



Security 360:

Informe anual de tendencias

Mac

```
1 Arc Browser Executables:
2 9d103cbad2b56f53a36f93316feda1de5513394d - ArcSetup.dmg
3 ba59bb35e8dfbe77676c8130c8c2d61c22b14564 - ArcSetup (Univ
4 d294b86c5a57e90ff1f7367eb9fdad8d47193f22 - ArcSetup (x86)
5 af33c2bc39373a5607b0c38a62919c59f5ad884 - ArcSetup (ARM)
6
7 5687190b00a1efald3671d0b03b8f69da6d534a - ArcInstaller.d
8 28c35f4d92f3a0b185f0ffab5b695119de823548 - ArcInstaller
9 28cc0be3aad1479c4d4ba618be6462a2c5c7ac18 - ArcInstaller
10 0ac59146723d72b2faad0a637cd9fb2a6221f7e - ArcInstaller
11
12 https://arcll.net
13 https://arcll.net
14 193[.]233[.]132[.]108 - Exfiltration IP
15
16 Meethub Executables:
17 7f22760d6d85f8173292d39ea087f35695ad65ab - Meethub.pkg
18 3865636ed27ae81f146ed509ac9a25f53a6d10a7 - sleeve (x86)
19
20 Chainbreaker Executables:
21 50b8af2019adbbea310bce0259b4a3f3da2e4d7d - game/installer
22 eecf5ffc338b97602b5b8fab8ccc51dcb8ffdb8a - game/installer
23 596fd483314c3cce43d8b5ed38b5202c29a60b14 - game/installer
24
25 https://meethub[.]gg
26 46[.]101[.]104[.]172 - Exfiltration IP
27
28 Suarometa Malware:
29 7aef8396238d96c1ffa845715373516da30e373 - SuaWorldLaunc'
```

Prólogo

En Jamf, nos encanta Mac. Es la primera máquina para la que comenzamos a desarrollar software, y sigue siendo la máquina que apasiona a muchos de nosotros. (Somos un **colaborador oficial del Proyecto de Cumplimiento de Seguridad de macOS**.) A lo largo de nuestra historia, hemos visto cómo la Mac se convertía en **una parte cada vez más importante del entorno de trabajo**. Lo que empezó como una máquina para los profesionales creativos y ejecutivos está cada vez más arraigado en las operaciones diarias para ingenieros y más usuarios. Pero con su continua integración en el trabajo, se convierte en una mayor superficie de ataque para los actores de amenazas.

El panorama de las amenazas para Mac es más diverso que nunca, con formas más creativas de poner en peligro estos dispositivos. En nuestra misión de "ayudar a las organizaciones a triunfar con Apple", analizamos en profundidad el panorama de las amenazas que afectan a los dispositivos Mac para servir a nuestros clientes y a la comunidad Apple en general.

– Jaron Bradley,
Director, Jamf Threat Labs

Introducción

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

Proporcionamos una evaluación de los diferentes vectores de ataque (como el malware, las vulnerabilidades y la ingeniería social) que se utilizan activamente para engañar a los usuarios, comprometer los dispositivos e infiltrarse en las organizaciones. El análisis incluye temas como las vulnerabilidades de los dispositivos, las amenazas web, el malware y otros.

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 en las que piensan los líderes de seguridad a la hora de proteger su Mac 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 de 12 meses anterior y abarcando globalmente 90 países.



Para preservar la privacidad y mantener las máximas normas de seguridad en la recopilación y el tratamiento de datos, los metadatos analizados en nuestra investigación proceden de registros agregados que no contienen información personal ni 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 forma en que las organizaciones y los usuarios pueden tomar medidas para mitigar los riesgos. También ofrece resúmenes de las investigaciones más impactantes de Jamf Threat Labs, incluyendo los descubrimientos de malware y vulnerabilidades.

Hay varias medidas que cualquiera puede tomar para mejorar la seguridad de su Mac. Por ejemplo, solo descargue software de fuentes en las que confíe. Pero hay otras buenas prácticas que cualquier organización puede aplicar:

- Actualizaciones continuas y puntuales del sistema operativo
- Educación y capacitación de los usuarios
- Verificación de solicitudes
- Autenticación multifactor
- Infraestructuras de seguridad de confianza cero
- Políticas de uso aceptable de los datos corporativos
- Implementación de los mejores flujos de trabajo de Apple en todos los casos de uso



Si bien algunos de ellos son básicos para todas las organizaciones, hay otros requisitos de seguridad de los dispositivos que son específicos de cada organización. Por ejemplo, las organizaciones de un sector regulado pueden tener que cumplir con los puntos de referencia o infraestructuras de la industria (como los puntos de referencia CIS o la HIPAA).

