jamf

Security 360:

Annual Trends Report

Mac

Table of contents

Introduction

Jamf's Security 360 is a report that is derived from the analysis of real-world customer incidents, threat research and industry events from the past year. This report is focused on exploring the Mac threat landscape to put a spotlight on the risks that organizations face.

We examine the diverse and impactful attack vectors that attackers use to cause harm. Mac devices' rise in popularity made it a hot commodity for attackers, who constantly craft new tactics to infiltrate devices and steal data.

In addition to analyzing the novel ways attackers target Mac, the report includes a perspective from Jamf's CISO, providing insight to security leaders and IT practitioners responsible for protecting Mac fleets.

Research methodology

To understand and quantify the real-world impact of the security trends identified in this report, we anonymously examined a sample group consisting of over 150,000 Mac devices. Our analysis was carried out at the end of 2025, revisiting the prior 12-month period. Data included in our malware investigation looked only at US-based devices, while our look into vulnerabilities included global data.

To preserve privacy and maintain the highest standards when gathering and handling data, the metadata analyzed in our research comes from aggregated logs that do not contain personal or organization-identifying information.

Key findings

44%

of **devices** have **malicious network traffic**

Attackers are always trying to compromise your devices. Detecting and containing malicious traffic requires constant diligence — and the right tools.

41%

of **devices** have **critically out-of-date** operating systems

Enforcing minimum software versions ensures your devices have the latest security patches, reducing the number of known exploitable vulnerabilities.

50%

of **malware** affecting Mac were **trojans**

Trojans topped the charts this year, increasing by over 33 percentage points since 2024. Trojans are back doors into your systems, leaving lasting damage and vulnerability to other attacks.

73%

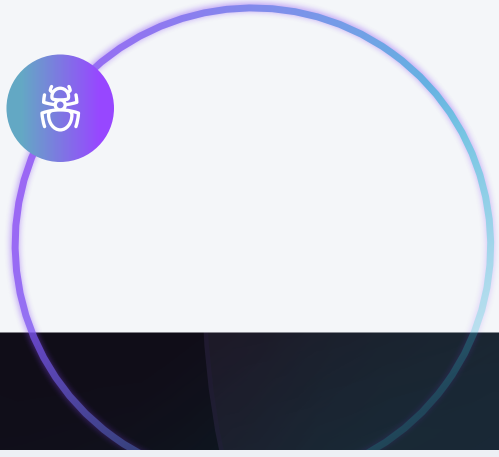
of **devices** have **vulnerable apps**

Your OS isn't the only software that introduces risk. Apps can contain vulnerable libraries, suffer supply chain compromises or mishandle data. Knowing what's installed across your organization is critical to managing risk.

26%

of **organizations** have at least **one device affected by cryptojacking**

Cryptojacking attacks use your device's processing power to mine cryptocurrency. While attackers gain wealth, your device loses performance and efficiency.



Key trends in the enterprise

1. Mac isn't a niche target anymore.

Organizations of all sizes and industries use Mac, more than ever before. From 2024 to 2025, Mac device's market share grew by 16.4% to nearly 10%, a greater increase than any other vendor.

With more than 2.7 million Mac shipments in 2025, it's clear that Mac is everywhere. Attackers have been paying attention to this trend, and Mac became a hot target for exploits. Despite robust security features, the days of "Mac can't get malware" are long gone.

As Mac computers' presence in the enterprise grows, attackers enhance and evolve their methods to create Mac-specific threats — and steal your data.

2. Infostealers are evolving and stealing more data than ever.

Infostealers are one of the most commonly distributed malware types. Malware authors work hard to craft effective and subversive ways to harvest your data at large scales. They tend to act fast, collecting credentials, session tokens, files and anything else they can get their hands on, before the user notices anything amiss.

Infostealers are often the first stage in larger attacks. They can hold data for ransom or use it to infiltrate other accounts and systems. These features make infostealers a hot commodity for attackers, so many developers offer them as a service. Modern infostealers may establish a backdoor and persistence, allowing them to survive reboots and logouts — and letting attackers send commands from C2.

3. APT groups continue to eye macOS.

If you explore the Mac threat landscape, you'll likely see some familiar faces. Advanced threats resembling DPRK-related threats continue to target macOS in campaigns and malware like Contagious Interview, FlexibleFerret and Odyssey infostealer evolutions.

Attackers continue to build backdoors and other persistence mechanisms. Jamf Threat Labs observed this in malware like ChillyHell.

Read more about Jamf Threat Labs' research near the end of this report.

