jamf

Security 360:

Informe anual de tendencias

Dispositivos móviles

Prólogo

En todos los sectores y casos de uso —desde los flujos de trabajo en el comercio minorista hasta las operaciones en el sector salud— los líderes empresariales están innovando con los dispositivos móviles para transformar la forma de trabajar de las personas y optimizar los resultados de la organización. Para muchos empleados de todos los sectores, los dispositivos móviles (p. ej., teléfonos inteligentes y tabletas) son los únicos dispositivos que se utilizan en el trabajo. Y el lugar de trabajo moderno consiste en dar a los empleados la posibilidad de conectarse desde cualquier lugar, en cualquier momento y con el dispositivo que deseen utilizar.

Uno de los principales impulsores del trabajo móvil comenzó con la adopción de la movilidad como servicio en el lugar de trabajo. Ya no son dispositivos de acompañamiento, sino cada vez más son el principal punto de entrada para realizar el trabajo. Aunque la movilidad no es ajena al lugar de trabajo, su integración continua en los flujos de trabajo clave es más pronunciada que nunca. El lugar de trabajo actual requiere no solo experiencias digitales excepcionales, sino experiencias digitales **seguras** que maximicen la productividad de los trabajadores independientemente de dónde decidan trabajar.

– Josh Stein,
Vicepresidente de Administración de Productos

Introducción

El informe Security 360 de Jamf fue elaborado a partir del análisis de incidentes reales de clientes, investigaciones sobre amenazas y acontecimientos de la industria del año pasado. Este informe se enfoca en explorar el panorama de las amenazas móviles para poner de relieve los riesgos a los que se enfrentan las organizaciones.

Proporcionamos una evaluación de los diversos vectores de ataque que se utilizan activamente para engañar a los usuarios, comprometer los dispositivos móviles e infiltrarse en las organizaciones. Estos ataques no se limitan a las vulnerabilidades de los dispositivos, por lo que nuestro análisis también incluye aplicaciones riesgosas, amenazas web y mucho más.

Además de analizar estas tendencias de amenazas, el informe incluye una perspectiva del CISO (Director de Seguridad de la Información) de Jamf para proporcionar las ideas que los líderes de seguridad tienen en cuenta en el momento de proteger sus flotas de móviles en los niveles de usuario, dispositivo, aplicación y red.

Metodología de la investigación

Para comprender y cuantificar el impacto en el mundo real de las tendencias de seguridad identificadas en este informe, examinamos un grupo de muestra formado por 1.4 millones de dispositivos protegidos por Jamf. Nuestro análisis se llevó a cabo en el primer trimestre de 2025, revisando el periodo anterior de 12 meses y abarcando 90 países por todo el mundo, así como múltiples plataformas, concretamente, dispositivos iOS y iPadOS y Android.

Para mantener la privacidad y preservar los más altos estándares al recopilar y manipular datos, los metadatos analizados en nuestra investigación proceden de registros agregados que no contienen información personal o identificativa de la organización.

Objetivo de la investigación

Nuestra intención con este análisis es permitir que las organizaciones y los usuarios comprendan la evolución de las tendencias de ciberseguridad que existen actualmente, así como mostrar la manera en que las organizaciones y los usuarios pueden tomar medidas para mitigar los riesgos. También ofrece un panorama general de las investigaciones más impactantes de Jamf Threat Labs, que incluye las amenazas y vulnerabilidades que encontraron. Al informar a nuestro público sobre lo que hay ahí fuera, esperamos disipar cualquier mito y mostrarle a usted cómo puede aplicar salvaguardas para proteger a sus usuarios y sus datos. Algunas de las mejores prácticas más comunes que pueden aplicar las organizaciones son:

- Actualizaciones continuas y puntuales del sistema operativo
- Educación y capacitación de los usuarios
- Verificación de solicitudes
- Autenticación multifactor
- Infraestructuras de seguridad de confianza cero
- Forma sencilla de establecer y administrar el cumplimiento de las líneas base
- Implementación de políticas de uso aceptable de los datos corporativos

Estructuramos nuestro análisis e informe en cuatro categorías que consideramos prioritarias para las organizaciones de todo el mundo:

I. Phishing móvil

II. Manejo de vulnerabilidades

III. Riesgo en las aplicaciones

IV. Malware y spyware

El análisis de este informe se basa en la Inteligencia sobre Amenazas de Jamf, una amplia colección de perspectivas derivadas de investigaciones originales sobre amenazas, métricas de uso en el mundo real, junto con análisis de noticias y fuentes de datos. La Inteligencia de Amenazas de Jamf se compone de la investigación dirigida por humanos de los equipos de Jamf Threat Labs y Data Science, que supervisan los dispositivos, las apps y el tráfico de red en busca de riesgos, amenazas y vulnerabilidades de día cero.