Este año, estructuramos nuestro análisis en tres categorías de riesgo que consideramos prioritarias para las organizaciones de todo el mundo:

I. Riesgo de aplicaciones y malware

II. Manejo de vulnerabilidades

III. Ingeniería social



También disponemos de un informe Security 360 enfocado en los **dispositivos móviles** que puede consultar [aquí](#).

Gran parte del 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.

Principales tendencias de Mac en la empresa

El malware introduce riesgos, incluso en plataformas seguras

Apple diseña sus **plataformas incluyendo la seguridad como factor central**. No se trata solo de las plataformas en sí, sino de cómo Apple comunica la seguridad a sus usuarios. Por ejemplo, el **sitio de seguridad de la plataforma de Apple** incluye una página que informa a los usuarios de Apple sobre la protección contra el malware en macOS. Las diferentes tecnologías de Apple (como App Store, XProtect o Gatekeeper) añaden capas de protección contra aplicaciones maliciosas en distintas fases del ciclo de vida de una aplicación.

Para los dispositivos Mac en el trabajo, la seguridad es un acto de equilibrio para proporcionar a los usuarios las aplicaciones que necesitan para hacer su mejor trabajo, pero para evitar el acceso a aplicaciones que pueden introducir riesgos. Las apps para Mac vienen en todas las formas y tamaños, como apps nativas para Mac, apps web y apps híbridas, creadas y diseñadas por desarrolladores para una variedad de casos de uso. Sin embargo, **muchas de las apps empresariales más comunes para Mac** hoy en día no proceden de la Mac App Store, sino que se empaquetan directamente desde el desarrollador. Por si fuera poco, los usuarios pueden descargar apps desde cualquier sitio al que tengan acceso.

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.

El Instituto Nacional de Normas y Tecnología (NIST) afirma:

"En el caso del software típico, los errores y vulnerabilidades existen con una frecuencia estimada de ~25 errores por cada 1000 líneas de código". Las vulnerabilidades y exposiciones comunes (CVE), publicadas en la Base Nacional de Datos sobre Vulnerabilidades (NVD), proporcionan al público:

- Conocimiento de las CVE
- El producto o proveedor afectado
- Descripción de las amenazas

Entre el momento en que se descubre una vulnerabilidad y se parcha, el daño puede estar hecho. Cuando se publica un parche, es necesario instalarlo en los dispositivos afectados. Las herramientas de seguridad que proporcionan información sobre las vulnerabilidades presentes y más críticas ayudan a los equipos de IT e InfoSec a priorizar los parches más urgentes y mejorar sus procesos.

La ingeniería social continúa comprometiendo a los usuarios

La ingeniería social, al igual que el phishing, sigue siendo una de las técnicas de ataque más frecuentes 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 orientaciones a sus usuarios para ayudarles a "evitar estafas y saber qué hacer si se reciben correos electrónicos, llamadas telefónicas u otros mensajes sospechosos". Los atacantes son cada vez más creativos en sus técnicas, haciéndose pasar por reclutadores, familiares, marcas de confianza, etc. Por muy segura que sea una plataforma o un sistema operativo, las técnicas de ingeniería social están diseñadas para infiltrarse en los datos empresariales empezando por la parte menos segura del dispositivo: el usuario.



Parte 1: Malware enfocado en Mac

Con este informe, queremos ofrecer una comprensión general del malware para Mac, incluyendo los tipos que hemos visto, cómo afecta cada uno de ellos a las organizaciones y con qué frecuencia. A medida que se extienda el uso del Mac en el lugar de trabajo y se acceda a más aplicaciones críticas a través de la plataforma, los usuarios de toda la organización se verán afectados.

La defensa contra el malware de Apple está estructurada en tres capas:

1. **Prevención del lanzamiento o ejecución de malware**
2. **Bloqueo del malware para que no opere en los sistemas de los clientes**
3. **Someter el malware que se ha ejecutado**

Las tecnologías de Apple (App Store, GateKeeper, XProtect y Notarization) ofrecen a los usuarios formas nativas de mitigar las amenazas. Por ejemplo, XProtect es un antivirus integrado. Y cuando se descubre malware, Apple puede responder de varias maneras, como revocar un ID de desarrollador.

