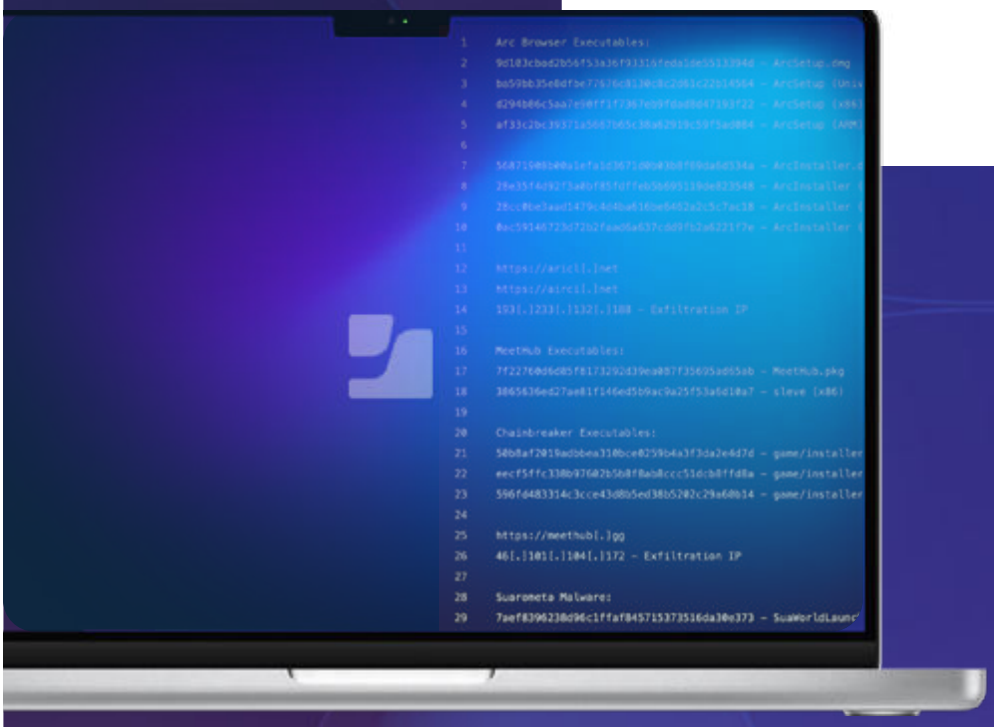
jamf

Security 360:
Annual Trends Report
Mac



Foreword

At Jamf, we love Mac. It is the first machine we developed software for, and it remains the machine so many of us are passionate about. (We are an **official contributor to the macOS Security Compliance Project.**) Throughout our history, we have seen Mac become a **bigger part of the work environment.** What started as a machine for creatives and executives is becoming more ingrained into the daily operations for engineers and more. But with its continued integration at work, it becomes a larger attack surface for threat actors.

The threat landscape for Mac is more diverse than ever, with more creative ways to compromise Mac. In our mission to 'help organizations succeed with Apple', we take a deeper look into the threat landscape affecting Mac devices to serve our customers and the Apple community at large.

– Jaron Bradley,
Director, Jamf Threat Labs

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 landscape to put a spotlight on the risks that organizations face.

We provide an assessment of the different attack vectors (like malware, vulnerabilities and social engineering) that are actively utilized to trick users, compromise devices and infiltrate organizations. The analysis includes topics like device vulnerabilities, web threats, malware and more.

In addition to analyzing these threat trends, the report includes a perspective from Jamf's CISO to provide the insights security leaders think about when protecting their Mac across the user, device, application and network levels.

Research methodology

To understand and quantify the real-world impact of the security trends identified in this report, we examined a sample group consisting of 1.4 million devices protected by Jamf. Our analysis was carried out in the first quarter of 2025, revisiting the prior 12-month period and spanning globally across 90 countries.

To preserve privacy and maintain the utmost security 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.