Las estadísticas de este documento incluyen dispositivos **Apple** y **Android**.

También disponemos de un informe Security 360 enfocado en **los dispositivos Mac** que se puede consultar **aquí**.

Tendencias clave para los móviles

I. El phishing sigue siendo un riesgo para las empresas

El phishing sigue siendo una técnica de ataque prevalente de los actores de amenazas, y su influencia en el panorama de las amenazas es tan activa como siempre. En septiembre de 2024, **Apple publicó una entrada en su blog** con consejos para los usuarios de iOS con el fin de ayudarles a "evitar estafas y saber qué hacer si reciben correos electrónicos, llamadas telefónicas u otros mensajes sospechosos". Por muy segura que sea una plataforma o un sistema operativo, las técnicas de ingeniería social —como el phishing— están diseñadas para infiltrarse en los datos empresariales empezando por la parte menos segura del dispositivo: el usuario.

II. Una sola vulnerabilidad puede ayudar a los atacantes a obtener acceso a todo el sistema

Es un hecho: se producen vulnerabilidades en el software (tanto en los sistemas operativos como en las aplicaciones) que utilizamos a diario. Según la **Publicación Especial 800-124rd del NIST**, "En el caso del software común, existen errores y vulnerabilidades con una frecuencia estimada de ~25 errores por cada 1000 líneas de código". Las vulnerabilidades y exposiciones comunes (CVE) publicadas en la Base de Datos Nacional de Vulnerabilidades (NVD) permiten al público conocer las CVE que se encuentran en la naturaleza. Estas actualizaciones son vitales, pero es necesario aplicar el parche antes de que puedan ser útiles para la organización.

Apple y Google proporcionan información importante cuando se descubre una vulnerabilidad, y qué actualización del sistema operativo la corrige. Por ejemplo, a principios de este año, Apple lanzó iOS 18.3.2 en respuesta a **CVE-2025-24201** , en el que el contenido web maliciosamente diseñado puede ser capaz de escapar de la caja de arena de contenido web. **Google publicó el boletín de seguridad de Android** en el que se abordan 43 vulnerabilidades de seguridad, incluidas dos vulnerabilidades críticas de día cero.

III. Las apps introducen riesgos, incluso en plataformas seguras

Desde su debut, la App Store de Apple y la tienda Google Play han protegido a usuarios y organizaciones por igual. Los usuarios de Apple disfrutan de garantías al descargar y utilizar una app de la App Store porque Apple "**analiza cada app en busca de malware y otro software que pueda afectar la seguridad y privacidad del usuario**". Para los usuarios de Android, Google Play Store dispone de Google Play Protect. Pero eso no detiene a los actores de las amenazas.En los últimos cinco años, Apple ha evitado más de 9,000 millones de dólares en transacciones potencialmente fraudulentas. La **Ley de Mercados Digitales de la Unión Europea** (DMA) permite la creación de mercados alternativos de apps y exige a los "guardianes" que abran sus jardines amurallados. Las apps distribuidas a través de tiendas alternativas de apps no siguen las mismas directrices que las de la App Store de Apple, lo que puede representar un riesgo para la seguridad y la privacidad de los usuarios. La ingeniería social (p. ej., el phishing), el ransomware, el spyware de consumo y otros se documentan como riesgos que pueden introducirse para los usuarios que descargan apps o utilizan sistemas de pago alternativos fuera de la App Store de Apple.

Para los dispositivos Android, a principios de este año, **Google advirtió sobre un nuevo troyano** que se descubrió "atacando más de 750 aplicaciones legítimas de banca y compras". Ahora, las dos tiendas de aplicaciones más comunes se han visto obligadas a permitir a los usuarios la carga lateral de aplicaciones en la UE, lo que abre la superficie de ataque a los actores de amenazas.

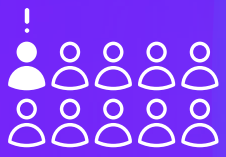
IV. Los ataques selectivos ponen en peligro los dispositivos móviles

Los dispositivos móviles proporcionan la flexibilidad necesaria para trabajar donde queramos o necesitemos; a menudo, los usuarios de alto nivel utilizan dispositivos móviles para realizar negocios en todo el mundo. **Pero los usuarios de alto perfil suelen ser el grupo de individuos más atacado** debido a los datos que contienen sus dispositivos: propiedad intelectual, datos financieros y mucho más. Los atacantes buscan personas bien conectadas y de alto perfil para obtener el máximo rendimiento de sus planes de chantaje.

