jamf

Security 360:

Annual Trends Report 2024

Summary

Jamf's annual security report takes a hard look at how the threat landscape is evolving by studying real-world customer data, cutting-edge threat research, and noteworthy industry events. We provide a thoughtful assessment of the diverse attack vectors that are actively utilized to compromise devices, trick users, infiltrate organizations and ultimately steal valuable business secrets and personal information. Our report concludes with a fresh perspective on industry best practices and actionable steps organizations of any size can take to improve their overall security posture.

Introduction

Security 360 offers a broad perspective on the evolving threat landscape; through real-world data, we analyze the most impactful attack vectors from the year, assess how organizations are aligning to security best practices, and explore the applications that are driving productivity and connecting workers in bold new ways.

We will structure our analysis around four categories of risk that organizations around the globe grapple to manage effectively:

I. Device risks

II. Application risks

III. Malware risks and attack evolution

IV. Web-based risks

In addition to these threat trends, Jamf also includes expert recommendations and guidance we've dubbed "back to basics," urging organizations to weave industry best practices into their device, application and infrastructure management processes.

Some examples of these best practices are the following:

- Use integrated management and security products to maximize the available policy controls while minimizing the number of agents you must maintain.
- Harden endpoints by following industry or regional best practice recommendations
- Manage threat exposure by maintaining up-to-date operating system (OS) and application releases and patches
- Implement multi-layered, defense-in-depth protections

Through this report, we will provide guidance to help organizations better defend against known threats while also reducing the exposed surface area that new attacks attempt to leverage. We will shine a light on the continued evolution of social engineering to provide insights on how to protect your users from these attacks that are more compelling than ever.

Finally, it's important to highlight that our research and advice is intended to apply to all devices working with business data – regardless of whether they're company-owned or BYO (bring your own) devices — Apple, Microsoft or Android — from threats that are targeting all platforms.

About the 360 report

We want to better understand the biggest security trends impacting the modern workplace.

This includes the pieces of the productivity puzzle – the devices, users and applications – that all must connect for work to get done. The information relating to key trends, the statistics found in this paper and how they all fit together is the result of our analysis of security trends within our customer base, as well as through the original research of the Jamf Threat Labs team on OS and application vulnerabilities and studies into the depths of malicious and proof of concept (PoC) attacks spread out over four distinct sections:

Research methodology

To understand and quantify the real-world impact of the security trends identified in this year's report, we examined a sample of 15 million desktop computers, tablets and smartphone devices protected by Jamf.

Our analysis was carried out in the fourth quarter of 2023, revisiting the prior 12-month period and spanning globally across 90 countries and multiple platforms – specifically, macOS, iOS/iPad, Android and Windows.

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.

Why it's critical

Our intention with this analysis is not to invoke fear but instead to educate organizations and users on the evolving cybersecurity trends that currently exist, as well as those that stand further to impact the security posture of devices and organizations alike. It also informs you of the best endpoint security options available and how to utilize safeguards to scale, keeping all aspects of device, user and organizational data secure.

Section I: Device risks

As work computing is modernized, a significant amount of complexity is introduced into the devices that employees utilize each day. This complexity includes embedded sensors to detect contextual information, co-processors that offload heavy compute cycles and deliver greater performance, and more connectivity from Bluetooth and NFC to WiFi and cellular. All of these additions are generally made with the best of intentions. Still, an often-overlooked side effect is that each component expands the surface area available for an attacker to exploit.

Modern devices are full of risks. And, fortunately for most organizations, these risks can be effectively managed with the right tooling and processes.

Maintaining an up-to-date operating system on each device is perhaps the single most impactful practice than an organization can implement, but not everyone is able to keep up with the pace of innovation.

Though there are many reasons to delay applying software updates from fear of conflicts to excessive agents that need to be tested for compatibility following each update, not applying OS updates means that work devices are likely running with known vulnerabilities that are waiting to be exploited.

These vulnerabilities affect more than desktops and laptops. We have found **40% of mobile users running a device with known vulnerabilities**. And as more critical line of business applications are run on mobile devices, these sensitive data repositories are increasingly subject to attacks that could be more effectively fended off with better practices.

In 2023, we found that

“8% of organizations had a mobile device accessing a third-party App Store.”

“40% of mobile users running a device with known vulnerabilities.”

In 2023, we found that “8% of organizations had a mobile device accessing a third-party App Store.” Vulnerabilities like these, though the intent behind accessing third-party app stores may be benign, are rife with applications that are often misleading to users with the express aim of tricking users into downloading and running suspicious apps that have their internal security broken to:

Run malicious code on devices
Features like Gatekeeper and the enterprise security API that should stop malicious code from running

Bypass internal security protections
Why you want to limit what's running on the device without proper vetting.

Gain access to unauthorized business data
Sensitive and confidential information is still one of the primary targets that drive threat actors.

Obtain privacy data without authorization
With evidence of Apple's Transparency, Consent and Controls, known as TCC, being circumvented by unauthorized code that's been installed, privacy protections are critical to endpoint security.

Spy on users without their knowledge or consent
Similar to the above point, threat actors are increasingly targeting mobile devices since these devices are always with us, using the connected nature of mobile to listen to conversations, intercept SMS and track physical movements through GPS.

