jamf

Sicherheit 360:

Jährlicher Trendbericht für

Macs

Inhaltsverzeichnis:

Einführung

DER BERICHT „Sicherheit 360“ von Jamf basiert auf der Analyse realer Kundenvorfälle, Bedrohungsanalysen und Branchenereignissen des vergangenen Jahres. Dieser Bericht konzentriert sich auf die Untersuchung der Bedrohungslage für Macs, um die Risiken, denen Unternehmen ausgesetzt sind, zu beleuchten.

Wir untersuchen die vielfältigen und folgenschweren Angriffsvektoren, die von Angreifern genutzt werden, um Schaden anzurichten. Die zunehmende Beliebtheit von Mac Geräten hat diese zu einem attraktiven Ziel für Angreifer gemacht, die ständig neue Taktiken entwickeln, um in Geräte einzudringen und Daten zu stehlen.

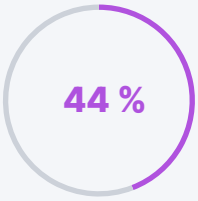
Der Bericht analysiert nicht nur die neuartigen Methoden, mit denen Angreifer den Mac angreifen, sondern enthält auch eine Stellungnahme des CISO von Jamf, die Sicherheitsverantwortlichen und IT-Fachleuten, die für den Schutz von Mac-Flotten zuständig sind, wertvolle Einblicke bietet.

Methodik der Forschung

Um die realen Auswirkungen der in diesem Bericht identifizierten Sicherheitstrends zu verstehen und zu quantifizieren, haben wir eine Stichprobe aus über 150.000 Mac Geräten anonym untersucht. Unsere Analyse wurde Ende 2025 durchgeführt, wobei der vorangegangene 12-Monats-Zeitraum überprüft wurde. Die Daten, die in unsere Malware-Untersuchung einflossen, betrafen ausschließlich Geräte in den USA, während unsere Schwachstellenanalyse globale Daten beinhaltete.

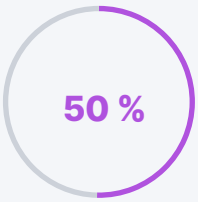
Zum Schutz der Privatsphäre und zur Wahrung höchster Standards bei der Datenerfassung und -verarbeitung stammen die in unserer Untersuchung analysierten Metadaten aus zusammengefassten Protokollen, die keine personenbezogenen Daten oder Informationen zur Identifizierung der Organisation enthalten.

Wichtigste Ergebnisse



der **Geräte** weisen **bösartigen Netzwerkverkehr auf**

Angreifer versuchen ständig, Ihre Geräte zu kompromittieren. Die Erkennung und Eindämmung von bösartigem Datenverkehr erfordert ständige Sorgfalt und die richtigen Tools.

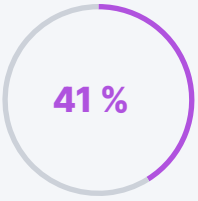


der **Malware**, die den Mac betreffen, waren **Trojaner**

Die Trojaner führten dieses Jahr die Hitliste an und legten seit 2024 um über 33 Prozentpunkte zu. Trojaner dienen als Hintertüren in Ihre Systeme und hinterlassen bleibende Schäden und Schwachstellen für andere Angriffe.

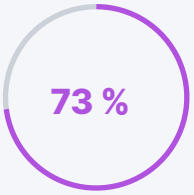
der **Unternehmen** melden mindestens **ein Gerät**, **das von Cryptojacking betroffen ist**

Cryptojacking-Angriffe nutzen die Rechenleistung Ihres Geräts, um Kryptowährungen zu schürfen. Während sich die Angreifer bereichern, verliert Ihr Gerät an Leistung und Effizienz.



der **Geräte** laufen mit **veralteten** Betriebssystemen

Durch die Durchsetzung von Mindestversionen für Software wird sichergestellt, dass Ihre Geräte über die neuesten Sicherheitspatches verfügen, wodurch die Anzahl bekannter Sicherheitslücken, die ausgenutzt werden können, verringert wird.



der **Geräte** haben **schwachstellenbehaftete Apps**

Ihr Betriebssystem ist nicht die einzige Software, die ein Risiko darstellt. Apps können schwache Bibliotheken enthalten, die Lieferkette kompromittieren oder Daten unsachgemäß verarbeiten. Für das Risikomanagement ist es entscheidend zu wissen, was in Ihrem Unternehmen installiert ist.

Wichtige Trends in Unternehmen

1. Der Mac ist kein Nischenprodukt mehr.

Unternehmen aller Größen und Branchen nutzen den Mac mehr als je zuvor. Von 2024 bis 2025 stieg der Marktanteil von Mac Geräten um 16,4 % auf fast 10 % – ein Zuwachs, der größer war als bei jedem anderen Anbieter.

Mit mehr als 2,7 Millionen ausgelieferten Macs im Jahr 2025 ist klar, dass der Mac mittlerweile überall vertreten ist. Auch Angreifer haben diesen Trend aufmerksam verfolgt, und der Mac wurde zu einem beliebten Ziel für Angriffe. Trotz robuster Sicherheitsfunktionen sind die Zeiten, in denen es hieß, dass Malware keinen Schaden aufs Mac anrichten kann, längst vorbei.

Mit der zunehmenden Präsenz von Mac Computern in Unternehmen verbessern und entwickeln Angreifer ihre Methoden, um Mac-spezifische Bedrohungen zu entwickeln - und Ihre Daten zu stehlen.

2. Infostealer entwickeln sich ständig weiter und stehlen mehr Daten als je zuvor.

Infostealer sind eine der am häufigsten verbreiteten Arten von Malware. Malware-Entwickler arbeiten intensiv an der Erstellung effektiver und subversiver Methoden, um Ihre Daten in großem Umfang zu entwenden. Sie neigen dazu, schnell zu handeln und Anmeldedaten, Sitzungs-Token, Dateien und alles andere, was sie in die Finger bekommen können, zu sammeln, bevor der Benutzer etwas bemerkt.

Infostealer bilden oft die erste Stufe bei größeren Angriffen. Sie können Daten als Lösegeld erpressen oder sie nutzen, um andere Accounts und Systeme zu infiltrieren. Diese Funktionen machen Infostealer zu einem begehrten Gut für Angreifer, weshalb viele Entwickler sie als Dienstleistung anbieten. Moderne Infostealer können eine Hintertür und Persistenz einrichten, so dass sie Neustarts und Abmeldungen überdauern und es Angreifern ermöglichen, Befehle über C2 zu senden.

3. Auch APT-Gruppen haben es auf macOS abgesehen.

Wenn Sie sich in der Mac-Bedrohungslandschaft umsehen, werden Sie wahrscheinlich auf einige bekannte Gesichter stoßen. Fortgeschrittene Bedrohungen, die den Bedrohungen der DVRK ähneln, zielen im Rahmen von Kampagnen und Malware-Varianten wie Contagious Interview, FlexibleFerret sowie Evolutionen des Odyssey-Infostealers auf macOS-Systeme ab.