En los últimos 12 meses, encontramos:

25%

de las organizaciones se vieron afectadas por un ataque de ingeniería social



1 de 10

usuarios hizo clic en un enlace malicioso de phishing

I. Phishing en móviles

El phishing es una de las amenazas más comunes y dañinas a las que se enfrentan las organizaciones hoy en día. Según la Agencia de Ciberseguridad y Seguridad de las Infraestructuras, "más del 90% de los ciberataques exitosos **comienzan con un correo electrónico de phishing**".

El phishing procede de diversos canales en los dispositivos móviles. Ya no se trata solo del correo electrónico, sino que los ataques se producen a través de mensajes de texto (llamados smishing), redes sociales o enlaces a sitios web falsos.

Pero, ¿por qué el phishing tiene tanto más éxito en los dispositivos móviles?

En primer lugar, es importante entender que **más del 62% de las visitas a páginas web de todo el mundo** proceden de dispositivos móviles. Esto significa que los dispositivos móviles representan una mayor parte del tráfico de Internet, lo que proporciona a los actores de amenazas un mayor número de objetivos potenciales para sondear en busca de vulnerabilidades.

Por el contrario, los dispositivos móviles son aparatos compactos con pantallas más pequeñas. Y esto es parte de su popularidad: su tamaño permite a los usuarios llevarlos a cualquier parte. También permite a las organizaciones implementar flujos de trabajo en los que intervienen dispositivos móviles como en:

- Comercio minorista (puntos de venta o inventarios)
- Asistencia médica (rondas de enfermería o junto a la cama del paciente)
- Fabricación (instrucciones para el operador/maquinaria)
- Aviación (bolsas de vuelo electrónicas o dispositivos bajo el ala)

Pero estas ventajas son las que propicia que los usuarios se distraigan cuando se trata de ataques maliciosos de phishing. Sigue existiendo la percepción de que los dispositivos móviles son intrínsecamente seguros, pero, como hemos documentado, basta un enlace para que un dispositivo se vea comprometido.

Las 20 marcas más utilizadas en campañas de phishing

Los dispositivos móviles permiten a las organizaciones implementar nuevos flujos de trabajo, agilizar la forma de conectar con los clientes y mejorar la experiencia del usuario. El uso de un dispositivo móvil es la forma en que muchos de nosotros trabajamos hoy en día, ya sea un dispositivo de acompañamiento o el principal punto de entrada. El móvil nos conecta con nuestra vida, tanto en el trabajo como en casa. Los atacantes conocen este hecho y lo utilizan para sus nefastas actividades.

En nuestra investigación, descubrimos que ciertas marcas populares se utilizan como parte de ataques de ingeniería social para explotar a los usuarios finales en dispositivos móviles. Hemos dividido estas marcas en **cuatro categorías** que son las más utilizadas para explotar la confianza del usuario final:

La miríada de razones por las que se utilizan los dispositivos móviles —acceder al correo electrónico del trabajo, encargar un artículo doméstico, realizar operaciones bancarias personales— fomenta que los actores de amenazas exploten estos casos de uso comunes, a menudo necesarios, para acceder a los datos. En la tabla siguiente, mostramos las 20 principales marcas que se utilizaron en ingeniería social, basándonos en esas cuatro categorías.

1.	2.	3.	4.
Entretenimiento	**Comercios**	**Servicios**	**Personal**
Netflix	Outlook	Servicio Postal de Estados Unidos	Amazon.com Inc
Bet365	Office365	Gazprom	Telegram
Steam	Allegro	AT&T Inc	Facebook, Inc
	InterActive Corp	Orange S.A.	Chase
	Tencent	DHL	WhatsApp
		BT Group	Yahoo, Inc.

Debido a su popularidad, prestigio e influencia tanto en empresas como en particulares, estas marcas son explotadas con frecuencia por los actores de amenazas en ataques de ingeniería social. Su reputación de confianza hace que los usuarios sean más propensos a participar en contenidos maliciosos disfrazados de comunicación legítima.

Aunque esta lista destaca las 20 marcas más atacadas el año pasado, dista mucho de ser exhaustiva. Los atacantes se adaptan constantemente, y las marcas que imitan pueden cambiar en cualquier momento. En última instancia, esto subraya cómo los atacantes utilizan la confianza que estas marcas han generado a lo largo de los años para engañar y explotar a los usuarios.