Mac malware and threats

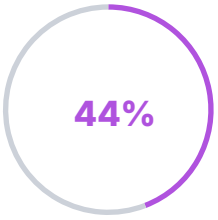
Mac and Windows computers are different, and therefore so is their malware. Attackers creating malware for Mac must consider these differences to know what to exploit. For an attack to work, bad actors are forced to bypass security features like:

1. **Gatekeeper**, which checks that apps are legitimate and safe by looking at its **notarization and developer information/signature**

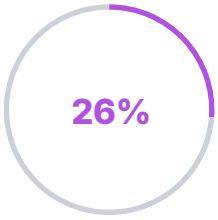
2. **System Integrity Protection (SIP),** which limits the ability to write to critical system files

3. **Transparency, Consent and Control (TCC),** which requires explicit user permission for access to the camera, microphone, files and other content

Despite those difficulties, **attackers are succeeding.**



of **devices** had **malicious network traffic**



of **organizations** were affected by **cryptojacking attacks**

That's why it's critical to **understand and uncover the latest threats**. There's a lot to keep up with.

Over 26k

the number of **malware samples** **Jamf Threat Labs** added to their database in 2025

Over 230

the number of **YARA rules** **Jamf Threat Labs** added in 2025

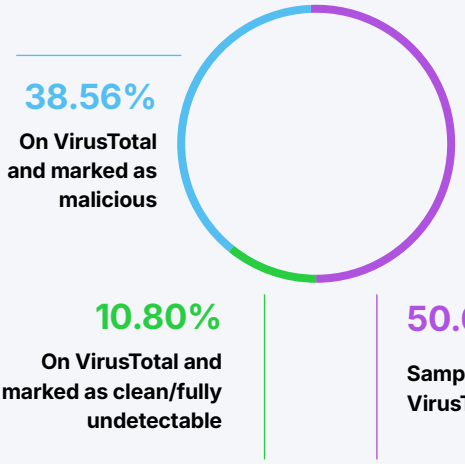
Once you know what you're dealing with, you need to know how to detect them. **YARA rules** help with this — researchers use them to identify and classify malware samples.

But what about the threats we don't know about? Attackers are working hard too, inevitably creating new attacks not yet discovered by the cybersecurity community.

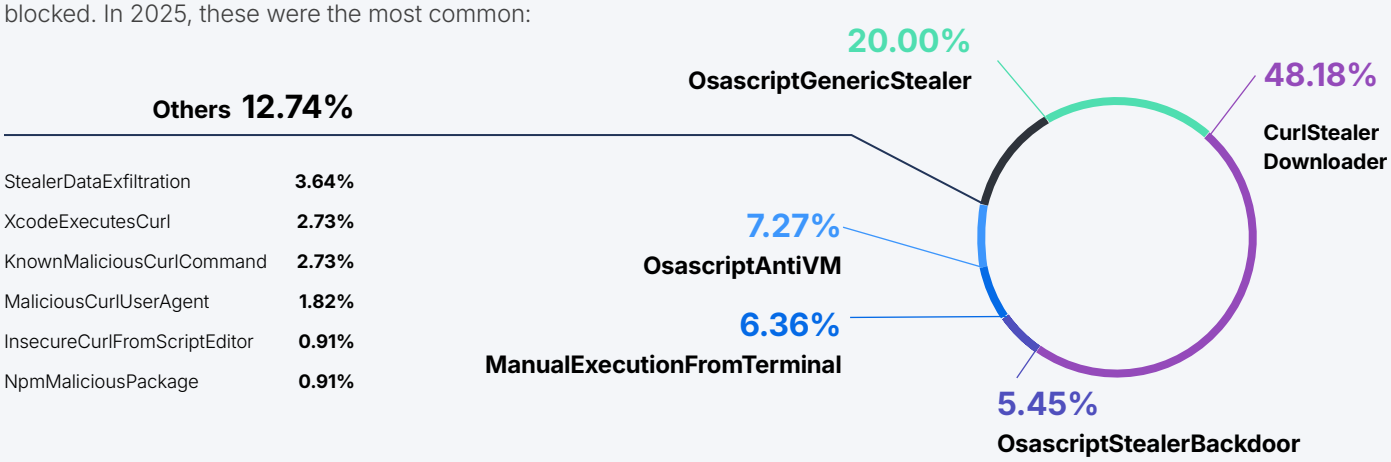
Jamf Threat Labs looks for these too, catching samples in the wild via static and behavior-based rules. When checking these samples with VirusTotal, about **50%** of the samples haven't been uploaded by other researchers.