El macOS, a pesar de sus potentes mecanismos de seguridad integrados en el sistema, no es inmune al malware. **En marzo de este año**, los equipos de Jamf Threat Labs y Data Science colaboraron en un artículo para hablar del mito del malware para Mac, para comprender el malware novedoso a partir del malware conocido y mostrar los vectores del malware para macOS con Titan, una herramienta de visualización 3D desarrollada por Jamf Threat Labs. Titan ayuda a proporcionar contexto e identificar muestras de malware relacionadas. Las familias de malware descubiertas muestran "el creciente número de nuevos programas maliciosos a la medida" para macOS. ¿Qué significa esto? El malware para Mac existe, hay familias de malware relacionadas y los actores de amenazas lo utilizan cada vez más.

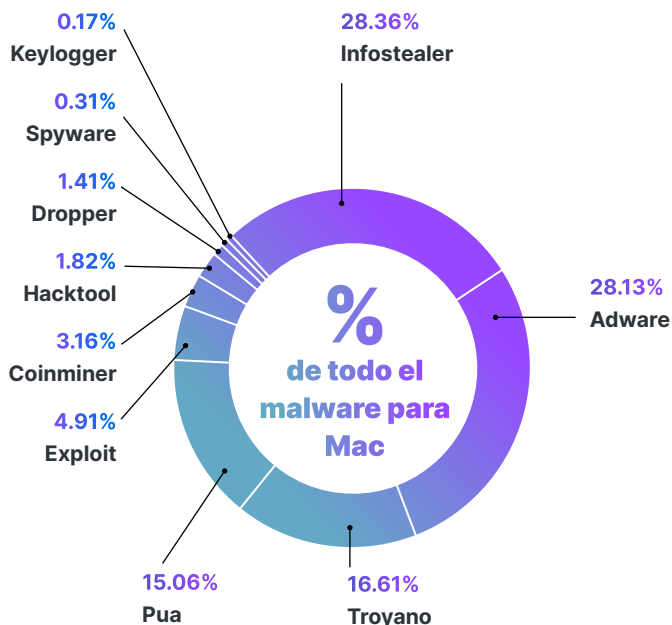


Este año, Jamf Threat Labs descubrió un programa malicioso, presuntamente vinculado a la República Popular Democrática de Corea (RPDC), **incrustado en una aplicación basada en Flutter**. Si bien el uso de aplicaciones desarrolladas con Flutter para soporte multiplataforma es común, lo que hace que este ataque sea digno de mención es que es la primera vez que el equipo de Jamf Threat Labs ha visto esta infraestructura utilizada para atacar dispositivos macOS. El equipo analiza el malware, sus variantes en Python y Golang y por qué "es probable que el malware esté siendo probado para una mayor militarización". También cabe destacar la oscuridad involuntaria que Flutter aplica al código escrito por los usuarios de su infraestructura.

Familias de malware dirigido a Mac

A continuación se muestra un desglose completo de los nuevos casos de malware para Mac estudiados en 2024, basado en nuestras conclusiones:

¿Qué nos dicen estos datos? Si los comparamos con el informe de programas maliciosos del año pasado, observamos algunas coincidencias: adware, troyanos, PUA (aplicaciones potencialmente no deseadas) y exploit (aplicaciones de las que se sabe que abusan de una vulnerabilidad) siguen encabezando la lista de categorías de programas maliciosos. (El año pasado, los troyanos tenían el mayor número de familias, con un 17%, ligeramente por debajo este año, con un 16.6%). El primer puesto este año es para los infostealers (ladrones de información). De hecho, los infostealers registraron un aumento del 28.08% del total del malware estudiado.



La presencia de infostealers sigue siendo consistente con las investigaciones que ha realizado Jamf Threat Labs durante el último año, siendo los entornos macOS objeto de constantes ataques por parte de este tipo de malware. Lo interesante de estas tácticas es que ambos atacantes no solo utilizan infostealers para acceder a los datos que desean, sino que también emplean otra estrategia mencionada anteriormente en este informe: la ingeniería social. Lo que esto nos muestra es que los actores de amenazas están utilizando una combinación de principios de ataque para engañar a sus víctimas. Para los empleados u organizaciones de sectores de alto perfil, como el de las criptomonedas, es importante mantenerse alerta, tanto desde el punto de vista de la capacitación como de las herramientas de seguridad. Los ataques no se producen por casualidad, sino que se diseñan.