Die Angreifer entwickeln kontinuierlich Hintertüren und andere Persistenzmechanismen. Jamf Threat Labs hat dies bei Malware wie ChillyHell beobachtet.

Am Ende dieses Berichts finden Sie weitere Informationen über die Untersuchungen von Jamf Threat Labs.

Malware und Bedrohungen für Macs

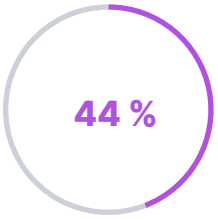
Mac- und Windows-Computer sind unterschiedlich, und damit auch ihre Malware. Angreifer, die Malware für Mac entwickeln, müssen diese Unterschiede berücksichtigen, um zu wissen, was sie ausnutzen können. Damit ein Angriff funktioniert, müssen Cyberkriminelle Sicherheitsfunktionen wie diese aushebeln:

1. **Gatekeeper** prüft die Integrität und Sicherheit von Apps, **indem die Notarisierung sowie die Entwicklerinformationen und die Signatur verifiziert werden**

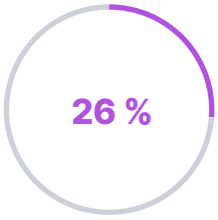
2. **Systemintegritätsschutz (SIP),** der die Schreibberechtigungen für kritische Systemdateien einschränkt

3. **Transparenz, Zustimmung und Kontrolle (TCC),** die eine ausdrückliche Genehmigung des Benutzers für den Zugriff auf Kamera, Mikrofon, Dateien und andere Inhalte erfordert

Trotz dieser Funktionen sind **die Angreifer erfolgreich.**



der **Geräte** wiesen **bösartigen Netzwerkverkehr auf**



der **Unternehmen** waren von **Kryptojacking-Angriffen** betroffen

Deshalb ist es so wichtig, **die neuesten Bedrohungen zu verstehen und zu finden**.
Es gibt eine Menge zu beachten.

Über 26.000

die Anzahl der **Malware-Samples**, die **Jamf Threat Labs** 2025 in seine Datenbank aufgenommen hat

Über 230

die Anzahl der **YARA-Regeln**, die **Jamf Threat Labs** 2025 hinzugefügt hat

Sobald Sie wissen, womit Sie es zu tun haben, müssen Sie wissen, wie Sie es erkennen können.
YARA-Regeln helfen dabei - Forscher verwenden sie, um Malware-Muster zu identifizieren und zu klassifizieren.

Aber was ist mit den Bedrohungen, von denen wir nichts wissen? Auch die Angreifer arbeiten intensiv und entwickeln unweigerlich neue Angriffe, die von der Cybersecurity-Community noch nicht entdeckt wurden.

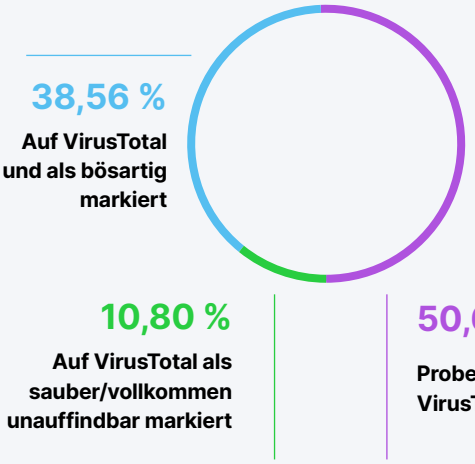
Jamf Threat Labs sucht danach und erfasst Proben unter realen Bedingungen über statische und verhaltensbasierte Regeln. Bei der Überprüfung dieser Proben mit VirusTotal wurde festgestellt, dass etwa **50 %** der Proben nicht von anderen Forschern hochgeladen wurden.

Wenn Malware zu leicht identifizierbar wird, nehmen die Autoren leider umfangreiche Änderungen vor, um sie wieder unkenntlich zu machen. Forscher müssen auf fortschrittliche Erkennungstechniken setzen, indem sie das *Verhalten* untersuchen, anstelle sich auf statische Dateimerkmale verlassen. Verhaltensbasierte Warnmeldungen, die als hochkritisch eingestuft werden, werden von den erweiterten Bedrohungskontrollen von Jamf erkannt und anschließend blockiert. Im Jahr 2025 waren dies die häufigsten:

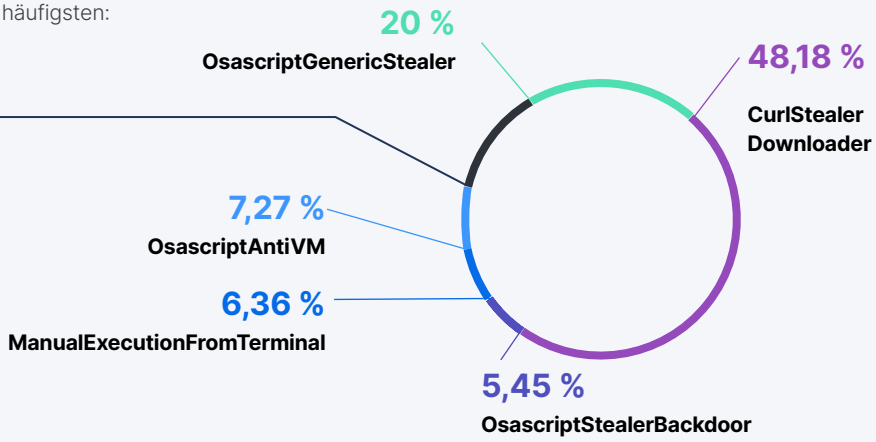
Andere 12,74 %

StealerDataExfiltration	**3,64 %**
XcodeExecutesCurl	**2,73 %**
KnownMaliciousCurlCommand	**2,73 %**
MaliciousCurlUserAgent	**1,82 %**
InsecureCurlFromScriptEditor	**0,91 %**
NpmMaliciousPackage	**0,91 %**

BEISPIELE, DIE VON JAMF THREAT LABS GEFUNDEN WURDEN



ERWEITERTE VERHALTENSERKENNUNGEN



Hier ist ein Beispiel dafür, wie sich diese Bedrohungen verhalten:

