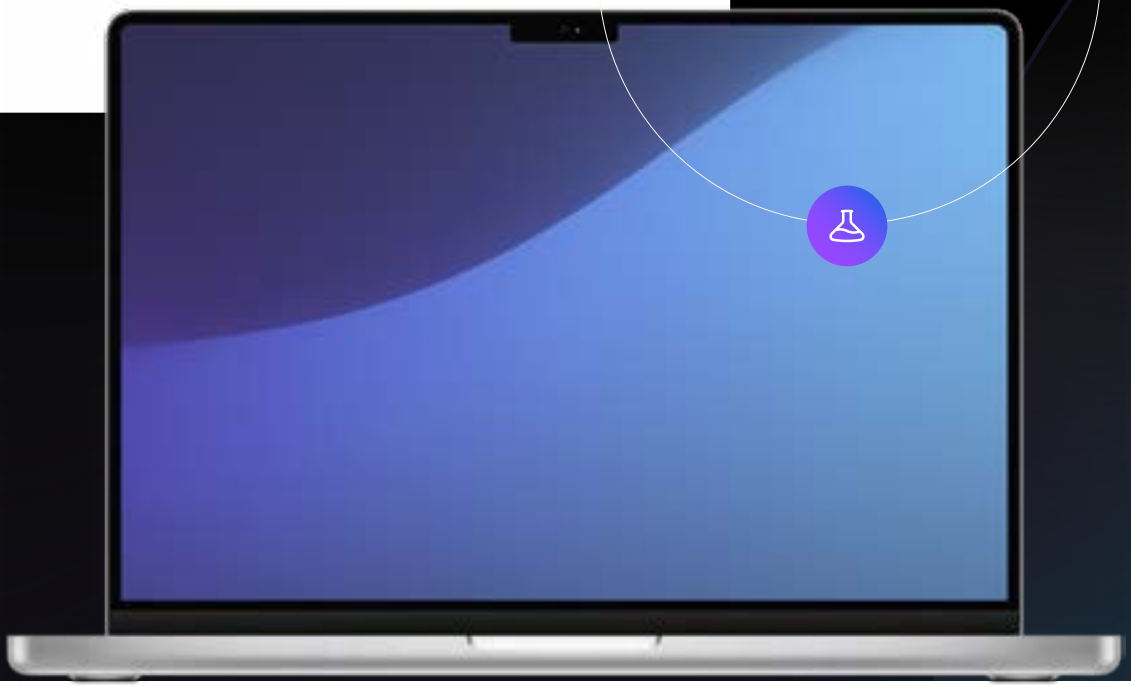
jamf

Security 360:

Informe anual de tendencias

Mac



Índice

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 Mac para poner de relieve los riesgos a los que se enfrentan las organizaciones.

Analizamos los diversos y letales vectores de ataque que utilizan los atacantes para causar daño. El aumento de la popularidad de los dispositivos Mac los ha convertido en un objetivo muy codiciado para los atacantes, quienes constantemente desarrollan nuevas tácticas para infiltrarse en los dispositivos y robar datos.

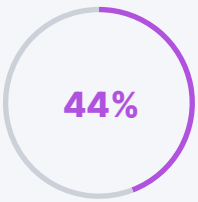
Además de analizar las nuevas formas en que los atacantes se dirigen a los dispositivos Mac, el informe incluye la opinión del director de seguridad de la información (CISO) de Jamf, lo que ofrece información valiosa a los responsables de seguridad y a los profesionales de TI encargados de proteger las flotas Mac.

Metodología de la investigación

Para comprender y cuantificar el impacto real de las tendencias de seguridad identificadas en este informe, hemos analizado de forma anónima una muestra compuesta por más de 150,000 dispositivos Mac. Nuestro análisis se llevó a cabo a finales de 2025, analizando los 12 meses anteriores. Los datos incluidos en nuestra investigación sobre malware se enfocaron únicamente en dispositivos ubicados en Estados Unidos, mientras que nuestro análisis de vulnerabilidades incluyó datos a nivel mundial.

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.

Aspectos clave



de los **dispositivos** presenta **tráfico de red malicioso**

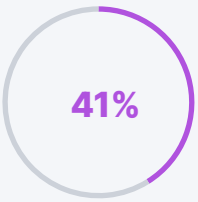
Los atacantes siempre están intentando comprometer sus dispositivos. Detectar y contener el tráfico malicioso requiere una atención constante, además de las herramientas adecuadas.

del**malware** que afecta a los Mac eran **troyanos**

Los troyanos encabezaron las listas este año, con un aumento de más de 33 puntos porcentuales desde 2024. Los troyanos son puertas traseras en sus sistemas, causando daños duraderos y quedando vulnerables a otros ataques.

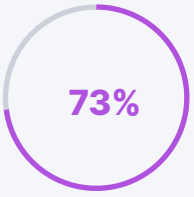
de las **organizaciones** tienen al menos **un dispositivo afectado por el criptojacking**

Los ataques de criptojacking utilizan la potencia de procesamiento de su dispositivo para minar criptomonedas. Mientras los atacantes se enriquecen, su dispositivo pierde rendimiento y eficiencia.



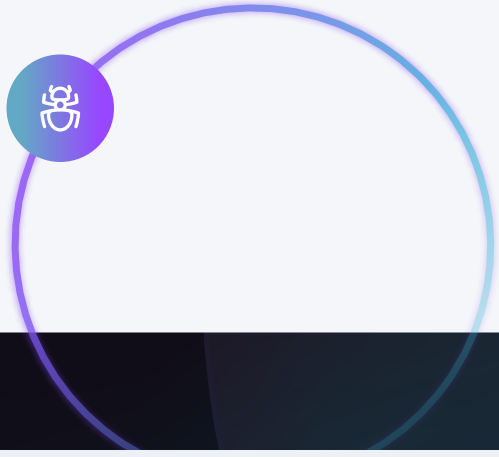
de los **dispositivos** tienen sistemas operativos **críticamente obsoletos**

Obligar el uso de versiones mínimas de software garantiza que sus dispositivos cuenten con los últimos parches de seguridad, lo que reduce el número de vulnerabilidades conocidas que puedan ser objeto de ataques.



de los **dispositivos** tienen **apps vulnerables**

Su sistema operativo no es el único software que introduce riesgos. Las apps pueden contener bibliotecas vulnerables, verse afectadas por brechas en la cadena de suministro o manejar datos de forma inadecuada. Saber qué está instalado en toda la organización es fundamental para administrar los riesgos.