Investigación del uso de PyInstallers para implementar infostealers en macOS

En abril de 2025, Jamf Threat Labs [descubrió nuevas muestras no detectadas de infostealers de macOS que empaquetan código Python en ejecutables Mach-O utilizando PyInstaller](#). (Jamf Threat Labs descubrió tres ladrones no detectados en VirusTotal)

PyInstaller es una herramienta legítima de código abierto que permite a los desarrolladores empaquetar scripts de Python en binarios independientes. Ahora los atacantes están aprovechando la misma técnica para entregar cargas útiles maliciosas que se ejecutan sin problema en macOS. El equipo revisó varias funciones clave para confirmar la verdadera naturaleza del malware: un ladrón de información. Entre las funciones clave se incluyen:

- Intentos de obtener las credenciales de los usuarios activando solicitudes de contraseña engañosas
- Ejecución de cargas útiles applescript arbitrarias desde el servidor del atacante
- Extracción de credenciales e información sensible guardadas directamente del llavero de macOS
- Escaneo del sistema de archivos en busca de carteras de criptomonedas conocidas para filtrar claves privadas y robar criptoactivos

A medida que los infostealers sigan siendo más frecuentes en el panorama de amenazas de macOS, los actores de amenazas seguirán buscando nuevas formas de distribuirlos. Sin embargo, existen medidas prácticas que las organizaciones pueden adoptar para protegerse contra el malware descrito anteriormente. Por ejemplo:

- Restringir la ejecución de software a las apps firmadas por Apple y los desarrolladores identificados.
- Marcar los avisos de osascript utilizados para procesos informáticos legítimos y capacitar al personal para que confirme la marca antes de introducir sus credenciales.

Malware a tener en cuenta

Poolrat

Poolrat, un infame backdoor de macOS por su implicación en el compromiso de la cadena de suministro de 3CX, permite a los atacantes recopilar datos cruciales del sistema y ejecutar comandos concurrentemente con operaciones de archivos. Recientemente, se ha descubierto una versión más ligera de Poolrat, apodada Pondrat.

Pondrat

Pondrat, un backdoor que presenta similitudes tanto con AppleJeuS como con Poolrat, se distribuyó a través de paquetes PyPi maliciosos. Tras su instalación, Pondrat establece conexiones con servidores de mando y control (C2) para facilitar la carga y descarga de archivos, pausar operaciones durante un tiempo predeterminado y ejecutar comandos arbitrarios.

NotLockBit

Ransomware basado en Golang que se hace pasar por una variante del infame ransomware LockBit. Desde su muestra inicial, el ransomware utiliza una clave pública incrustada para enumerar y cifrar una lista de extensiones codificadas. Las variantes más recientes de NotLockBit exfiltrarán datos a un bucket S3 controlado por el atacante y usarán osascript para cambiar el fondo de pantalla del Escritorio (LockBit 2.0). Se cree que NotLockBit está en desarrollo activo.

ThiefBucket

Thiefbucket, una familia de malware vinculada al grupo Lazarus de Corea del Norte, se dirige a las víctimas a través de sofisticadas campañas de ingeniería social. Se ha observado como una carga útil de segunda etapa, entregada a través de un desafío de codificación disfrazado. El backdoor demuestra varias capacidades, sobre todo su funcionalidad de robo automático de información. Entre otras capacidades se encuentran las siguientes: - Mecanismos de persistencia - Terminación de procesos - Eliminación de archivos - Descarga/subida de archivos - Autoeliminación - Ejecución de comandos de shell - Búsqueda rápida de archivos a través de Spotlight - Comunicación con servidores de comando y control

HZRat

HZ Rat, un backdoor para macOS, se dirigía inicialmente a usuarios de Windows, pero desde entonces ha evolucionado para dirigirse a usuarios de macOS a través de instaladores de software legítimo camuflados. Una vez instalado, HZ Rat establece conexiones con servidores de comando y control (C2) para permitir a los atacantes ejecutar comandos, robar archivos y extraer información confidencial como nombres de usuario, correos electrónicos, números de teléfono y otros datos personales de WeChat y DingTalk.

BansheeStealer

Anunciado en Telegram, Banshee Stealer funciona como un malware como servicio con una interfaz web para los atacantes. Especializado en el robo de información, puede filtrar una serie de datos confidenciales, como contraseñas de cuentas, datos del navegador, cookies de sesión y carteras de criptomonedas. Al igual que otros infostealers, Banshee abusa de las funciones de diálogo de AppleScript para engañar a los usuarios y hacerles proporcionar sus credenciales. Una vez introducida la contraseña del usuario, roba datos confidenciales adicionales del llavero de macOS. Banshee emplea varias técnicas de evasión, incluyendo medidas anti-VM y antidepuración para frustrar el análisis, así como la detección de sistemas en ruso.