Unfortunately, if malware becomes too identifiable, authors make major revisions in order to make it obscure again. Researchers must rely on advanced detection techniques by examining *behavior* instead of static file traits. Behavioral alerts marked as high severity get the attention of Jamf's advanced threat controls and are subsequently blocked. In 2025, these were the most common:

SAMPLES FOUND BY JAMF THREAT LABS



ADVANCED BEHAVIORAL DETECTIONS



Here's a sampling of how these detections behave:

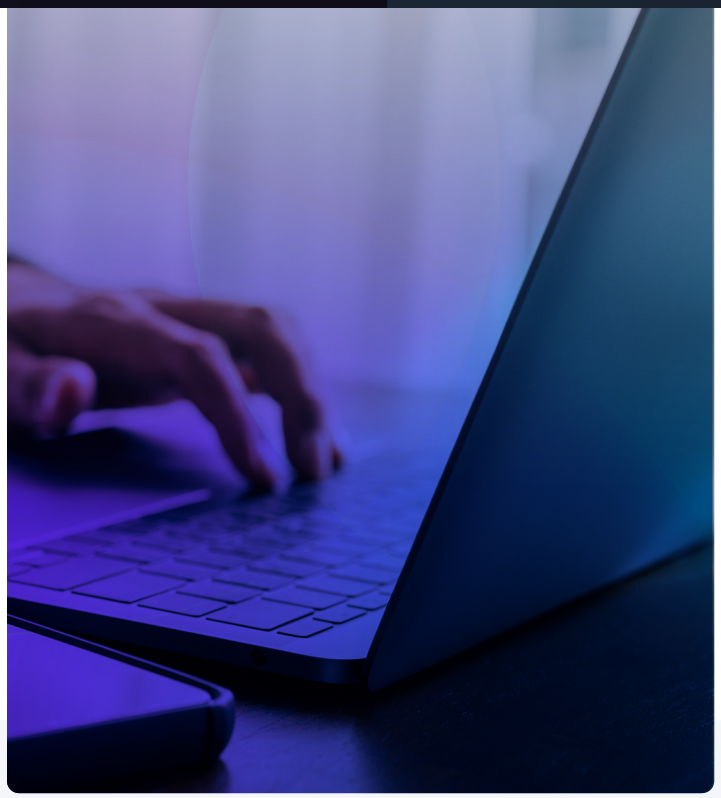
CurlStealerDownloader
suspicious use of curl to download and execute potential infostealer payloads

OsascriptGenericStealer
generic macOS infostealer activity detected via AppleScript execution

XcodeExecutesCurl
suspicious curl command executed during Xcode build process

NpmMaliciousPackage
execution of potentially malicious NPM package, indicating suspicious script activity during install or runtime

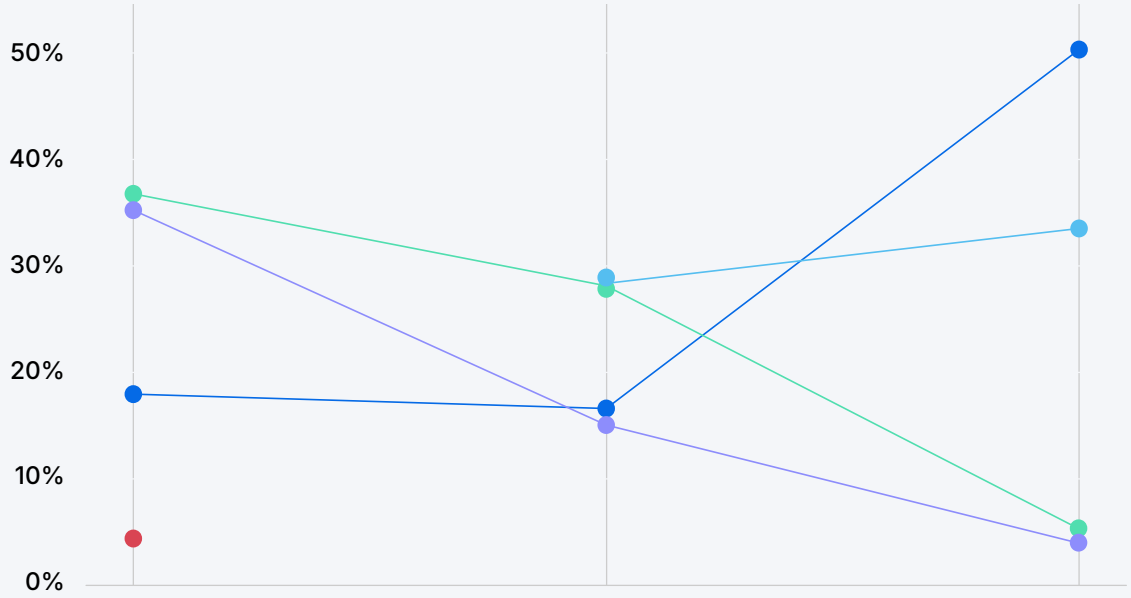
The point is, threats targeted at Mac are common and varied. Attackers are building malware for their own gain and to sell to the highest bidder — and the demand is higher than ever. To begin to stay protected, you need to know what malware you're fighting against.