Principales tendencias en la empresa

1. Mac ya no es un producto para un público minoritario.

Muchas organizaciones de todos los tamaños e industrias utilizan Mac, ahora más que nunca. Entre 2024 y 2025, la participación de mercado de los dispositivos Mac creció un 16.4%, hasta alcanzar casi el 10%, un incremento mayor que el de cualquier otro fabricante.

Con más de 2.7 millones de equipos Mac vendidos en 2025, está claro que Mac está en todas partes. Los atacantes se han dado cuenta de esta tendencia, y Mac se ha convertido en un objetivo muy codiciado para los ataques. A pesar de sus sólidas funciones de seguridad, los días en que se decía que "las Mac no podían contraer malware" ya quedaron atrás.

A medida que aumenta la presencia de computadoras Mac en las empresas, los atacantes perfeccionan y adaptan sus métodos para crear amenazas específicas para Mac y robar sus datos.

2. Los programas de robo de información están evolucionando y robando más datos que nunca.

Los programas de robo de información son uno de los tipos de malware más comunes. Los creadores de malware se esfuerzan por idear formas eficaces y subrepticias de recopilar sus datos a gran escala. Suelen actuar con rapidez, recolectando credenciales, tokens de sesión, archivos y cualquier otra cosa que puedan conseguir, antes de que el usuario se dé cuenta de que algo anda mal.

Los programas de robo de información suelen constituir la primera fase de ataques más amplios. Pueden retener los datos a cambio de un rescate o utilizarlos para infiltrarse en otras cuentas y sistemas. Estas características hacen que los programas de robo de información sean muy codiciados por los atacantes, por lo que muchos desarrolladores los ofrecen como servicio. Los programas modernos de robo de información pueden crear una puerta trasera y garantizar su persistencia, lo que les permite sobrevivir a los reinicios y cierres de sesión, y permite a los atacantes enviar comandos desde el servidor de comando y control (C2).

3. Los grupos APT siguen poniendo su mira en macOS.

Si analiza el panorama de amenazas para Mac, es probable que se encuentre con algunas caras conocidas. Las amenazas avanzadas similares a las relacionadas con la República Popular Democrática de Corea siguen dirigiéndose contra macOS en campañas y a través de malware como las nuevas versiones de los ladrones de información Contagious Interview, FlexibleFerret y Odyssey.

Los atacantes siguen creando puertas traseras y otros mecanismos de persistencia. Jamf Threat Labs observó esto en tipos de malware como ChillyHell.

Para más información sobre la investigación de Jamf Threat Labs, consulte el final de este informe.

Malware y amenazas para Mac

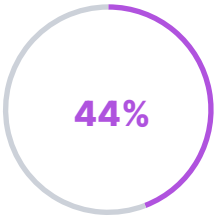
Las computadoras Mac y Windows son diferentes y, por lo tanto, también lo es el malware que las afecta. Los atacantes que crean malware para Mac deben tener en cuenta estas diferencias para saber qué vulnerabilidades pueden aprovechar. Para que un ataque tenga éxito, los atacantes se ven obligados a eludir medidas de seguridad como:

1. **Gatekeeper**, que comprueba que las apps sean legítimas y seguras analizando su **certificación notarial y la información o firma de los desarrolladores**

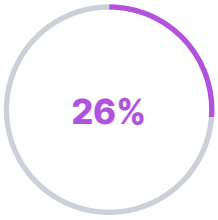
2. **Protección de la integridad del sistema (SIP),** que limita la capacidad de escribir en archivos críticos del sistema

3. **Transparencia, consentimiento y control (TCC),** que exige el permiso explícito del usuario para acceder a la cámara, el micrófono, los archivos y otros contenidos

A pesar de esas dificultades, **los atacantes están logrando sus objetivos.**



de los **dispositivos** presentaban **tráfico de red malicioso**



de las **organizaciones** se vieron afectadas por **ataques de criptojacking**

Por eso es fundamental **comprender y detectar las amenazas más recientes**.
Hay mucho de lo que estar al tanto.

Más de 26,000

es el número de **muestras de malware** que **Jamf Threat Labs** añadió a su base de datos en 2025

Más de 230

es el número de **reglas YARA** que **Jamf Threat Labs** añadió en 2025

Una vez que sepas a qué te enfrentas, debes saber cómo detectarlos. Las **reglas YARA** son de gran ayuda en este sentido: los investigadores las utilizan para identificar y clasificar muestras de malware.

¿Pero qué hay de las amenazas que desconocemos? Los atacantes tampoco se quedan atrás e, inevitablemente, crean nuevos ataques que la comunidad de ciberseguridad aún no ha descubierto.

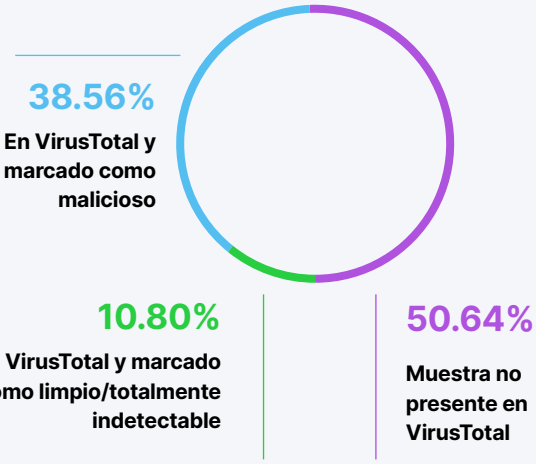
Jamf Threat Labs también busca estos elementos, detectando muestras en el entorno real mediante reglas estáticas y basadas en el comportamiento. Al analizar estas muestras con VirusTotal, se observa que alrededor del **50%** de ellas no han sido subidas por otros investigadores.