Purpose of the research

Our intention with this analysis is to enable organizations and users to understand the evolving cybersecurity trends that currently exist, as well as show how organizations and users can take steps to mitigate risks. It also provides overviews of the most impactful research by Jamf Threat Labs, including malware and vulnerability discoveries.

There are several actions anyone can take to improve their Mac security. For example, only download software from sources you trust. But there are other best practices any organization can implement:

- Continuous and timely operating system updates
- User education and training
- Application vetting
- Multi-factor authentication
- Zero-trust security frameworks
- Acceptable use policies for corporate data
- Implementing Apple-best workflows across use cases

While some of these are table stakes for all organizations, there are other device security requirements that are organization-specific. For example, organizations in a regulated industry might need to comply with industry benchmarks or frameworks (like CIS Benchmarks or HIPAA).

This year, we structure our analysis into three categories of risk we found are the highest priority for organizations around the globe:

I. Application Risk and Malware

II. Vulnerability Management

III. Social Engineering

We also have a Security 360 report focused on **mobile devices** which you can find **here**.

Much of the analysis in this report is informed by Jamf's Threat Intelligence, a broad collection of insights that are derived from original threat research, real-world usage metrics, along with news analysis and data feeds. Jamf's Threat Intelligence is made up of human-led research from the Jamf Threat Labs and Data Science teams who monitor devices, app and network traffic for risk, threats and zero-day vulnerabilities.

Key trends for Mac in the enterprise

Malware Introduces Risk – Even in Secure Platforms

Apple designs its **platforms with security at the core**. It's not just the platforms themselves, but how Apple communicates security to its users. For example, the **Apple Platform Security site** includes a page that informs Apple users on protection against malware in macOS. Apple's different technologies (like App Store, XProtect or Gatekeeper) layers protection against malicious apps at different parts of an app's lifecycle.

For Mac devices at work, security is a balancing act of providing users with the apps they need to do their best work, but to prevent access to apps that can introduce risk. Mac apps come in all shapes and sizes, like native Mac Apps, web apps, and hybrid apps, created and designed by developers for a variety of use cases. However, **many of the most common business apps for Mac** today do not come from the Mac App Store, but rather, are packaged directly from the developer. On top of that, users can download apps from any site they have access to.

A Single Vulnerability Can Help Attackers Gain Systemwide Access

It's a fact: vulnerabilities occur in the software (both OS and applications) we use daily.

The National Institute of Standards and Technology states, "In the case of typical software, errors and vulnerabilities exist at an estimated frequency of ~25 errors per 1000 lines of code." Common vulnerabilities and exposures (CVE), published in the National Vulnerability Database (NVD), provides the public with:

- An understanding of CVEs
- The product or vendor impacted
- A description of threats

Between the time a vulnerability is discovered and is patched, damage can be done. When a patch is made available, it still needs to be installed on the affected devices. Security tools that provide insights such as which vulnerabilities are present and most critical help IT and InfoSec teams prioritize the most urgent patches and improve their processes.

Social Engineering Continues to Compromise Users

Social engineering, like phishing, continues to be one of the most prevalent attack techniques from threat actors and its influence in the threat landscape is as active as ever. In September 2024, **Apple released a blog post** with guidance to its users to help "avoid scams and learn what to do if you receive suspicious emails, phone calls, or other messages". Attackers are getting more creative in their techniques, posing as recruiters, family members, trusted brands and more. No matter how secure a platform or operating system, social engineering techniques are designed to infiltrate business data starting with the least secure part of the device – the user.

Part 1: Mac focused malware

With this report, we want to provide an understanding of Mac malware, including the types we have seen, how they are each impacting organizations, and at what frequency. As Mac use is expanded in the workplace, and more critical applications are accessed through the platform, users across the organization will be targeted.

