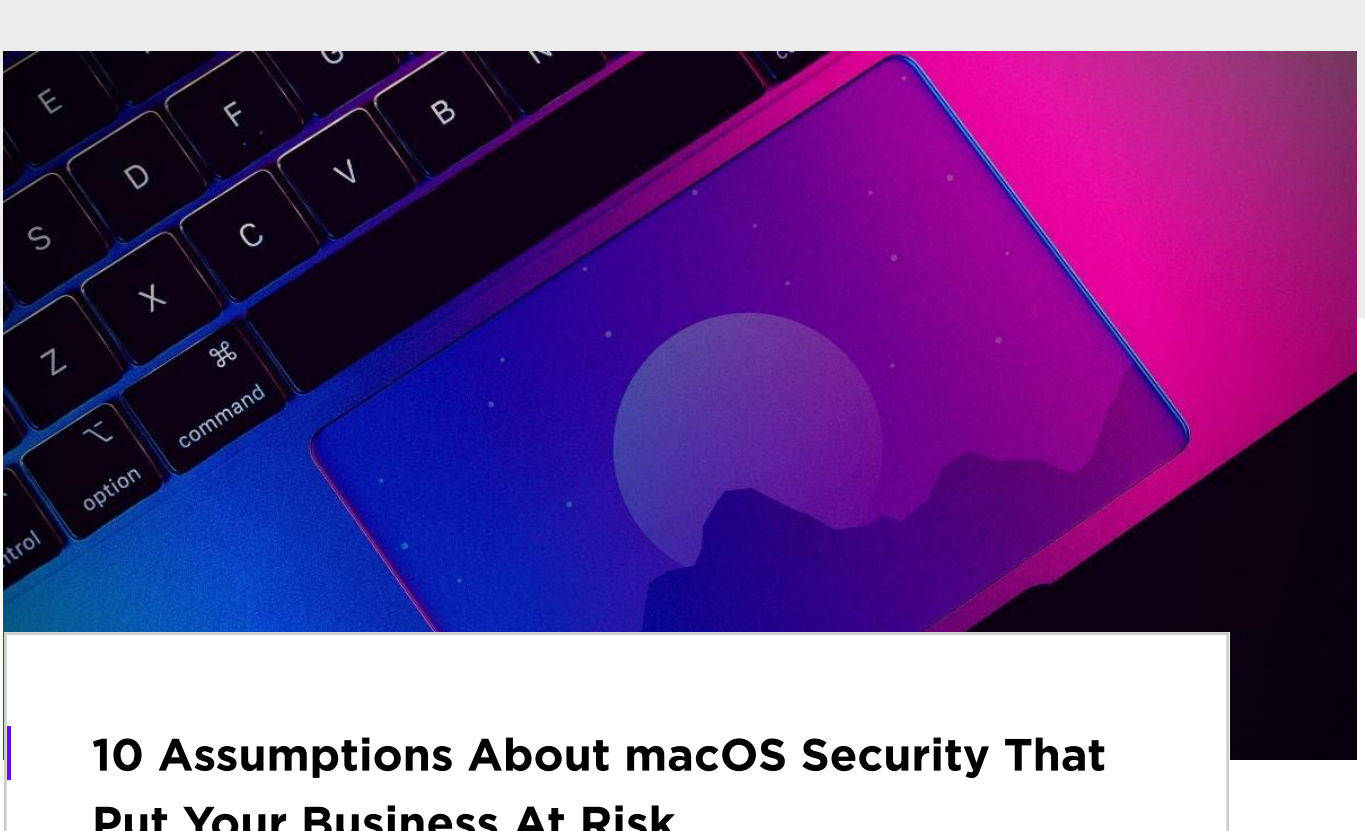
SentinelOne blog GET A DEMO



10 Assumptions About macOS Security That Put Your Business At Risk

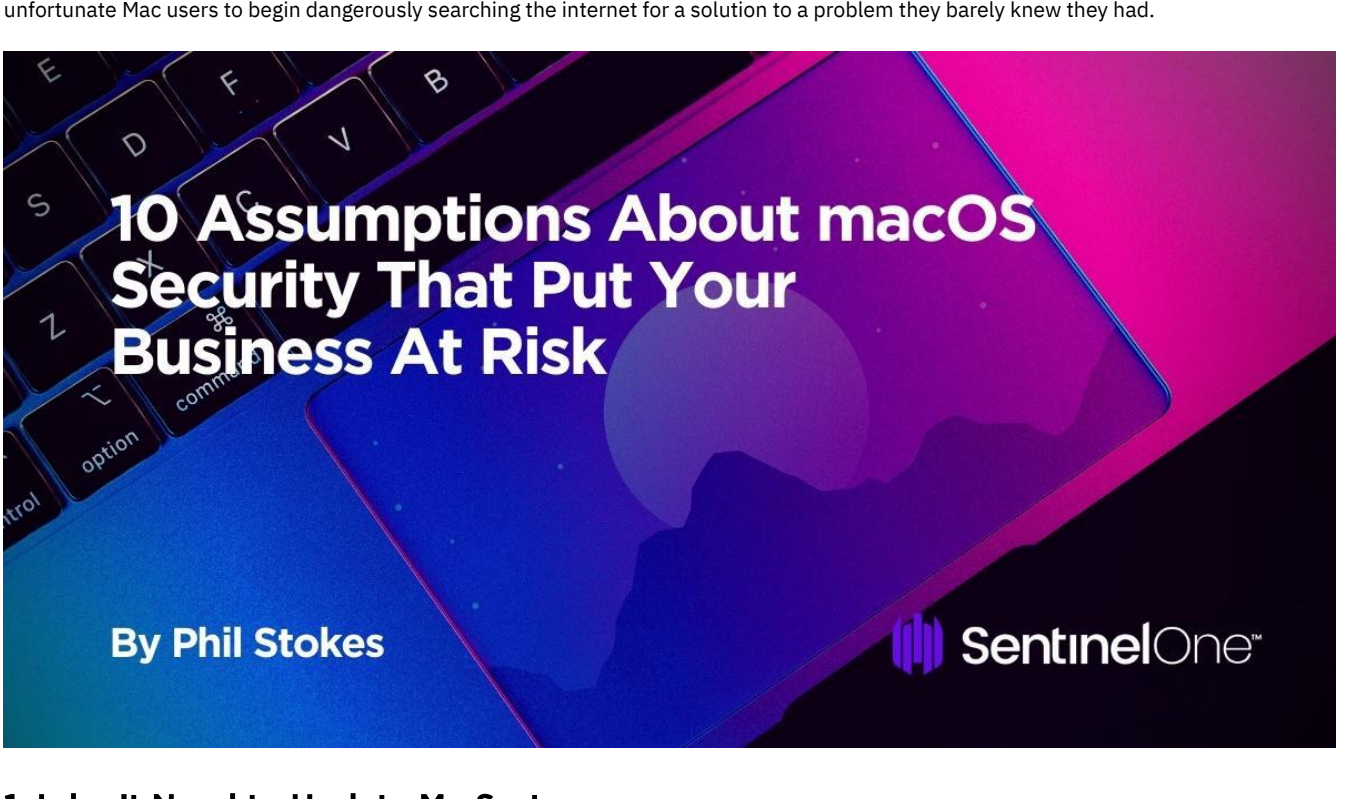
February 7, 2022
by Phil Stokes

Macs are great, aren't they? I have many. Aside from the two provided by my employer, I have five working Macs of my own, ranging from 2009 to 2021. I also run macOS on a number of virtual machines for research purposes. In fact, give me a few minutes and I could spin you up an instance of any version of macOS from 10.5.8 Leopard (circa 2008!) right through to the latest beta of macOS 12 Monterey. Yep, I'm an Apple nerd, a Mac geek, a macOS enthusiast, and I've spent over a decade now learning how Macs and macOS work. I'm also a Mac security researcher and having a catalogue of older versions of macOS is part of my arsenal of tools when it comes to understanding how to keep Macs and Mac users safe.