En el mundo moderno, nuestra información personal está constantemente en peligro. Con el aumento del uso de dispositivos móviles para fines personales y laborales, el alcance de los atacantes sigue ampliándose. Los atacantes emplean tácticas más sofisticadas, utilizando interfaces realistas, experiencias de usuario y estilos de comunicación auténticos para hacer caer en su trampa a víctimas desprevenidas. Pero existen salvaguardas (p. ej., capacitación continua de los empleados y herramientas de prevención de amenazas) que las organizaciones pueden emplear para proteger a sus usuarios y datos.

Jamf identificó aproximadamente **10 millones de ataques de phishing** durante el **periodo de 12 meses** que afectaron a nuestro grupo de muestra de **1.4 millones de dispositivos**.

Además, descubrimos que **del 1.5% al 2%** de estos ataques se clasificaban regularmente como **de día cero**, lo que significa que los atacantes utilizaban destinos totalmente nuevos y nunca vistos para engañar a los usuarios y hacerles hacer clic en enlaces maliciosos.

Identificar y verificar los ataques de phishing de día cero ayuda a las organizaciones a proteger a los usuarios para que no sean víctimas de sitios de phishing nuevos y no detectados

La perspectiva de un CISO

- **Introducir un sólido programa de capacitación:** Ha sido esencial para nuestro éxito. Llevamos a cabo sofisticadas campañas de phishing, impartimos capacitación gamificada, ofrecemos capacitación puntual a los usuarios que lo soliciten y permitimos a los usuarios denunciar correos electrónicos de phishing mientras que reciben confirmación y retroalimentación sobre sus envíos durante todo el año. Para nosotros no se trata de una capacitación de una vez al año y "ya está".
- **Manténgase al día de las nuevas tendencias y tácticas:** Esto puede parecer obvio, pero los atacantes siempre sacan provecho de todo lo que pueden y, a menudo, eso incluye algo nuevo, innovador o controvertido en las noticias. Hay que adaptar la capacitación y las tácticas de bloqueo para hacer frente a esas situaciones. Esto puede causar cierto malestar entre los usuarios, pero es clave la transparencia. El objetivo de la capacitación es prepararles para un posible malhechor que no tendrá en cuenta sus sentimientos al causar daño y que, a menudo, buscará una respuesta emocional para confundir y burlar a la víctima.
- **Adopte un enfoque estratificado:** No existe una única herramienta para evitar convertirse en víctima de una campaña de phishing dirigida. Asegúrese de estar cubierto desde múltiples ángulos. Bloquee dominios maliciosos. Asegúrese de que dispone de MFA. Adopte una metodología de confianza cero. Tenga activadas las reglas de velocidad imposible. Una o dos de esas cosas pueden no ser suficientes, pero aplicar múltiples capas de seguridad garantiza la forma más viable de evitar convertirse en otra víctima de un ataque de phishing.

II. Manejo de la vulnerabilidad

Se producen vulnerabilidades cuando existe una debilidad o defecto en un sistema, aplicación o protocolo que puede ser explotado por atacantes para comprometer su seguridad, integridad y/o disponibilidad. **Apple** y **Google** proporcionan una lista de vulnerabilidades conocidas que afectan sus sistemas operativos. Sin embargo, lo que esto significa es que estas vulnerabilidades "salen al mundo" antes de que Apple o Google proporcionen una actualización o un parche de seguridad. Del 1 de enero de 2024 al 1 de abril de 2025, Apple documentó **29 actualizaciones de seguridad** con CVE asociadas para versiones mayores y menores de iOS. Y en ese mismo periodo de tiempo, Android documentó **39 vulnerabilidades de sistema** con una CVE asociado en el Boletín de Seguridad de Android.

Apple (a través de **Rapid Security Responses**) y Google (a través de **Android Security Patches**) publican parches de seguridad independientes entre las actualizaciones de software. ¿Por qué son beneficiosos estos parches? Son actualizaciones puntuales, lo que significa que las organizaciones pueden aplicarlas automáticamente sin tener que esperar a que se produzcan actualizaciones mayores.

Las **ciberamenazas** modernas son creativas y complejas, y tanto los consumidores como las empresas deben estar atentos a la actualización de sus dispositivos. No solo se trata de actualizar el dispositivo, sino de verificar que la **actualización** sea **auténtica**.

Jamf Threate Labs investigó recientemente un método específico utilizado durante una secuencia de ataque: mantener la persistencia. Su investigación demostró cómo "los adversarios podrían explotar la interfaz de ajustes de iOS y manipular los ajustes de actualización del sistema, con avisos y notificaciones que indican una actualización disponible de iOS".