Most common Mac malware

Attack strategies shifted in 2025. In 2024, infostealers and adware dominated the field, each representing about **28%** of attacks. In 2025, trojans found themselves on top, representing about half all attacks, with infostealers trailing behind at about a third. Note that infostealers have evolved to use trojan backdoors, contributing to this growth. Comparing this year's data to our previous years' reports, we can see how threats change in popularity:

TOP MALWARE TRENDS



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%	-	-

The top four malware types represent **over 90% of all attacks.** They are:

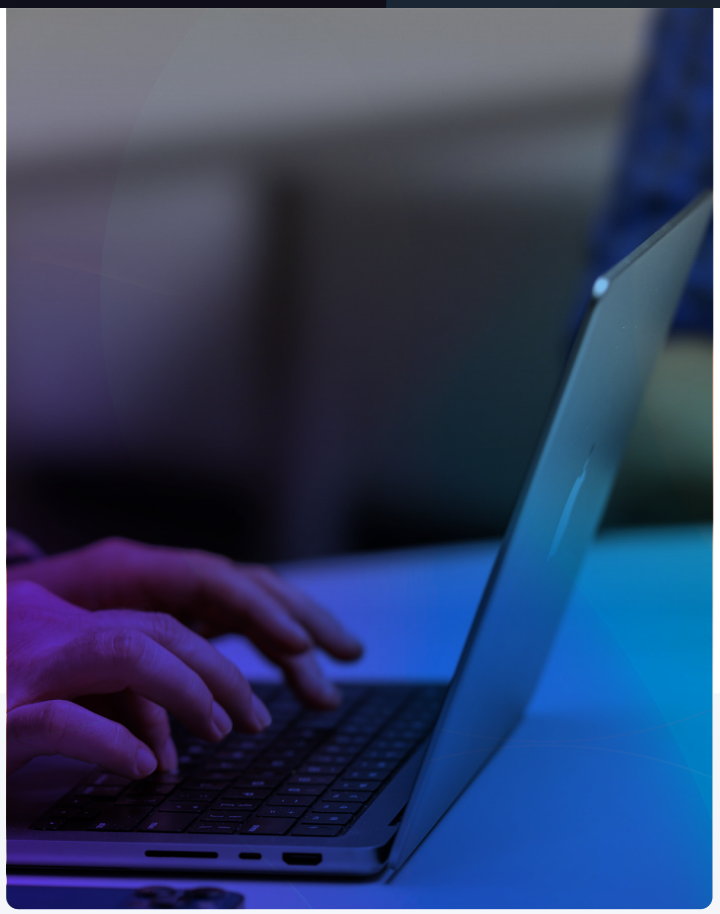
	Characteristics:	Intent:	Distribution:
Trojans 50.40%	Disguised as a legitimate application	Various, commonly used as a backdoor for other attacks	Social engineering, file repositories, etc.
Infostealers 33.52%	Steals system data immediately after infection	Harvest sensitive data like logins and personally identifiable information	Sometimes offered as a service and distributed via social engineering, malicious websites and software downloads
Adware 5.06%	Displays advertisements, may track user behavior for targeted advertising or spyware	Generate ad revenue or to collect information	Bundled with other software or present in malicious websites/attachments
Potentially unwanted applications (PUA) 4.84%	Can take many forms; may collect data, slow down devices or be disruptive	Not always explicitly malicious, but may monetize user data or generate revenue via other means	Bundled with other software or downloaded through misleading tactics

