Tiendas de aplicaciones de confianza: protegiendo la seguridad e integridad

Febrero de 2024

Redactado por:
Heather West | Directora sénior
+1 202.344.4597
HEWest@Venable.com

Tim McGiff | Gestor de proyectos
+1 202.344.4365
TCMcGiff@Venable.com

CENTER FOR CYBERSECURITY POLICY AND LAW

Índice

Resumen

A medida que la Unión Europea implementa nuevas políticas y regulaciones para su mercado digital, debe mantener un cuidadoso equilibrio entre las consideraciones económicas y el acceso, la privacidad y la seguridad. Lamentablemente, las disposiciones sobre tiendas de aplicaciones móviles de la Ley de Mercados Digitales (DMA, por sus siglas en inglés) podrían socavar los controles de seguridad fundamentales que han hecho que el ecosistema de teléfonos móviles sea tan fiable y resiliente. Al Centro de Política y Derecho de la Ciberseguridad (Center for Cybersecurity Policy & Law) le preocupa que la proliferación de distintas formas de instalar aplicaciones abrume a los usuarios y abra numerosas puertas a los ciberdelincuentes para que las exploten. Con esto no se pretende sugerir que no hay nada que hacer para proteger a los usuarios, pero será necesario que las empresas y los propios usuarios actúen para asegurarse de estar protegidos de formas que no necesitaban hacerlo en el pasado. Este ensayo presenta riesgos potenciales para los ciudadanos de la UE, sus dispositivos y datos, así como algunos planteamientos para mitigar dichos riesgos. Concluimos con algunas recomendaciones para ayudar a los reguladores y formuladores de políticas a garantizar que los usuarios puedan seguir confiando en el ecosistema móvil, y acerca de cómo mitigar posibles implicaciones de seguridad para los usuarios y las empresas. Esperamos que este ensayo también sea una buena fuente de información para otros países que deseen fomentar la competencia en sus propios mercados digitales al tiempo que protegen la seguridad y privacidad de sus ciudadanos.

Acerca del Centro de Política y Derecho de la Ciberseguridad

El Centro de Política y Derecho de la Ciberseguridad (Center for Cybersecurity Policy & Law) es una organización independiente dedicada a incrementar la ciberseguridad en todo el mundo proporcionando al gobierno, la industria privada y la sociedad civil prácticas y políticas para gestionar mejor las amenazas de seguridad. El Centro, establecido en 2017 como una organización sin ánimo de lucro 501(c)(6) dentro del grupo de servicios de seguridad Venable LLP, combina sus extensos conocimientos de políticas con su poder de convocatoria a nivel global, nacional y local para reunir a líderes de la industria y formuladores de políticas con el fin de formar coaliciones y lanzar iniciativas que produzcan resultados en el mundo real. Mediante un enfoque basado en el consenso y la gestión de riesgos, el Centro aspira a desmitificar las complejidades y eliminar la confusión en torno a la ciberseguridad fomentando soluciones pragmáticas y recomendaciones de políticas obtenidas desde las perspectivas y práctica de quienes se encuentran en primera línea de la protección de la infraestructura digital y los sistemas de información.

Introducción

En un mundo cada vez más conectado, utilizamos con frecuencia nuestros teléfonos móviles para interactuar con un rico ecosistema de servicios, información y recursos. Las ventajas de nuestros teléfonos móviles están ampliamente reconocidas[1]: son nuestra ventana al mundo, supervisan nuestra salud, nos permiten compartir con nuestros amigos, comprar productos y gestionar servicios. Y, como consecuencia, pasamos mucho tiempo en aplicaciones móviles; entre cuatro y cinco horas al día, o más[2]. Es esencial que nuestros dispositivos y aplicaciones se mantengan seguros y fiables.

Los estudios sugieren que, en los Estados Unidos, el 81 % de los consumidores de entre 18 y 34 años de edad creen que los dispositivos conectados que poseen son seguros[3]. Las personas tienen buenas razones para confiar en sus dispositivos y aplicaciones móviles, gracias a los esfuerzos de los desarrolladores de sistemas operativos y tiendas de aplicaciones para proteger estos ecosistemas.

En nuestro ensayo de 2021 *Mobile Future: Pathways to Continued Improvement in Mobile Security and Privacy*,[4] comentamos la seguridad móvil con 23 expertos en ciberseguridad de la industria, el mundo académico y la sociedad civil, y observamos que, "aunque continúan surgiendo nuevas amenazas para los dispositivos móviles, las protecciones existentes suelen funcionar mejor que en otras áreas de la ciberseguridad"[5]. El consenso de nuestro grupo focal fue que el entorno móvil se beneficiaba de la seguridad y las protecciones de privacidad integradas a nivel del sistema operativo y la tienda de aplicaciones, lo cual reduce de manera significativa la responsabilidad de los usuarios de protegerse a sí mismos.