Pivot attacks from the infected device to compromise networks
Occurring as the next steps following bad code being installed.

Configure for compliance

Compliance is often positioned as aligning to agency guidelines, like CIS Benchmarks or NIST standards, for governing data processing, usage and storage. But organizations have their own needs and approaches. Compliance here refers to all manner of ensuring that device configurations, data security and user workflows are standardized to align with any form of system in place to keep them safe from threat actors.

Some takeaways regarding compliance trends of Apple-specific security features:

FileVault: A basic feature that provides critical protection of user data by encrypting it within the volume was **"found disabled on 36% of devices"** in the research pool despite the ease of deployment, configuration and managing encryption keys via your MDM solution.

Gatekeeper: With an **"90% activation rate for App Store & Identified Developers,"** Gatekeeper is an important layer of security against installing malicious software. It is a boon for maintaining user privacy as Apple verifies each app to ensure that data collection does what developers claim it does.

Firewall: In light of bad actors increasingly targeting mobile devices with web-based threats, it is alarming to find the **"Firewall feature disabled on 55% of Macs."** Despite the ease with which to deploy configurations via MDM solutions, enabling Firewalls serves as an industry best practice that is known to prevent devices from accepting incoming connections from unauthorized applications and services.

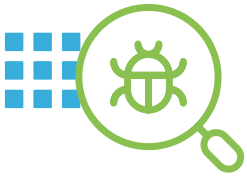
Lock screen: A fundamental feature of mobile devices that secures data from unauthorized access but also serves as the decryption key for all data stored locally on the volume. **In 2023, "3% of devices had lock screen disabled and 25% of organizations had at least one user with lock screen disabled."**

Section II: Application usage and expanding risks

Application vulnerability management

Even a brand new device running the latest hardware and the most up-to-date operating software can be vulnerable to attack if the applications running on that device are out of date and contain bugs that are actively being exploited by attackers. It is imperative that organizations manage vulnerabilities from hardware and the OS layer up through the applications that run on that device.

Jamf found that "2.5% of devices had a vulnerable application installed in 2023." If we were to extrapolate our modest percentage against the **estimated number of mobile devices worldwide of 16.8 billion at the end of 2023**, it would equate to approximately 420 million vulnerable devices globally.



2.5%

of devices had a vulnerable application installed

A tale of two apps

Our study of the threat landscape finds two fundamentally different types of applications in use by organizations. Native (on-device) applications utilize device resources to execute code and provide functionality to end users while web applications are hosted on the internet, typically in SaaS environments or private cloud deployments, and rely on data centers or remote servers for processing and data storage.

Our research shows that application risks are common regardless of the application type being used:

- Vulnerabilities need to be managed within the application software, and the connected nature of cloud-hosted applications causes them to be exposed more to remote tampering than those that reside on a particular device.
- Given the reality that several networks likely sit between a device and remote application mean that the **protection of data in transit** is of the utmost importance when managing the risks associated with cloud-hosted applications.
- **Protection of data at rest** is equally important for both application types. Even though cloud-hosted applications are often protected by the data center perimeter, modern applications are often built on open source software, common substrates and shared compute resources.

Organizations with managed devices gain insight into these endpoints through constant monitoring, but what of non-managed devices, like personally owned smartphones? Although there are differences, here's what holds true for enrolled and non-managed devices:

- There are vulnerabilities in both.
- Both house sensitive data.
- All need to be managed.
- All need real-time risk-driven access policies to realize the security dream of locking down applications and business data to authorized users only.

This leaves only one option for comprehensively protecting your infrastructure: be aware of both application types and implement layered security protections that address web-based and on-device app risks.

By implementing a more integrated IT program that brings together the functions of device and application management with the capabilities and insights of security tooling, organizations can achieve a more resilient workplace. The key to this is a defense-in-depth security strategy that provides holistic protection across your entire infrastructure by incorporating compensating controls to adjust to changes in the device's risk posture. At the same time, business data is routed over secure tunnels unique to each request for web-based apps.

Alongside this, another layer of security control marries the above to management, enforcing compliance with hardened configuration profiles and managed app deployment and automated vulnerability remediation workflows to provide a baseline and implement a foundational level of device security regardless of the device type, ownership model or network connection utilized to remain productive.

Managing vulnerabilities and risks

Though enticing for some, downloading a commercial app for free often comes with far more than what users bargained for when obtaining applications from third-party App Stores. For a more granular look by platform, Jamf research found that Android has 2x third-party app downloads compared to iOS.

While Apple continues doubling down on security and privacy protections across its hardware and software line, these findings show that they aren't immune to the threat trends increasingly targeting.

"Android has 2x third-party app downloads compared to iOS"

Business data security and modern devices

Data security lies at the intersection of work-life balance and the mobile technologies that make remote/hybrid work a possibility. When viewed as part of a matrix, the vertices that tie two points together also show their disparity from one another in some cases. For example, a device used by a medical professional conducting home health visits. The patient records, or Protected Health Information (PHI) stored within the device, are regulated through HIPAA in the U.S. A mobile device grants the professional greater ease when traveling (which represents one end of the vertices) while the relative ease with which a bad actor can steal the device itself, along with the data stored within it (represents the opposite end of the vertices). In simpler terms, the easier the device is to carry for the user, the easier it will be for an unauthorized person to steal it.

