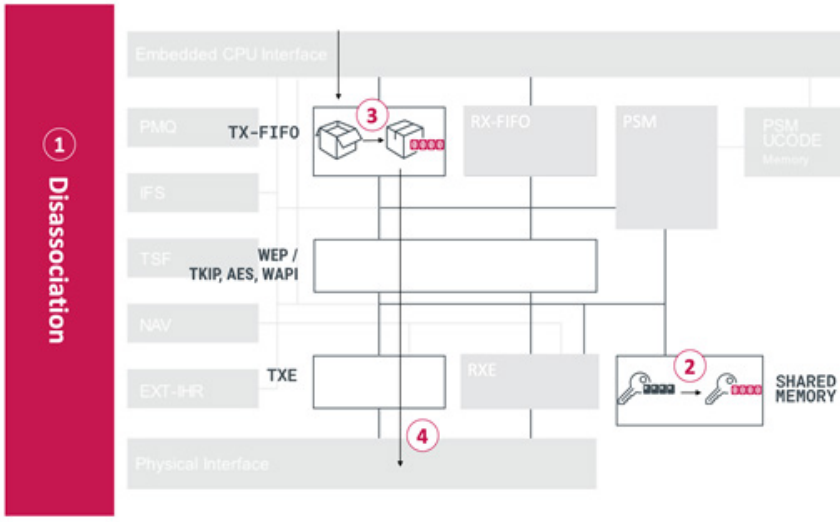



Figure 1 // Kr00k causes transmission of data encrypted with an all-zero key

Figura 39

**192.** https://www.welivesecurity.com/2020/08/06/beyond-kr00k-even-more-wifi-chips-vulnerable-eavesdropping/

Complementando las vulnerabilidades Wi-Fi en dispositivos móviles previas, a finales del año 2020 se publicaron tres (3) vulnerabilidades asociadas a tres (3) fabricantes móviles diferentes y, en concreto, a sus funcionalidades de compartición de fich eros de manera inalámbrica vía Wi-Fi o P2P (Peer-to-Peer), como extensión o personalizaciones propietarias del estándar Wi-Fi Direct[193], utilizado junto a UPnP. Las soluciones afectadas eran Huawei Share, LG SmartShare Beam y Xiaomi Mi Share, siendo posible, una vez se establece la conexión Wi-Fi P2P, que cualquier app local maliciosa pudiera hacer uso de dicho interfaz inalámbrico para interactuar tanto con el componente local como con el remoto (FTC, File Transfer Controller o Client, y FTS, File Transfer Server).

En el caso de Huawei Share el servicio es muy inestable, por lo que es posible abortar su ejecución de forma sencilla con múltiples peticiones HTTP por ejemplo por parte de una app local maliciosa, dando lugar a denegaciones de servicio. Este escenario puede ser empleado adicionalmente para suplantar el servicio que ha interrumpido su ejecución, y recibir las peticiones del otro extremo, incluyendo los identificadores de sesión, y secuestrando las transferencias de ficheros.

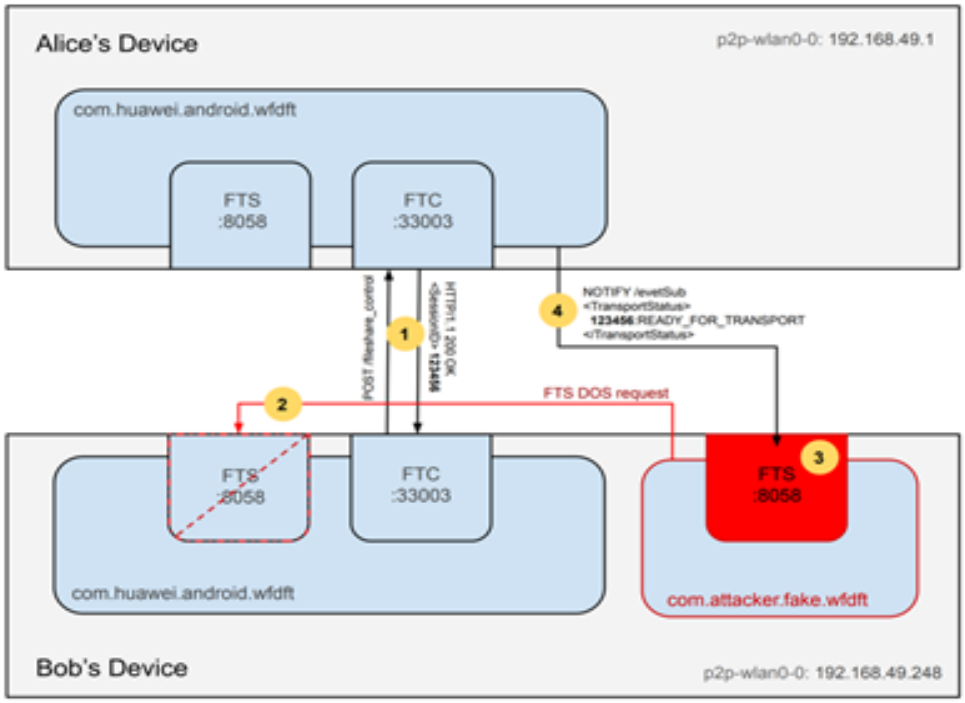



Figura 40

**193.** "Novel Abuses On Wi-Fi Direct Mobile File Transfers". Doyensec. Dec 2020. URL: https://blog.doyensec.com/2020/12/10/novel-abuses-wifi-direct-mobile-file-transfers.html

En el caso de LG SmartShare Beam no se requiere de autentificación (en forma de un identificador de sesión, aunque estos también son fácilmente adivinables, con valores entre 1 y 100) para enviar el fichero. Además, es posible modificar el nombre y el tipo de fichero respecto a los valores mostrados al usuario, y se pueden enviar varios ficheros simultáneamente sin confirmación del usuario.