Apple's malware defense is structured into three layers:

1. **Prevent launch or execution of malware**
2. **Block malware from running on customer systems**
3. **Remediate malware that has executed**

Apple's technologies – App Store, GateKeeper, XProtect and Notarization – provide users with native ways to mitigate threats. For example, XProtect is a built-in antivirus. And when malware is discovered, Apple can respond in several ways, like revoking a Developer ID.

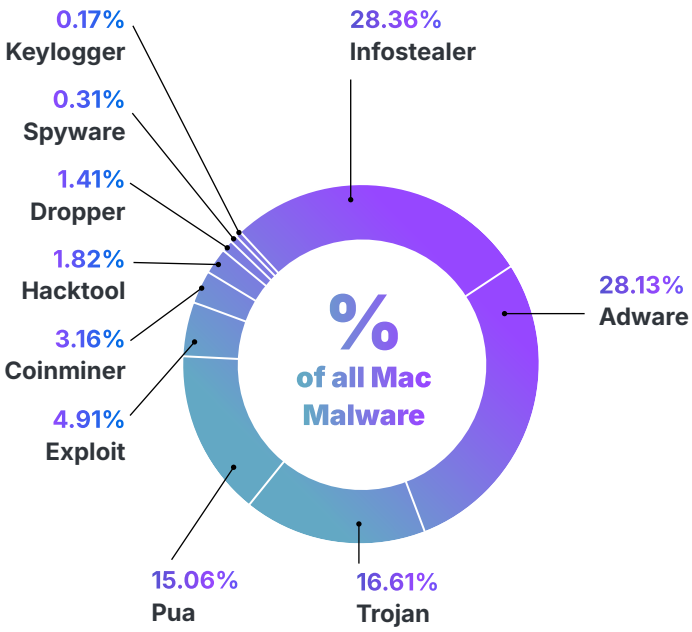
macOS – despite its strong, built-in system security mechanisms – is not immune to malware. **In March of this year**, the Jamf Threat Labs and Data Science teams collaborated on an article to discuss the Mac malware myth, understanding novel malware with known malware and show macOS malware vectors with Titan – a 3D visualization tool developed by Jamf Threat Labs. Titan helps provide context and identify related malware samples. The malware families uncovered shows "the ever-growing numbers of new, bespoke malware" for macOS. What does this mean? Mac malware exists, there are related families of malware and it is increasingly being used by threat actors.

This year, Jamf Threat Labs discovered malware, believed to be linked to the Democratic People's Republic of Korea (DPRK), **embedded in a Flutter-based application**. While using applications developed with Flutter for cross-platform support isn't uncommon, what makes this attack noteworthy is that it's the first time the Jamf Threat Labs team has seen this framework used to target macOS devices. The team breaks down the malware, its variants in Python and Golang and why the "malware is likely testing for greater weaponization". Also noted, is the unintentional obscurity that Flutter applies to code written by users of its framework.

Mac malware families

Below is a full breakdown of new Mac malware instances studied in 2024, based on our findings:

What is this data telling us? If we compare this with last year's report of malware, we see some consistencies: adware, trojans, PUA (potentially unwanted applications) and exploit (applications known to be abusing an exploit) remain near the top of the list of malware categories. (Last year, trojans had the greatest number of families at 17%, slightly down this year at 16.6%.) The top spot this year goes to infostealers. In fact, infostealers saw a 28.08% increase of the overall malware studied.



The presence of infostealers remains consistent with the research Jamf Threat Labs has done over the past year, with macOS environments being under constant attack by this malware type. What is interesting about these tactics is not only do both attackers use infostealers to gain access to the data they want, but they also employ another strategy mentioned earlier in this report: social engineering. What this shows us is that threat actors are using a combination of attack principles to trick their victims. For employees or organizations in high-profile industries – like crypto – it's important to remain vigilant, from both a training and security tool standpoint. Attacks are not just stumbled upon but engineered.

Investigating using PyInstallers to deploy infostealers on macOS

In April 2025, Jamf Threat Labs uncovered new undetected macOS infostealer samples that bundle Python code into Mach-O executables using PyInstaller. (Jamf Threat Labs discovered three undetected stealers on VirusTotal.)