Greater ease = greater risk.

Modern devices do not necessarily have to be company-owned or company-issued devices. Due to several factors, such as equipment availability and software licensing costs, employee choice programs, and ease of use, modern devices used for work are often a mix of personally owned and company-issued devices and apps. It is imperative that organizations embracing modern IT and security standards ensure that only authorized users on sanctioned devices that meet the organization's requirements are able to access sensitive resources and applications.

Because of this, one of the most significant trends impacting business data security centers around risks related to:

- Bring Your Own Device (BYOD) models
- Shadow IT

Both concerns see devices of all types, spanning multiple platforms, which vary from user to user – all to be as productive as possible with the hardware and software users have chosen. Empowering users is a critical aspect of productivity. Still, this lack of standardization shows that data security pays the ultimate price when various software tools and services – all with varying risk factors – get thrown into the mix. For example, web browsers—like Google Chrome, Microsoft Edge and Mozilla Firefox—perform a critical function of rendering websites for users to research and work virtually every minute of every day. Yet, multiple apps multiplied by differing versions of each app and multiplied by the Common Vulnerabilities and Exposures (CVE) related to each version equals an incalculable number of vulnerabilities present across the entire device fleet used to access organizational resources, which, in turn, handle and process business data on countless devices used for work and school worldwide.

Shadow IT has long been a thorn in their side due to users bypassing security protections, such as sideloading apps or users relying on their preferred cloud-based app which may not be fully vetted or approved for use with business data because of inherent risks to using insecure versions of apps. Our research indicates that Onion Browser and Tor were among the top sideloaded applications installed on work devices. On personal devices, where users can control which apps they wish to download and use on devices they own, messenger apps linked to Social Media platforms were in the top 20 list of vulnerable apps, no doubt because of the growing trends linked to **threat actors exploiting victims over social media** through fraudulent job postings. These bogus profiles communicate directly with targets over direct messages, scams involving cryptocurrency investments, or just generally spreading misinformation that appears legitimate but really isn't.

Monitoring shadow IT is one form of compliance management that is relevant to corporate devices. For personal devices, we want to ensure that the devices are not only configured properly and ready for work but that policies such as those governing how data flows from business apps and personal apps are managed according to the organization's standards.

The overarching message here is that IT and security teams are tasked with securing business resources, limiting access to authorized users only, but the mix of devices — from work-issued to personally owned are variables that impact security. Introducing greater risk are applications that companies granted open access to, allowing them to be accessed from anywhere — even non-work-issued devices since they don't want to stop users from being productive. Further muddying the waters, in an effort to make their lives easier, some employees have been found to circumvent work policies. For example, if the work network blocks access to a service (e.g., Cloud Storage A) because they want to restrict where work data is stored in the cloud, but an employee uses their personal device to place sensitive documents in another service (e.g., Cloud Storage B), the worker has violated policy and placed data at risk.

This is why the best practice is to implement policies that link together user authentication, device assessment and secure connectivity. Bridging the gap between management, identity and security by layering protections in a defense-in-depth strategy that secures and manages devices, users and data at each level, regardless of the device type, physical location, ownership model, OS platform or network connection.

Section III: Malware analysis and attack evolution

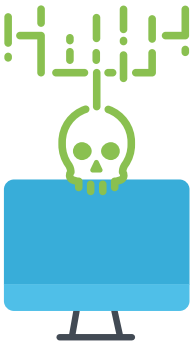
In this section, we dive into the granularity of what malware threats are the biggest threats impacting organizations and their frequency in the wild in 2023, and address continuing evolution of attacks affecting both platforms and how bad actors target vulnerabilities in OS-level tools to fool users into a false sense of security (more on that later in this section).

macOS threats

Users may turn a blind eye to the risks they face online, but organizations know that the increased use of business applications makes their users more targeted than ever before.

Did you know that

"57% of Mac users either agree or hesitate to disagree with the statement 'Malware does not exist on macOS"? According to **survey results reported by The Hacker News**, in 2023, "every third Mac user believes their data is of no interest to cybercriminals."



21

new malware families on Mac

While the myth that Mac doesn't get viruses persists, Jamf Threat Labs tracks around 300 malware families on macOS. In fact, 2023 saw the rise of 21 new malware families on Mac!

Below is a full breakdown of new Mac malware instances studied and counted in 2023, based on our findings:

Malware category	% of all Mac malware
Adware	36.77
PUA	35.24
Trojan	17.96
Exploit	4.40
Ransomware	2.00
Downloader	0.92
Hacktool	0.67
Coinminer	0.64
Certificate	0.64
Dropper	0.56
Infostealer	0.25
Spyware	0.23
Malware	0.20
Keylogger	0.04
Network	0.026
Virus	0.01
Rogue	0.01
Hyperlink	0.01

As you can see from the breakdown, each category is listed in order from the highest percentage of Mac malware to the lowest. That said, here are some interesting data points relating to some of the malware findings we discovered. Beginning with PUA, or potentially unwanted applications, this category is tricky to quantify since it could be that the application was installed knowingly by the user that is otherwise benign or could be something that was intentionally hidden from the user during installation to mask its detection. Because of these variables, users need to remain vigilant as to any unintended actions occurring within their Mac.