Ese documento, de apenas tres años de antigüedad, se escribió en el contexto de las arquitecturas móviles y funciones de seguridad actuales de desarrolladores de sistemas operativos acreditados y sus tiendas de aplicaciones oficiales de confianza. A lo largo de la última década, el ecosistema móvil se ha vuelto cada vez más seguro, pero las disposiciones de instalación de aplicaciones de la DMA[6] de la Unión Europea, enfocada en la competición, podrían hacer retroceder este ecosistema en lugar de continuar con el progreso efectuado en materia de seguridad. Debemos trabajar juntos para garantizar que este progreso se mantenga.

Las disposiciones de la DMA que requieren que los sistemas operativos permitan la instalación de aplicaciones procedentes de fuentes adicionales podrían resultar abrumadoras para los usuarios, lo cual supone un reto para los administradores de empresas que implementen la gestión de dispositivos móviles, y podría abrir nuevas puertas a los ciberdelincuentes. Para mitigar estos riesgos se deberá apoyar a los guardianes de los sistemas operativos móviles para equilibrar el propósito de la DMA al tiempo que se toman medidas razonables para atenuar los riesgos que acompañarán a un ecosistema más abierto.

---

[1] https://www.pewresearch.org/internet/2019/03/07/majorities-say-mobile-phones-are-good-for-society-even-amid-concerns-about-their-impact-on-children/

[2] A través de Techcrunch, Data.ai informa de que los usuarios de dispositivos móviles pasan entre 4 y 5 horas al día en aplicaciones - enlace

[3] https://staysafeonline.org/wp-content/uploads/2022/07/Cybersecurity-Awareness-Month-2020-Results-Report.pdf

[4] https://assets.website-files.com/62715f02a51b614ce64867fd/628e6ba29361afc22807be6b_mobile-future-pathways-to-continued-improvement-in-mobile-security-and-privacy.pdf

[5] https://assets.website-files.com/62715f02a51b614ce64867fd/628e6ba29361afc22807be6b_mobile-future-pathways-to-continued-improvement-in-mobile-security-and-privacy.pdf

[6] El texto original de la Ley de Mercados Digitales se puede encontrar en https://eur-lex.europa.eu/eli/reg/2022/1925

Este ensayo presentará un breve resumen de las disposiciones sobre tiendas de aplicaciones incluidas en la DMA, así como las amenazas al ecosistema móvil exacerbadas por dichas disposiciones, y examinará brevemente cómo las tiendas de aplicaciones nativas y los propietarios de sistemas operativos móviles han combatido estas amenazas históricamente. Este documento defenderá los tipos de estrategias de implantación de la DMA que los Estados miembros de la UE deberían respaldar para garantizar que no se responsabilice de improviso a los usuarios finales que no están preparados de la seguridad del ecosistema móvil y sus dispositivos.

El texto de la DMA hace referencia a posibles formas de proteger a los usuarios, incluyendo tanto mecanismos técnicos como contractuales. Asimismo, los legisladores y reguladores deben apoyar el papel de los desarrolladores de sistemas operativos para proteger a los usuarios mediante reseñas de aplicaciones, protección mejorada contra malware, requisitos de transparencia y ajustes sobre los permisos y modelos de seguridad integrados en los sistemas operativos de los dispositivos móviles. Es importante asegurarnos de que trabajamos juntos para garantizar un ecosistema móvil dinámico e innovador. Instamos a los responsables políticos a enfatizar la importancia de la seguridad en las medidas de implementación de la DMA y mientras los guardianes trabajan para establecer su cumplimiento.

Disposiciones de la DMA sobre tiendas de aplicaciones

Para marzo de 2024, las compañías que se incluyen en la definición de "guardián de acceso" que opera "servicios de plataforma esenciales" estarán sujetas a las disposiciones de la DMA relacionadas con sus tiendas de aplicaciones e interacciones de sistemas operativos móviles con aplicaciones y tiendas de aplicaciones de terceros. Los guardianes son aquellas compañías que, según lo designado por la Comisión Europea, tienen un impacto significativo en el mercado europeo y proporcionan un servicio de intermediario entre negocios (p. ej.: desarrolladores de aplicaciones) y usuarios finales (p. ej.: los usuarios de teléfonos móviles que instalan aplicaciones)[7]. La intención de la DNA es hacer que sea más fácil para las empresas europeas de pequeño tamaño competir con empresas que puedan tener una posición más consolidada en el mercado.

Las disposiciones de la DMA requieren que los sistemas operativos móviles permitan la instalación de aplicaciones de tiendas de aplicaciones no- guardianes u otros métodos, y que los sistemas operativos permitan el mismo acceso al sistema y herramientas a las aplicaciones de origen y las de terceros.