Lamentablemente, si el malware se vuelve demasiado fácil de identificar, sus creadores realizan modificaciones importantes para volver a ocultarlo. Los investigadores deben recurrir a técnicas de detección avanzadas que analicen el *comportamiento*, en lugar de basarse en las características estáticas de los archivos. Las alertas de comportamiento marcadas como de alta severidad llaman la atención de los controles avanzados contra amenazas de Jamf y, posteriormente, son bloqueadas. En 2025, estos eran los más comunes:

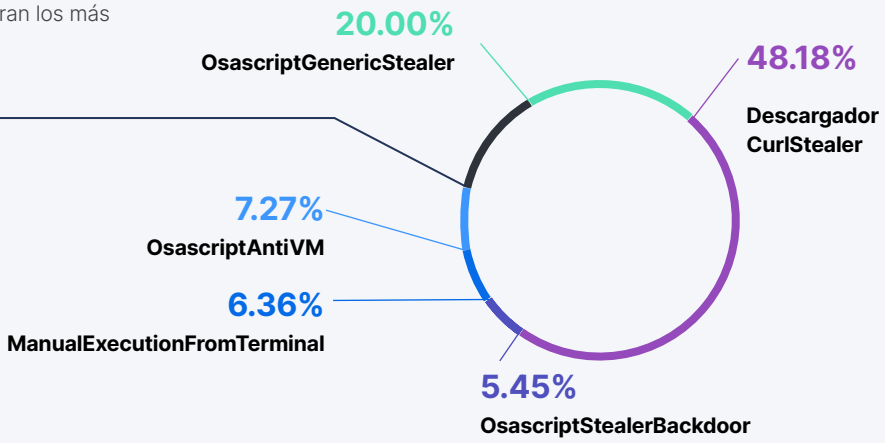
Otros 12.74%

StealerDataExfiltration	**3.64%**
XcodeExecutesCurl	**2.73%**
KnownMaliciousCurlCommand	**2.73%**
MaliciousCurlUserAgent	**1.82%**
InsecureCurlFromScriptEditor	**0.91%**
NpmMaliciousPackage	**0.91%**

MUESTRAS DETECTADAS POR JAMF THREAT LABS



DETECCIÓN AVANZADA DE COMPORTAMIENTOS



A continuación se presenta una muestra de cómo se comportan estas detecciones:

CurlStealerDownloader:
uso sospechoso de curl para descargar y ejecutar posibles cargas útiles de robo de información

OsascriptGenericStealer
actividad del programa de robo de información para macOS detectada a través de la ejecución de AppleScript

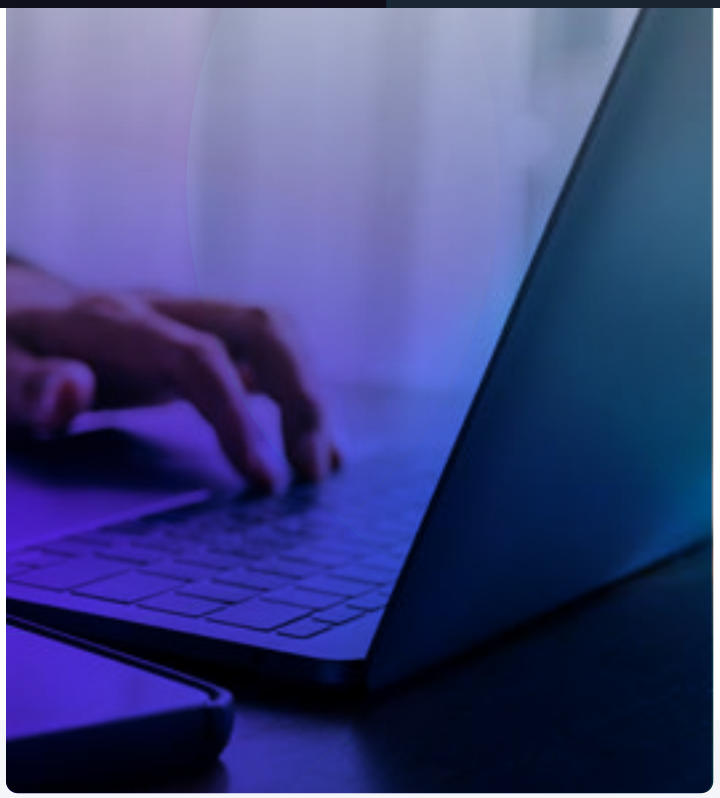
XcodeExecutesCurl
ejecuta un comando curl sospechoso durante el proceso de compilación de Xcode

NpmMaliciousPackage
ejecución de un paquete NPM potencialmente malicioso, lo que indica actividad sospechosa de scripts durante la instalación o en tiempo de ejecución

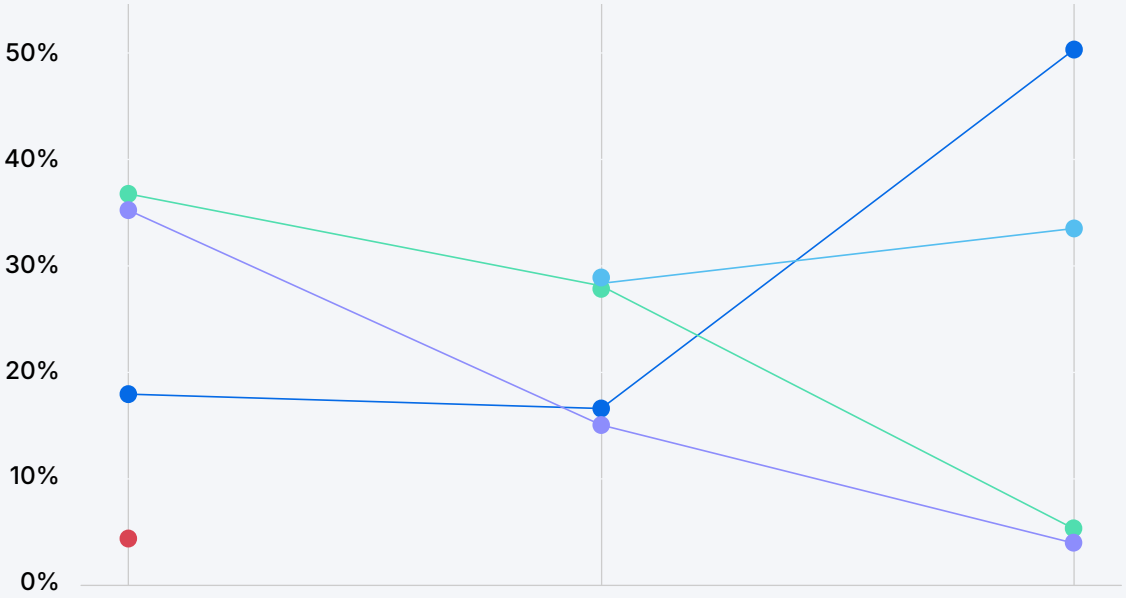
La cuestión es que las amenazas dirigidas a Mac son frecuentes y variadas. Los atacantes están creando malware para su propio beneficio y para venderlo al mejor postor, y la demanda es mayor que nunca. Para empezar a protegerte, debes saber contra qué tipo de malware estás luchando.