En el caso de Xiaomi Mi Share, disponible desde MIUI 11, y compatible con la funcionalidad de la Peer-to-Peer Transmission Alliance (PPTA), incluyéndose capacidades de seguridad más avanzadas como certificados TLS por sesión, por tanto, compatible con fabricantes con más de 400 millones de usuarios en conjunto.

Es posible manipular el tamaño de los ficheros enviados por el remitente a través de WebSockets, con un valor pequeño, para posteriormente remitir un fichero de gran tamaño y causar una denegación de servicio (DoS) en el almacenamiento del dispositivo móvil receptor, así como potencialmente adivinar identificadores de sesión por su baja entropía (aunque son de 19 dígitos), y ejecutar DoS en la ejecución del servicio por parte de una app local maliciosa.

# 11. Comunicaciones móviles

El despliegue de las tecnologías 5G sigue su curso y a lo largo del año 2020 y 2021 las redes de los operadores de telefonía móvil siguen evolucionando y ampliando su cobertura de 5G, despliegue que ha sido definido incluso en la hoja de ruta de España[194].

**194.** https://avancedigital.mineco.gob.es/5G/Paginas/Index.aspx

Al igual que para el caso de Wi-Fi 6 descrito en el apartado previo, -y habitualmente disponiéndose de soporte para ambos simultáneamente, Wi-Fi 6 y 5G, debido al SoC empleado por el dispositivo móvil- las tecnologías móviles 5G están soportadas por numerosos dispositivos móviles[195] Android actualmente, como el Xiaomi Mi 10(Pro), One Plus 8(Pro) y 8T, o los Samsung Galaxy S10, Note 10, Note 20, S20 y S21 (en sus variantes 5G), y en iOS a partir del iPhone 12 (y variantes) en adelante.

En agosto de 2020, durante la conferencia USENIX de seguridad, se presentaba ReVoLTE[196], una investigación que desvelaba la posibilidad de capturar y acceder a llamadas LTE cifradas con recursos reducidos por parte de un potencial atacante. Los investigadores de la universidad de Ruhr en Bochum y NYU Abu Dhabi, ya mencionados en el informe anual de 2018[197] por la vulnerabilidad aLTEr, profundizaban en las debilidades en el uso de Voice over LTE (VoLTE) para el establecimiento de llamadas de voz en redes de telefonía móvil mediante paquetes, ampliamente utilizado y estandarizado en la industria, y en consecuencia, con millones de potenciales usuarios afectados.

ReVoLTE explota una vulnerabilidad en la implementación de LTE para recuperar los contenidos de las llamadas de voz cifradas, aprovechándose de una debilidad criptográfica asociada a la reutilización de un *keystream* predecible en la capa de radio.

Ese *keystream* es utilizado mediante una operación XOR para el cifrado del tráfico, y si es reutilizado, la operación XOR de dos flujos cifrados, conocido uno de ellos, permite obtener el texto en claro del otro.

---

**195.** https://www.techietech.tech/wi-fi-6-compatible-smartphones/
**196.** "Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE". USENIX 29th. Aug 2020. URL: https://www.usenix.org/conference/usenixsecurity20/presentation/rupprecht URL: www.revolte-attack.net
**197.** "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

El estudio analiza la viabilidad de lanzar este tipo de ataques con éxito en las redes comerciales LTE ya desplegadas. De los 15 nodos o estaciones base (eNodeBs) analizados, 12 de ellos reutilizaban el mismo *keystream*. Los investigadores publicaron una app móvil para Android, denominada Mobile Sentinel, que requiere disponer de un dispositivo Android rooteado, para que los usuarios puedan verificar el estado de las redes LTE a las que se conectan respecto a la vulnerabilidad ReVoLTE[198].

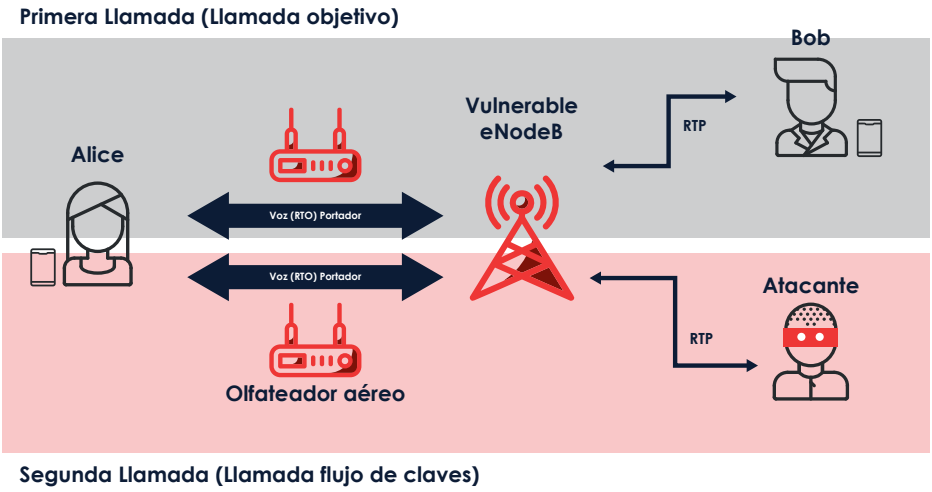
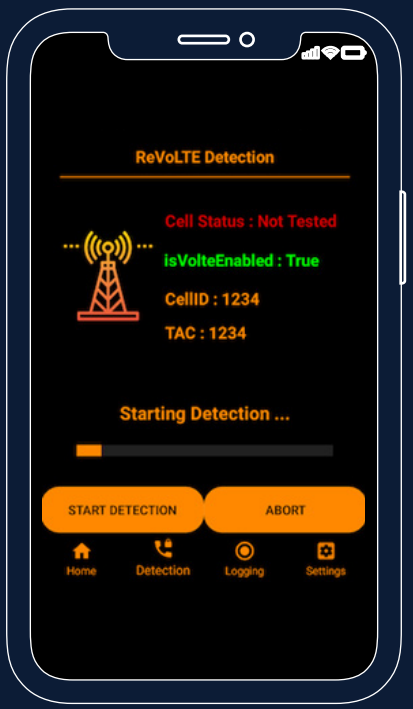



Figura 41

Los ataques IMP4GT (IMPersonation Attacks in 4G NeTworks), publicados en el NDSS Symposium en febrero de 2020 de nuevo por los investigadores del ataque ReVoLTE previo, combinan un ataque entre diferentes capas de LTE/4G, explotando una vulnerabilidad existente en la capa 2 (aLTEr, del año 2019) y extendiéndola a la capa 3[199]. En LTE/4G existen mecanismos de autentificación mutua entre el usuario y la red, para que ambos puedan verificar sus identidades, basados en un mecanismo de autentificación probado (*provably secure*) y un protocolo de intercambio de clave (*key agreement*) en el plano de control.