Entre estas disposiciones destaca lo siguiente:

- *Apartado 6.4: El guardián de acceso permitirá y habilitará técnicamente la instalación y el uso efectivo de aplicaciones de software o tiendas de aplicaciones de software de terceros que utilicen su sistema operativo o interoperen con él, y permitirá que se acceda a dichas aplicaciones de software o tiendas de aplicaciones de software por medios distintos de los servicios pertinentes de la plataforma central de dicho guardián de acceso.*

- *Apartado 6.7: El guardián de acceso permitirá a los proveedores de servicios y proveedores de hardware, de manera gratuita, la interoperabilidad efectiva con, y el acceso a efectos de interoperabilidad a, las mismas funciones de hardware y software a las que se accede o que se controlan a través del sistema operativo o del asistente virtual [...]. Además, el guardián de acceso permitirá [...] la interoperabilidad efectiva con, y el acceso a efectos de interoperabilidad a, las mismas características de sistema operativo, hardware o software, independientemente de que dichas características formen parte del sistema operativo, que estén a disposición de dicho guardián de acceso o sean utilizadas por este al prestar tales servicios.*

[7] En el momento de la publicación, el sistema operativo iOS de Apple y el sistema operativo Android de Google se consideran servicios de plataforma centrales. El sistema operativo Windows de Microsoft para PC también se considera un servicio de plataforma central, pero está fuera del ámbito del presente documento.. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

En la práctica, estas disposiciones de la DMA, cuando se combinan con otras leyes de la Unión Europea, requerirán a los guardianes permitir una instalación más fácil de aplicaciones y tiendas de aplicaciones de terceros en dispositivos móviles, permitir un acceso más fácil a las tiendas de aplicaciones de terceros por parte de los usuarios de dispositivos móviles y conceder a los desarrolladores y aplicaciones de terceros el mismo acceso, interoperabilidad y funcionalidad con los sistemas operativos móviles de los que disfrutan actualmente los guardianes.

Además de estas disposiciones, y subrayando la conciencia del riesgo de seguridad y privacidad que plantea "abrir" el ecosistema móvil, hay una reserva de seguridad que no ha recibido suficiente atención. La cláusula 50 de la DMA establece que el acceso adicional proporcionado a aplicaciones y tiendas de aplicaciones de terceros no debería socavar la seguridad de los usuarios y dispositivos. No obstante, la DMA no explica cómo espera que los sistemas operativos protejan los dispositivos móviles y a los usuarios teniendo en cuenta la restricciones respecto al modo en que los sistemas operativos pueden diferenciar o restringir el acceso a las aplicaciones. Si se implementan sin una minuciosa consideración, las disposiciones anteriores de la DMA podrían exacerbar el ecosistema actual de amenazas móviles.

El ecosistema de amenazas móviles

Combatir el malware móvil es una prioridad para los desarrolladores de sistemas operativos móviles y para las organizaciones de todo el mundo. A pesar de su exitosa arquitectura de seguridad protectora, los dispositivos móviles son un objetivo tentador debido a su ubicuidad, al hecho de que nos acompañan a lo largo del día y a que son una parte tan esencial de nuestras vidas y son el escenario de un gran número de nuestras interacciones digitales.

Las amenazas móviles también han ido creciendo a medida que los sistemas operativos se convertían en auténticas plataformas en lugar de ecosistemas cerrados, y desde entonces los desarrolladores de sistemas operativos móviles y operadores de tiendas de aplicaciones de renombre han estado trabajando para frenar las amenazas mediante elecciones de diseño arquitectónico de sistemas operativos que aíslan las aplicaciones y datos, la moderación de aplicaciones, comprobaciones de calidad y funcionalidad de las aplicaciones, y modelos de permisos cada vez más detallados. El informe *Mobile Threat Landscape Report* de CrowdStrike de 2019 concluyó que las plataformas móviles experimentan cada vez más ataques de cibercriminales, y que los adversarios menos cualificado ahora tienen acceso a prototipos de *malware* móvil que les permite intentar acceder a dispositivos móviles con facilidad[8].

Las principales amenazas móviles

Existen infinidad de amenazas para y al ecosistema móvil, pues tanto los actores maliciosos como los oportunistas buscan una forma de aprovechar estas plataformas tan populares. A medida que los guardianes y responsables políticos implementen la DMA, deben considerar formas de minimizar estas amenazas.

Desde hace mucho tiempo, las aplicaciones maliciosas han sido la amenaza más significativa para los dispositivos móviles debido a su potencial para interactuar directamente con datos sensibles almacenados, así como con las funcionalidades clave del dispositivo móvil. Según los estudios de Nokia[9] y Kaspersky[10], la mayoría del malware móvil accede a los dispositivos

[8] https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/

[9] https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/

[10] https://securelist.com/mobile-malware-evolution-2020/101029/

móviles a través de aplicaciones troyanizadas. Estas aplicaciones se hacen pasar por cosas que las personas realmente quieren instalar, como una aplicación de linterna o versiones gratuitas de un software caro, pero la aplicación troyanizada oculta comportamientos indeseados, como la recopilación de credenciales o información confidencial[11]. Para conseguir su objetivo, las aplicaciones solicitan permisos que no necesitarían para su función superficial, como podría ser el caso de una aplicación de linterna que solicita acceso a los datos de ubicación o los contactos almacenados en el teléfono[12]. El usuario instala lo que parece ser un juego o una aplicación benignos, normalmente gratis, pero está exponiendo su dispositivo y datos para actores maliciosos. Check Point ha reportado un aumento de dichas aplicaciones, especialmente aquellas que pretenden ofrecer una prueba gratuita o una funcionalidad adicional[13]. Indican que fiarse de lo familiar presenta riesgos, pues muchas de estas aplicaciones se aprovechan de marcas y nombres de productos familiares, pero roban datos o credenciales, o añaden el dispositivo a una *botnet*[14].