Analicemos en profundidad algunas vulnerabilidades dignas de mención de los últimos lanzamientos de Apple:
(este informe se redactó en abril de 2025)

Solución a la CVE de Apple	Fecha	Puntuación de vulnerabilidad	Impacto
iOS 18.4.1 y iPadOS 18.4.1	Abril de 2025	CVE-2025-31200 CVSS - Puntuación: 7.5 | Gravedad: Alta	CoreAudio
iOS 18.4 y iPadOS 18.4	Abril de 2025	CVE-2025-30430 CVSS - Puntuación: 9.8 | Gravedad: Crítica	Servicios de autenticación
iOS 18.3 y iPadOS 18.3	Enero de 2025	CVE-2025-24085 CVSS - Puntuación: 7.8 | Gravedad: Alta	CoreMedia
iOS 18.3 y iPadOS 18.3	Enero de 2025	CVE-2025-24154 CVSS - Puntuación: 9.1 | Gravedad: Crítica	Filtro de contenido web

Versiones AOSP* actualizadas	Fecha	Puntuación de vulnerabilidad	Impacto
13, 14, 15	Abril de 2025	CVE-2025-26416 Gravedad: Crítica	Escalada de privilegios
15	Marzo de 2025	CVE-2025-22403 Gravedad: Crítica	Ejecución remota de código
15	Febrero de 2025	CVE-2025-0096 Gravedad: Alta	Escalada de privilegios
12, 12L, 13, 14, 15	Enero de 2025	CVE-2024-43771 Gravedad: Crítica	Ejecución remota de código

*Proyecto Android de código abierto

Las vulnerabilidades —todas ellas registradas en el sitio web de Apple y Android— nos demuestran que cuando se desarrolla software, se producen vulnerabilidades. Lo importante para los profesionales de la seguridad es poder ver esas vulnerabilidades y actuar sobre ellas para mantener sus datos a salvo.

Una de las mejores formas de hacerlo es con sistemas operativos actualizados, y las herramientas para implementar esas actualizaciones.

Mantener una buena postura de seguridad con sistemas operativos actualizados

La mejor forma de que las empresas mitiguen las vulnerabilidades y mantengan su organización en cumplimiento es actualizando el sistema operativo de sus dispositivos. Como se muestra en la página anterior, tanto Apple como Android proporcionan actualizaciones de los sistemas operativos con vulnerabilidades conocidas de forma rutinaria.

Una forma habitual de que las organizaciones actualicen el sistema operativo (y las aplicaciones empresariales que sus empleados utilizan a diario) es a través de una solución de administración de dispositivos móviles (MDM). La MDM también proporciona informes de inventarios detallados sobre el sistema operativo que tiene instalado cada dispositivo administrado. Pero a menudo, las organizaciones tienen muchos dispositivos utilizados para diversos casos de uso, que ejecutan diferentes aplicaciones para diferentes usuarios. Es difícil (y a menudo inviable, p. ej., probar las aplicaciones antes de implementarlas) tener todos los dispositivos de una flota con el sistema operativo más reciente.

En los últimos 12 meses:

32%

de las organizaciones operan al menos un dispositivo con vulnerabilidades críticas (y parchables)

55.1%

de los dispositivos móviles utilizados en el trabajo utilizan un sistema operativo vulnerable

Se descubrió que las organizaciones utilizaban dispositivos móviles sin los últimos parches de seguridad. En nuestros datos, descubrimos que **el 4.8%** de todos los dispositivos Android con vulnerabilidades se utilizaron para acceder a recursos de la empresa.

La movilidad nos permite trabajar como queramos. Desde atender llamadas de trabajo en el auto hasta ampliar los flujos de trabajo de los empleados de primera línea y de cara al cliente, los dispositivos móviles abren las puertas a todo lo que es posible en el trabajo. Pero, como cualquier dispositivo informático, el sistema es vulnerable a las amenazas. Las organizaciones pueden tomar medidas para mitigar las amenazas a través de sus dispositivos móviles mediante herramientas que equilibren la usabilidad y la seguridad, la capacitación de los empleados y la comprensión de las amenazas más comunes en la actualidad.

La perspectiva de un CISO

- **Garantice la visibilidad de las vulnerabilidades en toda su organización:**
  Es un buen punto de partida obtener la máxima información sobre las vulnerabilidades presentes en los dispositivos de los usuarios finales o en la infraestructura. Puede partir de esos datos para analizar la huella específica de la aplicación, los riesgos potenciales, el radio de impacto, etc. Esta es una buena forma de empezar a priorizar sus vulnerabilidades en función de los datos.
- **Introduzca un programa de aplicación de parches sólido:**
  Retomando el punto de la MDM, contar con una herramienta que le permita mantenerse al día con las últimas versiones compatibles (N-X) de software o sistemas operativos es fundamental para mantener un entorno saludable y seguro. Hacer esto con poco o ningún impacto para los usuarios finales simplemente facilita la colaboración y el apoyo al negocio.
- **Aplique un enfoque de entrada basado en el riesgo:**
  Si tiene dispositivos que no cumplan la normativa e intentan acceder a los recursos de su empresa, debe restringir ese acceso hasta que el usuario final pueda corregir la situación y hacer que el dispositivo vuelva a cumplir, con el menor esfuerzo posible.