**198.** "Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE". USENIX 29th. Aug 2020. URL: https://www.usenix.org/conference/usenixsecurity20/presentation/rupprecht URL: www.revolte-attack.net

**199.** "IMP4GT: IMPersonation Attacks in 4G NeTworks". NDSS Symposium. Feb 2020. URL: https://imp4gt-attacks.net URL: https://www.ndss-symposium.org/ndss-paper/imp4gt-impersonation-attacks-in-4g-networks/

Estas protecciones de integridad existentes en el plano de control protegen el tráfico frente a manipulaciones. La ausencia de ese tipo de protecciones de integridad en el plano de usuario permite sin embargo a un potencial atacante manipular y redireccionar paquetes IP, como se describía en el informe anual de 2018[200] en relación a la vulnerabilidad aLTEr. Debido al comportamiento de las pilas TCP/IP de los sistemas operativos de los dispositivos móviles actuales, en concreto a un mecanismo de reflexión, es posible extender este ataque a la capa 3, lo que permite a un atacante suplantar a un usuario frente a la red, y viceversa.

La posibilidad de inyectar y de descifrar paquetes permite a un atacante realizar suplantaciones en ambas direcciones, uplink y downlink.

En uplink, el atacante puede hacerse pasar por una víctima de cara a la red, pudiendo hacer uso de servicios con la identidad de la víctima (servicios que hacen uso de mecanismos de autentificación en función de la dirección IP del usuario en la red móvil), ya que todo el tráfico que genera se asocia a la dirección IP de la víctima. En downlink, el atacante puede establecer conexiones TCP/IP al teléfono de la víctima evitando los cortafuegos de la red LTE, y tanto enviar como recibir paquetes del dispositivo móvil víctima. El estudio analiza para Android y para iOS la viabilidad de los ataques de reflexión tanto en IPv4 como en IPv6, con los siguientes resultados:

| Vulnerable | iOS | Android |
|---|---|---|
| IPv4 | no | yes |
| IPv6 | yes | yes |

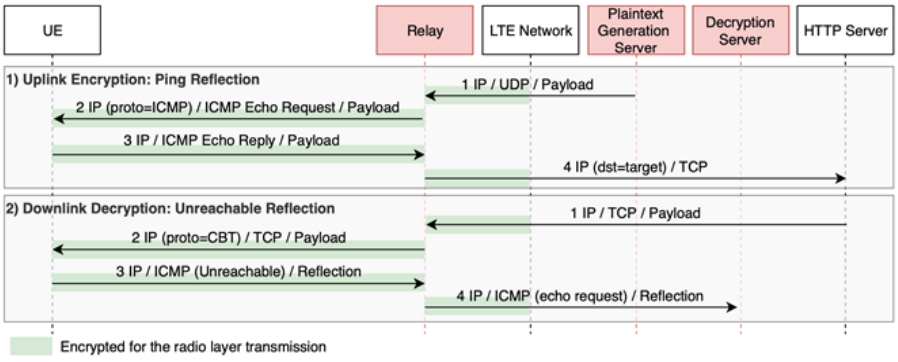



Fig. 7. The uplink IMP4GT attack consists of uplink encryption exploiting the ping reflection and the downlink decryption based on the unreachable reflection.

Figura 42

**200.** "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

Como resultado del estudio, se concluye que los operadores de telefonía no pueden basar su proceso de facturación, u otros mecanismos de autentificación y autorización, confiando en los mecanismos de autentificación mutua. La posibilidad de suplantación de la dirección IP del usuario en la red móvil también puede tener implicaciones en procedimientos legales e investigaciones.

Asimismo, como se ha comentado, los usuarios de las redes de telefonía móvil podrían recibir conexiones entrantes ya que un atacante podría evitar los cortafuegos del operador, lo que abre la puerta a la explotación de otras vulnerabilidades sobre apps o el sistema operativo móvil a nivel de red. El estudio, de nuevo, analiza la viabilidad de lanzar este tipo de ataques con éxito en las redes comerciales LTE/4G ya desplegadas, y en redes 5G iniciales.

Con respecto a las redes 5G, las redes NSA (Non-standalone) son también vulnerables, ya que, aunque se soportan mecanismos de protección de la integridad en el plano de usuario en las redes 5G, no son utilizados en las redes 5G NSA con conectividad dual donde se emplea 4G para los datos de control y 5G para los datos de usuario. En el caso de las redes 5G SA (Standalone), el uso de las protecciones de integridad en el plano de usuario es opcional, por lo que este vector de ataque sería potencialmente explotable. Posteriormente, en julio de 2020, se anunciaba en la *release* 16 de 5G la obligatoriedad de que los dispositivos móviles 5G soporten las protecciones de integridad en el plano de usuario para cualquier velocidad o ratio de transmisión, *full-rate integrity protection*, pero no obligan a que la utilicen[201]. Queda por tanto en mano de los operadores de telefonía habilitar estas capacidades independientemente del impacto que puedan tener en el rendimiento y ancho de banda de las redes 5G. En caso contrario, las vulnerabilidades aLTEr y IMP4GT seguirán estando presentes.