Most of my work nowadays revolves around identifying, tracking, and understanding Mac malware in the enterprise, and in the course of my work I inevitably come across more than my fair share of infected Macs. The users of these Macs are more often than not surprised to learn that their Mac got a dose of some nasty adware or malware.

Few ever know how the malware got on their device. Most thought that they didn't need to take any special security precautions when using a Mac. Some said that not having to run AV products was precisely the reason why they chose a Mac and ditched their previous Windows machine. All had no idea how to remove the infection, or verify that the Mac was indeed healthy after they had tried. Often, IT teams trained and tasked with ironing out problems with Windows devices are equally uncertain.

In this post, I will share with you what I have told those users and many others about macOS security. I will debunk some widely held myths about how to use and administrate Macs safely, and I will explain how you can ensure those in your organization are not the next unfortunate Mac users to begin dangerously searching the internet for a solution to a problem they barely knew they had.



1. I don't Need to Update My System

Many people believe that older versions of macOS are just as safe to run as the latest versions. While currently macOS Monterey, Big Sur and Catalina are still receiving critical security updates, anything older than that is certainly riddled with vulnerabilities.

But a bigger concern is devices that get the shiny upgrades but don't keep up with the mundane updates. From a security perspective, point updates (e.g., from Monterey 12.1 to 12.2 and so on) are far more important than OS upgrades, at least so long as you're not more than N-2 (more than two major upgrades behind the current OS). If you're still running Catalina or Big Sur, the only safe versions of those OSs are the most recent ones: 10.15.7 + the January 26 Security Update, and 11.6.3, respectively. At the time of writing, Monterey is on 12.2.

The reason point updates are far more critical is that unlike major OS upgrades, which are timed for marketing reasons and are generally built to add new (and sometimes buggy!) features, point updates are typically focused on fixing bugs and security vulnerabilities, including vulnerabilities known to be actively exploited in the wild. For example, in the recent 12.2 update, Apple patched CVE-2022-22587, of which they said they were "aware of a report that this issue may have been actively exploited". That update also addressed twelve other CVEs including:

- CVE-2022-22586 – AMD Kernel: A malicious application may be able to execute arbitrary code with kernel privileges
- CVE-2022-22584 – ColorSync: Processing a maliciously crafted file may lead to arbitrary code execution
- CVE-2022-22591 – Intel Graphics Driver: A malicious application may be able to execute arbitrary code with kernel privileges

Recently, I walked into an Apple Reseller store and noted with some surprise that, next to the Mac that was running the point-of-sale software, other staff were using what appeared to be a vintage 2012 MacBook Pro. How did I know? Because the last year Apple made a MacBook with an internal CD drive was 2012, and I could see the tell-tale slot on the side of the machine as I waited to make my purchase.

It's a testament to the longevity of Apple hardware that in 2022 a business can still use a 2012 machine for productive tasks, but it's also a potential problem. The mid-2012 MBP was released with OS X 10.8 Mountain Lion! The latest version of macOS that a mid-2012 MacBook Pro *could* run is Big Sur. I sure hope they updated to that 11.6.3 release the other week!

> Apple doesn't release point updates on a schedule like Microsoft's "Patch Tuesday". They release them when there's something urgent that needs fixing, and typically that's a security vulnerability. The bedrock of all computer security is to stay up to date with software updates. Make sure your users are updating!

2. Mac Malware is Rare

The amount of malware that is targeted at Windows machines is truly staggering. It's no wonder that every year a not-insignificant number of computer buyers turn to Macs for relief from the constant security headaches associated with Windows. While the amount of malware targeted at Macs is a small percentage of that, a small percentage of a large number can still be a large number. Relative to Windows, Mac malware is far less common, but it's a long way from 'rare'.

Last year, we saw 10 new targeted macOS malware families emerge, along with the continued expansion of adware delivery platforms like Shlayer, Bundlore, Surfbuyer, Pirrit, WizardUpdate and Adload.