Over the past year, trojans were observed as having the highest number of families. This indicates a high level of diversity when it comes to packaging and deploying this type of malicious code, which potentially serves as an indicator of a higher number of malware authors as well. **At 17%, the 'trojans' category** represents a significant risk that is growing in popularity within the macOS malware community. Think: What are the bad guys inserting into systems? Why are they using this tactic? After all, Trojans are, by definition, software that contains other bad things hidden inside. This underscores not only the need for vulnerability management but:

- getting applications from legitimate sources
- applying a vetting process (either through trusted third parties like Apple's App Store or through an organization's own security team)
- running up-to-date security software

Atomic Stealer

Advertised on Telegram, 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. Notably, Atomic abuses AppleScript dialog functions to deceive users into providing their credentials. Once the user's password is entered, it pilfers additional sensitive data from the macOS keychain. Distributed under the guise of legitimate applications like Tor Browser, Photoshop CC, Notion and Microsoft Office, the malware has also been observed being promoted via malvertising on Google Ads.

JokerSpy

Attributed to the BlueNoroff APT group, JokerSpy was first spotted targeting a cryptocurrency exchange in Japan. The malware employs a variety of backdoors to deploy spyware on compromised systems and uses open-source tools for reconnaissance. Its Python-scripted backdoors enable dynamic configuration loading and command execution, allowing for a diverse set of malicious actions. In addition to evaluating system permissions, JokerSpy is known to abuse Apple's Transparency, Consent and Control (TCC) settings. It may also deploy SwiftBelt, an open-source macOS post-exploitation toolset commonly used in red teaming exercises.

KandyKorn

This malware was discovered as part of a much larger sophisticated attack where DPRK threat actors targeted blockchain engineers. The attackers deployed a multi-stage malware attack via a fake bot on Discord. The initial compromise involved various malicious Python scripts, which downloaded additional malware components. Subsequently, the python scripts would act as droppers for the next stage of the malware, which established a connection to a C2 server. An additional stage malware was used after this that employed persistence and defense evasion techniques like reflective binary loading, which ultimate lead to the in-memory execution of the KandyKorn malware.

Lockbit

Described by VXUnderground as a milestone—the first instance of a major ransomware group targeting Apple products. LockBit appears to be an Apple port of its Linux counterpart, first surfacing in early 2022. Initial samples displayed ad hoc signing, triggering an invalid signature pop-up upon execution. As of the latest information, LockBit does not yet exfiltrate data and is believed to be under active development, suggesting additional functionalities could be forthcoming. When successfully executed, the ransomware encrypts files using open-source libraries and leaves a ransom note in the filesystem.

NokNok

NokNok is an APT malware chain attributed to an Iranian threat actor, designed for reconnaissance and backdoor deployment on victim systems. The attackers employ targeted phishing emails that impersonate the Royal United Services Institute (RUSI), enticing victims to download a malicious VPN application bearing the RUSI name. Once installed, NokNok leverages bash scripts to establish backdoors and receive server commands, capable of either self-termination or executing additional modules. These modules collect data on running processes, system information, and installed applications, and can also ensure persistence. For secure data transmission, NokNok employs its own encryption, further obfuscated through base64 encoding and segmentation.

iWebUpdate

iWebUpdate is a persistent downloader designed to fetch and execute arbitrary payloads from a remote server. It maintains persistence through a user launch agent named iwebupdate.plist. Upon activation, it performs reconnaissance by executing commands like system_profiler to collect OS version information, which is then sent to a command and control server. Payloads are downloaded to a temporary file at /tmp/iwup.tmp, unzipped, and subsequently executed. The malware checks back with the server every hour for additional tasking.

ObjCShellz

ObjCShellz, an Objective-C backdoor attributed to the BlueNoroff/Lazarus APT group, enables attackers to issue shell commands to compromised systems. Upon establishing a connection with its command and control server, it allows the execution of shell commands, the results of which are relayed back to the attacker. This malware was first identified by Jamf Threat Labs within the scope of the RustBucket campaign, a BlueNoroff operation often targeting small cryptocurrency-focused companies.

PureLand

PureLand is an info-stealing malware embedded in a pirated version of the legitimate indie video game "PureLand." Distributed via email, the trojanized game promises to generate cryptocurrency for users as they play. Notably, PureLand was discovered concurrently with Realst Stealer, another malware that employs a strikingly similar social engineering tactic but features a different final payload.

Realst Stealer

Realst Stealer, a Rust-based malware focused on info-stealing, primarily targets crypto assets on compromised systems. In a well-documented campaign, the malware was ingeniously embedded into lesser-known video games. To distribute it, attackers approached individuals offering exclusive early access to these games, presenting them as NFT-based opportunities to earn crypto. Once the user launches the game, Realst Stealer activates, compromising the system and initiating its crypto-stealing routines.

Rustbucket

RustBucket is a remote access trojan. Trojans are often focused on espionage capabilities rather than monetary gain, but some overlap may occur depending on attacker objectives. They generally include multiple different functionalities such as remote shell capabilities, keyloggers, infostealers and more.