**201.** https://davidrupprecht.github.io/nianullblog/5g/integrity_protection/2020/07/08/5G_full_rate_UPIP_support.html

El conocido investigador de seguridad en entornos móviles Ravishankar Borgaonkar publicaba en agosto de 2019 nuevas vulnerabilidades en la arquitectura de seguridad de 5G[202], y sus contramedidas asociadas, incluyendo dos vulnerabilidades del protocolo que permiten la posibilidad de obtener información de los dispositivos y lanzar ataques de identificación por parte de estaciones base falsas, y afectar la batería de los dispositivos, y una vulnerabilidad de implementación en la fase de registro de los dispositivos (ya mencionadas en el informe anual de 2019[203]). Este análisis constituyó la base para una nueva publicación del mismo investigador centrada en los problemas de las estaciones base falsas en 5G[204].

Los IMSI catchers (o estaciones base falsas) permiten identificar y seguir los dispositivos móviles de los usuarios o suscriptores, en base a diferentes identificadores permanentes, como el IMSI o el IMEI. Las tecnologías 5G incorporan contramedidas frente a este tipo de actividades, protegiendo el SUPI (equivalente al IMSI en redes 2/3/4G) mediante el SUCI. Desafortunadamente, la protección del SUPI mediante esquemas de criptografía de curva elíptica sólo aplica a redes 5G SA (StandAlone), por lo que las redes 5G NSA seguirán estando afectadas por estas actividades contra la privacidad del usuario.

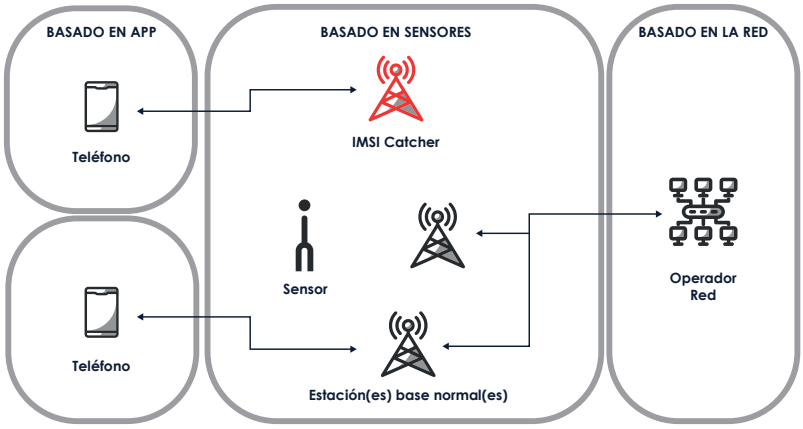



Figura 43

La nueva publicación reflexionaba sobre la viabilidad de los IMSI catchers en redes 5G, concretamente dispositivos comerciales, así como sobre las nuevas capacidades de detección de este tipo de celdas falsas por parte de los dispositivos móviles, en base al framework disponible específicamente para este propósito en 5G, concluyéndose que no será hasta el momento que se disponga de un despliegue completo de 5G SA cuando realmente existan protecciones efectivas frente a estos ataques.

Desde el punto de vista de seguridad y privacidad, la tecnología 5G sigue siendo una de las áreas de mayor interés y más relevantes en la actualidad, un papel que todavía se ha enfatizado más con la pandemia sanitaria a lo largo del año 2020, la adopción masiva y vertiginosa de modelos de teletrabajo, y las necesidades crecientes de conectividad para mejorar la productividad.

**202.** "New vulnerabilities in 5G Security Architecture & Countermeasures (Part 1)". Ravishankar Borgaonkar. Aug 2019. URL: https://infosec.sintef.no/en/informasjonssikkerhet/2019/08/new-vulnerabilities-in-5g-security-architecture-countermeasures/

**203.** "CCN-CERT IA-03/20: Informe Anual 2019 - Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html

**204.** "Hacking 5G Network Infrastructure – IMSI catchers and hackathon". Ravishankar Borgaonkar. Apr 2020. URL: https://infosec.sintef.no/en/informasjonssikkerhet/2020/04/hacking-5g-network-infrastructure-imsi-catchers-and-hackathon/

Por este motivo, ENISA publicó en diciembre de 2020 un amplio informe de amenazas de 5G[205] (de más de 250 páginas), complementando la primera edición de este informe ya publicada en diciembre de 2019[206].

Posteriormente, en febrero de 2021 publicó también un informe de los controles de seguridad en 3GPP, con el objetivo de afrontar la ciberseguridad en las redes 5G[207]. Ambos informes se analizan a continuación.

En relación a las versiones de las especificaciones técnicas de 5G de la 3GPP, la reléase 16 (mencionada previamente) se publicó en julio de 2020, y ENISA (en los informes mencionados) destaca la evolución y los plazos de las siguientes releases:

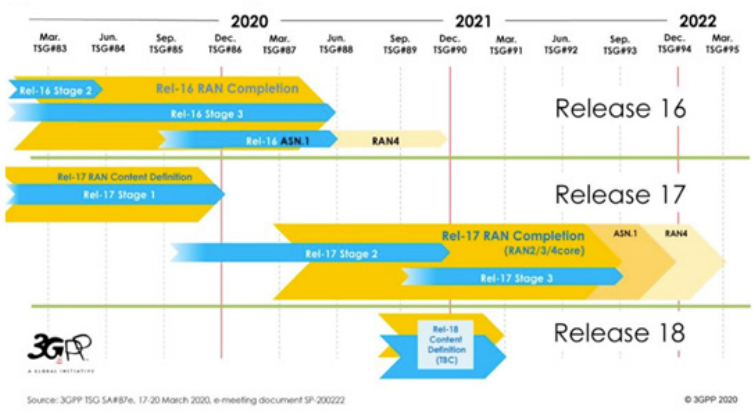



Figura 44. Cronología de las versiones de la especificación 3GPP

ENISA (European Union Agency for Cybersecurity), como organismo de referencia de ciberseguridad en la Unión Europea (UE) actualizaba su informe de amenazas con una segunda edición en la que evaluaba todas las novedades del año 2020, los nuevos desarrollos en las arquitecturas 5G, y los avances relativos al análisis de vulnerabilidades y amenazas que afectarán a las nuevas versiones de estas tecnologías.