III. Riesgo de la aplicación

A finales de noviembre de 2024, la Agencia de Ciberseguridad publicó **un informe sobre las vulnerabilidades más explotadas en 2023**. (Esta es la última versión del informe.) El informe profundiza en las 15 principales vulnerabilidades, incluyendo detalles sobre lo que la vulnerabilidad permite a los atacantes lograr. Las vulnerabilidades se producen en los sistemas operativos de todas las plataformas informáticas y en las aplicaciones que los empleados y estudiantes de las organizaciones utilizan a diario. Como menciona el informe, "los ciberactores maliciosos explotaron más vulnerabilidades de día cero para comprometer las redes empresariales en 2023 en comparación con 2022, lo que les permitió llevar a cabo operaciones contra objetivos de alta prioridad". A continuación, la Agencia de Ciberseguridad indica qué pueden hacer los desarrolladores y las organizaciones de usuarios finales para mitigar las vulnerabilidades. Para las organizaciones de usuarios finales, el informe menciona:

- Actualizar *oportunamente* el software, el sistema operativo, las apps y el firmware
- Realización rutinaria del descubrimiento automatizado de activos
- Implementar un sólido proceso de control de parches
- Documentar las configuraciones básicas seguras
- Realice periódicamente copias de seguridad seguras del sistema
- Mantener actualizado un plan de respuesta a incidentes de ciberseguridad

¿Qué hace que una aplicación sea "riesgosa"? Algunos de los principales atributos de las aplicaciones riesgosas son:

- Características anómalas
- Patrones de código malicioso
- Permisos peligrosos
- Comportamiento dinámico arriesgado
- Perfiles de desarrolladores sospechosos

La visibilidad de las versiones de las aplicaciones, de las aplicaciones con fugas y de otros datos ayuda a las organizaciones a anticiparse y a estar preparadas para investigar y remediar el riesgo de inmediato.

Es importante que las empresas conozcan el estado completo de sus aplicaciones. Algunos de los datos clave a los que las organizaciones deben prestar atención para identificar y remediar las aplicaciones riesgosas son:

- Número de usuarios con una aplicación obsoleta instalada
- Número de usuarios con una versión específica de la aplicación
- Lista de apps con implementaciones de cifrado defectuosas, lo que provoca la filtración de datos confidenciales a redes desprotegidas
- Apps que solicitan determinados permisos para acceder a datos de otras partes del dispositivo

Una mirada en profundidad a una vulnerabilidad del mundo real
Eludir la transparencia, el consentimiento y el control (TCC)

En todos los sistemas operativos de Apple, la TCC es un marco de seguridad crucial que permite a los usuarios conceder o rechazar solicitudes de aplicaciones individuales para acceder a datos sensibles como fotos, contactos y detalles de localización. Una vulnerabilidad para eludir TCC se produce cuando falla este control, permitiendo que una aplicación acceda a información privada sin el consentimiento o conocimiento del usuario. Lo que esto significa es que los atacantes pueden obtener acceso no autorizado a archivos y carpetas, datos médicos, el micrófono o la cámara y mucho más sin alertar a los usuarios.

Jamf Threat Labs descubrió la CVE-2024-44131, una vulnerabilidad para eludir el TCC que afecta a File Provider en los dispositivos iOS. Apple respondió rápidamente a este descubrimiento con un parche en iOS 18.0. Las CVE, como la CVE-2024-44131, son importantes recordatorios de la necesidad de mantener actualizados los dispositivos de la organización.