PyInstaller is a legitimate, open-source tool that allows developers to package Python scripts into standalone binaries. Attackers are now leveraging the same technique to deliver malicious payloads that execute smoothly on macOS. The team reviewed several key functions to confirm the true nature of the malware – an infostealer. Several key functions include:

- Attempts to harvest user credentials by triggering deceptive password prompts
- Executes arbitrary applescript payloads from attacker server
- Extracts saved credentials and sensitive information directly from the macos keychain
- Scans the filesystem for known cryptocurrency wallets to exfiltrate private keys and steal crypto assets

As infostealers continue to become more prevalent in the macOS threat landscape, threat actors will continue the search for new ways to distribute them. However, there are actionable steps organizations can take to protect themselves against malware described above. For example:

- Restrict software execution to apps signed by Apple and identified developers.
- Brand osascript prompts used for legitimate IT processes and train staff to confirm branding before entering their credentials.

Malware to look out for

Poolrat

Poolrat, a macOS backdoor infamous for its involvement in the 3CX supply chain compromise, allows attackers to collect crucial system data and execute commands concurrently with file operations. A leaner version of Poolrat, dubbed Pondrat, has recently been discovered.

Pondrat

Pondrat, a backdoor that exhibits similarities to both AppleJeus and Poolrat, was distributed through malicious PyPi packages. Upon installation, Pondrat establishes connections to command-and-control servers (C2) to facilitate file uploads and downloads, pause operations for a predetermined duration, and execute arbitrary commands.

NotLockBit

Golang-based ransomware that masquerades as a variant of the infamous LockBit ransomware. Since its initial sample, the Ransomware uses an embedded public key to enumerate and encrypt a list of hard-coded extensions. The most recent variants of NotLockBit will exfiltrate data to an attacker-controlled S3 bucket and use osascript to change the Desktop wallpaper(LockBit 2.0). NotLockBit is believed to be under active development.

ThiefBucket

Thiefbucket, a malware family linked to North Koreas Lazarus Group, targets victims through sophisticated social engineering campaigns. It has been observed as a second-stage payload, delivered through a disguised coding challenge. The backdoor demonstrates several capabilities, most notably its automated infostealer functionality. Among the other capabilities are the following: - Persistence mechanisms - Process termination - File deletion - Downloading/Uploading files - Self-deletion - Running shell commands - Quick file search via Spotlight - Communication with command-and-control servers

HZRat

HZ Rat, a macOS backdoor, initially targeted Windows users but has since evolved to target macOS users through disguised legitimate software installers. Once installed, HZ Rat establishes connections to command-and-control servers (C2) to enable attackers to execute commands, steal files, and extract sensitive information such as usernames, emails, phone numbers, and other personal details from WeChat and DingTalk.

BansheeStealer

Advertised on Telegram, Banshee Stealer operates as a Malware-as-a-Service with a web interface for attackers. Specializing in info-stealing, it can exfiltrate a range of sensitive data, such as account passwords, browser data, session cookies, and cryptocurrency wallets. Like other infostealers, Banshee abuses AppleScript dialog functions to deceive users into providing their credentials. Once the users password is entered, it pilfers additional sensitive data from the macOS keychain. Banshee employs various evasion techniques, including anti-VM and anti-debugging measures to thwart analysis, as well as detecting Russian language systems.

InvisibleFerret

InvisibleFerret is a Python-based trojan that has been used by malware embedded within disguised applications. Most notably, it has been seen dropped by the BeaverTail InfoStealer (attributedby some to the DPRK) as a stage two implant. The malicious Python script is cross-platform and allows an attacker to perform reconnaissance, data exfiltration, copying of the clipboard, and execution of remote commands. It is also capable of installing the AnyDesk software if additional remote control is desired.