Other 6.26%

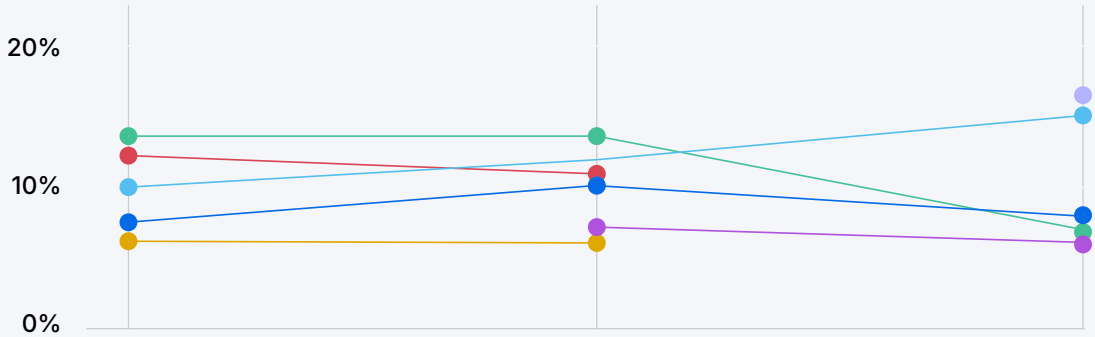
2.0% Exploit, **1.4%** Hacktool, **0.9%** Coinminer, **0.4%** Downloader, **0.4%** Keylogger, **0.3%** Ransomware,**0.2%** Dropper

Most common Mac malware families

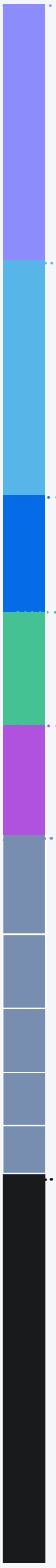
A wide variety of malware families affect Mac with no clear leader. In 2025, PuAgent was most common at **16.41%**. In 2023 and 2024, Genio adware was most common at **13.63%** until it fell into fourth place at **7.19%** in 2025.



TOP MALWARE TRENDS



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%	-



	Characteristics:	Distribution:
PuAgent Adware **16.4%**	Modifies browsers by changing search engines, homepages, settings, extensions and other features. Deploys ad popups and tracks user behavior.	Email attachments, malicious downloads/ links, freeware
Generic Various **15.1%**	Files exhibit suspicious behavior indicative of malware, but do not have signatures specific to a known malware family.	Various
Multiverze Trojan **7.5%**	Collects user data, including private information like passwords, credit card numbers, crypto wallets and other information. May record everything you type and see on your screen. May not be visible to the user.	Phishing emails, malicious websites, malvertising, freeware, social media
Genio Adware **7.2%**	Hijacks web browsers to collect user information; poses as a search engine to show sponsored results; is difficult to uninstall.	Bundled with legitimate software, malicious downloads
Mackeeper PUA **7.1%**	Appears as a legitimate application but may not meet performance claims. Delivers ad popups, may make false claims about device health and degrade device performance.	Malvertising, malicious downloads

Imobie 6.3%

Revproxy 4.7%

atomic_stealer 4.1%

Ccleanmac 3.4%

Macinformer 3.1%

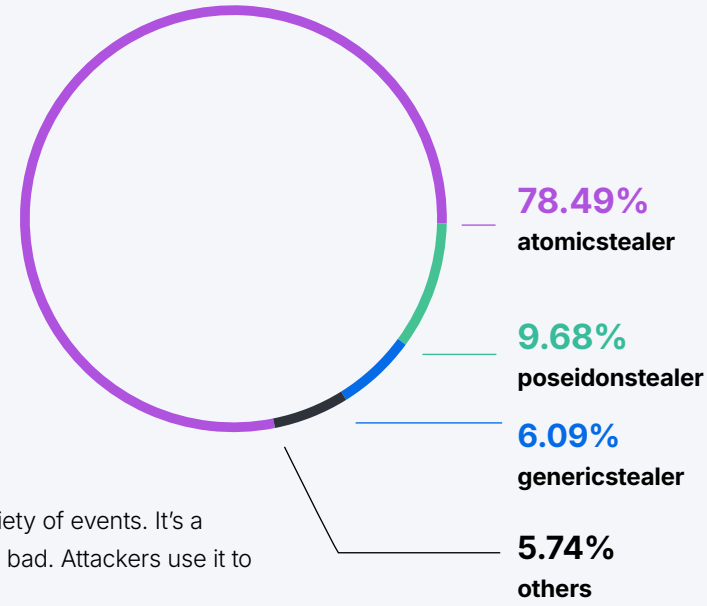
Others 25.1%

Infostealers

If you wanted to steal something (please don't), the faster you can get in and out, the less likely you'll be caught. Infostealers usually try to act quickly to steal your data soon after they've infected your device. Sometimes, they self-delete after the damage is done, while modern infostealers may establish persistence.

