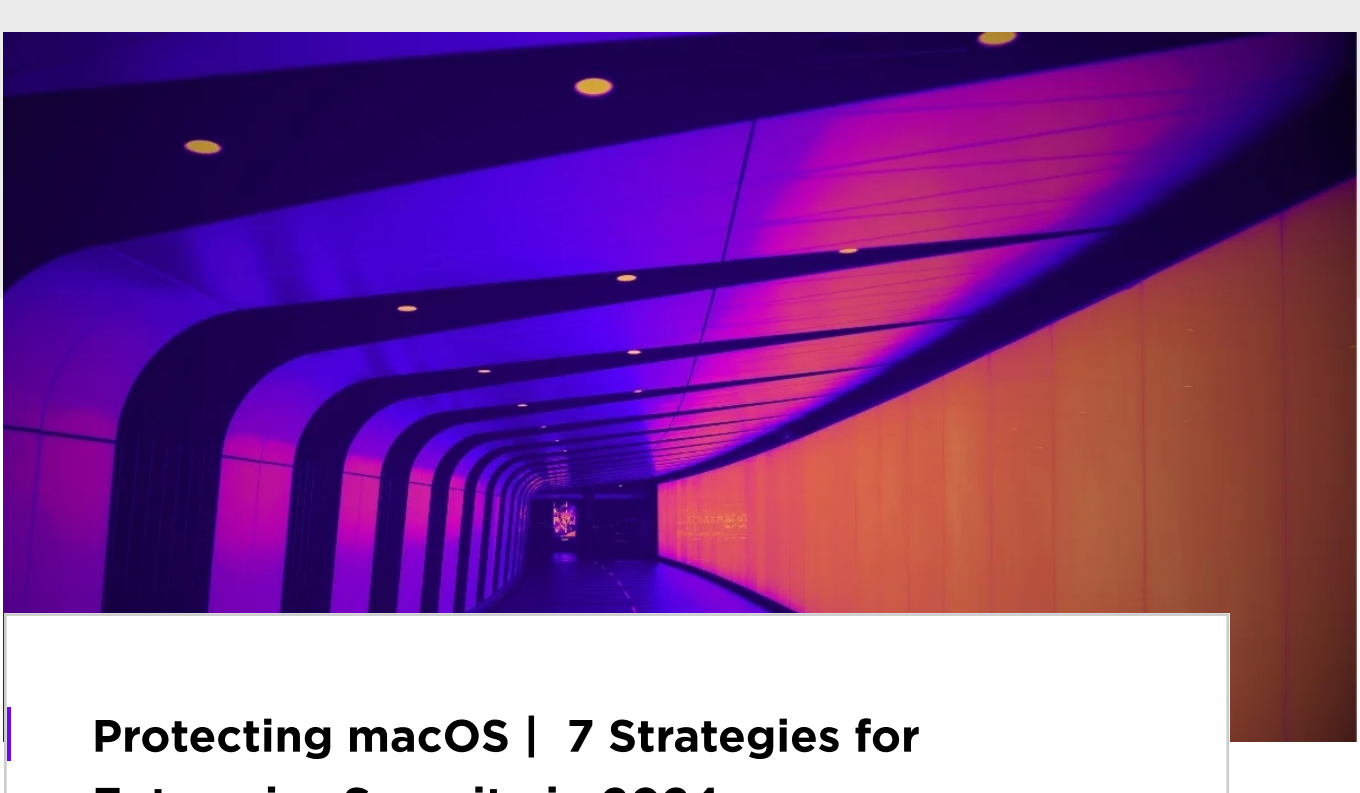


Protecting macOS | 7 Strategies for Enterprise Security in 2024

January 2, 2024
by Phil Stokes

Welcome to 2024! It may be a new year for us all, but it's very much business as usual for cybersecurity professionals. Last year saw an increase in number and variety of new threats targeting the macOS platform, and as the influence of the Mac continues to expand in enterprise environments, t little doubt that 2024 will continue that trend.

In this post, we reflect on the lessons we can learn from the last 12 months of threat activity against Apple's desktop operating system, and offer 7 strategies for defenders to help bolster their threat hunting, detection and mitigation efforts.