**205.** "ENISA Threat Landscape for 5G Networks Report". ENISA. Dec 2020. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

**206.** https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

**207.** "Security in 5G Specifications - Controls in 3GPP". ENISA. Feb 2021. URL: https://www.enisa.europa.eu/publications/security-in-5g-specifications URL: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-for-5g-enisa-releases-report-on-security-controls-in-3gpp

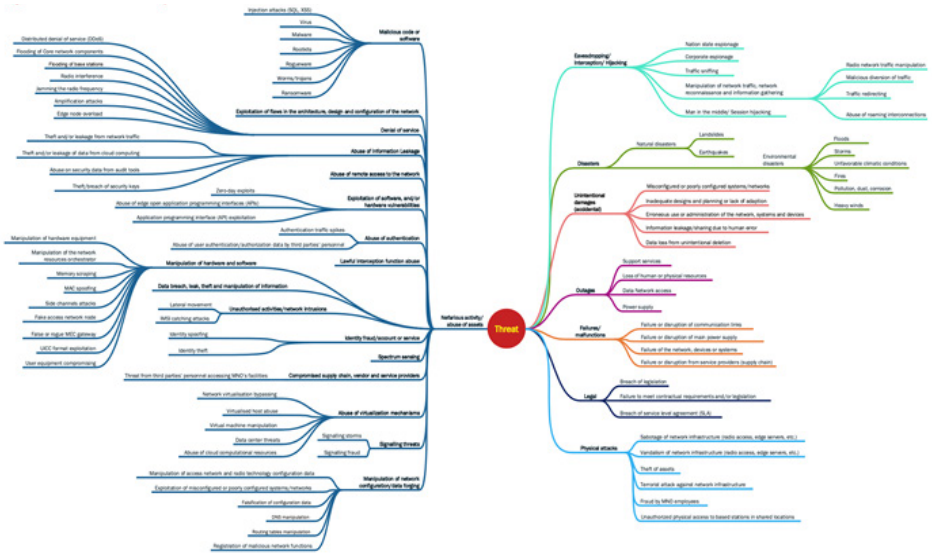



Figura 45. Taxonomía de la amenaza 5G

Complementariamente, el segundo informe[208] (englobado dentro del programa o estrategia digital conocida como "EU Toolbox for 5G security"[209] y, más concretamente, en la medida técnica TM02) profundiza en esos controles de seguridad de aplicación a las tecnologías y redes 5G, explicando las especificaciones técnicas de seguridad del 3GPP (incluyendo las características de seguridad opcionales), las buenas prácticas de la industria, y el papel y objetivo de cada control para obtener un nivel de seguridad global adecuado en 5G.

La seguridad de 5G se aborda desde múltiples puntos de vista, incluyendo el diseño de la red, el desarrollo de productos, su configuración y despliegue, las tareas de operación, mantenimiento y gestión, y las actividades de test, auditoría y evaluación.


Figura 46. Organizaciones de normalización relevantes para la seguridad de la 5G

**208.** "Security in 5G Specifications - Controls in 3GPP". ENISA. Feb 2021. URL: https://www.enisa.europa.eu/publications/security-in-5g-specifications URL: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-for-5g-enisa-releases-report-on-security-controls-in-3gpp

**209.** https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

Por petición de la Comisión Europea, dentro de los requisitos del Cybersecurity Act y del European Cybersecurity Certification Framework, en febrero de 2021 se anunciaba que ENISA sería el organismo encargado de las tareas de certificación de ciberseguridad de las redes 5G a nivel europeo[210] y de la preparación y coordinación de un esquema de certificación unificado, en colaboración con ciertos grupos de trabajo europeos como el European Cybersecurity Certification Group (ECCG), y con las agencias de certificación de los distintos países, como el OC-CCN[211] en España.

El esquema de certificación de ciberseguridad en 5G se basará en otros esquemas ya existentes, y en su adecuación a las tecnologías 5G, proporcionando detalles y confianza en las capacidades y características de seguridad de los productos y servicios asociados a 5G. Como resultado de esta unificación, España tendrá que adecuar su anteproyecto de Ley de Ciberseguridad 5G[212], presentado en diciembre de 2020, para que esté alineado con los avances a nivel europeo. El anteproyecto traslada a España las contramedidas contempladas en el Toolbox 5G europeo previamente mencionado para mitigar los riesgos de seguridad de las actuales y futuras infraestructuras 5G.

A lo largo del año 2020 se ha ampliado ligeramente el número de entradas en el Hall of Fame oficial de la GSMA[213], reconociendo las contribuciones de seguridad de diferentes investigadores, pero sin publicarse directamente los detalles asociados a las vulnerabilidades reportadas.