InvisibleFerret

InvisibleFerret es un troyano basado en Python que ha sido utilizado por malware incrustado dentro de aplicaciones camufladas. Más notablemente, se ha visto lanzado por el BeaverTail InfoStealer (atribuido por algunos a la RPDC) como un implante de fase dos. El malicioso script Python es multiplataforma y permite a un atacante realizar tareas de reconocimiento, exfiltración de datos, copia del portapapeles y ejecución de comandos remotos. También es capaz de instalar el software AnyDesk si se desea un control remoto adicional.

BeaverTail

BeaverTail es un ladrón de información que se ha visto disfrazado de aplicación legítima antes de ser enviado a las víctimas a través de campañas de ingeniería social. Al igual que otros infostealers, toma detalles valiosos del llavero de las víctimas, cookies del navegador, criptocarteras, etc., y los sube a un servidor controlado por el atacante. También es capaz de ejecutar cargas útiles remotas adicionales en el sistema víctima, como el backdoor InvisibleFerret. Algunos lo han atribuido a la RPDC.

PoseidonStealer

Anunciado en Telegram, Poseidon Stealer (competidor de Atomic Stealer) funciona como un malware como servicio con una interfaz web para los atacantes. Especializado en el robo de información, puede filtrar una serie de datos confidenciales, como contraseñas de cuentas, datos del navegador, cookies de sesión y carteras de criptomonedas. Al igual que Atomic, Poseidon abusa de las funciones de diálogo de AppleScript para engañar a los usuarios para que proporcionen sus credenciales. Una vez introducida la contraseña del usuario, roba datos confidenciales adicionales del llavero de macOS. Distribuido bajo la apariencia de aplicaciones legítimas, se ha observado que el malware se promociona a través de publicidad maliciosa en Google Ads.

Kuiper

Kuiper es un ransomware como servicio (RaaS) desarrollado en Go, que fue anunciado en foros clandestinos por un usuario llamado Robinhood. Utiliza una combinación de RSA, ChaCha20 (archivos de menos de 600 megabytes) y AES (archivos de más de 600 megabytes) para cifrar archivos. Mientras que la mayor parte de la funcionalidad del malware se centra en Windows, la variante para macOS generará una clave aleatoria y un vector de inicialización (IV) aleatorio utilizando `/dev/urandom`, descifrará una nota de rescate, cifrará el objetivo de forma recursiva (añadiendo una extensión `.kuiper`), limpiará la clave y el IV de la memoria y reiniciará el sistema.

Malware para Mac observado

Para un análisis más detallado del malware para Mac observado en los entornos de los clientes, nuestros resultados indican que las siguientes familias de malware se encuentran entre las 10 primeras:

Apellidos	Categoría	Porcentaje	
Genieo	Adware	13.63	
Imobie	PUA	10.96	
Multiverze	Adware	9.44	
Mackeeper	PUA	7.19	
Tnt	PUA	6.07	
Jailbreak	PUA	5.74	
Ccleanmac	Adware	4.33	
Puagent	Troyano	3.07	
Macinformer	PUA	2.33	
Pirrit	Adware	2.33	

Estas cifras muestran que, aunque muchos tipos de malware, como los infostealers, están aumentando mucho en cantidad, el adware y las aplicaciones potencialmente no deseadas (PUA) siguen siendo las aplicaciones más descargadas e instaladas por los usuarios. Es una tendencia común que se observa en todas las plataformas de sistemas operativos, dado el amplio alcance del adware y la naturaleza más selectiva de los infostealers.



Jamf Threat Labs publicó un blog sobre **infostealers que tienen como objetivo a individuos de la industria del cripto**. ¿El objetivo de los atacantes? Recolección de credenciales con datos de varias criptocarteras. El equipo rastreó dos ataques que introdujeron infostealers en los sistemas de las víctimas:

1. A través de anuncios patrocinados de Google: al buscar “Arc Browser” los usuarios eran redirigidos a un sitio malicioso al hacer clic en un anuncio de Google.
2. A través de reuniones virtuales: Al ponerse en contacto para hablar de una oportunidad (como una entrevista de trabajo), los atacantes solicitan el uso de Meethub para programar una reunión.

En ambos casos, se pedía a los usuarios que descargaran la aplicación saltándose Gatekeeper y que introdujeran su contraseña de inicio de sesión en macOS.

Las familias de programas maliciosos que hemos estudiado y los ejemplos que ofrecemos muestran la necesidad de principios básicos de seguridad, como:

- Obtener solicitudes de fuentes legítimas
- Aplicar un proceso de verificación (ya sea a través de terceros de confianza, como la tienda de apps de Mac, o de un proveedor de administración de dispositivos)
- Ejecutar software de seguridad actualizado

La perspectiva de un CISO

- **Introducir una solución EDR específica para Mac:**

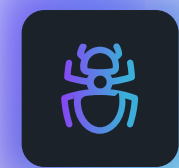
A menudo vemos que el software se centra en Windows y trata los dispositivos Apple como algo secundario en la empresa. Hace tiempo que sucedió eso, sobre todo en lo que respecta a la seguridad. Tenemos que enfocarnos en productos de seguridad desarrollados desde cero para productos Apple, a medida que madura el panorama de las amenazas.