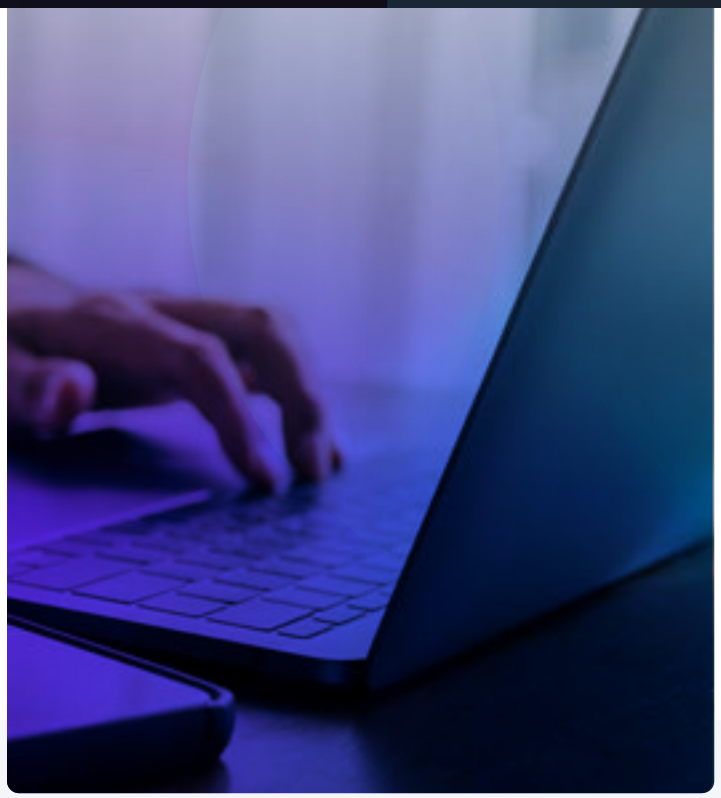
CurlStealerDownloader:
verdächtige Nutzung von Curl zum Herunterladen und Ausführen potenzieller Infostealer-Nutzlasten

OsascriptGenericStealer
generische macOS-Infostealer-Aktivität über die AppleScript-Ausführung erkannt

XcodeExecutesCurls:
verdächtiger Curl-Befehl, der während des Xcode-Erstellungsprozesses ausgeführt wird

NpmMaliciousPackage:
Ausführung eines potenziell bösartigen NPM-Pakets, das auf verdächtige Skriptaktivitäten während der Installation oder Laufzeit hinweist

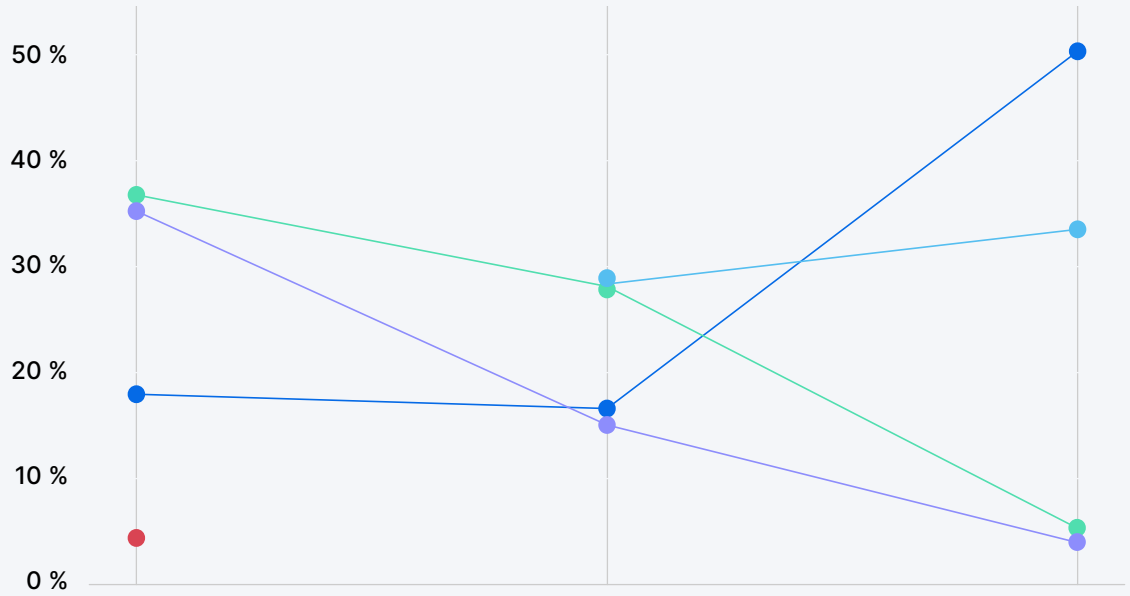
Der Punkt ist, dass Bedrohungen, die auf Mac abzielen, häufig und vielfältig sind. Angreifer entwickeln Malware zu ihrem eigenen Vorteil und zum Verkauf an den Meistbietenden - und die Nachfrage wird immer größer. Um sich zu schützen, müssen Sie zunächst wissen, gegen welche Malware Sie kämpfen.



Die am häufigsten vorkommende Malware auf Macs

2025 haben sich die Angriffsstrategien geändert. 2024 dominierten Infostealer und Adware mit jeweils etwa **28 %** der Angriffe. 2025 belegten Trojaner den Spitzenplatz und machten etwa die Hälfte aller Angriffe aus, während Infostealer mit rund einem Drittel dahinter lagen. Dabei ist zu beachten, dass sich Infostealer weiterentwickelt haben und nun Trojaner-Backdoors nutzen, was zu diesem Anstieg beiträgt. Ein Vergleich der diesjährigen Daten mit den Berichten der Vorjahre zeigt, wie sich die Popularität der Bedrohungen verändert:

DIE WICHTIGSTEN MALWARE-TRENDS



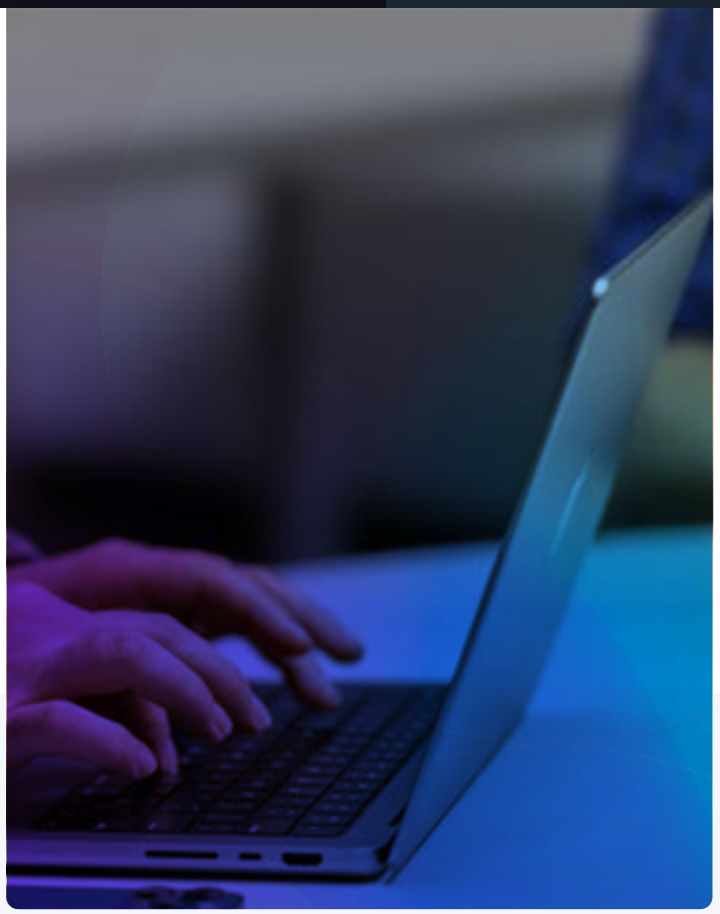
Malware Type	2023	2024	2025
Trojaner	17,96 %	16,61 %	50,32 %
Infostealers	-	28,36 %	33,52 %
Adware	36,77 %	28,13 %	5,06 %
PUA	35,24 %	15,06 %	4,84 %
Exploit	4,40 %	-	-