RustBucket, employed by the APT group BlueNoroff—a North Korean subgroup of the well-known Lazarus Group—is a multi-stage malware targeting users via intricate social engineering campaigns. The initial droppers are written in Objective-C, Swift and AppleScript, while the final payload is crafted in Rust. In typical campaigns, the malware disguises itself as a benign PDF reader. Users are convinced to open a specific PDF document using this rogue application, triggering a callback to the attacker's Command and Control server.

WTFMiner

WTFMiner is an evasive cryptojacking malware spreading through pirated macOS apps. Its origins can be tied back to a torrent uploader who bundled the miner into multiple pirated macOS applications since 2019. By obtaining copies, Jamf charted its incremental development across three generations, each version employing additional stealth techniques. It uses dark web routing for stealthy communication, obfuscates itself as legitimate processes, and shuts down when Activity Monitor is opened. Latest variants avoid writing persistence to disk and rely on users launching the trojanized apps to initiate mining.

Lastly, our research discovered that ransomware, despite having some of the lowest families, still managed to crack the top five on the list of new malware in the wild because of the significant number of instances identified as belonging to this malware classification type. Although a few new ransomware families were discovered last year such as the **Turtle Ransomware** and **Lockbit for macOS**, Jamf Threat Labs has found that most samples labeled as 'ransomware' continue to belong to the EvilQuest ransomware originally discovered is 2020.

Although this is interesting, many believe that EvilQuest samples are primarily being generated via a sandbox bug that continues to generate minuscule differences in sample. The ransomware is not actively being delivered to victims and has not been since its discovery in 2020.

What we've actually found

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

Rank	Family	% of total seen in wild	Category
1	genieo	13.63	Adware
2	imobie	12.25	PUA
3	generic	10.02	Adware
4	multiverze	6.84	Adware
5	tnt	6.19	PUA
6	ccleanmac	5.28	Adware
7	mackeeper	4.55	Adware
8	pirrit	4.45	Adware
9	macinformer	4.37	Adware
10	installcore	3.98	Adware

Mobile threats

Despite the misconception that Macs are immune to malware, mobile threats, especially on platforms like iOS, are genuine and challenging to quantify with simple statistics. Security professionals face the real-world impact of these threats on business data and user privacy. Later in the section, we'll reveal some surprising discoveries made by security researchers in 2023, highlighting the detailed nature of these mobile threats.

Note: the percentages displayed in this section based on our findings appear significantly lower, especially when compared to other sections in this report. But as the idiom goes, "Don't judge a book by its cover", which is especially crucial in cybersecurity because:

- The world **population reached 8 billion in 2022**, as estimated by the United Nations
- As of 2023, the **total number of mobile devices worldwide is estimated to sit at 16.8 billion** and climbing
- The percentage of **global users with a desktop or laptop computer at home** hovers at 47.1% when last reported in 2019
- 3.6 represents **the average number of devices per person globally**.

Why are all these stats about population counts, device types and average devices per person critical to understanding the impact of modern, mobile security threats? It is important context to the numbers in our research.

> "**<1%** of devices and **2%** of organizations had a potentially unwanted app installed within their device fleet in 2023."

As stated previously, 1% may not appear very concerning and less than that is, well, less concerning, right?

Wrong. Here's where the stats above are extrapolated to give an accurate, real-world view of how critical these percentages truly are.

Let's start with the 16.8 billion mobile devices currently in use worldwide. By determining 1% of that, we're left with 168,000,000 mobile devices with malware installed. Now let's turn our attention to the global population of 8 billion and remove the 47.1% of computer users to refine our numbers for mobile usage only. This leaves us with a population of 4.232 billion potential mobile device users. Last, and here's where it gets tricky, we multiply our refined population count by the global average of 3.6 mobile devices per user to arrive at 15.2 billion mobile devices.

Now, it doesn't take a math whiz to see that 15.2 billion is less than 16.8 billion. Here's where the tricky part comes in. The global average is just that, a number that averages all the individual regions to determine a single global metric. However, each region has different baselines, some under the global average, like the Latin America region (3.1), while other regions average three to four times the global average, such as Western Europe (9.4) and North America (13.4) respectively. Rerunning the numbers to adjust for regional fluctuations, we arrive at the following mobile device counts for the regions noted above:

- Latin America: 13,119,200,000
- Western Europe: 39,780,800,000
- North America: 56,708,800,000

Last bit of math, we promise! Now let's revisit what just 1% of mobile devices infected with malware equates to when extrapolated based on the values adjusted by region:

- Latin America: 131,192,000
- Western Europe: 397,808,000
- North America: 567,088,000

Remember that any device – even if *just* one is compromised – is all it takes for bad actors to successfully execute a data breach.

Attack evolution

2023 presented the Jamf Threat Labs team with exceptional opportunities in the discovery of not one but several different and complex, yet powerful mobile threats – all targeting iOS-based mobile devices and their users.

And while mobile devices are made up of more than just Apple's platform, a significant portion of our research points to growing trends strongly underscoring the position that threat actors are increasingly targeting the Apple ecosystem with considerable technical resources directed toward developing novel and difficult-to-detect attacks to compromise the iOS/iPadOS platforms.