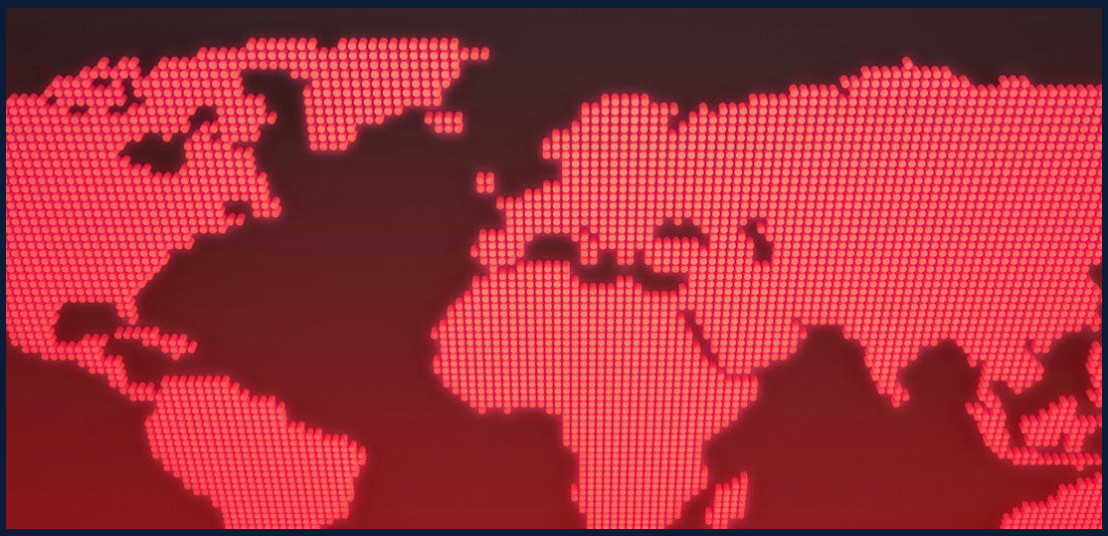
Dentro de las comunicaciones de las plataformas móviles, específicamente relacionadas con los servicios de mensajería, un año más se conoce la existencia de campañas de ataque, como el conocido bajo el nombre de "The Great iPwn", publicado por Citizen Lab[214]. La cadena de exploits empleada es conocida como KISMET, donde destaca un 0-day asociado a una vulnerabilidad en iMessage para iOS, al menos hasta la versión 13.5.1 y con posibilidad de éxito en el último iPhone 11 disponible en ese momento (como se mencionaba en el apartado "7. Mecanismos de seguridad avanzados en dispositivos móviles", el exploit parece haber sido mitigado en iOS 14 gracias a BlastDoor).

El análisis del incidente parece confirmar que otros ataques similares con KISMET ya se llevaron a cabo entre los meses de octubre y diciembre de 2019. Este hecho, junto a la amplia aplicación de estos exploits en las últimas versiones de iOS y últimos modelos hardware, hacen entrever que probablemente se hayan empleado en campañas de mucho mayor alcance, independientemente a este incidente, y que no han sido descubiertas.

En el caso de Android, y también en relación con las capacidades de mensajería, en este caso con los mensajes multimedia MMS, el equipo del Project Zero de Google publicaba en julio cinco (5) artículos técnicos, incluyendo vídeos con pruebas de concepto y ejemplos reales de la explotación, detallando la posibilidad de ejecutar código remoto en dispositivos móviles Samsung (en el vídeo de ejemplo, en un Galaxy Note 10+ con Android 10 y el nivel de parches de febrero de 2020) a través de un mensaje MMS malicioso sin la intervención del usuario.

---

**210.** "Securing EU's Vision on 5G: Cybersecurity Certification". ENISA. Feb 2021. URL: https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification
**211.** https://oc.ccn.cni.es
**212.** https://www.eleconomista.es/economia/noticias/11050301/02/21/Espana-tendra-que-alinear-los-criterios-de-su-Ley-de-Ciberseguridad-5G-con-el-esquema-que-la-Comision-Europea-ha-encargado-a-Enisa.html
**213.** https://www.gsma.com/security/gsma-mobile-security-hall-of-fame/
**214.** "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit". Citizen Lab. Dec 2020. URL: https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/



Esta vulnerabilidad 0-day (con CVE-2020-8899 y SVE-2020-16747, resuelta en mayo de 2020) afectaba al códec de imágenes Qmage propietario de Samsung[215]. Este ejemplo permite generalizar cómo este tipo de vulnerabilidades críticas remotas afectan tanto a iOS como a Android, y a diferentes fabricantes.

Es importante tener en cuenta que la lista de zero-days (o 0-days) acumulada a lo largo de los últimos meses y años sigue creciendo, encontrándose entre estas vulnerabilidades y exploits múltiples para iOS y Android (junto a otras tecnologías). De nuevo, desde el Project Zero de Google han creado en 2020 un proyecto público para poder hacer el seguimiento de los mismos y recopilar un repositorio de referencias, de cara a analizar tendencias, tiempos de respuesta, etc., y principalmente identificar las causas raíz de este tipo de vulnerabilidades de alto impacto (Root Cause Analyses), denominado "0-days In-the-Wild"[216].

El proyecto fue presentado también durante la BlackHat USA 2020, focalizándose en once (1)1 vulnerabilidades concretas, que han sido ampliadas posteriormente.

Por último, también en diciembre de 2020, Citizen Lab publicaba otro extenso informe sobre las actividades ofensivas de Circles, que explota vulnerabilidades en la infraestructura global de telefonía móvil para interceptar llamadas, mensajes (monitorizando los registros de los teléfonos o CDRs, Call Detail Records) y la ubicación de dispositivos móviles en todo el planet[217]. Circles parece estar afiliada a NSO Group, y a su infraestructura Pegasus (aunque la integración entre ambas soluciones parece que tiene algunas carencias[218]), y que indica igualmente que sus productos sólo se venden para gobiernos y estados.

---

**215.** "MMS Exploit Part 1: Introduction to the Samsung Qmage Codec and Remote Attack Surface". Google Project Zero. Jul 2020. URL: https://googleprojectzero.blogspot.com/2020/07/mms-exploit-part-1-introduction-to-qmage.html URL: https://www.youtube.com/watch?v=nke8Z3G4jnc

**216.** "0-days In-the-Wild". Google Project Zero. 2020. URL: https://googleprojectzero.github.io/0days-in-the-wild/ URL: https://www.blackhat.com/us-20/briefings/schedule/#reversing-the-root-identifying-the-exploited-vulnerability-in--days-used-in-the-wild-20308

**217.** "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles". Citizen Lab. Dec 2020. URL: https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

**218.** https://www.vice.com/en/article/ep48kp/nso-group-cyprus-circles-bulgaria-ss7

Los productos de Circles no atacan a los dispositivos móviles directamente, sino a las redes de telefonía móvil, pudiendo desplegarse en las infraestructuras de los operadores de telefonía locales.