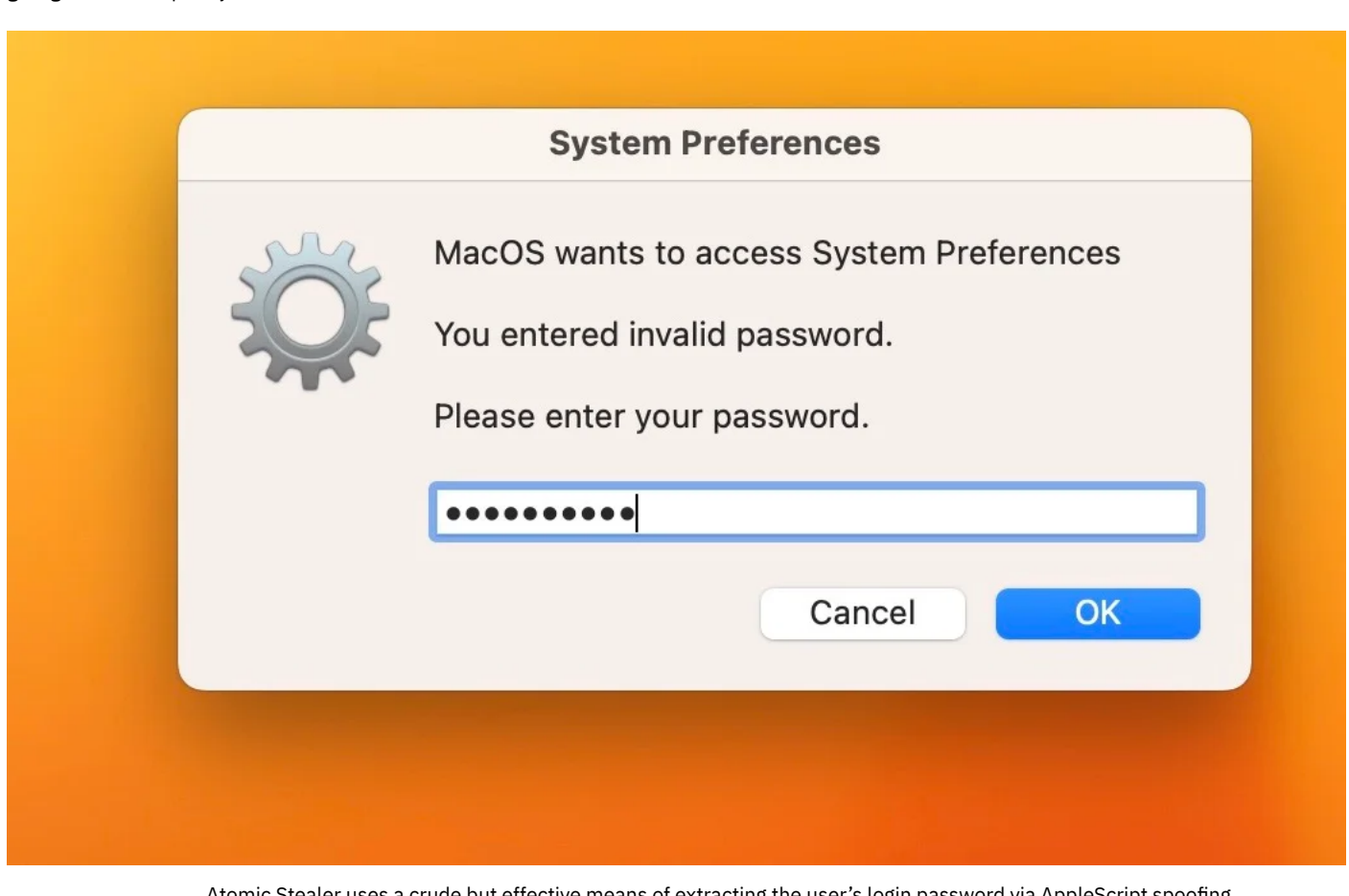
1. Don't Rely on Persistence for Detection

Perhaps the most important lesson that defenders learned from 2023's crop of macOS malware was that monitoring for persistence methods beca much less reliable way of detecting and hunting threat activity.