> *Infostealers have played a significant role in the rise of malware within the macOS ecosystem. AppleScript, while historically useful for power users, has also been widely abused in malware.*
>
> Jaron Bradley, Jamf

MOST COMMON INFOSTEALERS



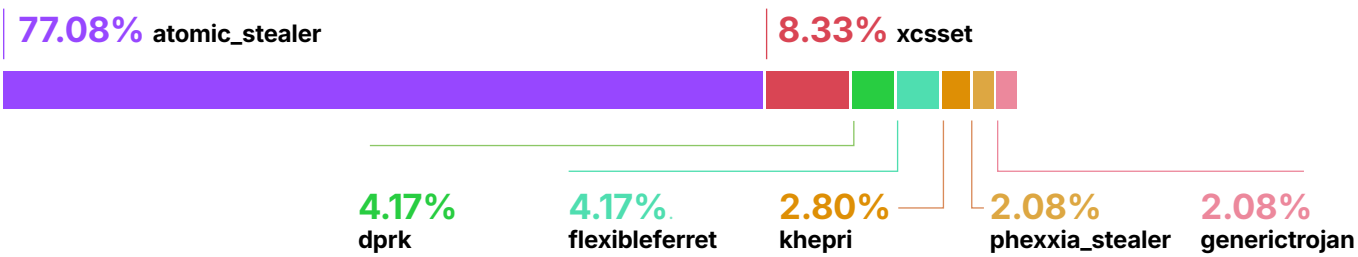
Developers and power users use AppleScript to automate a variety of events. It's a powerful tool, capable of endless possibilities — both good and bad. Attackers use it to deceive users to steal their information.

Infostealers became a lot more common after 2023, where they only made up a meager **0.25%** of attacks. In 2024 this increased immensely to **28.36%**, finally landing at **33.52% in 2025**. As popular as they are, more attacks consist of other types of malware, like trojans. Speaking of...

Trojans

Trojans soared in popularity in 2025, finally topping the charts at **50.3% of all malware attacks**. The most common trojan, **atomic_stealer**, was involved with **77.08% of attacks**. You likely noticed it's resemblence to 2025's dominant infostealer — this is no coincidence. Many stealers use trojans to establish backdoors that allow reentry.

ACTIVE TROJANS



Knowing your enemy is half the battle.

A lot of the malware we've talked about is well known. Your threat detection software will likely identify it. As we hinted at earlier, not all malware is identifiable by its code. Advanced detections that identify suspicious behavior is critical for finding threats yet to be analyzed by the cybersecurity community. Implementing advanced tools will go a long way in protecting your organization from zero-day attacks.

Configuration matters too. Malware often takes advantage of a user's behavior, like if they perform a risky download or fall for a social engineering attack. Security policies and user training help.

Detection is crucial; prevention starts with the software itself. Cyber attacks rely on software vulnerabilities — flaws in both app and operating system designs that leave room for exploit. Enforcing updates to your devices and apps is your best shot at closing these vulnerabilities and keeping attackers out. We'll talk more about this in the next section.

Thoughts from our CISO

As Apple devices continue to expand across the enterprise, the selected security solutions should be built specifically for the Apple ecosystem, not adapted from a Windows-first approach. Organizations should prioritize security products architected from the ground up for macOS, ensuring that threat detection, compliance enforcement and response capabilities are fully aligned with how Apple platforms operate, not treated as an afterthought.

App and OS vulnerabilities

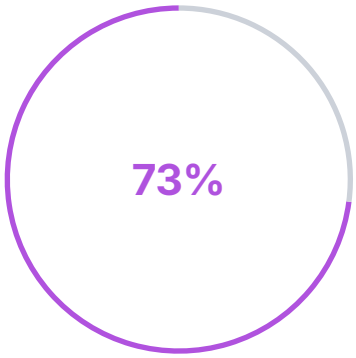
The operating system is a device's foundation. It powers the tools, services, applications and security of your device. Attackers are constantly searching for cracks in its armor to infiltrate its defenses.

Vulnerabilities add up. Even less severe vulnerabilities can become a crucial step in an attack, and sometimes patching these vulnerabilities gets deprioritized.

Speaking of patching — it's a big deal. Unfortunately, even the most secure operating systems are vulnerable somewhere. It's inevitable, but not incurable. Apple constantly puts out software updates to address vulnerabilities. To remain protected, your organization needs to enforce these updates. But this doesn't always happen.

Apps matter too. Each introduces their own sets of vulnerabilities, data handling policies, development libraries and more.

of **organizations** had at least **one device** with a **critically out-of-date OS**



of **devices** contain at least one **vulnerable app**

What is a CVE?

The Common Vulnerabilities and Exposures (CVE) program acts as a database of vulnerabilities discovered by the cybersecurity community. Each CVE listing identifies the affected software or library, lists a severity score and offers potential methods of exploitation

Out-of-date software is extremely common. Users aren't always keen on updates, especially if they perceive disruption to their workflows. But enforcing update deadlines and minimum OS versions go a long way to protecting your device fleet and data — like from exploits that leverage these vulnerabilities.