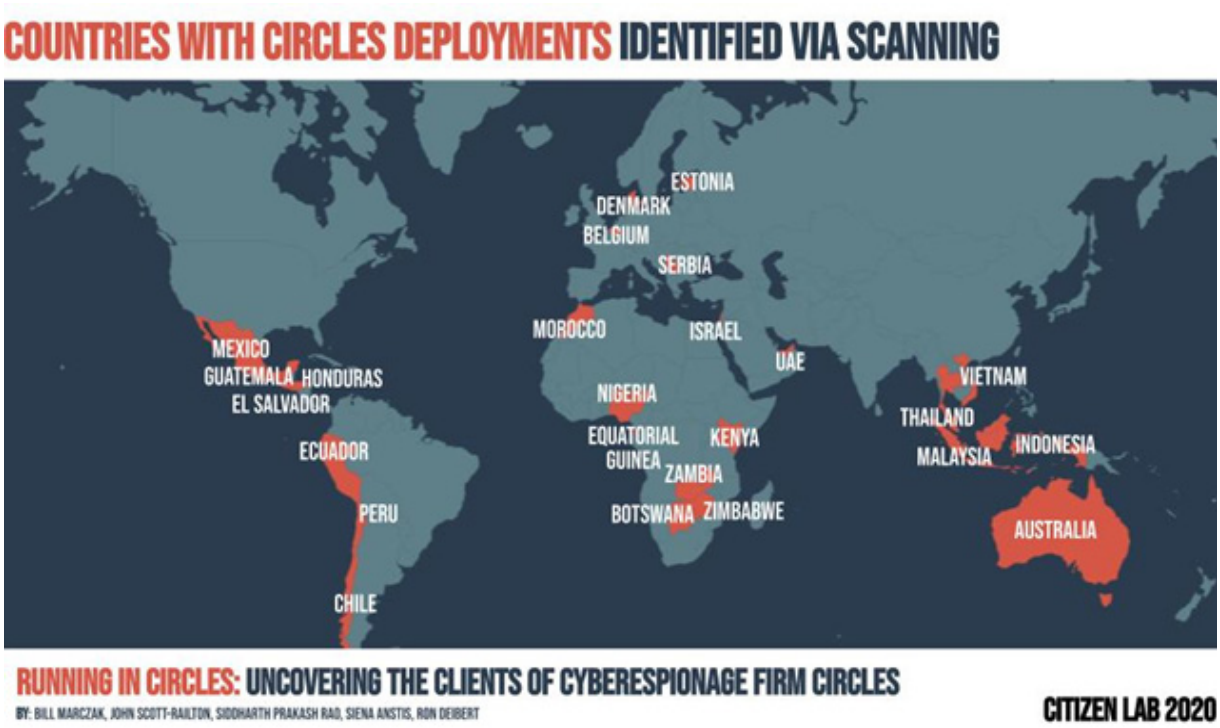


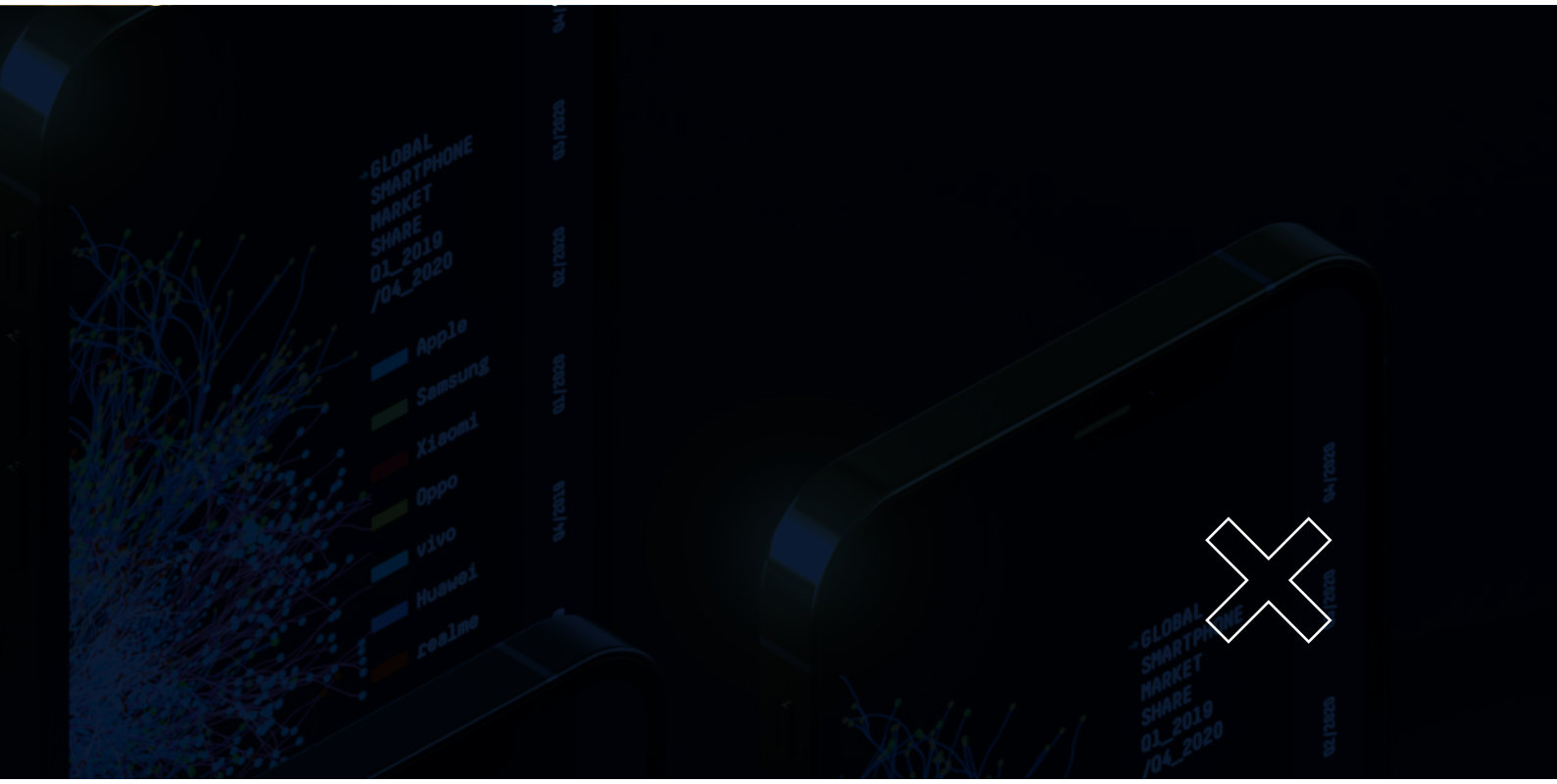

Figura 47

Los informes anuales de años pasados ya referenciaban las vulnerabilidades y ataques a la red de señalización y al protocolo SS7, empleados también por Circles en sus tecnologías ofensivas para las redes 2G y 3G, junto a Diameter en redes 4G. Circles tienen desplegada incluso a nivel mundial una infraestructura denominada "Circles Cloud" con acuerdos y capacidades de *roaming* entre operadores de diferentes países.


GLOBAL
SMARTPHONE
MARKET
SHARE
01_2019
/04_2020
Apple
Samsung
Xiaomi
Oppo
vivo
Huawei
realme
Others
GLOBAL
SMARTPHONE
MARKET
SHARE
01_2019
/04_2020
Apple
Samsung
Xiaomi
Oppo
vivo
Huawei
realme
Others


# 12. Tendencias para el año 2021

Dentro de las principales tendencias esperadas para el año 2021, será necesario confirmar la adopción más generalizada de redes Wi-Fi con WPA3, y también de redes basadas en Wi-Fi 6, ahora que tanto Android como iOS consolidan el soporte para estas capacidades de seguridad, y que futuros modelos proporcionarán soporte para Wi-Fi 6.




Sin embargo, Wi-Fi WPA 3 no acaba de ser ampliamente adoptado por la industria. También será relevante seguir la evolución del despliegue de las redes móviles e infraestructuras 5G, y en particular la migración de las actuales NSA a las futuras SA, progresando a una adopción generalizada de redes 5G nativas.

Respecto a los futuros avances y usos de los dispositivos móviles, Google continúa evolucionando la posibilidad de emplear el móvil como identificador electrónico (ID) universal, y su integración con diferentes apps, de manera similar al carnet de conducir[219]. Los avances en la estandarización de estas capacidades y de las apps asociadas, podrán extender su utilización a múltiples ámbitos, como podría ser el carnet de vacunación frente a la COVID-19, mencionado al final del presente apartado.

El transcurso del año 2021 confirmará el descubrimiento de nuevas vulnerabilidades 0-day y su utilización en el mundo real por parte de los atacantes en campañas dirigidas de espionaje, como ha ocurrido en todos estos años previos, una tendencia que no cesa debido a las vulnerabilidades y a la complejidad de las tecnologías móviles, y al desarrollo y evolución de nuevos ataques sofisticados aprovechando todas sus capacidades, ya sean las asociadas a la mensajería disponible por defecto, como iMessages o MMS, a las comunicaciones inalámbricas como Bluetooth o BLE, propias de infraestructuras distribuidas como la de rastreo de contactos de la COVID-19, y más aún, a las futuras capacidades y el despliegue de las nuevas infraestructuras y redes móviles 5G, sin por ello menospreciar las debilidades todavía presente en las infraestructuras de 4G/LTE, tan ampliamente utilizadas hoy en día.