Estas aplicaciones maliciosas suelen conseguir ocultar su verdadera naturaleza. Hay una proliferación de aplicaciones troyanizadas (incluyendo herramientas de hackeo, *accesware*, *spyware*, *adware*, marcadores y programas de bromas) que tienen un comportamiento molesto o dañino que no es deseado por el usuario[15]. Incluso hay proveedores de malware como servicio que crean aplicaciones para tomar el control de cuentas y unir dispositivos móviles a *botnets*[16].

Algunas de estas aplicaciones se utilizan con mucha frecuencia entre los ciberdelincuentes. Por ejemplo, varias estafas de aplicaciones de préstamos instantáneos han estado circulando por la India y otros países de Asia, África y Latinoamérica. Tras instalarla, es posible que la aplicación proporcione un préstamo, pero también extrae información del teléfono; tanto información sobre el usuario como otros datos que hay en el teléfono, incluyendo fotografías de desnudos, que a continuación se utilizan para acosar, intimidar y extorsionar[17].

Una vez identificada la principal amenaza móvil, la pregunta lógica es: "¿pero cómo se instalan estas aplicaciones maliciosas?". Las tiendas de aplicaciones nativas, como Google Play Store y Apple App Store, no son infalibles a la hora de mantener a raya las aplicaciones maliciosas, pero la mayoría de aplicaciones que hay en sus tiendas son benignas, debido a sus esfuerzos por mantener sus tiendas seguras. El mayor riesgo de malware procede de las tiendas de aplicaciones de terceros y del *sideloading* (la transferencia de archivos entre dos dispositivos). Aunque cuantificar con exactitud el nivel de riesgo que plantea cada método es increíblemente difícil, algunos estudios sugieren riesgos sustanciales para los usuarios.

Tiendas de aplicaciones de terceros

Aunque algunos estudios han sugerido que las principales tiendas de aplicaciones de terceros *pueden* ser seguras en comparación con las tiendas de aplicaciones propias, como Google Play Store, las pruebas sugieren que las tiendas de terceros aumentan los riesgos de seguridad y privacidad para los usuarios de dispositivos móviles, pero eso no se debe a que

---

[11] https://www.mcafee.com/blogs/mobile-security/mobile-spyware/, https://www.appdome.com/dev-sec-blog/mobile-payment-security/

[12] https://blog.avast.com/flashlight-apps-on-google-play-request-up-to-77-permissions-avast-finds

[13] Check Point, *2023 Cyber Security Report*, 2023

[14] https://www.verizon.com/business/resources/T9bc/reports/mobile-security-index-report.pdf

[15] https://docs.broadcom.com/doc/istr-23-03-2018-en

[16] https://www.androidpolice.com/android-botnet-trojan-steal-banking-data/

[17] https://www.bbc.co.uk/news/world-asia-india-66964510

no estén asociadas con el sistema operativo. El motivo es que generalmente no llevan a cabo o no pueden llevar a cabo la misma diligencia a la hora de supervisar sus aplicaciones; lo cual probablemente sea una de las razones por las que, históricamente, los principales sistemas operativos móviles no han permitido las tiendas de aplicaciones de terceros por defecto[18]. Y existen algunos ejemplos de tiendas de aplicaciones que han sido concebidas en sí mismas para instalar aplicaciones maliciosas[19]. En un grupo de discusión de 2021, CrowdStrike observó que la mayoría del malware móvil es distribuido por fuentes de terceros que no realizan comprobaciones exhaustivas de las aplicaciones que ponen a disposición de los usuarios[20].

A pesar de que cuantificar el riesgo exacto es difícil, un estudio de 2020 observó que los usuarios de Android de "otros mercados alternativos importantes" corrían un riesgo cinco veces mayor de media, y era hasta 19 veces más probable que se toparan con malware o una aplicación maliciosa que aquellos que utilizaban Google Play Store[21]. Además, la empresa de seguridad Symantec informó en 2018 que un total del 99,9 % del malware móvil que habían descubierto estaba alojado en tiendas de aplicaciones de terceros[22].

Esto ha llevado a un consenso entre los expertos de seguridad y reguladores de que descargar aplicaciones de la mayoría de tiendas de aplicaciones de terceros es mucho más arriesgado que hacerlo de una tienda nativa de confianza. Los principales Gobiernos y organizaciones privadas desaconsejan descargar aplicaciones de fuentes no oficiales o que no sean de confianza, incluyendo advertencias procedentes de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), la Europol,[23] la Agencia Nacional de Seguridad de EE. UU. (NSA) [24], la Comisión Federal de Comercio de EE. UU. (FTC) encargada de la protección al consumidor, el Centro de Seguridad Nacional del Reino Unido (NCSC)[25], el Equipo de Respuesta a Emergencias Informáticas de la India (CERT-In)[26], la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) del Departamento de Seguridad Nacional (DHS) de EE. UU.[27], el Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de EE. UU.[28], el Equipo de Respuesta a Emergencias Informáticas de Nueva Zelanda (CERT NZ)[29] y otros. A pesar de ello, los estudios han mostrado que los consumidores utilizarán tiendas de aplicaciones de terceros si

---

[18] https://citrixready.citrix.com/content/dam/ready/partners/wa/wandera/wanderas-web-gateway-for-mobile/mobile-threat-landscape-2020-whitepapers.pdf

[19] https://www.makeuseof.com/what-are-the-dangers-of-third-party-app-stores/#:~:text=Many%20malicious%20actors%20have%20created,hidden%20trackers%20and%20malicious%20code.