El malware más común para Mac

Las estrategias de ataque cambiaron en 2025. En 2024, los programas de robo de información y el adware dominaron el panorama, representando cada uno de ellos alrededor del **28%** de los ataques. En 2025, los troyanos ocupaban el primer lugar, representando aproximadamente la mitad de todos los ataques, seguidos por los programas de robo de información, con alrededor de un tercio. Cabe señalar que los programas de robo de información han evolucionado hasta utilizar puertas traseras de tipo troyano, lo que ha contribuido a este crecimiento. Al comparar los datos de este año con los informes de años anteriores, podemos observar cómo varía la prevalencia de las amenazas:



PRINCIPALES TENDENCIAS EN MALWARE



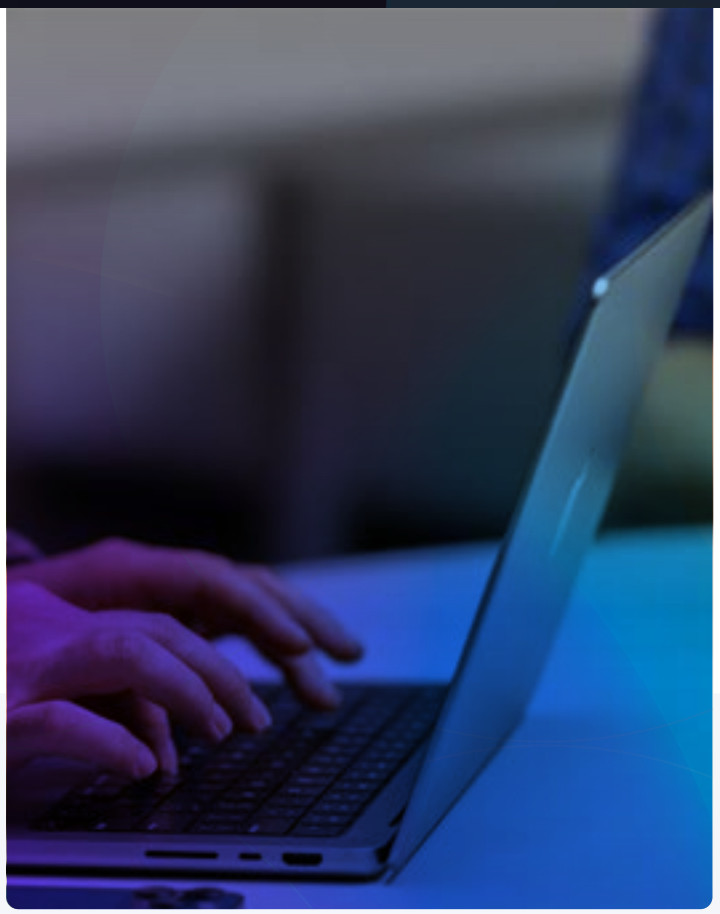
Malware Type	2023	2024	2025
Trojan	17.96%	16.61%	50.32%
Infostealer	-	28.36%	33.52%
Adware	36.77%	28.13%	5.06%
PUA	35.24%	15.06%	4.84%
Exploit	4.40%	-	-

Los cuatro tipos principales de malware representan **más del 90% de todos los ataques.** Son:

	Características:	Propósito:	Distribución:
Troyanos 50.40%	Haciéndose pasar por una aplicación legítima	Diversos; se utiliza habitualmente como puerta trasera para otros ataques	Ingeniería social, repositorios de archivos, etc.
Infostealers 33.52%	Roba datos del sistema inmediatamente después de la infección	Recopila datos confidenciales, como credenciales de inicio de sesión e información de identificación personal	A veces se ofrece como un servicio y se distribuye mediante ingeniería social, sitios web maliciosos y descargas de software
Adware 5.06%	Muestra anuncios; puede rastrear el comportamiento del usuario con fines de publicidad personalizada o como spyware	Genera ingresos publicitarios o recopila información	Incluido en paquetes de otro software o presente en sitios web o archivos adjuntos maliciosos
Aplicaciones potencialmente indeseables (PUA) 4.84%	Puede adoptar muchas formas; puede recopilar datos, ralentizar los dispositivos o causar problemas	No siempre son explícitamente maliciosos, pero pueden monetizar los datos de los usuarios o generar ingresos por otros medios	Incluido en paquetes de software u descargado mediante tácticas engañosas

Otro 6.26%

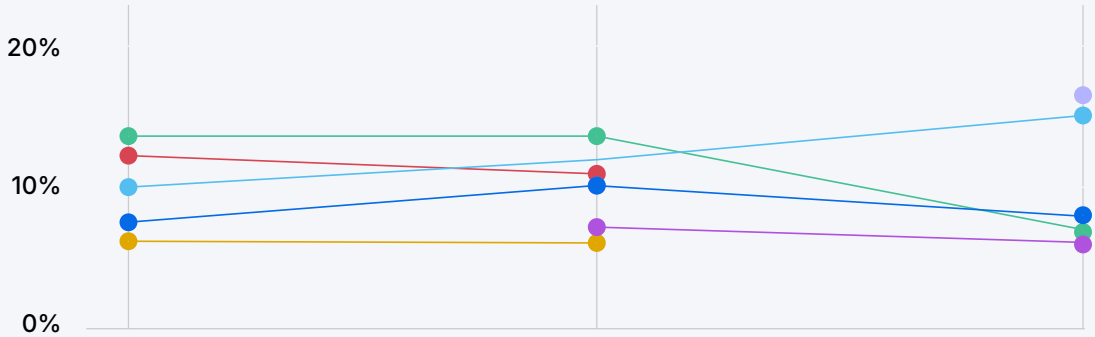
2.0% Exploit, **1.4%** Hacktool, **0.9%** Coinminer, **0.4%** Downloader, **0.4%** Keylogger, **0.3%** Ransomware,**0.2%** Dropper



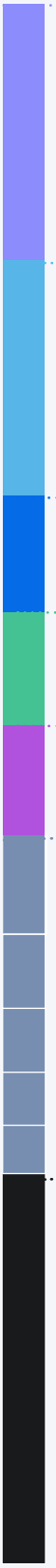
Familias de malware más comunes para Mac

Hay una gran variedad de familias de malware que afectan a los dispositivos Mac, sin que haya una que destaque claramente sobre las demás. En 2025, PuAgent fue el más común, con un 16.41%. En 2023 y 2024, el adware Genio fue el más común, con un 13.63%, hasta que cayó al cuarto lugar, con un 7.19% en 2025.