BeaverTail

BeaverTail is an InfoStealer that has been seen disguised as a legitimate application before being sent to victims via social engineering campaigns. Similar to other InfoStealers, it takes valuable details from the victims keychain, browser cookies, crypto-wallets, etc. and uploads them to an attacker-controlled server. It is also capable of executing additional remote payloads on the victim system, such as the InvisibleFerret backdoor. It has been attributed by some to the DPRK.

PoseidonStealer

Advertised on Telegram, Poseidon Stealer (a competitor to Atomic Stealer) operates as a Malware-as-a-Service with a web interface for attackers. Specializing in info-stealing, it can exfiltrate a range of sensitive data, such as account passwords, browser data, session cookies, and cryptocurrency wallets. Like Atomic, Poseidon abuses AppleScript dialog functions to deceive users into providing their credentials. Once the users password is entered, it pilfers additional sensitive data from the macOS keychain. Distributed under the guise of legitimate applications, the malware has been observed being promoted via malvertising on Google Ads.

Kuiper

Kuiper is a Ransomware-as-a-Service (RaaS) developed in Go, which was advertised on underground forums by a user named Robinhood. It uses a combination of RSA, ChaCha20 (filessmaller than 600 megabytes), and AES (files larger than 600 megabytes) for encrypting files. While most of the malwares functionality is focused on Windows, the macOS variant will generate a random key and random initialization vector (IV)using `/dev/urandom`, decode a ransom note, encrypt the target recursively (appending a `.kuiper` extension), clean the key and IV from memory, and reboot the system.

Observed Mac Malware

For a more granular look at Mac malware observed across customer environments, our findings indicate that the following malware families ranked in the top 10:

Family Name	Category	Percentage
Genieo	Adware	13.63
Imobie	PUA	10.96
Multiverze	Adware	9.44
Mackeeper	PUA	7.19
Tnt	PUA	6.07
Jailbreak	PUA	5.74
Ccleanmac	Adware	4.33
Puagent	Trojan	3.07
Macinformer	PUA	2.33
Pirrit	Adware	2.33

These numbers show that although many types of malware, such as infostealers, are greatly increasing in quantity, adware and potentially unwanted applications (PUA) continue to be the most frequently downloaded and installed applications by users. A common trend seen across all OS platforms given the broad reach of adware and the more targeted nature of infostealers.

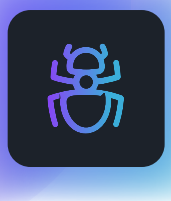
Jamf Threat Labs published a blog about **infostealers targeting individuals in the crypto industry**. The attackers goal? Harvesting credentials with data from various crypto wallets. The team tracked two attacks that dropped infostealers into the victim's systems:

1. Through sponsored Google Ads: Searching for "Arc Browser" brought users to a malicious site when clicking on a Google Ad.
2. Through virtual meetings: When reaching out to discuss an opportunity (like a job interview), attackers request the use of Meethub to schedule a meeting.

In both instances, users were prompted to download the application by bypassing Gatekeeper and for the user to input their macOS login password.

The malware families we studied and the examples we provide show the need for core security principles, such as:

- Getting applications from legitimate sources
- Applying a vetting process (either through trusted third parties like the mac app store or sourced from a device management vendor)
- Running up-to-date security software



A CISO's Perspective

- **Introduce a purpose built, Mac focused EDR solution:** We often see software take a Windows first approach and treat Apple devices as an afterthought in the enterprise. That day has long passed, especially regarding security. We have to focus on security products that are developed for Apple products from the ground up as the threat landscape matures.
- **Implement a robust MDM solution:** Management of devices is crucial to securing them. Given the amount of freedom users have and access they may possess, having a robust framework to manage devices and users on those devices is paramount to stopping potential malware outbreaks before they start.
- **Ensure strong communication strategies:** From collaboration between Security and IT, Security brand outreach, training programs, end-user awareness to executive memos. Effective communication of your security program, the tools you're using and your current strategies help everyone align and focus on a common goal.