[20] Ensayo del Centro de 2021

[21] https://arxiv.org/pdf/2010.10088.pdf

[22] https://docs.broadcom.com/doc/istr-23-03-2018-en

[23] Europol: https://www.europol.europa.eu/sites/default/files/documents/infographic_-_apps.pdf

[24] Mejores prácticas para dispositivos móviles (V3) de la Agencia Nacional de Seguridad de Estados Unidos: https://media.defense.gov/2020/Jul/28/2002465830/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF

[25] Centro de Seguridad Nacional del Reino Unido (NCSC): https://www.ncsc.gov.uk/files/Protecting-devices-from-viruses-malware-infographic.pdf

[26] https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0013

[27] CISA, EE. UU.: https://www.cisa.gov/sites/default/files/publications/CEG_Mobile_Device_Cybersecurity_Checklist_for_Organizations_0.pdf

[28] NIST, EE. UU: https://www.nccoe.nist.gov/sites/default/files/legacy-files/mtc-nistir-8144-draft.pdf

[29] CERT NZ: https://www.cert.govt.nz/individuals/guides/keep-mobile-phone-safe-secure/

las aplicaciones son gratuitas o contienen versiones modificadas de juegos y aplicaciones bien conocidos[30]. Los usuarios no tienen en cuenta su propia seguridad, sólo quieren conseguir rápidamente (y, a ser posible, gratis) una aplicación que suena demasiado bien para ser verdad.

El *sideloading*

En comparación, el *sideloading*, también denominado "transferencia local", no requiere ningún tipo de tienda de aplicaciones tradicional, y una aplicación obtenida por estos medios puede ser distribuida o promocionada con muy poco contexto, sin ningún escrutinio y con alegaciones falsas o engañosas acerca de su seguridad y autenticidad. No hay ningún intermediario que realice estas tareas, ya que el *sideloading* puede tener lugar desde cualquier ubicación: un sitio web, un adjunto a un mensaje o un enlace oculto.

El *sideloading* no requiere que el individuo confíe en un tercero que quizá no tenga la reputación, la experiencia o los medios necesarios para garantizar que la aplicación no ha sido manipulada, aunque los usuarios no piensan en ello cuando encuentran un juego nuevo que quieren probar. A pesar de que un gran número de sitios webs y tiendas de terceros son seguros, es improbable que un usuario encuentre el mismo nivel de transparencia en cuanto a cómo se ha investigado la aplicación y qué permisos podría solicitar, y es mucho más sencillo fingir ser algo que no eres sin la infraestructura de una tienda de aplicaciones reputada.

El *sideloading* es la forma más arriesgada que tienen los usuarios de adquirir aplicaciones móviles. Aunque este riesgo normalmente queda compensado por el hecho de que esta práctica suele requerir un cierto nivel de dominio técnico que la mayoría de usuarios finales no posee, si los sistemas operativos móviles permiten el *sideloading* por defecto, dicha fricción desaparecerá. Incluso los usuarios finales bien informados que recurren a este método suelen terminar confiando en tiendas de aplicaciones y desarrolladores desconocidos o cuestionables, y ni todos los conocimientos técnicos del mundo podrían reducir el riesgo de manera fidedigna, a no ser que sólo se descargue de compañías bien establecidas.

El fracaso de la responsabilidad del usuario final

Los estudios muestran que las decisiones de seguridad de un usuario no tienen por qué presentar una correlación con su conocimiento de las amenazas de seguridad[31]. A pesar del daño muy real que pueden causar las aplicaciones maliciosas, los usuarios de dispositivos móviles rara vez están dispuestos a dedicar una cantidad de tiempo considerable a examinar de manera crítica qué permisos solicita una aplicación y, si lo intentan, no suelen comprender sus implicaciones[32]. Y cuando se interrumpe a los usuarios con advertencias de seguridad, la inmensa mayoría las ignora[33].