- **Implementar una solución MDM sólida:**

La administración de los dispositivos es crucial para protegerlos. Dado el grado de libertad de los usuarios y el acceso que pueden poseer, es primordial disponer de una infraestructura sólida para administrar los dispositivos y los usuarios en esos dispositivos, con el fin de detener posibles brotes de malware antes de que se inicien.

- **Garantizar estrategias de comunicación sólidas:**

Desde la colaboración entre Seguridad e IT, divulgación de la marca de Seguridad, programas de capacitación, concientización del usuario final hasta memorandos ejecutivos. La comunicación eficaz de su programa de seguridad, las herramientas que utiliza y sus estrategias actuales ayudan a todos a alinearse y a enfocarse en un objetivo común.



Manejo de vulnerabilidades

No todas las vulnerabilidades son iguales. Varían según el nivel de gravedad y la mayoría tienen asignada una puntuación.

Apple proporciona una lista de vulnerabilidades de seguridad parchadas que afectan a macOS y al sistema operativo que corrige la vulnerabilidad. Por ejemplo, en 2024, Apple lanzó macOS 15.1.1 en respuesta a las vulnerabilidades [CVE-2024-44308](#) y [CVE-2024-44309](#), en las que el contenido web malintencionadamente manipulado podía escapar del sandbox de contenido web. Esta CVE tenía una puntuación de gravedad alta. Pero Apple también publica actualizaciones de seguridad para CVE con puntuaciones bajas. ¿Qué significa esto? Priorizar es importante. Cuando los equipos de IT y de seguridad pueden tener una visión completa de las vulnerabilidades en su huella de dispositivos, incluidos los sistemas y las aplicaciones, entonces son capaces de abordar adecuadamente lo que es más apremiante.

Apple dispone de una versión más especializada de actualizaciones de seguridad denominada Respuestas rápidas de seguridad, que ofrece **importantes mejoras de seguridad** entre actualizaciones de software. ¿Por qué son beneficiosos estos parches? Son actualizaciones ligeras, lo que significa que las organizaciones pueden aplicarlas automáticamente sin romper los sistemas internos. Por ejemplo, entre junio de 2024 y abril de 2025, Apple documentó **20 actualizaciones de seguridad** con CVE asociadas a versiones mayores y menores de macOS.

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

En todos los sistemas operativos de Apple, Transparencia, Consentimiento y Control (TCC) sirven como marco de seguridad crucial, ya que pide a los usuarios que concedan o rechacen las solicitudes de apps individuales para acceder a datos sensibles como el micrófono, la cámara web y el acceso a todo el disco. 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. Esto significa que los atacantes pueden obtener acceso no autorizado a archivos y carpetas, datos de salud, el micrófono o la cámara, y más sin alertar a los usuarios



Jamf Threat Labs descubrió [CVE-2024-44131, una vulnerabilidad para eludir TCC](#) que afecta a File Provider en los dispositivos Mac. Apple respondió rápidamente a este descubrimiento con un parche en macOS 15. Las CVE, como CVE-2024-4413, amplifican la necesidad de que las organizaciones cuenten con herramientas que puedan detectar y bloquear comportamientos inesperados. Ser proactivo al supervisar el comportamiento de las aplicaciones y evitar el acceso no autorizado a los datos ayuda a las organizaciones a ir un paso adelante antes de que puedan abordarse las vulnerabilidades.

Echemos un vistazo en profundidad a algunas vulnerabilidades dignas de mención de versiones recientes (este informe se escribió en abril de 2025) de Apple:

Solución a la CVE de Apple	Fecha	Puntuación de vulnerabilidad	Impacto
macOS Sequoia 15.4.1	Abril de 2025	CVE-2025-31200 CVSS - Puntuación: 7.5 Gravedad: Alta	CoreAudio
macOS Sequoia 15.4	Marzo de 2025	CVE-2025-24234 CVSS - Puntuación: 7.8 Gravedad: Alta	AccountPolicy
macOS Sequoia 15.4	Marzo de 2025	CVE-2025-24180 CVSS - Puntuación: 8.1 Gravedad: Alta	Servicios de autenticación
macOS Sequoia 15.3	Enero de 2025	CVE-2025-24085 CVSS - Puntuación: 7.8 Gravedad: Alta	CoreMedia

Como ya se ha dicho, al crear software se producen vulnerabilidades (unos 25 errores por cada 1000 líneas de código). Lo importante para los profesionales de la seguridad es poder captar esas vulnerabilidades y tomar medidas al respecto para mantener los datos a salvo. No siempre es posible mantener los sistemas operativos actualizados (p. ej., para probar aplicaciones/agentes), pero las organizaciones deben estar atentas y protegidas.