Protecciones e intentos de fraude en la App Store

Como ya se ha mencionado anteriormente en este informe, en los últimos cinco años Apple ha evitado transacciones fraudulentas por valor de más de $9,000 millones de dólares. Solo en 2024, la empresa bloqueó más de $2,000 millones de dólares en transacciones fraudulentas. Para ir más lejos, en 2024 Apple:

- Canceló más de 146,000 cuentas de desarrolladores por situaciones fraudulentas
- Rechazó otras 139,000 inscripciones de desarrolladores
- Rechazó más de 43,000 aplicaciones por contener características ocultas o no documentadas
- Rechazó más de 320,000 envíos que copiaban otras apps, eran spam o de alguna manera inducían a errores a los usuarios.
- Detectó y bloqueó más de 10,000 aplicaciones ilegítimas en tiendas pirata

La App Store suele considerarse la forma más segura, fácil de usar y privada de descargar apps. La App Store para iOS utiliza sandboxing, peticiones de permiso al usuario y solo permite ejecutar código firmado en el dispositivo. Pero, como muestran los datos, persisten los agentes maliciosos y el potencial fraude. El compromiso de Apple de mantener la App Store como un lugar seguro y de confianza para las aplicaciones ha protegido a usuarios y desarrolladores desde su lanzamiento en 2008. Sin embargo, las "apps cargadas lateralmente" (apps de tiendas de apps de terceros, como AltStore) no gozan de la misma protección.

La perspectiva de un CISO

Una seguridad móvil eficaz requiere un enfoque estratificado. Utilizar el hardware más reciente de un proveedor de confianza y el sistema operativo más actual sigue sin ser suficiente para proteger su organización y sus activos más sensibles frente a los riesgos. Las buenas prácticas de seguridad deben extenderse a cada capa de su pila tecnológica, y eso incluye también las aplicaciones.

- **Introduzca un programa de verificación de aplicaciones para las aplicaciones móviles sensibles de su organización:** empiece por las apps más críticas y compruebe de forma rutinaria que se ejecuten las versiones más recientes y seguras en toda la organización. A medida que amplíe el programa, investigue todas las aplicaciones que entren en la tienda de aplicaciones de su empresa.
- **Desarrolle políticas que etiqueten los dispositivos como "no cumplen"** cuando se instalen aplicaciones no deseadas; impida que estos dispositivos en riesgo accedan a sus aplicaciones SaaS, centros de datos críticos o cargas de trabajo remotas hasta que se actualicen o eliminen las aplicaciones riesgosas.
- **Introduzca la seguridad de las aplicaciones móviles en los programas de capacitación** para que los usuarios se conviertan en parte de la solución aplicando actualizaciones cuando sea necesario en dispositivos que permanezcan con ellos durante toda la jornada laboral o la semana de trabajo.
- **Si su organización no requiere mercados de aplicaciones alternativos**, establezca políticas para evitar que se acceda a tiendas alternativas en dispositivos de trabajo. Además, impida las aplicaciones cargadas en forma lateral para asegurarse de que solo se utilicen en el dispositivo las que proceden de fuentes oficiales.

El equipo de Jamf Threat Labs publicó una demostración de cómo una aplicación de redes sociales de carga lateral puede monitorear fotos y subirlas al servidor de un atacante. Esta aplicación fue "modificada, pero era perfectamente funcional". El equipo ofrece algunas garantías claras para mejorar la seguridad, a saber:

- Activar y revisar periódicamente el informe de privacidad de la aplicación
- Ser selectivo con los permisos de las aplicaciones
- Evitar almacenar información sensible

Descargar apps solo de fuentes confiables (como la App Store)

Tanto las aplicaciones nativas como las aplicaciones web alojadas en la nube son susceptibles de sufrir riesgos. Las aplicaciones alojadas en la nube están más expuestas a los riesgos debido a la mayor superficie de ataque. Sin embargo, con las capacidades adecuadas de visibilidad, control y reparación, las organizaciones pueden mitigar las aplicaciones de riesgo en el trabajo.

IV. Ataques selectivos y programas espía sofisticados

Desde 2021, **Apple ha enviado** notificaciones de amenazas a usuarios de más de 150 países. Estas notificaciones informan y ayudan a los usuarios, normalmente personas de alto perfil como periodistas, políticos o diplomáticos, que son blanco de ataques de spyware mercenario. Y, a finales de abril de 2025, Apple "envió notificaciones esta semana a varias personas que la compañía cree que fueron blanco de spyware del gobierno". Pero no se trata solo de Apple. Estos ataques se dirigen a todo tipo de sistemas operativos y aplicaciones. **Según The Citizen Lab,** "se había cargado software espía en WhatsApp, así como en otras apps de sus dispositivos [Android]".

El malware y el spyware, como aquellos sobre los que Apple envía notificaciones de amenazas, son algunas de las amenazas más avanzadas a las que se enfrentan hoy en día las organizaciones y los particulares. Pero existen protecciones para mantener a todos los usuarios —a cualquier nivel de su organización— a salvo de estas amenazas avanzadas.