Noteworthy macOS vulnerabilities, 2025

CVE-2025-46287 | Severity: 9.8 (critical)	CVE-2025-43539 | Severity: 8.8 (high)	CVE-2025-46285 | Severity: 7.8 (high)
DESCRIPTION:		
An attacker may be able to spoof their FaceTime caller ID.	Processing a file may lead to memory corruption.	An app may be able to gain root privileges.
AFFECTED COMPONENT		
Calling framework	AppleJPEG	Kernel
IMPACT:		
By displaying misleading info, the attacker can trick the user into performing the wrong action.	An attacker can modify data to execute unauthorized code.	An attacker can execute arbitrary code.
PATCHED OS:		
macOS Tahoe 26.2, Sequoia 15.73 and Sonoma 14.8.3	macOS Tahoe 26.2, Sequoia 15.73 and Sonoma 14.8.3	macOS Tahoe 26.2, Sequoia 15.73 and Sonoma 14.8.3

Vulnerabilities discovered by Jamf

CVE-2025-43296 | Oct 2025
System Settings Gatekeeper bypass, patched in macOS Tahoe 26.

CVE-2025-43348 | Nov 2025
Finder Gatekeeper bypass, patched in macOS Tahoe 26.1.

Additional vulnerabilities that we confirmed were exploited in 2025 are shown in the following table.

CVE ID	COMPONENT	IMPACT
CVE-2025-24113 CVSS score: 4.3 | Severity: medium	Safari	Visiting a malicious website may lead to user interface spoofing.
CVE-2025-46289 CVSS score: 5.5 | Severity: medium	AppSandbox	An app may be able to access protected user data.
CVE-2025-43482 CVSS score: 5.5 | Severity: medium	Audio	An app may be able to cause a denial of service.
CVE-2025-43517 CVSS score: 3.3 | Severity: low	Call history	An app may be able to access protected user data, due to a logging issue.
CVE-2025-43542 CVSS score: 7.5 | Severity: high	FaceTime	Password fields may be unintentionally revealed when remotely controlling a device over FaceTime.
CVE-2025-43532 CVSS score: 2.8 | Severity: low	Foundation	Processing malicious data may lead to unexpected app termination due to memory corruption.
CVE-2025-43512 CVSS score: 7.8 | Severity: high	Kernel	An app may be able to elevate privileges.

Managing vulnerabilities is a continuous battle — but not a losing one.

To stay on top of software vulnerabilities, you need a good strategy. At its most simple, you must continuously identity, mitigate and monitor for vulnerabilities that affect your systems and devices.

Depending on the size and abilities of your IT and Security teams, you may or not be able to hunt for threats yourselves. Thankfully, the cybersecurity community has your back. Threat researchers and software vendors are constantly on the prowl for the latest exploits, adding potential vulnerabilities to databases to help organizations understand where they're vulnerable. Your teams can reference them to get a sense of your current security posture and respond accordingly. Security tools are available to make this process easier.

The exact tools your organization needs will differ depending on your size, capabilities, industry and more. But in general, you'll need a way to:

- **Configure devices and enforce policies**
- **Manage user accounts and identities**
- **Keep devices and software up to date**
- **Monitor device health**
- **Enforce access policies**

Mobile device management, endpoint protection, identity management and telemetry tools help with these tasks, so you can stay in front of threats as they come.

Thoughts from our CISO

A robust security strategy is built on the core tenets of visibility, telemetry, and automation and nowhere is this more critical than in vulnerability management. **Security teams** should:

Understand their vulnerabilities

Visibility into vulnerabilities across the organization is the critical first step. Gaining comprehensive insight into what vulnerabilities exist on end-user devices and infrastructure provides the foundation for a data-driven security posture. From there, teams can analyze application footprint, assess potential risk and determine impact radius, enabling security teams to prioritize vulnerabilities based on evidence rather than assumption.

Implement a risk-based approach to device access

When non-compliant devices attempt to access corporate resources, access should be restricted until the device is brought back into compliance, with remediation processes designed to be as seamless and low-friction as possible for the end user.

Introduce a solid patching program

To bring back the MDM point, having a tool to ensure compliance with the latest or supported N-X versions of software or OS is paramount to keeping a healthy and safe environment. Doing this with little to no impact to end users just makes it easier to partner and enable the business with.