Die vier wichtigsten Malware-Typen machen **über 90 % aller Angriffe aus.** Sie sind:

	Merkmale:	Absicht:	Verbreitung:
Trojaner 50,4 %	Getarnt als legitime App	Verschiedene, werden häufig als Hintertür für andere Angriffe verwendet	Social Engineering, Datei-Repositories, etc.
Infostealers 33,52 %	Stehlen von Systemdaten unmittelbar nach der Kompromittierung	Sammeln sensibler Daten wie Logins und personenbezogener Daten	Wird manchmal als Dienstleistung angeboten und über Social Engineering, bösartige Websites und Software-Downloads verbreitet
Adware 5,06 %	Zeigt Werbung an, kann das Verhalten des Benutzers für gezielte Werbung oder Spyware verfolgen	Werbeeinnahmen generieren oder Informationen sammeln	In Kombination mit anderer Software oder in bösartigen Websites/Attachments
Potenziell unerwünschte Anwendungen (PUA) 4,84 %	Kann viele Formen annehmen; kann Daten sammeln, Geräte verlangsamen oder störend sein	Sie sind nicht immer explizit bösartig, können aber Benutzerdaten zu Geld machen oder auf andere Weise Erlöse erzielen.	In Kombination mit anderer Software oder durch irreführende Taktiken heruntergeladen

Andere 6,26 %

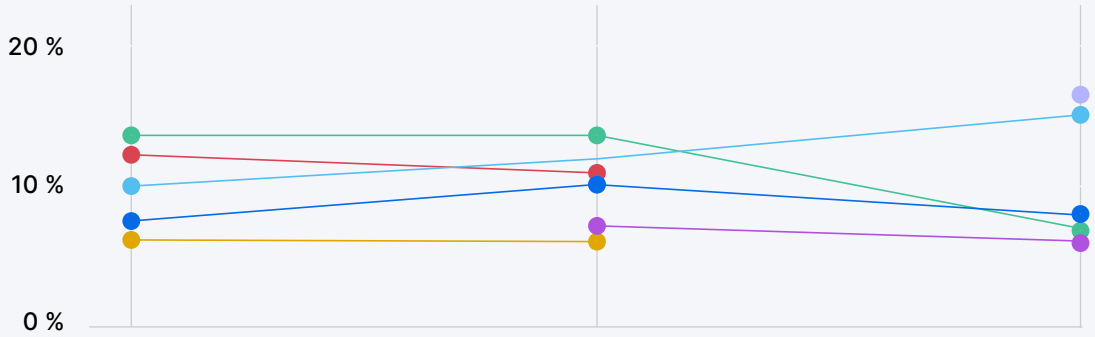
2,0 % Exploit, **1,4 %** Hacktool, **0,9 %** Coinminer, **0,4 %** Downloader, **0,4 %** Keylogger, **0,3 %** Ransomware, **0,2 %** Dropper



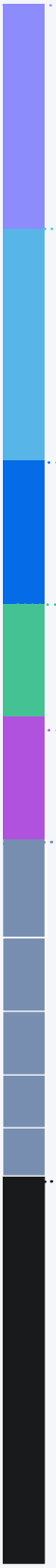
Die am häufigsten vorkommende Malware-Familien auf Macs

Es gibt eine Vielzahl von Malware-Familien, die Mac-Systeme angreifen, wobei es keinen eindeutigen Spitzenreiter gibt. 2025 war PuAgent mit **16,41 %** am weitesten verbreitet. In den Jahren 2023 und 2024 war die Adware Genio mit **13,63 %** am häufigsten verbreitet, bis sie 2025 mit **7,19 %** auf den vierten Platz zurückfiel.

DIE WICHTIGSTEN MALWARE-TRENDS



Malware Type	2023	2024	2025
PuAgent	-	-	16,41 %
Generische	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 %	-



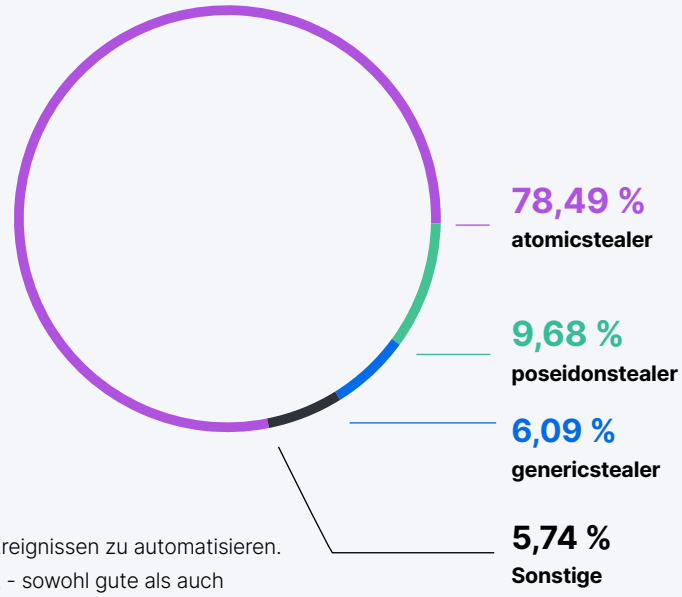
	Merkmale:	Verbreitung:
PuAgent Adware **16,4 %**	Modifiziert Browser, indem er Suchmaschinen, Homepages, Einstellungen, Erweiterungen und andere Funktionen ändert. Nutzt Werbe-Popups und verfolgt das Verhalten der Benutzer.	E-Mail-Anhänge, bösartige Downloads/Links, Freeware
Generische/ Verschiedene **15,1 %**	Dateien weisen verdächtiges Verhalten auf, das auf Malware hindeutet, haben aber keine Signaturen, die für eine bekannte Malware-Familie spezifisch sind.	Verschiedene
Multiverze- Trojaner **7,5 %**	Sammelt Daten von Benutzern, einschließlich privater Informationen wie Passwörter, Kreditkartennummern, Krypto-Wallets und anderer Informationen. Kann alles aufzeichnen, was Sie eingeben und kann Ihren Bildschirm sehen. Darf für den Benutzer nicht sichtbar sein.	Phishing-E-Mails, bösartige Websites, Malvertising, Freeware, soziale Medien
Genio Adware **7,2 %**	Kapert Webbrowser, um Benutzerinformationen zu sammeln; gibt sich als Suchmaschine aus, um gesponserte Ergebnisse anzuzeigen; ist schwer zu deinstallieren.	In Kombination mit legitimer Software, bösartige Downloads
Mackeeper PUA **7,1 %**	Erscheint wie eine vertrauenswürdige Anwendung, erfüllt aber möglicherweise nicht die Leistungsanforderungen. Generiert Werbe-Popups, kann falsche Behauptungen über den Zustand des Geräts aufstellen und die Leistung des Geräts beeinträchtigen.	Malvertising, bösartige Downloads
Imobie **6,3 %**		
Revproxy **4,7 %**		
atomic_stealer **4,1 %**		
Ccleanmac **3,4 %**		
Macinformer **3,1 %**		
Andere **25,1 %**		