Es algo más que las vulnerabilidades de un sistema operativo. A finales de noviembre de 2024, la Agencia de Ciberseguridad de EE.UU. 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 la CVE y lo que cada vulnerabilidad permite hacer a los actores de amenazas. Las vulnerabilidades se producen en los sistemas operativos de 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". La Agencia de Ciberseguridad a continuación 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

Como se ha indicado anteriormente, Apple proporciona de forma rutinaria actualizaciones de los sistemas operativos con vulnerabilidades conocidas. No dejamos de mencionarlo, pero actualizar el software es clave. La forma más habitual que tienen las organizaciones de actualizar el sistema operativo (y las aplicaciones empresariales que sus empleados utilizan a diario) es a través de una solución de administración de dispositivos móviles. Sin embargo, existen otros niveles de ciberdefensa. Los planes de respuesta a incidentes, la recopilación y el análisis de telemetría o los procesos internos de aplicación de parches son ejemplos de cómo las organizaciones pueden ir un paso adelante. Al realizar lo anterior también se desbloquean capas adicionales de ciberdefensa, como la identificación de los niveles de vulnerabilidad del software o el descubrimiento de riesgos que pueden permanecer latentes en los endpoints a través de flujos de trabajo de caza de amenazas, todo lo cual trabaja en conjunto para ayudar a las organizaciones a mitigar el riesgo.



Jamf Threat Labs descubrió una vulnerabilidad Gatekeeper en macOS, asignada CVE-2023-41067. Esta vulnerabilidad afectaba a Launch Services y podía llevar a la ejecución de una aplicación no firmada ni registrada sin mostrar al usuario los avisos de seguridad adecuados. Gatekeeper es la primera línea de defensa para garantizar que las aplicaciones descargadas de Internet se bloqueen si no están firmadas con un ID de desarrollador válido. Aunque esta CVE fue rápidamente parchada por Apple, demuestra que pueden producirse vulnerabilidades en cualquier sistema. Disponer de los controles y la capacitación adecuados ayuda a mitigar los riesgos causados por vulnerabilidades como la que Jamf Threat Labs encontró en Gatekeeper.

En los últimos doce meses,
encontramos que:



32%

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

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 parchado sólido:**

Retomando el punto de la MDM, es primordial disponer de una herramienta que garantice estar al día con las versiones N-X más recientes o compatibles de software o sistema operativo para mantener un entorno sano 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 hay dispositivos que no cumplan la normativa e intentan acceder a los recursos de la 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.

Parte 3: Ingeniería social

La ingeniería social es la práctica mediante la cual los atacantes manipulan y engañan a las personas para que faciliten datos confidenciales o credenciales de acceso. Según [el informe Global Cybersecurity Outlook 2025](#) del Foro Económico Mundial, "el 42% de las organizaciones experimentaron un ataque de ingeniería social con éxito el año pasado".

El phishing —un tipo de ingeniería social— es una de las amenazas más comunes y dañinas a las que se enfrentan las organizaciones hoy en día. Aunque el phishing es más frecuente en los dispositivos móviles (debido al pequeño tamaño de sus pantallas, su portabilidad y su uso en lugares alejados de la oficina), las Mac (y todas las computadoras de escritorio o PC), son un atractivo objetivo de ataque para los actores de amenazas. Al fin y al cabo, las Mac siguen siendo utilizadas por el eslabón más vulnerable de la cadena de ciberseguridad: el usuario.

A medida que los ataques se vuelven más creativos y realistas, nuestra información personal y laboral está en peligro constantemente. Dado que los dispositivos Mac son cada vez más comunes en el trabajo, la superficie de ataque 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.

En los últimos doce meses, encontramos que:



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



Jamf Threat Labs publicó un artículo sobre [la investigación en curso del FBI sobre la obtención de beneficios financieros por parte de la RPDC](#) a través de medios ilícitos, concretamente en el sector de las criptomonedas. El equipo señala un ataque concreto "en el que un usuario fue contactado en LinkedIn por un individuo que decía ser un reclutador del equipo de RRHH de una empresa tecnológica". Los atacantes envían al usuario un reto de codificación comprimido (un paso habitual en un puesto de desarrollo actual) para conocer sus habilidades. Una vez que el usuario hace clic, se inicia el malware (en este caso, un infostealer). La capacitación de los empleados en el uso de las redes sociales y la descarga de programas informáticos sigue siendo un tema importante que todas las organizaciones deben poner en práctica.