**219.** "Privacy-preserving features in the Mobile Driving License". Google Security Blog. Oct 2020. URL: https://security.googleblog.com/2020/10/privacy-preserving-features-in-mobile.html

A este respecto, habrá que seguir muy de cerca la evolución del malware para Android e iOS, y corroborar si los mecanismos de seguridad adicionales introducidos con las nuevas versiones de sistema operativo de ambas plataformas móviles fuerza a los creadores de malware, como en el caso del ransomware MalLocker.B para Android, a evolucionar significativamente e ir un paso más allá en su nivel de complejidad y sofisticación.

Un año más, ahora que se consolidan proyectos como Treble o Mainline en Android, será necesario ver la evolución durante este próximo año 2021 de las versiones de Android, para comprobar realmente su efectividad en la adopción de versiones más modernas, agilizando los procesos de distribución de actualizaciones de los fabricantes y, definitivamente, confirmar si se reduce la fragmentación en el ecosistema Android. De manera similar, la evolución de la comunidad de jailbreak será clave en 2021, donde los terminales afectados por checkra1n empiezan a ir quedando obsoletos, y será necesario disponer de capacidades forenses avanzadas en terminales modernos y versiones recientes de iOS.

Sin duda, este pasado año 2020, y lo que llevamos de año 2021, ha demostrado la relevancia desde el punto de vista de privacidad y de seguridad, tanto sanitaria como tecnológica, de las apps y de las comunicaciones inalámbricas en los dispositivos móviles, especialmente de Bluetooth y BLE, a través de numerosas vulnerabilidades y de las tecnologías de rastreo de contactos para la COVID-19 desplegadas por Apple, Google y por las autoridades sanitarias de los diferentes gobiernos a nivel mundial.

La distribución internacional de apps móviles para la COVID-19 por parte de múltiples naciones parece haberse estabilizado, y su uso y crecimiento no parece evolucionar significativamente en estos momentos de la pandemia, tras unos ocho (8) meses de uso. Sin embargo, con todos los esfuerzos actuales centrados en las campañas de vacunación, será necesario prestar mucha atención a lo largo de 2021 a las nuevas apps móviles que sean publicadas por los países para gestionar qué población realmente se ha vacunado frente al virus, y la nueva posible existencia de carnets digitales de vacunación y certificación (por ejemplo, en forma de app móvil con un código QR asociado) para facilitar o simplificar los viajes entre naciones, con una infraestructura común y distribuida entre países.