PRINCIPALES TENDENCIAS EN MALWARE



Malware Type	2023	2024	2025
PuAgent	-	-	16.41%
Generic	10.02%	-	15.09%
Genio	13.63%	13.63%	7.19%
Multiverze	6.84%	9.44%	7.47%
Mackeeper	-	7.19%	7.13%
Imobie	12.25%	10.96%	-
TNT	6.19%	6.07%	-



	Características:	Distribución:
Adware **PuAgent** **16.4%**	Modifica los navegadores cambiando los motores de búsqueda, las páginas de inicio, la configuración, las extensiones y otras funciones. Implementa ventanas emergentes con anuncios y rastrea el comportamiento de los usuarios.	Archivos adjuntos de correo electrónico, descargas o enlaces maliciosos, software gratuito
Genéricos diversos **15.1%**	Los archivos muestran un comportamiento sospechoso indicativo de la presencia de malware, pero no presentan firmas específicas de ninguna familia de malware conocida.	Diversa
Troyano **Multiverze** **7.5%**	Recopila datos de los usuarios, incluida información privada como contraseñas, números de tarjetas de crédito, carteras de criptomonedas y otros datos. Puede registrar todo lo que escribas y lo que veas en la pantalla. Es posible que el usuario no lo vea.	Correos electrónicos de phishing, sitios web maliciosos, publicidad maliciosa, software gratuito, redes sociales
Adware **Genio** **7.2%**	Secuestra los navegadores web para recopilar información de los usuarios; se hace pasar por un motor de búsqueda para mostrar resultados patrocinados; es difícil de desinstalar.	Incluido en paquetes de software legítimo, descargas maliciosas
Mackeeper PUA **7.1%**	Parece una aplicación legítima, pero es posible que no cumpla con lo prometido en cuanto al rendimiento. Muestra ventanas emergentes con anuncios, puede mostrar información errónea sobre el estado del dispositivo y reducir su rendimiento.	Publicidad maliciosa, descargas maliciosas

Imobie 6.3%

Revproxy 4.7%

atomic_stealer 4.1%

Ccleanmac 3.4%

Macinformer 3.1%

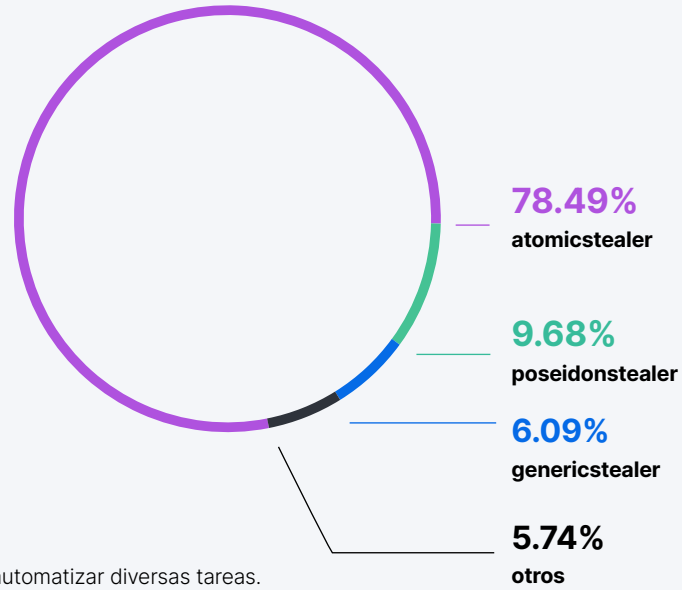
Otros 25.1%

Programas de robo de información

Si usted quisiera robar algo (por favor, no lo haga), cuanto más rápido pueda entrar y salir, menos probabilidades tendrá de que lo descubran. Los programas de robo de información suelen actuar con rapidez para sustraer sus datos poco después de haber infectado su dispositivo. A veces, se eliminan solos una vez causado el daño, mientras que los ladrones de información modernos pueden establecer persistencia.

> *Los programas de robo de información han desempeñado un papel importante en el aumento del malware dentro del ecosistema de macOS. AppleScript, aunque históricamente ha resultado útil para los usuarios avanzados, también ha sido objeto de un uso indebido generalizado en el malware.*
>
> Jaron Bradley, Jamf

LADRONES DE INFORMACIÓN MÁS COMUNES



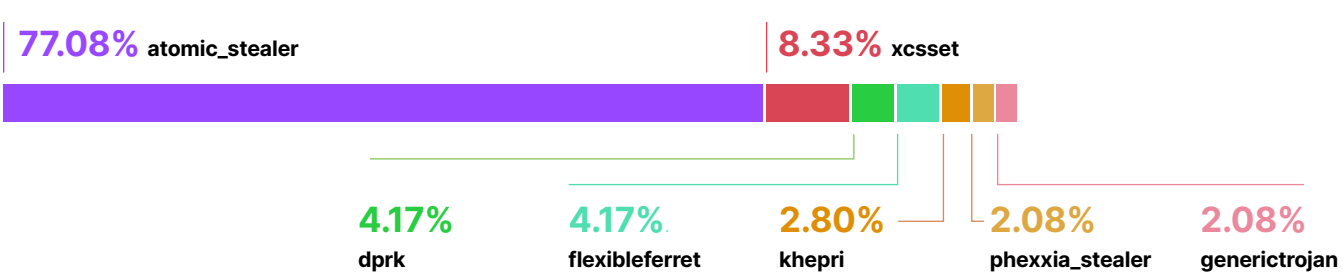
Los desarrolladores y los usuarios avanzados utilizan AppleScript para automatizar diversas tareas. Es una herramienta poderosa, capaz de ofrecer infinitas posibilidades, tanto buenas como malas. Los atacantes lo utilizan para engañar a los usuarios y robarles su información.

Los programas de robo de información se hicieron mucho más comunes a partir de 2023, año en el que solo representaban un escaso **0.25%** de los ataques. En 2024, esta cifra aumentó enormemente hasta alcanzar el **28.36%**, para finalmente situarse en el **33.52% en 2025**. A pesar de lo populares que son, se llevan a cabo cada vez más ataques mediante otros tipos de malware, como los troyanos. Hablando de eso...