Muchos usuarios ni siquiera toman las medidas de seguridad básicas para proteger sus dispositivos móviles. Por ejemplo, un estudio descubrió que el 40 % de los usuarios indicó que no actualiza su sistema operativo o aplicaciones a no ser que sea conveniente, y el 28 % no utiliza ningún sistema de bloqueo de pantalla[34]. Otro estudio halló que tres cuartos de los usuarios

---

[30] https://www.jamf.com/blog/what-are-third-party-app-stores-and-are-they-safe/

[31] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5352308/

[32] https://link.springer.com/chapter/10.1007/978-3-031-35822-7_36

[33] https://news.sophos.com/en-us/2016/08/19/why-people-ignore-security-alerts-up-to-87-of-the-time/

[34] https://www.pewresearch.org/short-reads/2017/03/15/many-smartphone-owners-dont-take-steps-to-secure-their-devices/

de teléfonos inteligentes creen que las aplicaciones que descargan de tiendas de aplicaciones son inherentemente seguras[35], por lo que es improbable que se muestren escépticos frente a ellas. Este estudio incluso observó que los usuarios de aplicaciones no podían o no se molestaban en diferenciar el nivel de seguridad proporcionado por distintas tiendas de aplicaciones. Otros estudios recientes han confirmado que los usuarios sí se preocupan por los riesgos de seguridad, pero carecen del conocimiento y las habilidades necesarios para protegerse a sí mismos con eficacia, y a menudo ni siquiera intentan hacerlo[36].

Aunque esperamos que los usuarios adopten un papel más activo en su propia protección en línea, la mejor práctica consiste cada vez más en quitarles toda la responsabilidad posible. Las estrategias cibernéticas nacionales y las mejores prácticas de los Gobiernos intentan desequilibrar cada vez más la balanza en dirección contraria a los usuarios y poner la responsabilidad de proteger los dispositivos, los datos y las personas en manos de las empresas que los distribuyen. En 2023, las agencias de ciberseguridad nacional de los EE. UU. (CISA), la República Checa, Israel, Singapur, Corea, Noruega, CSIRTAmericas Network de la OEA/CICTE y Japón (JPCERT/CC y NISC) lanzaron conjuntamente unas guías sobre cómo retirar la responsabilidad del riesgo de los usuarios finales[37]. Muchas organizaciones tanto del sector público como privado eligen utilizar un software de gestión de dispositivos móviles (MDM, por sus siglas en inglés) para garantizar que solo las aplicaciones aprobadas sean instaladas en dispositivos que también tienen acceso a datos o aplicaciones sensibles, y en un futuro estas herramientas podrían permitir a los administradores determinar qué tiendas de aplicaciones se permiten.

Teniendo en cuenta la extensión y complejidad de los riesgos anteriores, es irracional esperar que los usuarios finales tengan de pronto la conciencia y comprensión necesarias acerca de la seguridad y privacidad móvil, incluyendo cómo protegerse a sí mismos mediante una solución de seguridad multicapa, configurando una combinación de ajustes óptima para el riesgo que aceptan; y otros métodos sencillamente no son viables a escala. Los usuarios finales tienden a asumir que las tiendas de aplicaciones disponibles de manera universal son seguras. Hay otros enfoques, pero requerirán protecciones como las que los guardianes de acceso ya han implementado en sus propias tiendas de aplicaciones.

Cómo combaten estas amenazas Google y Apple

Muchas tiendas de aplicaciones nativas, como Apple App Store y Google Play Store y otras que no han sido determinadas por los guardianes de acceso en virtud de la DMA, toman amplias medidas para mitigar los riesgos identificados anteriormente mediante políticas y procesos diseñados para examinar las aplicaciones nuevas y actualizadas en busca de malware o cambios significativos respecto a su funcionalidad original. Tanto Apple como Google han creado políticas y procesos que se extienden desde el desarrollador, pasando por sus tiendas de aplicaciones oficiales, hasta los consumidores. Si bien ninguna tienda de aplicaciones es completamente segura, estos esfuerzos han logrado que Google Play Store y Apple App Store se labren una reputación de confianza y seguridad entre los consumidores gracias a años de inversiones y aprendizaje para conformar sus planteamientos de protección de los usuarios.

Las principales aplicaciones nativas, como Apple App Store y Google Play Store, logran la seguridad implementando procesos como el establecimiento de requisitos y directrices de referencia, el requerimiento de autocertificaciones y la revisión de

[35] https://www.sciencedirect.com/science/article/pii/S0167404812001733#fn6

[36] https://dl.acm.org/doi/fullHtml/10.1145/3491102.3517504#sec-21

[37] https://www.cisa.gov/resources-tools/resources/secure-by-design

aplicaciones[38]. Los desarrolladores de aplicaciones deben satisfacer sus diversos requisitos de seguridad, privacidad y transparencia para que sus aplicaciones puedan publicarse en una de estas tiendas de aplicaciones. Esto podría incluir garantizar que una aplicación hace lo que anuncia que hace, solicita únicamente los permisos apropiados y cuenta con políticas de privacidad funcionales. Las tiendas de aplicaciones de Apple y Google también requieren transparencia en los anuncios de sus tiendas de aplicaciones, incluyendo los permisos que la aplicación utiliza, así como información sobre la recopilación de datos[39, 40].

Las tiendas de aplicaciones nativas también podrían tener protecciones adicionales más allá de la revisión de la aplicación en sí, como examinar las cuentas de los desarrolladores. Por ejemplo, Google Play Store analiza "la cuenta de Google de un desarrollador, sus acciones, historial, datos de facturación, información del dispositivo y más" para identificar posibles señales de alarma[41].