Read the latest research for macOS from Jamf Threat Labs

OpenClaw: the helpful AI that could quietly become your biggest insider threat

FEBRUARY 2026

OpenClaw is an open-source framework for building autonomous AI agents that can execute shell commands, access files and interact with applications without built-in security boundaries, creating significant enterprise security risks. The framework becomes dangerous through unrestricted system access, data exfiltration potential and vulnerability to indirect prompt injection attacks where malicious instructions are embedded in legitimate business content. Recent security advisories have demonstrated how attackers can exploit various flaws to gain persistent access, making OpenClaw deployments a high-risk insider threat that requires comprehensive detection, prevention and governance strategies to manage safely in enterprise environments.

Threat actors expand abuse of Microsoft Visual Studio Code

JANUARY 2026

DPRK-linked threat actors have evolved the Contagious Interview campaign to abuse Visual Studio Code task configuration files, delivering a JavaScript backdoor when victims open malicious Git repositories. The backdoor establishes persistent command-and-control communication, collects system information and enables remote code execution. This technique exploits developer trust workflows — when users mark a repository as trusted, malicious configuration files automatically execute hidden commands, demonstrating how threat actors continue adapting their tactics to integrate with legitimate development tools.

From ClickFix to code signed: the quiet shift of MacSync Stealer malware

DECEMBER 2025

MacSync Stealer has evolved beyond drag-to-terminal techniques, now deploying through a code-signed and notarized Swift application that silently retrieves and executes payloads without requiring Terminal interaction. Distributed via fake installers, this variant uses a sophisticated dropper that performs connectivity checks, enforces rate limiting, validates payloads and removes quarantine attributes before execution. This shift toward signed and notarized delivery reflects a broader trend where attackers disguise malicious code as legitimate applications to evade detection and bypass macOS security controls.

FlexibleFerret malware continues to strike

NOVEMBER 2025

FlexibleFerret, a DPRK-aligned malware family, targets macOS users through sophisticated fake recruitment campaigns that trick victims into executing malicious Terminal commands disguised as hiring assessments. The multi-stage attack uses JavaScript on fake job sites to deploy a backdoor with extensive capabilities including file exfiltration and command execution, while harvesting credentials through fake Chrome prompts that send data to attacker-controlled Dropbox accounts. This evolving threat bypasses Gatekeeper by convincing users to manually execute commands, making user awareness of unsolicited “interview” assessments and Terminal-based instructions critical for defense.

DigitStealer: a JXA-based infostealer that leaves little footprint

NOVEMBER 2025

DigitStealer is a sophisticated macOS infostealer that remained completely undetected on VirusTotal while employing advanced anti-analysis techniques, including hardware feature detection that restricts execution to Apple Silicon M2 chips or newer. The malware deploys four memory-resident payloads that steal browser data, cryptocurrency wallets, and credentials, trojanizes Ledger Live by merging three separate components to evade detection and establishes persistence through a dynamic backdoor. Its use of legitimate Cloudflare services for payload hosting and multi-stage obfuscation demonstrates a deep understanding of macOS internals, making behavioral detection critical since most execution happens entirely in memory.

ChillyHell: a deep dive into a modular macOS backdoor

September 2025

ChillyHell is a sophisticated macOS backdoor that remained notarized and undetected since 2021, originally linked to attacks targeting Ukrainian government officials. This modular C++ malware establishes multiple persistence mechanisms, communicates via DNS and HTTP, and deploys capabilities including reverse shells, self-updating, payload delivery and password brute-forcing. Its advanced evasion techniques demonstrate that signed and notarized apps aren't always safe.

Signed and stealing: uncovering new insights on Odyssey infostealer

July 2025

A sophisticated macOS infostealer successfully obtained Apple code-signing and notarization, allowing it to bypass built-in security controls while deploying a persistent backdoor and replacing legitimate cryptocurrency apps with trojanized versions. The malware uses a deceptive SwiftUI interface to harvest passwords, dynamically downloads obfuscated payloads and establishes continuous command-and-control for remote code execution. Most concerning: it actively fingerprints analysis environments and blacklists research systems to avoid detection, demonstrating nation-state-level sophistication.

A python in disguise: unpacking PyInstaller malware on macOS

May 2025

Attackers are using PyInstaller to disguise malicious Python code as native macOS executables — the first time this technique has been observed for macOS infostealers. The malware runs without requiring Python to be installed, stealing credentials through fake password prompts, harvesting Keychain data and collecting cryptocurrency wallets while using multiple obfuscation layers to evade detection. This technique represents a significant evolution in macOS malware distribution, allowing attackers to deploy sophisticated infostealers while potentially bypassing traditional security mechanisms.

jamf

Contact us to learn more about the mac threat landscape.