In 2021, Craig Federighi – Apple's VP of Software Engineering – said that he'd "had a couple of family members who have gotten some malware on their Macs". In comments that surprised many Mac users but absolutely no security researchers, Federighi further noted that "Each week, Apple identifies a couple of pieces of malware on its own or with help of third parties" and that Apple was fighting "an endless game of whack-a-mole" and facing a "significantly larger malware problem" now than in the past.

> Listen to Craig. Funnily enough, he knows what he's talking about! Take the threat of macOS malware seriously.

3. Adware Isn't Dangerous

To those that hold this view, my first reaction is: define 'Dangerous'.

Adware is code running on your machine, often without your knowledge or consent, that fingerprints your device and collects PII about you, exfiltrates it to unknown 3rd parties and installs persistence agents, makes itself difficult to remove, and – as the name suggests – serves up unwanted adverts while you're browsing by hijacking your searches.

Adware like Adload and Shlayer typically contact obscure URLs and download unwanted software in the background without informing the user.

Some adware is akin to spyware, and some adware developers take such extreme measures to avoid detection by security software or analysis by security professionals that they could legitimately go into business teaching malware authors a few new tricks. So, what's your definition of 'dangerous'?

> Any 3rd party code that runs on your machines without the user's and/or the company's express and explicit permissions should be considered a danger to the business. From that perspective, adware is just a kind of malware and should be treated as so.

4. Apple Is All The Security You Need

Apple has worked hard to establish the reputation of "the safe Mac", but the gap between the marketing message and the reality is increasingly clear to see. It's not that Apple doesn't take security seriously – it really does, and we are always pleased to support Apple's product security team by sharing intelligence when we can. The problem is that Apple's security technologies on macOS are easily defeated, and it's worth exploring for a moment why that is the case.

Unlike iOS and Apple mobile devices, macOS and the Mac provide – and we hope always will provide – an environment where device owners are able to customize and use their computers in all sorts of novel, interesting and creative ways. The use case for a powerful computing platform is utterly different from that of a mobile device, and for that reason there is only so much Apple can do with security without falling into the trap that Microsoft has fallen into of becoming an after-sales vendor to shore up the security of its own OS.

With the Mac, Apple tread lightly. Gatekeeper, Codesigning and Notarization provide barriers to entry but they do not keep out professional adware and malware authors. On-device protection like XProtect and MRT.app also help clean up some of the main discovered malware and adware variants, but there are many that they do not. XProtect is an old-fashioned file scanning technology that needs to be updated (something Apple does silently in the background, more or less once a month or so) after new malware has already struck some hapless victims.

Crucially, it's simple for malware authors to inspect XProtect on their own machines and see how the signatures are catching their work. MRT.app is a little more obtuse to inspect, but regardless of how well Apple tries to obfuscate their signatures, there's always a simple test available to a malware author: test your malware on your Mac and if it's removed or blocked, adjust it till it isn't.

Malware authors always have direct access to the very software that Apple is using to block or remove malware. In part, notarization was supposed to help Apple get around this, but threat actors soon discovered that the automated malware service could be beaten, and the game of 'whack-a-mole', as Mr Federighi rightly described it, goes on.

> If you want to help your Macs stay secure, get some additional security!

5. I'd Know If My Mac Was Infected

One of the most overlooked weaknesses of the Mac is the paucity of end user tools it provides both for security and administration purposes. The once useful Console.app is now a no-go zone for anyone other than the most masochistic of Mac diehards; the Terminal provides some useful but obscure command line tools for examining things like running processes, listing open files and ports and gathering certain kinds of system and user data.

But – and it's a big but – none of these provide users or admins with any actual way to look at, track or identify malicious changes. None of the native tools allow a user to see what process was responsible for changing which file(s), executing which binaries, or changing what system data.

Deep-dive IR and digital forensics investigations can, sometimes, recreate certain historical chains of events, but these require expertise, time and money.

In short, the question that no Mac user can really answer without adding some 3rd party software is: how would I know if my Mac was infected by some backdoor such as SysJoker or spyware like DazzleSpy or XcodeSpy?