Troyanos

Los troyanos experimentaron un gran aumento de popularidad en 2025, hasta alcanzar finalmente el primer puesto en las estadísticas, con un **50.3% del total de ataques de malware**. El troyano más común, **atomic_stealer**, estuvo presente en el **77.08% de los ataques**. Seguramente habrá notado su parecido con el programa de robo de información más extendido de 2025; no es ninguna coincidencia. Muchos ladrones utilizan troyanos para crear puertas traseras que les permiten volver a acceder al sistema.

TROYANOS ACTIVOS



Conocer al enemigo es la mitad de la batalla.

Gran parte del malware del que hemos hablado es muy conocido. Es probable que su software de detección de amenazas lo identifique. Como ya hemos insinuado anteriormente, no todo el malware se puede identificar por su código. Las detecciones avanzadas que identifican comportamientos sospechosos son fundamentales para detectar amenazas que aún no han sido analizadas por la comunidad de ciberseguridad. La implementación de herramientas avanzadas contribuirá en gran medida a proteger a su organización contra los ataques de día cero.

La configuración también es importante. El malware suele aprovecharse del comportamiento de los usuarios, por ejemplo, cuando realizan una descarga peligrosa o caen en una trampa de ingeniería social. Las políticas de seguridad y la capacitación de los usuarios son de gran ayuda.

La detección es fundamental; la prevención empieza por el propio software. Los ciberataques se aprovechan de las vulnerabilidades del software: fallos en el diseño tanto de las aplicaciones como de los sistemas operativos que dejan margen para su explotación. Aplicar las actualizaciones en sus dispositivos y apps es la mejor manera de corregir estas vulnerabilidades y mantener a raya a los atacantes. Hablaremos más sobre esto en la siguiente sección.

Reflexiones de nuestro CISO

A medida que los dispositivos de Apple siguen extendiéndose en el ámbito empresarial, las soluciones de seguridad elegidas deben estar diseñadas específicamente para el ecosistema de Apple, y no ser adaptaciones de un enfoque diseñado para Windows. Las organizaciones deben dar prioridad a los productos de seguridad diseñados desde cero para macOS, asegurándose de que las capacidades de detección de amenazas, conformidad y respuesta estén totalmente adaptadas al funcionamiento de las plataformas de Apple, y no se traten como un elemento secundario.

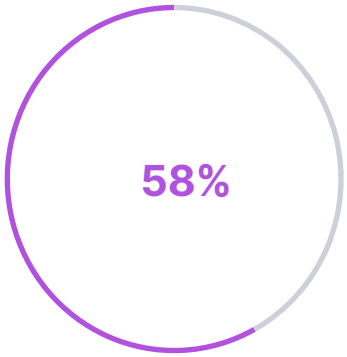
Vulnerabilidades de las apps y los sistemas operativos

El sistema operativo es la base de un dispositivo. Es el motor que impulsa las herramientas, los servicios, las aplicaciones y la seguridad de su dispositivo. Los atacantes buscan constantemente puntos débiles en su armadura para infiltrarse en sus defensas.

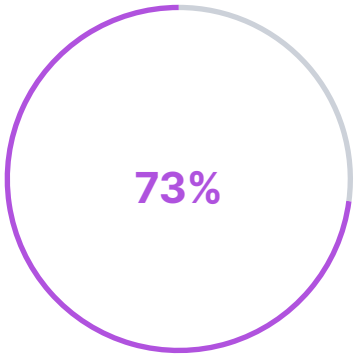
Las vulnerabilidades se acumulan. Incluso las vulnerabilidades menos graves pueden convertirse en un paso crucial en un ataque y, a veces, la corrección de estas vulnerabilidades pasa a un segundo plano.

Hablando de parches... son muy importantes. Por desgracia, incluso los sistemas operativos más seguros tienen algún punto vulnerable. Es inevitable, pero no incurable. Apple a menudo lanza actualizaciones de software para solucionar vulnerabilidades. Para mantener la protección, su organización debe aplicar estas actualizaciones. Pero esto no siempre ocurre.

Las apps también son importantes. Cada una presenta sus propias vulnerabilidades, políticas de manejo de datos, bibliotecas de desarrollo y mucho más.



de las **organizaciones** al menos tenían **un dispositivo** con un **sistema operativo muy desactualizado**



de los **dispositivos** *contienen*al menos una **app vulnerable**

¿Qué es un CVE?

El programa "Common Vulnerabilities and Exposures" (Vulnerabilidades y exposiciones comunes, CVE) funciona como una base de datos de vulnerabilidades descubiertas por la comunidad de ciberseguridad. Cada entrada del CVE identifica el software o la biblioteca afectados, indica un nivel de gravedad y ofrece métodos potenciales de explotación

El software desactualizado es muy común. Los usuarios no siempre ven con buenos ojos las actualizaciones, sobre todo si consideran que alteran sus flujos de trabajo. Sin embargo, hacer cumplir los plazos de actualización y las versiones mínimas del sistema operativo contribuye en gran medida a proteger su parque de dispositivos y sus datos, por ejemplo, frente a ataques que aprovechan estas vulnerabilidades.

Vulnerabilidades relevantes de macOS, 2025

CVE-2025-46287 | Gravedad: 9.8 (crítica)	CVE-2025-43539 | Gravedad: 8.8 (alta)	CVE-2025-46285 | Gravedad: 7.8 (alta)
DESCRIPCIÓN:		
Un atacante podría falsificar su identificador de llamada de FaceTime.	El procesamiento de un archivo puede provocar daños en la memoria.	Es posible que una app pueda obtener privilegios de root.
COMPONENTE AFECTADO:		
Marco de llamadas	AppleJPEG	Kernel
IMPACTO:		
Al mostrar información engañosa, el atacante puede inducir al usuario a realizar una acción incorrecta.	Un atacante puede modificar datos para ejecutar código no autorizado.	Un atacante puede ejecutar código arbitrario.
SISTEMA OPERATIVO PARCHADO:		
macOS Tahoe 26.2, Sequoia 15.73 y Sonoma 14.8.3	macOS Tahoe 26.2, Sequoia 15.73 y Sonoma 14.8.3	macOS Tahoe 26.2, Sequoia 15.73 y Sonoma 14.8.3

Vulnerabilidades descubiertas por Jamf

CVE-2025-43296 | Oct 2025
Evasión de Gatekeeper en Ajustes del Sistema, corregida en macOS Tahoe 26.

CVE-2025-43348 | Nov 2025
Evasión de Gatekeeper en Finder, corregida en macOS Tahoe 26.1.

En la siguiente tabla se muestran otras vulnerabilidades que confirmamos que fueron explotadas en 2025.