Vulnerability management

Not all vulnerabilities are created equal. They vary on severity level and most have a score assigned to them. **Apple** provides a list of patched security vulnerabilities affecting macOS and the operating system that fixes the vulnerability. For example, in 2024, Apple released macOS 15.1.1 in response to **CVE-2024-44308** and **CVE-2024-44309** – in which maliciously crafted web content may be able to break out of Web Content sandbox. This CVE had a high severity score. But Apple also releases security updates for CVEs with low scores. What does this mean? Prioritizing matters. When IT and security teams can take a complete view of the vulnerabilities in their device footprint, inclusive of systems and applications, then they are able to properly address what is most pressing.

Apple has a more specialized version of security updates called Rapid Security Responses, which delivers **important security improvements** between software updates. Why are these patches beneficial? They are lightweight updates – meaning organizations can automatically apply updates without breaking internal systems. For example, between June 2024 – April 2025, Apple documented **20 security updates** with CVEs associated with major and minor versions of macOS.

An in-depth look at a real-world vulnerability Bypassing Transparency, Consent and Control (TCC)

Across Apple's operating systems , Transparency, Consent and Control (TCC) serves as a crucial security framework, prompting users to grant or deny requests from individual apps to access sensitive data such as microphone, webcam, and full disk access. A TCC bypass vulnerability occurs when this control fails, allowing an application to access private information without the user's consent or knowledge. This means attackers can get unauthorized access to files and folders, Health data, the microphone or camera, and more without alerting users

Jamf Threat Labs uncovered **CVE-2024-44131, a TCC bypass vulnerability** affecting File Provider on Mac devices. Apple quickly responded to this discovery with a patch in macOS 15. CVEs, like CVE-2024-4413, amplifying the need for organizations to have tools that can detect and block unexpected behaviors. Being proactive in monitoring app behavior and preventing unauthorized data access helps organizations stay a step ahead before vulnerabilities can be addressed.

Let's take a deeper look at some noteworthy vulnerabilities from recent (this report was written in April, 2025) Apple releases:

Apple CVE Fix	Date	Vulnerability Scoring	Impact
macOS Sequoia 15.4.1	April, 2025	CVE-2025-31200 CVSS – Score: 7.5 | Severity: High	CoreAudio
macOS Sequoia 15.4	March, 2025	CVE-2025-24234 CVSS – Score: 7.8 | Severity: High	AccountPolicy
macOS Sequoia 15.4	March, 2025	CVE-2025-24180 CVSS – Score: 8.1 | Severity: High	Authentication Services
macOS Sequoia 15.3	January, 2025	CVE-2025-24085 CVSS – Score: 7.8 | Severity: High	CoreMedia

As stated earlier, when building software, vulnerabilities (about 25 errors per 1000 lines of code) will occur. What is important for security professionals is being able to view and take action on those vulnerabilities to keep data safe. Keeping operating systems up to date is not always possible (for example, to test applications/agents), but organizations need to stay aware and protected.

It is more than just vulnerabilities in an operating system. Late November 2024, the Cybersecurity Agency published **a report on the top routinely exploited vulnerabilities in 2023**. (This is the latest version of the report.) The report digs deeper into the top 15 vulnerabilities – including the CVE and what each vulnerability allows threat actors to do. The vulnerabilities occur in operating systems across computing platforms and applications organization's employees and students use daily. As the report mentions, "Malicious cyber actors exploited more zero-day vulnerabilities to compromise enterprise networks in 2023 compared to 2022, allowing them to conduct operations against high priority targets." The Cybersecurity Agency goes on to provide what developers and end-user organizations can do to mitigate vulnerabilities. For end-user organizations, the report mentions:

- Update software, OS, apps, and firmware in a timely manner
- Routinely perform automated asset discovery
- Implement a robust patch management process
- Document secure baseline configurations
- Perform regular secure system backups
- Maintain an updated cybersecurity incident response plan

As shown above, Apple routinely provides updates to OSes with known vulnerabilities. We keep mentioning it, but updating software is key. The most common way for organizations to update the OS (and the business apps their employees use daily) is via a mobile device management solution. However, there are other layers to cyber defense. Incident response plans, collecting and analyzing telemetry, or internal patching processes are all examples of how organizations can stay a step ahead. Performing the above also unlocks additional cyber defense layers, such as identifying software vulnerability levels or uncovering risks that may lay dormant within endpoints through threat hunting workflows – all of which work together to help organizations mitigate risk.