A la hora de revisar las propuestas de aplicaciones, las tiendas de aplicaciones nativas pueden tomar una serie de acciones para garantizar su función: la tienda podría revisar los certificados del desarrollador de la aplicación, aplicar varias revisiones automatizadas y hacer que una persona revise manualmente la aplicación. Estas revisiones pueden emplear diversas herramientas y técnicas para efectuar revisiones estáticas y dinámicas en busca de *malware* u otros elementos potencialmente dañinos o indeseados. Además, más allá de las inspecciones rutinarias de las aplicaciones que se han propuesto recientemente, las tiendas de aplicaciones nativas, como la de Apple, comprueban las actualizaciones de aplicaciones para garantizar que cualquier funcionalidad nueva sea segura. Por último, las tiendas de aplicaciones nativas tienden a ejecutar revisiones en función de las quejas o avisos de los consumidores o investigadores de seguridad cuando una aplicación presenta comportamientos no deseados.

Si una aplicación no logra cumplir y mantener los requisitos y directrices necesarios para incluirse en la tienda de aplicaciones, suele ser eliminada. El alcance de estos problemas es considerable: Apple indica que en 2022 rechazó más de 1,5 millones de propuestas de aplicaciones y eliminó más de 186 000 aplicaciones de su tienda de aplicaciones[42]. Estas eliminaciones fomentan un entorno de seguridad y confianza en la tienda de aplicaciones, protegen a los usuarios finales e incentivan a los ciberdelincuentes a buscar otras formas más fructíferas de infectar dispositivos.

A nivel del consumidor, Apple y Google han realizado esfuerzos significativos para hacer que sus protecciones y requisitos de seguridad y políticas sean fácilmente accesibles y comprensibles para la mayoría de usuarios de sus tiendas de aplicaciones. Asimismo, ambos han tratado de crear más transparencia con respecto a los permisos que las aplicaciones aprobadas solicitan, de manera que los consumidores puedan tomar decisiones informadas sobre el nivel de privacidad y seguridad que desean más allá del punto de partida oficial de la tienda de aplicaciones. La Google Play Store incluso ha empezado a mostrar

---

[38] https://developer.apple.com/app-store/review/guidelines/, https://play.google.com/about/developer-content-policy/

[39] https://support.google.com/googleplay/android-developer/answer/10144311?hl=en

[40] https://developer.apple.com/app-store/user-privacy-and-data-use/#:~:text=In%20order%20to%20submit%20new,websites%20owned%20by%20other%20companies.

[41] https://developers.google.com/android/play-protect/cloud-based-protections

[42] https://www.apple.com/legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf

una insignia en las aplicaciones que han completado una revisión de seguridad independiente[43]. Estos procesos y políticas han demostrado ser eficaces, pero suponen inversiones considerables.

La seguridad es una inversión para las tiendas de aplicaciones móviles

Como ya se ha establecido, trasladar la responsabilidad en materia de seguridad a los usuarios finales no es eficaz, y va en contra de las mejores prácticas de ciberseguridad, que fomentan cada vez más políticas y procesos para garantizar que los usuarios estén protegidos por defecto. Si bien las grandes entidades con muchos recursos como Google y Apple tienen los conocimientos, recursos y voluntad necesarios para hacerlo, pocas otras pueden decir lo mismo.

Los tipos de protecciones nombrados anteriormente, que las tiendas de aplicaciones de terceros rara vez o nunca implementan en la misma medida, eliminan la mayoría de aplicaciones maliciosas, engañosas y de mala calidad. Las tiendas de aplicaciones de terceros no tienen el mismo grado de recursos, experiencia, conocimientos de la plataforma y el sistema operativo ni incentivos para proteger su tienda de aplicaciones o investigar las aplicaciones que alojan que las tiendas de aplicaciones nativas. Además, las tiendas de aplicaciones de terceros podrían querer diferenciarse de las tiendas establecidas de mayor tamaño siendo más permisivos respecto a aplicaciones que, de lo contrario, se considerarían indeseadas. Frente a ellas están las tiendas de aplicaciones nativas, que dedican recursos considerables a mejorar la seguridad de las aplicaciones en su plataforma.

Una hoja de ruta para implementar la DMA

La necesidad de sistemas operativos móviles tendrá, inevitablemente, efectos negativos en la privacidad y seguridad del ecosistema móvil, pero hay formas de permitir a los usuarios un mayor acceso a las aplicaciones y tiendas de aplicaciones de terceros de manera segura al tiempo que se concede a los desarrolladores de aplicaciones de terceros un mayor acceso a la funcionalidad a nivel del sistema operativo. Como hemos indicado antes, y como han demostrado actores como Apple, lo más seguro es que el cumplimiento de la DMA aumente la prevalencia de "*malware*, fraudes y estafas, contenido ilícito y dañino, y otras amenazas de privacidad y seguridad"[44]. No obstante, los legisladores y formuladores de políticas pueden mitigar estos problemas con una orientación constructiva para la implementación que permita a los guardianes de acceso proteger a los consumidores.