ID DEL CVE	COMPONENTE	IMPACTO
CVE-2025-24113 Puntuación CVSS: 4.3 | Gravedad: **media**	Safari	Visitar un sitio web malicioso puede dar lugar a la suplantación de la interfaz de usuario.
CVE-2025-46289 Puntuación CVSS: 5.5 | Gravedad: **media**	AppSandbox	Es posible que una app pueda acceder a datos protegidos del usuario.
CVE-2025-43482 Puntuación CVSS: 5.5 | Gravedad: **media**	Audio	Una app podría provocar un rechazo del servicio.
CVE-2025-43517 Puntuación CVSS: 3.3 | Gravedad: **baja**	Historial de llamadas	Es posible que una app pueda acceder a datos protegidos del usuario debido a un problema de registro.
CVE-2025-43542 Puntuación CVSS: 7.5 | Gravedad: **alta**	FaceTime	Los campos de contraseña pueden quedar expuestos de manera no intencional al controlar un dispositivo de forma remota a través de FaceTime.
CVE-2025-43532 Puntuación CVSS: 2.8 | Gravedad: **baja**	Fundación	El procesamiento de datos maliciosos puede provocar el cierre inesperado de la app debido a un error en la memoria.
CVE-2025-43512 Puntuación CVSS: 7.8 | Gravedad: **alta**	Kernel	Es posible que una app pueda elevar privilegios.

El manejo de vulnerabilidades es una lucha constante, pero no una batalla perdida.

Para estar al tanto de las vulnerabilidades del software, necesita una buena estrategia. En pocas palabras, debe identificar, mitigar y supervisar continuamente las vulnerabilidades que afecten a sus sistemas y dispositivos.

Dependiendo del tamaño y las capacidades de sus equipos de TI y seguridad, es posible que usted pueda detectar o no amenazas por su cuenta. Por suerte, la comunidad de ciberseguridad le respalda. Los investigadores de amenazas y los proveedores de software están constantemente al acecho de los últimos exploits, y añaden posibles vulnerabilidades a sus bases de datos para ayudar a las organizaciones a identificar sus puntos débiles. Sus equipos pueden consultarlos para hacerse una idea de su situación actual en materia de seguridad y actuar en consecuencia. Existen herramientas de seguridad que facilitan este proceso.

Las herramientas exactas que su organización necesite variarán en función de su tamaño, sus capacidades, su industria y otros factores. Pero, en general, necesitará una forma de:

- **Configurar dispositivos y aplicar políticas**
- **Administrar cuentas de usuario e identidades**
- **Mantener actualizados los dispositivos y el software**
- **Monitorear el estado del dispositivo**
- **Obligar la aplicación de políticas de acceso**

Las herramientas de administración de dispositivos móviles, protección de terminales, administración de identidades y telemetría le ayudan con estas tareas, para que pueda adelantarse a las amenazas a medida que surgen.

Reflexiones de nuestro CISO

Una estrategia de seguridad sólida se basa en los principios fundamentales de visibilidad, telemetría y automatización, y en ningún ámbito esto es más importante que en la administración de vulnerabilidades. **Los equipos de seguridad** deben:

Comprender sus vulnerabilidades

El primer paso fundamental es tener una visión clara de las vulnerabilidades en toda la organización. Obtener una visión completa de las vulnerabilidades que existen en los dispositivos de los usuarios finales y en la infraestructura sienta las bases para una estrategia de seguridad basada en datos. A partir de ahí, los equipos pueden analizar la huella de las aplicaciones, evaluar los riesgos potenciales y determinar el alcance del impacto, lo que permite a los equipos de seguridad priorizar las vulnerabilidades basándose en datos concretos en lugar de suposiciones.

Implementar un enfoque basado en riesgos para el acceso a los dispositivos

Cuando los dispositivos que no están en conformidad intentan acceder a los recursos corporativos, se debe restringir el acceso hasta que el dispositivo vuelva a estar en conformidad, mediante procesos de solución diseñados para que sean lo más fluidos y sencillos posible para el usuario final.

Introducir un programa de parches sólido

Volviendo al tema de la MDM, es fundamental contar con una herramienta que garantice la conformidad con las versiones más recientes o compatibles de software o sistemas operativos 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.

Lea la última investigación para macOS de Jamf Threat Labs

OpenClaw: la servicial IA que podría convertirse silenciosamente en su mayor amenaza interna

FEBRERO DE 2026

OpenClaw es un marco de código abierto para crear agentes de IA autónomos que pueden ejecutar comandos de shell, acceder a archivos e interactuar con aplicaciones sin límites de seguridad integrados, lo que genera riesgos significativos para la seguridad empresarial. El marco se vuelve peligroso debido al acceso sin restricciones al sistema, al riesgo de fuga de datos y a su vulnerabilidad ante ataques indirectos de inyección de comandos, en los que se incrustan instrucciones maliciosas en contenido empresarial legítimo. Los avisos de seguridad recientes han puesto de manifiesto cómo pueden aprovechar los atacantes diversas vulnerabilidades para obtener acceso persistente, lo que convierte a las implementaciones de OpenClaw en una amenaza interna de alto riesgo que requiere estrategias integrales de detección, prevención y gobernanza para administrarlas de forma segura en entornos empresariales.

Los atacantes amplían el uso malintencionado de Microsoft Visual StudioCode

ENERO DE 2026

Los actores maliciosos vinculados a la RPDC han perfeccionado la campaña "Contagious Interview" para aprovechar los archivos de configuración de tareas de Visual Studio Code, instalando una puerta trasera de JavaScript cuando las víctimas abren repositorios Git maliciosos. La puerta trasera establece una comunicación persistente de comando y control, recopila información del sistema y permite la ejecución remota de código. Esta técnica se aprovecha de los flujos de trabajo de confianza de los desarrolladores: cuando los usuarios marcan un repositorio como de confianza, los archivos de configuración maliciosos ejecutan automáticamente comandos ocultos, lo que demuestra cómo los actores maliciosos siguen adaptando sus tácticas para integrarse en herramientas de desarrollo legítimas.