2023 saw Mac malware make a significant shift away from OS persistence mechanisms, in part due to Apple introducing notifications for backgrour items. Instead, infostealers grabbed "all the good stuff" – online credentials, session cookies, keychains – and exfiltrated it in a single hit. Other thr actors made clever use of trojanizing regularly launched software, effectively using the victim's own behavior as a method of persistence.

Atomic Stealer – (*aka* "Amos" / "Soma") provided one of the most widespread examples of a number of different infostealers that emerged during that eschewed LaunchAgents, LaunchDaemons and other background login mechanisms. Instead, the malware makes use of an AppleScript passw spoof to grab the user's login password in clear text, and uses this to decrypt the keychain and access other stored credentials.

Having stolen everything – including those all important session cookies and internet account credentials – in one fell swoop, the threat actors had to ensure the malware ran again. Importantly, avoiding persistence meant evading detection via Apple's recently introduced Login Items notificatio giving the thieves plenty of time to make use of the stolen credentials.



Atomic Stealer uses a crude but effective means of extracting the user's login password via AppleScript spoofing

In a different approach, the SmoothOperator (*aka* 3CX Supply Chain Attack) campaign similarly avoided using OS persistence mechanisms, instead on trojanizing an application that the user would launch frequently.

A more elaborate version of the same idea was employed in the KandyKorn campaign, which trojanized the Discord application. A Mach-O payload written to `/Applications/Discord.app/Contents/MacOS/Discord` by a previous malware stage, temporarily renaming the genuine Discord exe to `.lock`. When the user subsequently launches Discord, the payload renames itself to MacOS.tmp, renames the `.lock` file back to `Discord`, and e both the genuine Discord binary and the previous stage malware, causing the entire renaming/reloading process to repeat.

2. Assume Users Can and Will Override Apple Security

Apple has done much work to improve macOS security in recent iterations of the operating system, focusing heavily on privacy and data protection on that below) as well as making improvements to its malware remediation tools (formerly MRT, now known as XProtectRemediator). Other change development – in 2023, we saw the first signs of XProtect's prototype "bastion rules", which at present silently log access to various data files.

However, unlike iOS, it is part of the DNA of macOS that users can, if they choose, perform actions that contradict the standing OS security policy. U execute unsigned code if they choose, or even override XProtect's warning that a file is known malware.

A malicious file's Info panel allows users to override XProtect

The ability of users to override Apple's built-in security is a boon for threat actors and a headache for Mac admins. Without deploying an enterprise- security solution that prevents users from executing suspicious or malicious code, Mac admins are powerless to prevent social engineering attacks compromising their networks.

In 2023, unsigned or ad-hoc signed malware were by far the most common threats seen across the macOS platform. Such malware was used by al of actors, from DPRK-aligned campaigns like RustBucket to infostealers like MetaStealer and Realst Stealer. Such social engineering ranges from sophisticated campaigns involving impersonation and engagement via social media to simply offering users cracked versions of software they do n to pay for.

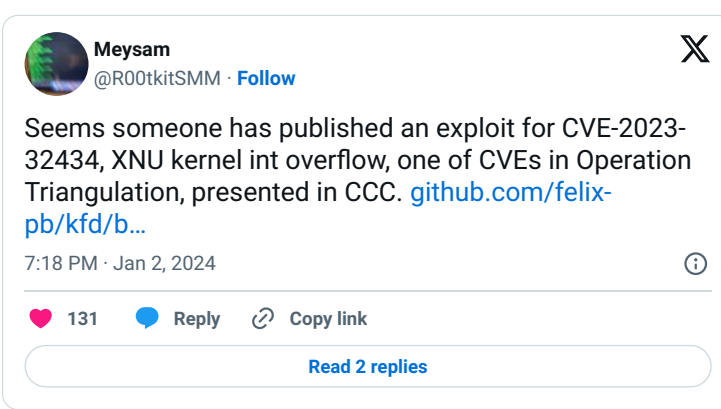
In either case, the route to compromise involves only convincing the user to take a few extra steps to launch the malware. This works regardless of the user is admin or not.