Apple has led the defensive on this front by making security and privacy crucial tenets of their design philosophy. According to their research, **mobile threats against consumer and business data**, *"The total number of data breaches more than tripled between 2013 and 2022 — exposing 2.6 billion personal records in the past two years alone,"* and they note that, "continued to get worse in 2023.

Social engineering evolution

Mobile threats are very real. Many new third-party apps and services are getting more common and advanced each year. Our Jamf Threat Labs team found some new security threats for iOS in 2023, called Social Engineering 2.0, which demonstrate this trend.

Pegasus discoveries

In April, Jamf Threat Labs released research following an in-depth investigation into two devices compromised by Pegasus. The first, an iPhone 12 Max Pro belonging to a human rights activist in the Middle East, proved to be “a treasure trove for our analysis given the compounded set of compromise indicators and the clear association with Pegasus.” The findings showed “unique indicators of compromise (IOCs) and evidence of active spyware campaigns.”

Additionally, during their analysis, Jamf discovered a new IOC while analyzing the filesystem of the second device, an iPhone 6s, belonging to a journalist in Europe working for a global news agency. Their research revealed that threat actors continue to target older devices, serving as a reminder that they will stop at nothing to “exploit any vulnerabilities in an organization’s infrastructure, attacking wherever possible.”

Fake airplane mode

In August, Jamf Threat Labs developed a post-exploit technique to achieve persistence on iOS 16. By editing the UI to show the appropriate on-screen icons while also cutting internet connections to all apps, an attacker tricks users into believing that Airplane Mode is enabled when in actuality, they maintain network access to the device on exploited or jailbroken iPhones.

Airplane Mode provides an additional layer of privacy and compliance with certain regulations during travel, offering peace of mind for security and privacy-conscious users. However, by modifying and thereby interrupting this functionality, victims of this attack could have their devices compromised unbeknownst to them while potential threat actors achieve persistence, maintaining unauthorized access to impacted iOS-based devices, as they move along the attack chain.

Fake lockdown mode

In December, Jamf Threat Labs created a new technique after the proof of concept mentioned earlier. This method has more significant consequences for the safety, security and privacy of users. Focusing on Apple’s Lockdown Mode, this tampering technique provides all of the visual cues associated with a functioning Lockdown Mode, without any of the protections that would normally be implemented by the service.

Attackers compromising the device could implant malicious code to implement the attack described here. Upon enabling Lockdown Mode, the high-risk user on a vulnerable device inadvertently triggers the attacker's code that implements the visual cues of Lockdown Mode but makes no changes to the device’s configuration. So instead of the protection and minimizing the functionality that is remotely accessible, the result is an iPhone that is believed to be protected to some degree by the end-user while actually remaining unprotected, compromised and fully accessible to threat actors.

Section IV: Web threats and online risks

Attacks that leverage the connected nature of modern devices — to attack the user or device over the network, to convey command & control signals, or to exfiltrate data — are classified as web-based threats. This umbrella term describes various threats and not just one type. This type of threat also accounts for some of the largest, most sophisticated, deadly and, unfortunately for its victims, successful attacks across the modern threat landscape.

Web threats are a very important and strategic part of the attack chain for mobile devices. A common starting point that has broad exposure to users and devices. Perhaps it's different in nature than CVE exploits in an app or an OS but it's an important part of an attack chain that orgs have some powerful controls over if they choose to implement them

We shouldn't treat web threats as an "alternative" to other threat vectors. It's simply a delivery vehicle. These attacks are often combined with more traditional tactics to launch a successful attack. These are all pieces in the bigger puzzle that often:

1. Provide threat actors with the greatest level of success for the least amount of effort.
2. Can bypass even the most stringent of security policies and controls.

Looking closer at the first half of the answer, it doesn't take a crystal ball to know that the top threat is and continues to be phishing. Sending out a malicious link via SMS to hundreds or thousands of targets only takes seconds, and the likelihood that at least some of the targets will click on it is high enough to make the campaign a success.

Moving on to the second half of the answer, it doesn't get any clearer than this: all the security controls in the world don't mean a thing if users simply hand out their credentials and subsequently, access to personally identifiable information (PII). There's no technical wizardry at play nor complex code to develop—just merely asking your target to provide their credentials in a semi-convincing way is all that's required to compromise a system or service.

Below, we dig deeper into our research, identifying the top threats impacting devices.

Phishing

As mentioned above, phishing is the top threat and for good reason: minimal effort for maximum success.

9%
of users fell for a phishing attack

and phishing attacks were 50% more successful on mobile devices than on Macs

Bad news first: This is up 1% from 2022 when 8% of users fell for a phishing attack.

What this means is that while organizations appear to have better protections and education focused on data security, individual users are seeing an uptick in compromises, which gels with the threat trend that attackers are targeting users directly and more aggressively through other avenues, such as social media, no doubt capitalizing on remote/hybrid workforces that are using personally owned devices for work. In 2023, phishing attacks were 50% more successful on mobile devices than on Macs. And with **CISA** indicating that "more than 90% of all cyber attacks begin with phishing," it's no surprise that bad actors would target users' primary devices as a stepping stone to pivot from compromising personal data to business data.

Cryptojacking

"Cryptojacking 1% of devices and 9% of organizations."