Los Estados miembros de la UE deberían estar dispuestos a respaldar las tiendas de aplicaciones nativas y a los propietarios de sistemas operativos móviles, así como a los usuarios de dispositivos móviles, apoyando lo siguiente:

- Los guardianes de acceso deberían llevar a cabo revisiones de referencia de las aplicaciones independientemente del canal de distribución. Esto podría requerir que se integrasen nuevos mecanismos en los sistemas operativos o contratos con las tiendas de aplicaciones. También es posible que haya una forma de usar los certificados y evaluaciones de terceros para demostrar que las aplicaciones son seguras.
- Los formuladores de políticas deberían considerar la inclusión de avisos en las descripciones de aplicaciones respecto a su funcionalidad básica e información esencial para ayudar a los usuarios y otros a comprender cómo funcionan las aplicaciones y qué están concebidas para hacer.
- Los sistemas operativos podrían implementar protecciones móviles mejoradas para evitar que el *malware* dañe la seguridad e integridad del dispositivo móvil, incluyendo herramientas adicionales para hacer pruebas y proteger las aplicaciones las unas de las otras, así como proteger el sistema operativo, los datos de usuario y el hardware del

[43] https://security.googleblog.com/2022/12/app-defense-alliance-expansion.html

[44] https://www.apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/

dispositivo de las aplicaciones maliciosas. Estas herramientas podrían incluir herramientas de gestión de dispositivos móviles para administradores de empresas.

- Los guardianes de acceso deberían implementar controles contractuales y técnicos para las tienda de aplicaciones de terceros con el fin de garantizar que son de confianza. Es probable que cada guardián de acceso elija un equilibrio diferente entre distintos tipos de mitigación, pero deberían tener una amplia gama de opciones para proteger a los usuarios a medida que trabajan para aplicar la DMA.
- Las empresas móviles consideradas guardianes de acceso necesitan una orientación clara para poder proteger a sus usuarios, y se les debe dar el tiempo adecuado para conceptualizar, construir, probar y comprobar nuevos sistemas para consolidar a sus usuarios.
- Los reguladores deberían prestar atención a las preocupaciones de seguridad e integridad tanto acerca de las aplicaciones como de las tiendas de aplicaciones, y reconocer que no todas las aplicaciones y tiendas son iguales. Deberían respaldar el desarrollo de mecanismos para evaluar y garantizar que los desarrolladores de aplicaciones y tiendas de aplicaciones se comporten de manera responsable, y que deban rendir cuentas si no lo hacen.
- Los guardianes de acceso que desarrollan sistemas operativos móviles deben tener la flexibilidad necesaria para ajustar los modelos de seguridad y permisos, así como su funcionamiento, con el fin de garantizar que los desarrolladores no se puedan aprovechar del ecosistema cambiante. Los formuladores de políticas deben proteger la capacidad de las tiendas de aplicaciones y los sistemas operativos de dispositivos para hacer evolucionar los tipos de mecanismos y limitaciones de seguridad que están disponibles para integrar en su ecosistema.
- Las políticas dirigidas a ecosistemas móviles no deben debilitar la seguridad de dichos ecosistemas. Los formuladores de políticas deben garantizar que la seguridad y privacidad de las plataformas móviles continúe mejorando, y que ambas estén integradas en las plataformas y aplicaciones desde el principio. Las propuestas que amenacen el progreso alcanzado deberían ser reconsideradas.
- Los formuladores de políticas deben ser realistas respecto a las cargas y responsabilidades de seguridad que los usuarios están dispuestos a, y equipados para, asumir. Los estudios indican que no hay una correlación entre la conciencia de seguridad y la toma de buenas decisiones de seguridad[45].
- Los formuladores de políticas deberían respaldar las prácticas basadas en el análisis de riesgos para dispositivos móviles en lugar de exigir prácticas particulares sobre el funcionamiento de los dispositivos móviles y las aplicaciones que se pueden instalar.

Conclusión

Ahora que la DMA se ha aprobado y los guardianes de acceso están trabajando para garantizar su cumplimiento, estamos llegando a una transición decisiva para el ecosistema móvil. El Centro de Política y Derecho de la Ciberseguridad espera que los formuladores de políticas y los guardianes de acceso, así como el resto del ecosistema móvil, puedan trabajar juntos para mantener a los usuarios y sus dispositivos móviles seguros y protegidos. Los formuladores de políticas deberían considerar el impacto de la seguridad en las empresas, el ecosistema y los consumidores. Aunque el impacto de muchos de estos elementos de revisión y supervisión de las tiendas de aplicaciones existentes es difícil de cuantificar, las inversiones efectuadas por los desarrolladores de tiendas de aplicaciones para proteger a sus usuarios deberían ser reconocidas y recompensadas. Cuando los desarrolladores y propietarios de tiendas de aplicaciones toman medidas para aumentar la seguridad y la privacidad, los usuarios se benefician de formas de las que no son conscientes.

No existe ningún sistema perfecto que proteja a los usuarios de todo el *malware* móvil, pero sabemos cómo reducir de manera significativa el número de actividades indeseadas o maliciosas que los usuarios deben considerar.

[45] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5352308/