Malware beats Gatekeeper with simple instructions for users

3. Don't Let iOS Exploits Come Back to Haunt Unpatched Macs

2023 saw a record number of zero days impact Apple's mobile iOS platform, with multiple reports throughout the year of vulnerabilities said to hav exploited in the wild. Although these primarily targeted iPhone users, many of these bugs have a potential exploitation path on macOS.

As enterprise Mac users are under less pressure to update than iOS users, there is undoubtedly a large attack surface waiting to be exploited by att It is not uncommon for threat actors (or, indeed, red teams) to await write ups from security researchers describing patched bugs and then develop for them.



The 19 zero days Apple patched in 2023 were less than 4% of the 515 patched throughout the year. For security teams defending macOS endpoint keeping the OS up-to-date is a straightforward policy that should be implemented with as little delay as possible.

0-Day CVE ID	Module
CVE-2022-42856	WebKit
CVE-2023-23529	WebKit
CVE-2023-28204	WebKit
CVE-2023-28205	WebKit
CVE-2023-28206	IOSurfaceAccelerator
CVE-2023-32373	WebKit
CVE-2023-32409	WebKit
CVE-2023-32434	Kernel
CVE-2023-32435	WebKit
CVE-2023-32439	WebKit
CVE-2023-37450	WebKit
CVE-2023-38606	Kernel
CVE-2023-41061	Wallet
CVE-2023-41064	ImageIO
CVE-2023-41990	FontParser
CVE-2023-41991	Security
CVE-2023-41992	Kernel
CVE-2023-41993	WebKit
CVE-2023-42824	Kernel

4. macOS Ransomware Makes Headlines, But Focus on Data Theft

With ransomware a leading cause of compromise of enterprise Windows systems and increasingly targeting Linux, Cloud and ESXi servers, any new ransomware threats targeting macOS are always headline news. Macs have remained stubbornly immune to major ransomware campaigns largely l locking individual endpoints (as opposed to servers) with no obvious wormable propagation method to spread from Mac to Mac means ransomware developers have had little motive to invest in developing Mac-specific ransomware payloads.

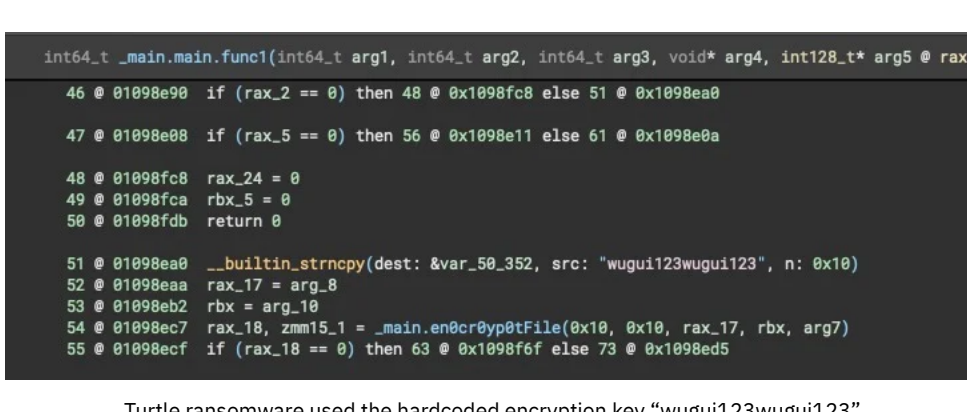
2023 saw the first signs that might change after researchers discovered a prototype LockBit payload for Macs. The macOS samples are compiled s the Apple ARM M1/M2 (aka Apple silicon) architecture. No macOS Intel sample is known at this time.

Importantly for concerned users, no occurrences of LockBit for Mac have been reported in the wild, no victims claimed, and no distribution method known to be associated with the malware. The Mac variant appears to be a direct descendant of the LockBit for Linux variant first spotted in Jan 20 contains much the same code.