While the cybersecurity industry was initially warned about cryptojacking in 2011, modest attacks notwithstanding, its first real surge was reported in 2022, when incidents rose to 140 million, or an **increase of 43% globally**, as noted by Statista. Continuing its surge, Sonic Wall found that **cryptojacking attacks swelled by 399% to 332.3 million** incidents in just the first half of 2023 alone.

As an indicator of how pervasive cryptojacking is, look no further than our security researchers when the **Jamf Threat Labs team identified cryptojacking malware** embedded within pirated copies of commercial software for macOS earlier in 2023. As multiple pieces of research corroborate, cryptojacking continues to be a dangerous trend that threat actors are literally and figuratively banking on. One that organizations need to take seriously moving forward since it's well past the point of merely stealing resources and crossing into the territory where the criminal action is making threat actors a lot of money, keeping it and other cyber threats going.

Malicious network traffic

Not to be confused with malware installs (see our analysis of this threat type later in the report), malicious network traffic pose a significant threat to "11% of devices" in our overall research pool. When looking at the organizational level, we found that "20% of organizations were impacted by malicious network traffic."

Examples of malicious network traffic are:

- Malware download
- Command and control
- Data exfiltration
- Scams
- Drilling down more granularly from that percentage, we saw that "mobile devices running Android and iOS made up 8% and 6% of that total respectively." Other notable findings were:
- **2% of organizations experienced a password leak** (credentials released online without consent)
- **1% of users connected to a risky hotspot** (wireless networks that are unsecured, often free to use)
- **About 1% were impacted by MitM** (Man-in-the-Middle) attacks (when a threat actor makes independent connections between two victims and relays messages between them, often altering them, to gather data)

Though these percentages are not the big, attention-drawing numbers that get plastered in the media, when they are put into context against the number of devices in our sample pool, we get to see what those modest percentages equate to in real-world numbers.

- 300,000 devices experienced a password leak
- 150,000 users connected to a risky hotspot
- Just under 150,000 were impacted by MitM attacks

These numbers represent, at a minimum, 150,000 opportunities for:

- **Threat actors to compromise a device**
  - Capture business data
  - Pivot attacks to other endpoints
  - Breach a network or service
  - Devices to be found out of compliance
  - Found in violation of local, state, federal and/or regional regulatory requirements
  - Legally responsible for fallout stemming from incidents
  - Subject to civil and/or criminal charges
  - Companies to have their reputation tarnished
  - Subject to termination of partnerships
  - Loss of business opportunities
  - Business closure/ceasing of operations

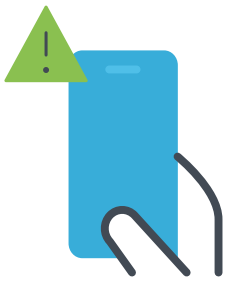
Device compliance

While we've touched upon each of the three threat trends, we're not quite done with our research findings. For this section, however, we're going to shift focus from threat trends to mitigation strategies to better maintain device compliance and manage configuration vulnerability.

In this report, this is achieved through data-driven guidance, based on our research findings, that drills down into three specific sections, each with unique areas that IT and security teams should refocus their efforts to achieve and maintain holistic compliance through comprehensive management and defense-in-depth security strategies.

Back to basics

Our first area of focus will be among the most critical of sections on device compliance since it sets the foundation upon which the tools and strategies in other sections will be built. As the title suggests, 'back to basics' is the driver for your security plan by doubling down on the critical functions that have been proven time and again to be a cornerstone in protecting your endpoints.



39%

of organizations had at least one device with known vulnerabilities

Patching and security updates

Jamf identified that a whopping "39% of organizations had at least one device with known vulnerabilities." Security professionals know that zero-day threats are difficult to identify and even more challenging to mitigate against as developers have yet to produce patches to neutralize that type of threat. But as the findings highlight, the issue here relates to known vulnerabilities, or those with patches available…only the devices lack the crucial patches or updates to remediate the vulnerability.

While the finding above relates to all device types within affected organizations, another troubling finding targets mobile device usage, concerning **"40% of mobile users running an OS version with known vulnerabilities."** This is a trend within itself, as all stakeholders – not just organizations – are responsible for the security of their devices. Together, they play a critical role in fine-tuning baselines for their fleet through iterative workflows to close the rings as quickly as possible on newly released OS updates and application patches.

One of the leading reasons for delays in updating devices is cited as fear of conflicts and too many agents that require updating.

Rapid security response (RSR)

In a concerted effort to combat delays in getting critical security updates installed on Mac and iOS-based platforms, Apple implemented Rapid Security Response in early 2023. The introduction of RSR streamlines the delivery of critical patches to mitigate risk by automating their download and installation on supported devices. Apple devices and users are better protected against the introduction of exploits existing in the wild by minding the gap between the major software updates.

macOS security compliance project (mSCP)

The open-source project, known as mSCP, serves to aid IT and security teams tasked with managing and securing Apple devices to implement security benchmarks that align with their compliance goals. Based on your organization's unique compliance needs, mSCP provides a logical, systematic approach to generating configuration payloads and settings to enforce compliance after deploying them to your device fleet.