Las 20 marcas más utilizadas en campañas de phishing

En nuestra investigación, descubrimos que ciertas marcas de alto perfil con frecuencia reciben ataques de phishing, tal vez debido a sus nombres reconocibles y de confianza. Hemos dividido estas marcas en cuatro categorías:

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

Los diferentes motivos para utilizar la Mac (solicitar trabajo, descargar una aplicación o trabajar en un sector específico como el de las criptomonedas) propician que los actores de amenazas exploten estos casos de uso comunes, a menudo necesarios, para acceder a los datos. En la tabla anterior, mostramos los 20 sitios más utilizados en los ataques de phishing, basándonos en esas cuatro categorías.

Estas marcas, debido a su popularidad, prestigio e impacto en empresas y particulares por igual, son utilizadas por actores nefastos que intentan comprometer a los usuarios en ataques de ingeniería social. Son jugadores involuntarios en un juego cada vez más sofisticado. También cabe señalar que esta lista no es exhaustiva de todas las marcas utilizadas por los actores de amenazas. Estas son las 20 marcas más importantes del año pasado, pero puede cambiar el año, mes o semana que

viene, pero arroja luz sobre cómo piensan los atacantes. Están utilizando la confianza que las marcas han desarrollado con su base de clientes durante años para explotar a los usuarios. Con el aumento del trabajo híbrido y a distancia, los atacantes están probando nuevas formas de conseguir que alguien haga clic.

En el mundo moderno, nuestra información personal está constantemente en peligro. Al volverse la Mac cada vez más común en el trabajo, la superficie de ataque continúa expandiéndose. 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** en 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 lanzan nuevos dominios para alojar ataques de phishing que aún no se han detectado o identificado como maliciosos en las bases de datos comunes. Identificar y verificar los ataques de phishing de día cero ayuda a las organizaciones a proteger a los usuarios de ser víctimas de sitios de phishing totalmente 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, etc. 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.

Puntos clave

El malware para Mac avanza. Pero hay medidas que las organizaciones pueden tomar para mitigar los riesgos del malware de macOS. Por ejemplo, la recolección y análisis de telemetría ayuda a identificar e informar sobre el malware. Los actores de amenazas siguen buscando nuevas formas de comprometer a usuarios y sistemas. Pero con las herramientas adecuadas, las organizaciones pueden reducir el impacto del software malicioso.

Establecer una higiene de seguridad adecuada mitiga los riesgos. La actualización periódica de los sistemas operativos y la desactivación de controles innecesarios (p. ej., tiendas de apps de terceros) ayudan a las organizaciones a mantener el cumplimiento de las líneas de base internas y los marcos externos. Mediante la creación de una tienda de apps empresariales y la revisión continua de las aplicaciones (especialmente las privadas y personalizadas), las organizaciones pueden supervisar, corregir y parchar mejor las aplicaciones vulnerables.

La ingeniería social es una de las formas más comunes que tienen los atacantes de acceder a información sensible. Más del 90% de los ciberataques tienen su origen en el phishing. El phishing se presenta en todas las formas y tamaños, no solo por correo electrónico. Es importante implementar la protección en todo el dispositivo (navegadores y aplicaciones) para mantener seguros a los usuarios y a las organizaciones.



```
1 filename: stl
2 sha1: 35ce8d5817ab7a7c5be33ea83c3234181206f061
3 contacted domains:
4 hxxps://grand-flash[.]com/connect
5 hxxpi://vapotruster[.]com/mac/stl
6
7
8 filename: stl-deobf.py
9 sha1: cd2ef119c9120ea56548f5cf0a3ff7d6ffc7613a
10
11
12 filename: installer
13 sha1: 878dcf854287e1dae3d5a55279df87eb6bdf96b3
14 contacted domains:
15 hxxps://grand-flash[.]com/connect
16
17
18 filename: sosorry
19 sha1: 90d33f249573652106a2b9b3466323c436da9403
20 contacted domains:
21 hxxp://138[.]68[.]93[.]238/connect
22 hxxp://138[.]68[.]93[.]238/Ledger-Live.dmg
```



Póngase en contacto con nosotros para obtener más información sobre el panorama de las amenazas para Mac.O comuníquese con su distribuidor preferido.