Another ransomware payload dubbed 'Turtle' also came to light in November. Unlike the LockBit sample, Turtle is written in Go and targets the Inte architecture.

Turtle ransomware is written in Go

However, Turtle ransomware – while technically capable of locking files – has also yet to be seen in the wild or associated with any means of distrib Given that the sample uses symmetric encryption with a hardcoded key, this also seems like a proof of concept, as victims could decrypt any locke using the same key.



Turtle ransomware used the hardcoded encryption key "wugui123wugui123"

While it's reasonably likely that threat actors will continue to experiment with macOS ransomware payloads, we maintain that file locking remains a priority threat for Mac defenders. As we have seen elsewhere in the ransomware ecosystem, extortion via data theft has become far more profitabl threat actors.

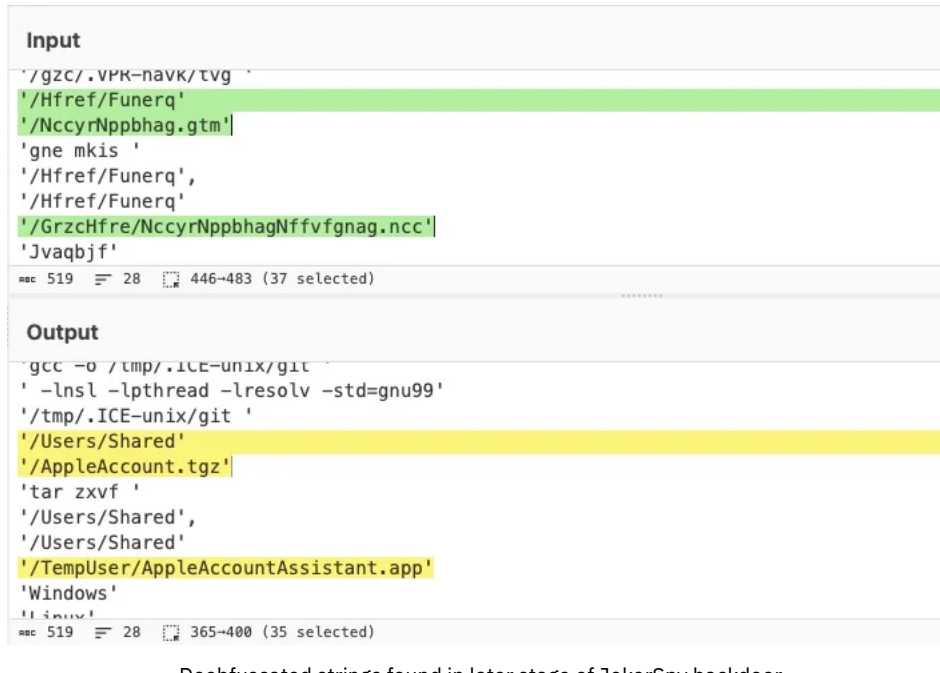
Given the continued increase in use of Mac computers by C-suite level executives and by developers with access to highly valuable proprietary cod suggest that the most likely avenue for existing ransomware gangs to pursue regarding macOS targets is the same as the infostealers mentioned ab stealing data, login credentials, and keychains is by far the most lucrative way to extort money from enterprises with Macs in their fleets.

5. Monitor Where Apple's Data Privacy Protections Fail to Tread

Much of Apple's focus in hardening macOS over the last few years has revolved around extending a series of data privacy protections known as "TC transparency, consent and control. Any Mac user of recent versions of the OS will have encountered TCC in some form or another: usually via promp asking for permission to access folders such as the Desktop, Document or Downloads, or hardware such as the microphone or camera.

We have discussed TCC at length in the past, and much of what we said then remains true as we head into 2024. Threat actors (and researchers) co to find multiple, creative ways around these controls, and patches for many known TCC bypasses figure prominently in 2023's macOS updates. Oth remain unpatched.

In addition to bypassing or hijacking TCC permissions of other applications, malware authors have also taken to simply avoiding writing or accessin that might require TCC consent. Two destinations that are always accessible to read and write that malware commonly makes use of are `/Users/S` and `/private/etc/tmp` (aka "tmp"). We've also seen some use of the separate `/private/var/tmp` and the Darwin users' `$TEMP` directory for stag malware and downloading payloads.