Desde ClickFix al código firmado: la silenciosa transformación del malware MacSync Stealer

DICIEMBRE DE 2025

MacSync Stealer ha evolucionado más allá de las técnicas de arrastrar a la terminal; ahora se despliega a través de una aplicación Swift con firma de código y notarizada que recupera y ejecuta cargas útiles de forma silenciosa, sin requerir interacción con la terminal Distribuida a través de programas de instalación falsos, esta variante utiliza un dropper sofisticado que realiza comprobaciones de conectividad, aplica límites de velocidad, valida las cargas útiles y elimina los atributos de cuarentena antes de la ejecución. Este cambio hacia la distribución de archivos firmados y notarizados refleja una tendencia más amplia en la que los atacantes disfrazan el código malicioso como aplicaciones legítimas para eludir la detección y burlar los controles de seguridad de macOS.

El malware FlexibleFerret sigue causando estragos

NOVIEMBRE DE 2025

FlexibleFerret, una familia de malware vinculada a la República Popular Democrática de Corea, ataca a los usuarios de macOS mediante sofisticadas campañas de reclutamiento falsas que engañan a las víctimas para que ejecuten comandos maliciosos en Terminal, disfrazados de pruebas de selección de personal. El ataque en varias etapas utiliza JavaScript en sitios web falsos de empleo para realizar la implementación de una puerta trasera con amplias capacidades, entre las que se incluyen la sustracción de archivos y la ejecución de comandos, mientras recopila credenciales a través de mensajes falsos de Chrome que envían datos a cuentas de Dropbox controladas por los atacantes. Esta amenaza en constante evolución elude Gatekeeper al convencer a los usuarios de que ejecuten comandos manualmente, por lo que es fundamental que los usuarios estén al tanto de las evaluaciones de "entrevistas" no solicitadas y de las instrucciones que se dan a través de Terminal para protegerse.

DigitStealer: un programa de robo de información basado en JXA que deja pocas huellas

NOVIEMBRE DE 2025

DigitStealer es un sofisticado programa de robo de información para macOS que pasó totalmente desapercibido en VirusTotal gracias al uso de técnicas avanzadas de evasión de análisis, entre las que se incluye la detección de características de hardware que restringe su ejecución a los chips Apple Silicon M2 o posteriores. El malware realiza la implementación de cuatro cargas útiles residentes en memoria que roban datos del navegador, carteras de criptomonedas y credenciales; troyaniza Ledger Live fusionando tres componentes distintos para eludir la detección y establece persistencia a través de una puerta trasera dinámica. Su uso de servicios legítimos de Cloudflare para el alojamiento de la carga útil y su ofuscación multietapa demuestran un profundo conocimiento de los componentes internos de macOS; esto hace que la detección basada en el comportamiento sea crítica, ya que la mayor parte de la ejecución ocurre íntegramente en memoria.

ChillyHell: un análisis en profundidad de una puerta trasera modular para macOS

Septiembre de 2025

ChillyHell es una sofisticada puerta trasera para macOS que ha permanecido notarizada y sin ser detectada desde 2021, y que en un principio se relacionó con ataques dirigidos contra funcionarios del gobierno ucraniano. Este malware modular escrito en C++ establece múltiples mecanismos de persistencia, se comunica a través de DNS y HTTP, y cuenta con capacidades que incluyen shells inversos, autoactualización, implementación de carga útil y ataques de fuerza bruta contra contraseñas. Sus avanzadas técnicas de evasión demuestran que las aplicaciones firmadas y notarizadas no siempre son seguras.

Firmado y robando: nuevas revelaciones sobre el infostealer Odyssey

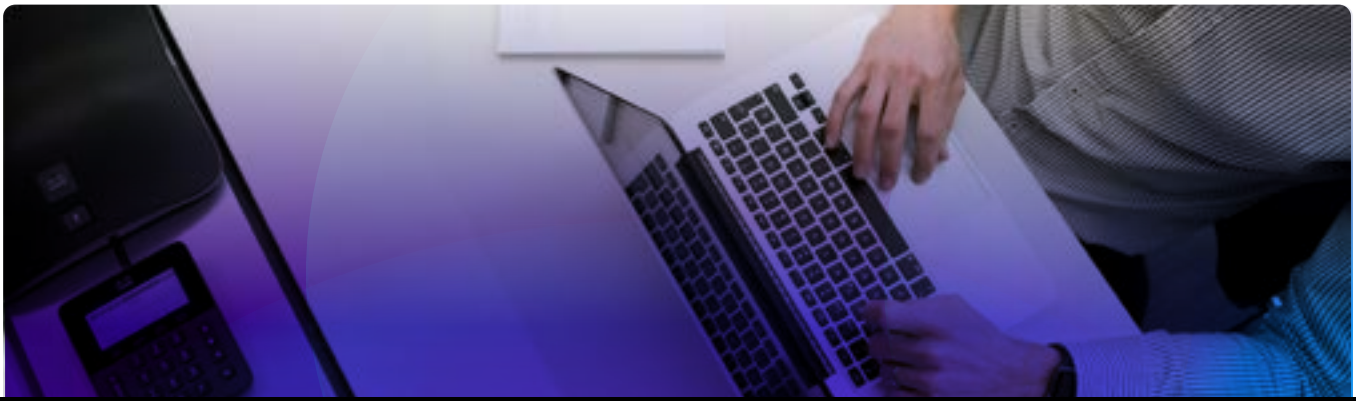
Julio de 2025

Un sofisticado programa de robo de información para macOS logró obtener la firma de código y la certificación notarial de Apple, lo que le permitió eludir los controles de seguridad integrados durante la implementación de una puerta trasera persistente y la sustitución de aplicaciones legítimas de criptomonedas por versiones troyanizadas. El malware utiliza una interfaz engañosa de SwiftUI para robar contraseñas, descarga dinámicamente cargas útiles ofuscadas y establece un canal de comandos y control continuo para la ejecución remota de código. Lo más preocupante es que identifica activamente los entornos de análisis e incluye en listas negras a los sistemas de investigación para evitar ser detectado, lo que demuestra una sofisticación propia de un Estado-nación.

Una pitón encubierta: análisis del malware PyInstaller en macOS

Mayo de 2025

Los atacantes están utilizando PyInstaller para encubrir código malicioso de Python como ejecutables nativos de macOS; es la primera vez que se observa esta técnica en programas de robo de información para macOS. El malware se ejecuta sin necesidad de tener instalado Python, roba credenciales mediante ventanas de solicitud de contraseña falsas, extrae datos del llavero y recopila carteras de criptomonedas, al tiempo que utiliza múltiples capas de ofuscación para eludir la detección. Esta técnica conlleva una evolución significativa en la distribución de malware para macOS, ya que permite a los atacantes realizar la implementación de sofisticados programas de robo de información, mientras podrían eludir los mecanismos de seguridad tradicionales.



jamf

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