Jamf Threat Labs discovered a Gatekeeper vulnerability in macOS, assigned CVE-2023-41067. This vulnerability affected Launch Services that may lead to the execution of an unsigned and unnotarized application without displaying appropriate security prompts to the user. Gatekeeper is the first line of defense to ensure applications downloaded from the internet are blocked if they are not signed with a valid developer ID. While this CVE was swiftly patched by Apple, it shows that vulnerabilities can occur in any system. Having the right controls and training helps mitigate risks caused by vulnerabilities like the one Jamf Threat Labs found in Gatekeeper.

Over the last twelve months, we found that:

32%

of organizations operate at least one device with critical (and patchable) vulnerabilities

A CISO's Perspective

- **Ensure visibility into the vulnerabilities across your organization:**
  Gaining as much insight into what vulnerabilities are present on your end user devices, or infrastructure, is a great starting point. You can start with that data to analyze specific app footprint, potential risks, impact radius, etc. This is a great way to start prioritizing your vulnerabilities in a data-driven way.
- **Introduce a solid patching program:**
  To bring back the MDM point, having a tool that ensures you keep up 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.
- **Implement a risk-based entry approach:**
  If you have non-compliant devices attempting to access company resources, you should restrict that access until the end user can correct the situation and bring that device back to compliance with as little effort as possible.

Part 3: Social engineering

Social engineering is the practice where attackers manipulate and trick individuals into providing sensitive data or access credentials. According to the World Economic Forum's **Global Cybersecurity Outlook 2025 report**, "42% of organizations experienced a successful social engineering attack in the past year."

Phishing – a type of social engineering – is one of the most common and damaging threats facing organizations today. While phishing is more prevalent on mobile devices (because of their small screen size, portability and use in locations away from the office), Mac (and all desktops or PCs), are an attractive attack target for threat actors.

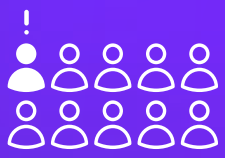
Afterall, Mac are still used by the most vulnerable link in the cybersecurity chain – the user.

As attacks get more creative and realistic, our personal and work information is constantly at risk. With Mac devices becoming more common at work, the attack surface continues to expand. Attackers are employing more sophisticated tactics, using realistic interfaces, user experiences and authentic communication styles to lure unsuspecting victims into their trap. But there are safeguards (e.g., continuous employee training and threat prevention tools) organizations can employ to protect their users and data.

Over the past twelve months, we found that:

25%

of organizations were impacted by a social engineering attack



1 in 10

users clicked on a malicious phishing link

Jamf Threat Labs published an article about **the FBI's ongoing research into DPRK** obtaining financial gains through illicit means, specifically in the crypto industry. The team notes a specific attack "in which a user was contacted on LinkedIn by an individual claiming to be a recruiter on the HR team at a tech company." The attackers send the user a zipped coding challenge (a common step in a modern-day development role) to understand their skills. Once a user clicks, the malware (in this case, an infostealer) starts. Training employees in social media use and downloading software remains an important topic for all organizations to practice.