Deobfuscated strings found in later stage of JokerSpy backdoor

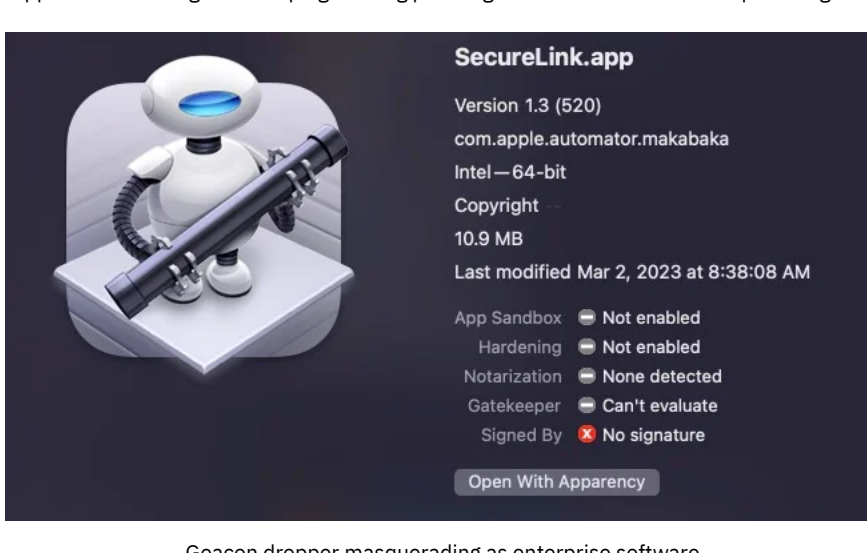
Typically, these locations are used to create malicious application bundles or binaries, launch them, and then ask for permissions to access data of an execution chain that can sidestep TCC controls just so long as the victim willingly offers up a password.

Defenders are advised to pay increasing attention to these locations particularly in light of the rise of infostealers that eschew persistence and othe common behavioral patterns noted earlier.

6. Have Runtime, Will Travel | Treat Larger Downloads With Suspicion

Python 2.6 was an ever-present staple in the macOS environment, even long after the widespread adoption of Python 3 elsewhere, and macOS mal authors have a long history of abusing it. However, after Apple removed Python as a system binary, many threat actors responded by switching to cr platform languages like Go.

In 2023, we saw a great deal of Go-based malware, from infostealers like Atomic to Cobalt Strike implementations like Geacon. In the wild, Geacor payloads were observed in what appeared to be targeted campaigns using phishing document lures and masquerading as fake enterprise-level sof



Geacon dropper masquerading as enterprise software

Along with Go, Rust payloads have also started to become more common. In some cases, malware authors that preferred to continue using python responded by packaging the python runtime with their malware.