Infostealer

Im Falle eines Diebstahls (rein hypothetisch gesprochen), ist die Wahrscheinlichkeit, gefasst zu werden, umso geringer, je schneller man ein- und wieder ausbricht. Infostealer versuchen in der Regel, schnell zu handeln, um Ihre Daten zu stehlen, kurz nachdem Ihr Gerät infiziert wurde. Manchmal löschen sie sich selbst, nachdem der Schaden angerichtet ist, moderne Infostealer können hingegen eine Persistenz aufbauen.

> *Infostealer haben eine wichtige Rolle bei der Verbreitung von Malware im macOS-Ökosystem gespielt. AppleScript ist zwar für erfahrene Benutzer nützlich, wurde aber auch häufig für Malware missbraucht.*
>
> Jaron Bradley, Jamf

DIE HÄUFIGSTEN INFOSTEALER



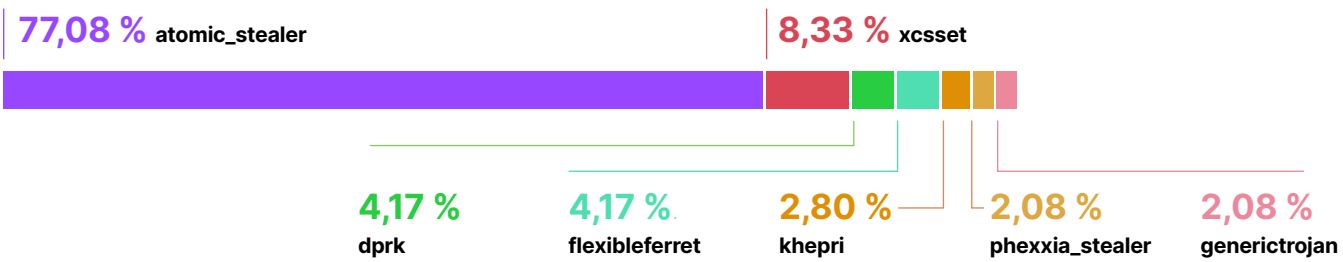
Entwickler und Benutzer verwenden AppleScript, um eine Vielzahl von Ereignissen zu automatisieren. Es ist ein mächtiges Werkzeug, das unendlich viele Möglichkeiten bietet - sowohl gute als auch schlechte. Angreifer nutzen sie, um Benutzer zu täuschen und ihre Daten zu stehlen.

Infostealer sind seit 2023 deutlich häufiger geworden, als sie lediglich einen geringen Anteil von **0,25 %** der Angriffe ausmachten. Im Jahr 2024 gab es einen steilen Anstieg auf **28,36 %**, um schließlich **im Jahr 2025** bei 33,52 % zu landen. So beliebt sie auch sind, die meisten Angriffe erfolgen durch andere Arten von Malware, wie Trojaner. Apropos ...

Trojaner

Trojaner wurden 2025 immer beliebter und führten schließlich mit **50,3 % aller Malware-Angriffe** die Hitliste an. Der am häufigsten auftretende Trojaner, **atomic_stealer**, war an **77,08 % der Angriffe** beteiligt. Wahrscheinlich ist Ihnen die Ähnlichkeit zum dominierenden Infostealer des Jahres 2025 aufgefallen – das ist kein Zufall. Viele Diebe verwenden Trojaner, um Hintertüren einzurichten, die ein erneutes Eindringen ermöglichen.

AKTIVE TROJANER



Den Feind zu kennen ist die halbe Miete.

Ein Großteil der Malware, über die wir gesprochen haben, ist bekannt. Ihre Software zur Erkennung von Bedrohungen wird ihn wahrscheinlich erkennen. Wie wir bereits angedeutet haben, ist nicht jede Malware an ihrem Code zu erkennen. Fortschrittliche Erkennungsverfahren, die verdächtiges Verhalten identifizieren, sind entscheidend für das Aufspüren von Bedrohungen, die von der Cybersicherheits-Community noch nicht analysiert wurden. Die Implementierung fortschrittlicher Tools trägt wesentlich dazu bei, Ihr Unternehmen vor Zero-Day-Angriffen zu schützen.

Auch die Konfiguration ist wichtig. Malware nutzt oft das Verhalten eines Benutzers aus, z. B. wenn er einen riskanten Download durchführt oder auf einen Social Engineering-Angriff hereinfällt. Sicherheitsrichtlinien und Benutzerschulungen leisten hierbei Abhilfe.

Die Erkennung ist entscheidend; Prävention beginnt bereits bei der Software selbst. Cyberangriffe beruhen auf Schwachstellen in der Software – Schwachstellen im Design von Apps und Betriebssystemen, die sich ausnutzen lassen. Die beste Möglichkeit, diese Schwachstellen zu beseitigen und Angreifer fernzuhalten, ist die Durchsetzung von Updates für Ihre Geräte und Apps. Wir werden im nächsten Abschnitt noch näher darauf eingehen.

Stellungnahme von unserem CISO

Da sich Apple-Geräte im Unternehmen immer weiter ausbreiten, sollten die ausgewählten Sicherheitslösungen speziell für das Apple-Ökosystem entwickelt und nicht von einem Windows-first-Ansatz übernommen werden. Unternehmen sollten sich für Sicherheitsprodukte entscheiden, die von Grund auf für macOS entwickelt wurden, um sicherzustellen, dass die Funktionen zur Erkennung von Bedrohungen, zur Durchsetzung von Konformität und zur Reaktion auf Bedrohungen vollständig auf die Funktionsweise von Apple-Plattformen abgestimmt sind und nicht bloß als zweitrangige Ergänzung behandelt werden.