Top 20 brands used in phishing campaigns

In our research, we found that certain high profile brands are frequently leveraged in phishing attacks, perhaps due to their recognizable and trusted names. We broke these brands into four categories:

1. Entertainment	2. Business	3. Utilities	4. Personal
	Outlook	United States Postal Service	Amazon.com Inc
Netflix	Office365	Gazprom	Telegram
Bet365	Allegro	AT&T Inc	Facebook, Inc
Steam	InterActive Corp	Orange S.A.	Chase
	Tencent	DHL	WhatsApp
		BT Group	Yahoo, Inc.

The differing reasons for Mac use – applying to jobs, downloading an app or by working in a specific industry like Crypto – have threat actors exploiting these common, often needed, use-cases to gain access to data. In the table above, we show the top twenty sites that were used in phishing attacks, based on those four categories.

These brands, because of their popularity, prestige, and impact on businesses and individuals alike, are used by nefarious actors attempting to compromise users in social engineering attacks. They are unwitting players in an increasingly sophisticated game. It is also worth noting that this list is not comprehensive of all brands used by threat actors. These are the top 20 brands for the past year, but it can change next year, month or week, but it does shed light on how attackers think. They are using the trust brands have developed with their customer base over years to exploit users. With the increase in hybrid and remote work, attackers are trying new ways to get someone to click.

In the modern world, our personal information is constantly at risk. With Mac becoming more common at work, the attack surface continues to expand. Attackers are employing more sophisticated tactics, using realistic interfaces, user experiences and authentic communication styles to lure unsuspecting victims into their trap. But there are safeguards (e.g., continuous employee training and threat prevention tools) organizations can employ to protect their users and data.

Jamf identified approximately **10 million phishing attacks** over the 12-month period that impacted our sample group of **1.4 million devices**. Additionally, we found that **1.5 – 2%** of these attacks were regularly being classified as zero day, meaning the attckers are launching new domains to host phishing attacks that have not yet been detected or identitied as malicious in comon databases. Identifying and verifying zero-day phishing attacks helps organizations protect users from falling victim to brand new and undetected phishing sites

A CISO's Perspective

- **Introduce a robust training program:**
  This has been integral to our success. We run sophisticated phishing campaigns, run gamified training, offer one off trainings for users that request it and allow users to report phishing emails while seamlessly receiving confirmation and feedback on their submissions all throughout the year. This is not just a once a year and "done" training for us.
- **Keep up with new trends and tactics:**
  This may seem obvious, but attackers will always capitalize on anything that they can and oftentimes that includes something new, groundbreaking or controversial in the news. You need to adapt your training and blocking tactics to address those situations. This may cause some unease amongst users, but transparency is key. The training is to prepare them for a potential bad actor that will not take their feelings into consideration when causing harm and will often actually look to garner an emotional response to confuse and outwit a victim.
- **Have a layered approach:**
  There is no one-stop-shop or tool to prevent you from becoming a victim of a targeted phishing campaign. Make sure you are covered from multiple angles. Block malicious domains. Ensure you have MFA in place. Adopt a zero-trust methodology. Have impossible velocity rules enabled, etc. One or two of those things may not be enough, but enforcing multiple layers of security ensures the most viable way to avoid becoming another victim of a phishing attack.

Key takeaways

Mac malware is advancing. But there are steps organizations can take to mitigate macOS malware risks. For example, collecting and analyzing telemetry helps identify and report on malware. Threat actors continue to look for novel ways to compromise users and systems. But with the right tools in place, organizations can reduce the impact of malicious software.

Establishing proper security hygiene mitigates risks. Regularly updating operating systems and disabling unnecessary controls (e.g., third-party app stores) helps organizations stay compliant with internal baselines and external frameworks. By establishing an enterprise app store and continually vetting applications (especially for private and custom apps), organizations can better monitor, remediate and patch vulnerable applications.

Social engineering is one of the most common ways for attackers to gain access to sensitive information. Over 90% of cyber attacks originate from phishing. Phishing comes in all shapes and sizes – not just email. It's important to implement protection across the entire device (browsers and apps) to keep users and organizations secure.

jamf

Contact us to learn more about the Mac threat landscape. Or contact your preferred reseller.