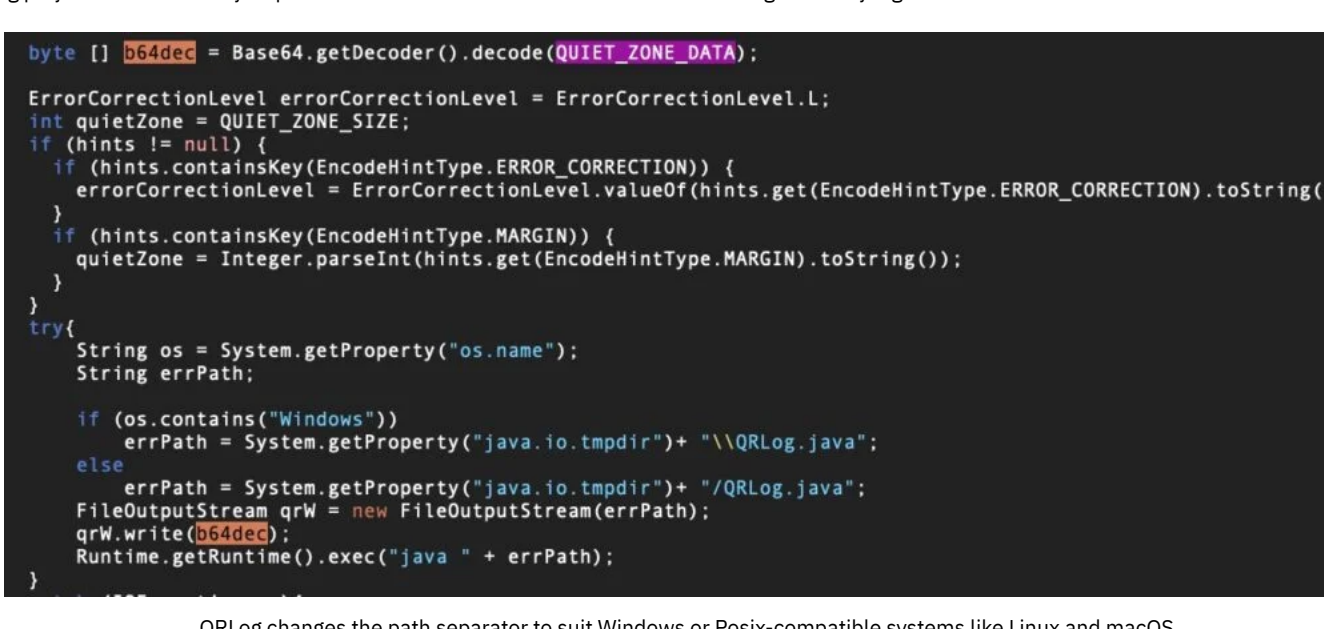
Whether its Go, Rust or Python, all these approaches result in larger payloads as they carry their own runtime environment with them, a fact that m defenders can and should factor into their detection and threat hunting routines.

7. Secure the Software Supply Chain

Some of the severest attacks on organizations occur through the supply chain. The previously mentioned 3CX/SmoothOperator campaign is notable these. A trend in evidence extending beyond last year involves compromise of open source software projects including libraries distributed via pack managers and public repositories like PyPI, Crate.io and of course GitHub.

As threat actors continue to increase their focus on Macs in the enterprise, we expect to see further attention paid to vulnerabilities in widely used s as well as the creation and spoofing of code repos for common tasks, particularly with the availability of LLMs like ChatGPT that can easily reproduc code.

Last year, for example, JokerSpy malware appeared to be using a trojanized QR code generator to achieve initial compromise. The threat actors use existing project for a commonly required task and inserted a small malicious file among the many legitimate files included.



QRLog changes the path separator to suit Windows or Posix-compatible systems like Linux and macOS

This puts the onus on security teams to fully vet code introduced from external sources, to ensure that the code – once vetted – is versioned and maintained by the organization and that updates are also properly scrutinized. That's not a simple task and it means thinking about a full dev/sec o environment, or ensuring that macOS-related code is included in any dev/sec ops processes that currently exist.

Conclusion

Enterprise security has, for good reason, been focused on securing Windows systems for so long that it is easy to overlook the Macs in the organiza fleet. Apple has worked hard to market Macs as 'secure by design', but the reality has always been that Macs flew under the radar because the ince target them was not nearly so great.

That's a situation that's been slowly but steadily changing for some years now, and a look back at 2023 should be enough to convince anyone that l threats are becoming both more numerous and more serious for enterprises. Just like other endpoints, Mac devices need to be protected with first- security software to prevent threats and provide visibility.

If you would like to learn more about how SentinelOne can help defend the macOS devices in your fleet, contact us or request a free demo.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Geacon Brings Cobalt Strike Capabilities to macOS Threat Actors
- WatchTower | Trends and Top Cybersecurity Takeaways from 2022
- 7 Ways Threat Actors Deliver macOS Malware in the Enterprise
- Atomic Stealer | Threat Actor Spawns Second Variant of macOS Malware Sold on Telegram
- Session Cookies, Keychains, SSH Keys and More | 7 Kinds of Data Malware Steals from macOS Users
- macOS 14 Sonoma | Toughening up macOS for the Enterprise?