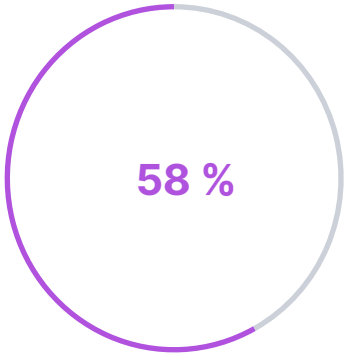
Schwachstellen in Apps und Betriebssystemen

Das Betriebssystem ist die Grundlage eines Geräts. Es steuert die Tools, Dienste, Apps und die Sicherheit Ihres Geräts. Angreifer suchen kontinuierlich nach Schwachstellen im System, um seine Verteidigung zu infiltrieren.

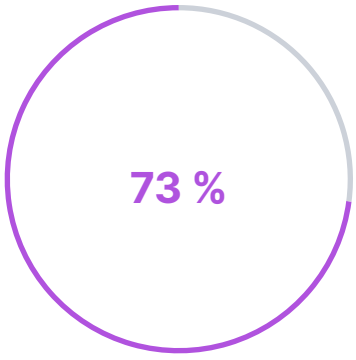
Und Schwachstellen summieren sich. Selbst weniger schwerwiegende Schwachstellen können zu einem entscheidenden Schritt bei einem Angriff werden, und manchmal wird das Patchen dieser Lücken vernachlässigt.

Apropos Patchen - das ist eine wichtige Sache. Leider haben auch die sichersten Betriebssysteme irgendwo Lücken. Dies ist unvermeidlich, aber reparabel. Apple bringt ständig neue Software-Updates heraus, um diese Schwachstellen zu beheben. Wenn Sie und Ihr Unternehmen geschützt sein soll, müssen Sie diese Aktualisierungen durchführen. Doch das wird nicht immer konsequent gemacht.

Auch Apps sind wichtig. Jede hat ihre eigenen Schwachstellen, Richtlinien für den Umgang mit Daten, Entwicklungsbibliotheken und vieles mehr.



der **Unternehmen** hatten mindestens **ein Gerät** mit einem **veralteten Betriebssystem**



der **Geräte** *enthalten* mindestens eine **anfällige App**

Was ist ein CVE?

Das Programm „Allgemeine Schwachstellen und Gefährdungen" (CVE) dient als Datenbank für Schwachstellen, die von der Cybersicherheits-Community entdeckt wurden. Jede CVE-Liste identifiziert die betroffene Software oder Bibliothek, listet einen Schweregrad auf und beschreibt mögliche Methoden zur Ausnutzung

Veraltete Software ist weit verbreitet. Benutzer sind nicht immer begeistert von Aktualisierungen, insbesondere wenn dadurch ihre Arbeit gestört wird. Doch das Durchsetzen von Update-Fristen und Mindestversionen des Betriebssystems trägt entscheidend zum Schutz Ihrer Geräteflotte und Ihrer Daten bei – etwa vor Exploits, die genau diese Schwachstellen ausnutzen.

Signifikante macOS-Sicherheitslücken des Jahres 2025

CVE-2025-46287 | Schweregrad: 9,8 (kritisch)	CVE-2025-43539 | Schweregrad: 8,8 (hoch)	CVE-2025-46285 | Schweregrad: 7,8 (hoch)
BESCHREIBUNG:		
Ein Angreifer könnte in der Lage sein, seine FaceTime-Anrufer-ID zu fälschen.	Die Verarbeitung einer Datei kann zu einer Beschädigung des Speichers führen.	Eine App ist unter Umständen in der Lage, sich Root-Privilegien zu verschaffen.
BETROFFENE KOMPONENTE		
Anruf-Framework	AppleJPEG	Kernel
AUSWIRKUNGEN:		
Durch die Anzeige irreführender Informationen kann der Angreifer den Benutzer dazu verleiten, etwas Falsches zu tun.	Ein Angreifer kann Daten verändern, um nicht autorisierten Code auszuführen.	Ein Angreifer kann beliebigen Code ausführen.
GEPATCHTES OS:		
macOS Tahoe 26.2, Sequoia 15.73 und Sonoma 14.8.3	macOS Tahoe 26.2, Sequoia 15.73 und Sonoma 14.8.3	macOS Tahoe 26.2, Sequoia 15.73 und Sonoma 14.8.3

Von Jamf entdeckte Schwachstellen

CVE-2025-43296 | Okt 2025
Systemeinstellungen Gatekeeper-Umgehung, gepatcht in macOS Tahoe 26.

CVE-2025-43348 | Nov 2025
Finder Gatekeeper-Umgehung, gepatcht in macOS Tahoe 26.1.

Weitere Schwachstellen, die nach unserer Bestätigung im Jahr 2025 ausgenutzt wurden, sind in der folgenden Tabelle aufgeführt.

CVE-ID	KOMPONENTE	AUSWIRKUNGEN
CVE-2025-24113 CVSS-Score: 4,3 | Schweregrad: **mittel**	Safari	Das Aufrufen einer bösartigen Website kann zu einem Spoofing der Benutzeroberfläche führen.
CVE-2025-46289 CVSS-Score: 5,5 | Schweregrad: **mittel**	AppSandbox	Eine App kann sich möglicherweise Zugriff auf geschützte Daten des Benutzers verschaffen.
CVE-2025-43482 CVSS-Score: 5,5 | Schweregrad: **mittel**	Audio	Eine App kann möglicherweise eine Dienstverweigerung verursachen.
CVE-2025-43517 CVSS-Score: 3,3 | Schweregrad: **niedrig**	Anrufverlauf	Eine App kann aufgrund eines Protokollierungsproblems möglicherweise auf geschützte Daten des Benutzers zugreifen.
CVE-2025-43542 CVSS-Score: 7,5 | Schweregrad: **hoch**	FaceTime	Passwortfelder könnten unbeabsichtigt offengelegt werden, wenn ein Gerät per Fernsteuerung über FaceTime gesteuert wird.
CVE-2025-43532 CVSS-Score: 2,8 | Schweregrad: **niedrig**	Foundation	Die Verarbeitung bösartiger Daten kann zu einer unerwarteten Beendigung der App aufgrund einer Speicherbeschädigung führen.
CVE-2025-43512 CVSS-Score: 7,8 | Schweregrad: **hoch**	Kernel	Eine Anwendung kann möglicherweise die Berechtigungen erweitern.

Der Umgang mit Schwachstellen ist ein ständiger Kampf – aber kein aussichtsloser.