Role of management in security

Management and security hold a symbiotic relationship. Simply put: one should not exist without the other. Endpoint security ensures that devices are protected against threats by actively monitoring endpoints but without management, remediation becomes a manual, time-consuming effort that becomes exponentially challenging the more devices you have and the more remote they are. Conversely, management workflows can't automate device compliance without the up-to-date device telemetry that outlines what deficiencies are present within your fleet.

To this end, the aforementioned RSR from Apple is one such critical patch service that benefits from management, providing IT with the mechanism to configure devices so that security responses and system files are automatically installed on devices, regardless of whether they are locked or logged out.

Finally, a critical component in the role of management is how active monitoring aids compliance initiatives. Drawing upon the considerations between native and cloud-based apps in the prior section, insight gleaned from monitoring provides IT/Security with an X-ray scan of an endpoint's health. Armed with rich telemetry data, these teams can make data-driven decisions about app safety and data security. Without this data, how would organizations know the security status of endpoints remotely accessing web apps, for example?

Jamf Compliance Editor (JCE)

Designed on the foundation set forth by mSCP, Jamf's take on it takes the compliance tool and marries it with our MDM solutions to achieve a native macOS app that not only generates customized compliance assets for your organization but interface built-in to JCE also integrates with your Jamf Pro instance via secure API to upload your newly generated assets, seamlessly bridging the gap between generation and deployment, helping administrators to save time by enforcing compliance sooner and more efficiently.

Defense in depth

No tool is foolproof. There is no silver bullet solution that captures all threats all of the time. Somehow, somewhere, something will inadvertently slip by. It's simply the nature of the beast, but that doesn't mean that there aren't steps that IT and security teams alike can't take to minimize the risk of threats impacting organizational resources. Hence the beauty of layered protections – if one layer doesn't catch it, the other layers can before that risk becomes something far worse.

Beyond simply cobbling together any number of solutions, defense in depth is more of a security paradigm to strive for when organizations are building (or upgrading) their security plan. The core aim is to integrate various solutions into layers, like a cake, where each layer being its own security tool but also one that acts as a safety net for the previous one. Should a threat manage to squeeze by the next layer can mitigate it.

Trusted Access

Jamf's very own security paradigm is a prime example of how combining Jamf Pro (management), Jamf Connect (identity) and Jamf Protect (security) solutions form an integrated platform from which administrators can effectively extend management of their entire fleet holistically across their infrastructure while simultaneously providing comprehensive security protections to Mac and mobile devices running macOS, iOS/iPadOS/tvOS, Android and Windows.

> "<1% of organizations had a jailbroken or rooted device in 2023."

This finding is evidence that fewer users are jailbreaking/rooting devices used for work, which is a good thing. However, it also serves as proof that active monitoring of mobile devices (security) combined with Zero Trust Network Access (identity) dynamic security policy enforcement and automated remediation (management) makes a great workflow to prevent non-compliant devices from putting your organization's data at risk of compromise.

Employee choice programs that rely on BYOD and COPE (Corporate Owned Personally Enabled), are great for user productivity but under-managing and/or over-securing a device leads to a litany of problems impacting data security and end-user privacy. A solution to the under- over for management and security is to implement tiered workflows that support both company- and personally-owned devices so that both types have a baseline security posture.

For example, company-issued devices are automatically enrolled with MDM with zero-touch deployment (management) while personal devices are user-enrolled with their credentials (identity). The latter have similar configurations to the former, except that a business volume stores all business apps and data in an encrypted volume that is separate from the personal volume storing the user's personal apps and data. Additionally, privacy on the network is upheld by routing all business traffic through encrypted microtunnels (security) while personal network traffic is routed directly to the internet. Lastly, endpoint security performs the same level of threat detection and prevention on both personal and company-owned devices, relying on up-to-date device health data to determine the endpoint's state of health each time a request to access business resources is made. Based on the zero-trust model, only when a device has been verified will the access be approved; if verification fails, the request remains disapproved with an automated workflow deployed to remediate the device (management). Afterward, device verification is attempted again. If verified, then and only then will the request be approved.

Key takeaways

- Establish management for all your devices — corporate-owned and BYOD
- Use endpoint security products to stop malware and collect telemetry for further analysis and threat-hunting
- Align with compliance standards
- Implement security at the edge, including for those devices that leave your corporate campus
- Connect securely using encrypted tunnels to avoid data intercepts
- Start to implement a zero-trust program
- Remember to respect end-user privacy

About this research

We wanted to better understand the biggest security trends impacting the modern workplace, including the devices, users, and applications that all must connect to get work done. The information and statistics found in this paper is the result of our analysis of security trends within our customer base, as well as through our original research of OS and application vulnerabilities and a study of the malicious underground. To understand the real-world impact of these security trends we looked at a sample of 15 million devices protected by Jamf, spanning iOS, macOS, iPadOS, Android, and Windows, across 90 countries, over a period of 12 months. This analysis was carried out in Q4 of 2023. The metadata analyzed in this research comes from aggregated logs that do not contain personal or organization-identifying information. Our intention with this analysis is not to invoke fear, but instead to educate you and your users on the options available and how to best keep all aspects of device, user and organizational data secure. Contact us to learn how you can put safeguards in place and scale your security posture.

Source: Jamf Threat Labs