Apple ofrece orientaciones a todos los usuarios sobre cómo protegerse del malware, muchas de las cuales ya hemos tratado en este documento. En concreto, Apple aconseja a los usuarios que:

- Actualicen los dispositivos al software más reciente, ya que incluye las últimas correcciones de seguridad
- Protejan los dispositivos con una contraseña
- Utilicen la autenticación de doble factor y una contraseña segura para su cuenta de Apple
- Instalen aplicaciones desde la App Store
- Utilicen contraseñas seguras y únicas en Internet
- No hagan clic en enlaces o archivos adjuntos de remitentes desconocidos

Jamf Threat Labs: Comprometer un dispositivo sin el conocimiento de la víctima

Jamf Threat Labs demostró que un dispositivo — sin software de seguridad de protección — se veía comprometido sin que la víctima lo supiera. La demostración mostró cómo un atacante pudo obtener acceso al correo electrónico, la mensajería corporativa, la autenticación de dos factores y más datos personales. A continuación, el equipo muestra cómo las organizaciones pueden proteger los datos organizativos y personales:

1. Implemente configuraciones seguras para mantener el cumplimiento tanto en dispositivos propiedad de la empresa como en dispositivos BYO
2. Habilite la prevención y el monitoreo de amenazas con acciones específicas, conservando la privacidad del usuario final
3. Aplique el cifrado de dispositivos en todos los dispositivos administrados

La perspectiva de un CISO

El malware no está tan extendido en los móviles como en otros dispositivos informáticos primarios. Sin embargo, cuando se descubre, a menudo se encuentra que hace uso de técnicas muy avanzadas y se utiliza para atacar a individuos.

- **No se duerma en sus laureles** y suponga que el malware móvil nunca afectará a su organización. El año pasado, Apple envió avisos de software espía que comprometía a usuarios de unos 100 países.
- **Como mínimo, designe a un responsable de seguridad móvil** y encárguele la elaboración de informes periódicos sobre el estado del despliegue móvil de su organización. Catalogue incidentes de teléfonos robados, phishing selectivo, caídas de rendimiento y cualquier otra cosa que capte un comportamiento irregular. Lo ideal es establecer un flujo de telemetría desde sus herramientas de administración de dispositivos y de seguridad, e incorporar esos datos a su centro de operaciones de seguridad. Trate el móvil como cualquier otro endpoint.
- **Cuando sea posible, recopile datos del sistema móvil y busque pruebas de ataques de día cero.** Para ello se necesitarán conocimientos especializados que pueden ser internos o contratados. Las organizaciones empresariales que cuenten con analistas de seguridad dedicados invierten en el desarrollo de una pericia forense móvil dentro de sus equipos.

Puntos clave

El phishing en móviles es una de las formas más comunes que tienen los atacantes de acceder a información sensible. Las organizaciones que pueden implementar un programa de capacitación, mantenerse al día de las tendencias y tácticas (incluida la adaptación de dicha capacitación) y tener un enfoque de la seguridad por capas, proporcionan a las organizaciones protección desde distintos ángulos.

Las vulnerabilidades aparecen en software de todo tipo. Establecer una higiene de seguridad adecuada mitiga los riesgos que pueden introducir las vulnerabilidades. La actualización periódica de los sistemas operativos y la desactivación de controles innecesarios (p. ej., tiendas de aplicaciones de terceros) ayudan a las organizaciones a mantener el cumplimiento de las líneas de base internas y los marcos externos.

Una administración inadecuada de las apps y su uso conllevan riesgos. No siempre se trata de la propia app, sino también de las apps que realizan conexiones de red maliciosas. Mediante la creación de una tienda de aplicaciones empresariales y la revisión continua de las aplicaciones (especialmente las privadas y personalizadas), las organizaciones pueden supervisar, reparar y parchar mejor las aplicaciones vulnerables.

Las APT y los ataques de spyware son cada vez más frecuentes. Estas amenazas (a menudo originadas por estados-nación o grupos especializados) afectan a organizaciones de todo el mundo, y con frecuencia se dirigen a personas de alto perfil con datos confidenciales en sus dispositivos. Al proporcionar una estrategia de seguridad de defensa en profundidad y tratar el móvil como cualquier otro dispositivo, las organizaciones pueden garantizar medidas de protección de su ecosistema de dispositivos móviles y de los datos a los que se conectan los dispositivos.

Establezca y mantenga políticas de uso aceptable para los dispositivos propiedad de la empresa que requieran políticas de uso aceptable de cumplimiento obligado se conecten a recursos de trabajo o deban cumplir políticas organizativas. En el caso de los dispositivos BYO, estos requerirán controles de privacidad adicionales, como **las protecciones de privacidad que Apple proporciona** a los dispositivos.

jamf

Póngase en contacto con nosotros para obtener más información sobre el panorama de las amenazas móviles.