Um den Überblick über Software-Schwachstellen zu behalten, brauchen Sie eine gute Strategie. Im einfachsten Fall müssen Sie Schwachstellen, die sich auf Ihre Systeme und Geräte auswirken, fortlaufend identifizieren, entschärfen und überwachen.

Je nach Größe und Kapazitäten Ihrer IT- und Sicherheitsteams sind Sie unter Umständen in der Lage, selbst auf Bedrohungssuche zu gehen – oder auch nicht. Zum Glück steht die Cybersicherheits-Community hinter Ihnen. Bedrohungsforscher und Softwareanbieter sind ständig auf der Suche nach den neuesten Schwachstellen und fügen potenzielle Schwachstellen in Datenbanken ein, damit Unternehmen wissen, wo sie verwundbar sind. Ihre Teams können sich anhand dieser Informationen einen Überblick über Ihre aktuelle Sicherheitslage verschaffen und entsprechend reagieren. Außerdem gibt es Sicherheitstools, die diesen Prozess vereinfachen.

Welche Tools Ihr Unternehmen konkret benötigt, hängt von der Größe, den Kompetenzen, der Branche und anderen Faktoren ab. Aber im Allgemeinen müssen Sie diese Dinge tun können:

- **Geräte konfigurieren und Richtlinien durchsetzen**
- **Benutzerkonten und Identitäten verwalten**
- **Geräte und Software aktuell halten**
- **Zustand der Geräte überwachen**
- **Zugriffsrichtlinien durchsetzen**

Mobile Device Management, Endpunktschutz, Identitätsverwaltung und Telemetrie-Tools helfen Ihnen bei diesen Aufgaben, so dass Sie Bedrohungen stets im Voraus erkennen können.

Stellungnahme von unserem CISO

Eine robuste Sicherheitsstrategie basiert auf den Grundpfeilern Sichtbarkeit, Telemetrie und Automatisierung und nirgendwo ist dies wichtiger als beim Schwachstellenmanagement. **Sicherheitsteams** sollten:

ihre Schwachstellen verstehen

Die Erkennung von Schwachstellen im gesamten Unternehmen ist der erste wichtige Schritt. Ein umfassender Überblick über die Schwachstellen der Geräte und die Infrastruktur von Endbenutzern bildet die Grundlage für eine datengesteuerte Sicherheitsstrategie. Auf dieser Grundlage können die Teams den digitalen Fußabdruck der Anwendung analysieren, das potenzielle Risiko bewerten und den Auswirkungsradius bestimmen. Dies erlaubt eine Priorisierung von Sicherheitslücken, die sich auf konkrete Belege stützt und nicht auf bloßen Annahmen beruht.

Implementierung eines risikobasierten Ansatzes für den Zugriff auf Geräte

Wenn nicht konforme Geräte versuchen, auf Unternehmensressourcen zuzugreifen, sollte der Zugang blockiert werden, bis das Gerät wieder konform ist, wobei die Korrekturmaßnahmen so nahtlos und reibungslos wie möglich für den Endbenutzer ablaufen sollten.

Etablierung eines soliden Patching-Programms

Kommen wir noch einmal auf den Punkt MDM zurück: Ein Tool, das sicherstellt, dass Sie mit den neuesten oder unterstützten N -X-Versionen von Software oder OS Schritt konform sind, ist für eine stabile und sichere Umgebung von größter Bedeutung. Wenn dies mit geringen oder gar keinen Auswirkungen auf die Endbenutzer geschieht, ist es einfacher, Partnerschaften einzugehen und das Unternehmen zu unterstützen.

Lesen Sie die neuesten Forschungsergebnisse zu macOS von Jamf Threat Labs

OpenClaw: die nützliche KI, die heimlich zu Ihrer größten Insider-Bedrohung werden könnte

FEBRUAR 2026

OpenClaw ist ein Open-Source-Framework für die Entwicklung autonomer KI-Agenten, die Shell-Befehle ausführen, auf Dateien zugreifen und mit Apps interagieren können, ohne über integrierte Sicherheitsbarrieren zu verfügen. Dadurch entstehen erhebliche Sicherheitsrisiken für Unternehmen. Das Framework stellt aufgrund des uneingeschränkten Systemzugriffs, dem Potenzial zur Exfiltration von Daten und den Schwachstellen bei indirekten Prompt-Injection-Angriffen, bei denen bösartige Anweisungen in legitime Geschäftsinhalte eingebettet werden, ein Sicherheitsrisiko dar. Jüngste Sicherheitshinweise haben gezeigt, wie Angreifer verschiedene Schwachstellen ausnutzen können, um sich dauerhaften Zugang zu verschaffen. Dadurch stellen OpenClaw-Implementierungen eine hochriskante Insider-Bedrohung dar, deren sichere Verwaltung in Unternehmensumgebungen umfassende Strategien zur Erkennung, Prävention und Governance erfordert.

Bedrohungsakteure missbrauchen Microsoft Visual Studio Code für ihre Zwecke

JANUAR 2026

Nordkoreanische Bedrohungsakteure haben die Contagious Interview-Kampagne weiterentwickelt, um die Task-Konfigurationsdateien von Visual Studio Code zu missbrauchen und eine JavaScript-Hintertür einzubauen, sobald Opfer bösartige Git-Repositories öffnen. Die Backdoor stellt eine dauerhafte Befehls- und Kontrollkommunikation her, sammelt Systeminformationen und ermöglicht die Ausführung von Remotecode. Diese Technik nutzt die Vertrauensabläufe in der Entwicklung aus – wenn Benutzer ein Repository als vertrauenswürdig markieren, führen bösartige Konfigurationsdateien automatisch versteckte Befehle aus. Dies zeigt, wie Angreifer ihre Taktiken kontinuierlich anpassen, um sich in legitime Entwicklungstools einzubinden.

Von ClickFix zu signiertem Code: der stille Wandel der MacSync Stealer Malware

DEZEMBER 2025

MacSync Stealer hat sich über die Drag-to-Terminal-Techniken hinaus weiterentwickelt und wird jetzt über eine code-signierte und notarisierte Swift-Anwendung bereitgestellt, die heimlich Payloads abruft und ausführt, ohne dass eine Terminal-Interaktion erforderlich ist. Diese über gefälschte Installer verbreitete Variante nutzt einen hochentwickelten Dropper, der Verbindungstests durchführt, Ratenbegrenzung erzwingt, Payloads validiert und vor der Ausführung Quarantäneattribute entfernt. Diese Verlagerung hin zur signierten und notarisierten Bereitstellung spiegelt einen breiteren Trend wider, bei dem Angreifer bösartigen Code als legitime Anwendungen tarnen, um die macOS-Sicherheitskontrollen zu umgehen und zu verhindern, dass sie entdeckt werden.

FlexibleFerret-Malware schlägt weiter zu

NOVEMBER 2025

FlexibleFerret, eine mit Nordkorea verbundene Malware-Familie, zielt auf macOS Benutzer ab und nutzt dazu ausgeklügelte gefälschte Stellenanzeigen, mit denen die Opfer dazu verleitet werden, bösartige Terminal-Befehle auszuführen, die als Einstellungsprüfungen getarnt sind. Der mehrstufige Angriff nutzt JavaScript auf gefälschten Jobbörsen, um eine Backdoor mit umfassenden Funktionen wie Dateiexfiltration und Befehlsausführung zu installieren. Gleichzeitig werden Zugangsdaten über manipulierte Chrome-Eingabefenster abgegriffen und an vom Angreifer kontrollierte Dropbox-Konten gesendet. Diese Bedrohung umgeht Gatekeeper, indem sie Benutzer dazu bringt, Befehle manuell auszuführen. Für die Abwehr ist es daher unerlässlich, das Bewusstsein für dubiose Bewerbungstests und die Risiken von Anweisungen über das Terminal zu schärfen.

DigitStealer: ein JXA-basierter Infostealer, der kaum Spuren hinterlässt

NOVEMBER 2025

DigitStealer ist ein ausgeklügelter macOS-Infostealer, der bei VirusTotal völlig unentdeckt blieb, obwohl er fortschrittliche Anti-Analyse-Techniken einsetzt, einschließlich der Erkennung von Hardware-Merkmalen, die die Ausführung auf Apple Silicon M2-Chips oder neuere Versionen beschränken. Die Malware stellt vier speicherresidente Payloads bereit, die Browserdaten, Kryptowährungs-Wallets und Anmeldedaten stehlen. Sie trojanisiert Ledger Live, indem sie drei separate Komponenten zusammenführt, um die Erkennung zu umgehen, und stellt über eine dynamische Backdoor eine Persistenz her. Die Nutzung legitimer Cloudflare-Dienste für das Payload-Hosting sowie die mehrstufige Verschleierung belegen, dass die Cyberkriminellen sich mit den macOS-Interna auskennen. Da die Ausführung größtenteils im Arbeitsspeicher erfolgt, ist eine verhaltensbasierte Erkennung unerlässlich.

ChillyHell: ein umfassender Einblick in eine modulare macOS Backdoor

September 2025

ChillyHell ist eine hochentwickelte macOS-Backdoor, die seit 2021 unentdeckt blieb und von Apple notarisiert war. Ursprünglich wurde er mit Angriffen auf ukrainische Regierungsbeamte in Verbindung gebracht. Diese modulare C++-Malware verfügt über mehrere Persistenzmechanismen, kommuniziert über DNS und HTTP und verfügt über Funktionen wie Reverse Shells, Selbstaktualisierung, Payload-Zustellung und Brute-Forcing von Passwörtern. Seine fortschrittlichen Umgehungstechniken zeigen, dass signierte und notarisierte Apps nicht immer sicher sind.

Signiert und gestohlen: neue Erkenntnisse über Odyssey Infostealer

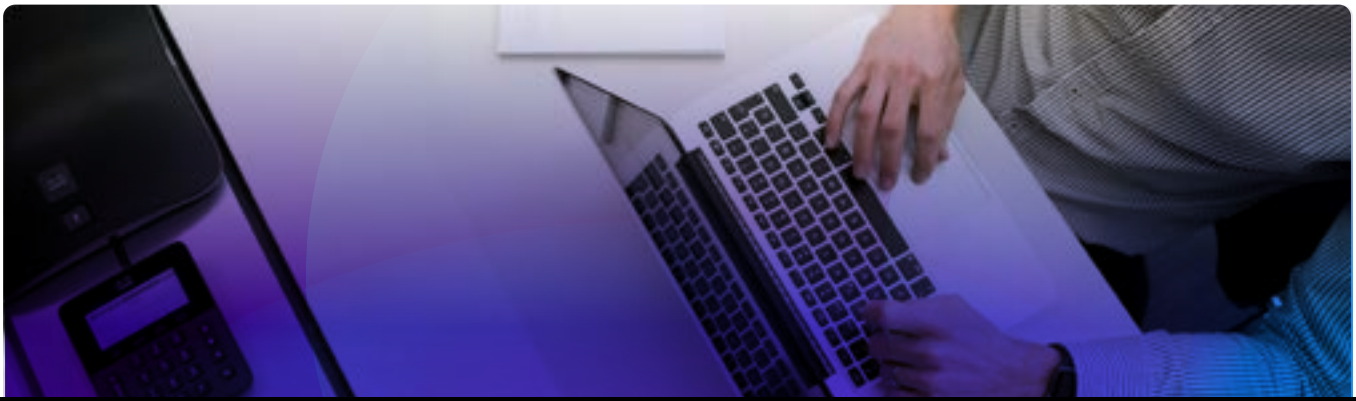
Juli 2025

Ein ausgeklügelter macOS-Infostealer hat es geschafft, die Code-Signierung und Notarisierung von Apple zu erhalten. Dadurch konnte er die integrierten Sicherheitskontrollen umgehen, eine dauerhafte Backdoor bereitstellen und legitime Apps für Kryptowährungen durch trojanisierte Versionen ersetzen. Die Malware nutzt eine trügerische SwiftUI-Oberfläche, um Passwörter abzufangen, lädt dynamisch verschleierte Payloads herunter und stellt eine kontinuierliche Befehls- und Kontrollfunktion für die Remotecodeausführung her. Besonders besorgniserregend: Die Malware führt aktiv ein Fingerprinting von Analyseumgebungen durch und setzt Forschungssysteme auf eine schwarze Liste, um eine Entdeckung zu vermeiden, was auf eine Professionalität auf staatlichem Niveau hindeutet.

Ein getarntes Python: Entpacken der PyInstaller Malware unter macOS

Mai 2025

Angreifer nutzen PyInstaller, um bösartigen Python-Code als native macOS-Ausführungsdateien zu tarnen - das ist das erste Mal, dass diese Technik bei macOS-Infostealern beobachtet wurde. Die Malware läuft, ohne dass Python installiert werden muss, und stiehlt Anmeldedaten durch gefälschte Passwortabfragen, sammelt Keychain-Daten und Kryptowährungs-Wallets, während sie verschiedene Verschleierungstaktiken verwendet, um nicht erkannt zu werden. Diese Technik stellt eine bedeutende Weiterentwicklung bei der Verbreitung von Malware für macOS dar und ermöglicht es Angreifern, ausgeklügelte Infostealer bereitzustellen und dabei möglicherweise herkömmliche Sicherheitsmechanismen zu umgehen.



jamf

Kontaktieren Sie uns, um mehr über die Bedrohungen für Macs zu erfahren.