> For businesses, the only sensible choice is a security solution that offers deep visibility as well as advanced protection and detection.

6. My Data Is Safe On My Mac

Data privacy has become increasingly important, and increasingly targeted, in recent years as almost all of us have moved some or all of our most sensitive data onto our devices.

In line with this trend, Apple has made a number of changes to macOS to try and protect PII and other data on our Macs, but the results have been less than stellar. In the first instance, all Apple's user privacy protections are bypassed by any app that requests, and is granted by the user, Full Disk Access (FDA). Apple's default assumption is that users won't grant that permission without understanding the risks, but that's an assumption that is fatally flawed. Many common apps request this permission to function properly, and users are more interested in having the apps work than making detailed inquiries of developers about how that permission will be used or could be abused.

One app that has Full Disk Access regardless of the user's preference is Apple's own Finder. This allows a sneaky backdoor via automation that only requires a consent click (rather than a password authorization) to get past the users.

Further, in many enterprise settings, administrators will require the Terminal to have Full Disk Access. Unfortunately, there's no granularity here, so when one user grants FDA to the Terminal, it's now available to all users (and all processes).

As we've noted before, this isn't an accident or a bug, it's by design, but bugs in the same framework (aka TCC) responsible for user data privacy protection have become so common they are almost uninteresting!

> Be sure that you understand just what and what isn't protected by the operating system and under what conditions.

7. Criminals Aren't Interested in Mac Users

It's a common myth in computer security that most malware authors aren't interested in Mac users because "the market is too small" to be worth their time. After all, it is supposed, it takes a considerable investment in resources to develop, distribute and manage malware infections, and for that effort criminals want a good ROI. Consequently, it's assumed, they don't bother targeting Macs and stick to the easier pickings of Windows users.

There's plenty of fallacy to unpack here. First, the market is too small? This thinking is about 15 years out of date, or pre-iPhone's 2007 launch to be accurate. Macs may have once been the niche buy of certain kinds of 'creatives' and a few vociferous enthusiasts, but their market share has steadily increased over the last decade or so.

At first, this was off the back of iOS/macOS (or OS X as it was then) ecosystem integration, but it's long been the case that Macs have become popular in their own right for their longevity, stability and – relative to Windows – security. Developers of all stripes love them, executives love them, and this last quarter Apple reported that Mac sales alone accounted for more than $10 billion of revenue. That's a pretty healthy-sized market to attack for any malware author, just ask the developers of XLoader, XCSSET and OSAMiner.

Second, mac malware isn't particularly difficult to create. If you can create any kind of Mac app, making it do something malicious is a fairly trivial tweek (an unfortunate fact that makes macOS malware difficult to catch for certain kinds of security solutions that rely on identifying malware by file characteristics rather than behavior). Add to that that macOS malware is increasingly cross-platform – malware authors are targeting multiple platforms with the same source code written in languages like Java, Go and Kotlin – and the "heavy investment for no return" argument doesn't really hold any water.

> Sure, the most common and profitable threats found on Macs are adware, but they didn't get that way by being stopped by nothing more than 'a savvy user'.

8. Nation-States Don't Target Mac Users

Well, if the criminals looking to make a quick buck are on board, what about the APTs? As noted above, developers and execs love to buy Macs – they're powerful and chic – and they have a reputation for being secure (although we note it's Chromebooks that now enjoy the "these don't get viruses" meme).

APTs have always been busy targeting Macs just as they have any other devices used by "persons of interest". This past year, we saw not only targeted attacks against political activists but also what was very likely an espionage attack against a US business.

We also learned last month that, while most Mac malware requires some level of social engineering, there are in-the-wild exploits that can infect a Mac user who simply visits the wrong website. Both macOS.Macma and OSX.DazzleSpy were delivered by leveraging exploits to drop and execute code with privileges in a watering-hole attack. And as noted above, CVE-2022-22587, patched a few weeks ago, was an actively exploited zero-day that allowed malicious attackers to execute arbitrary code with kernel privileges. At this time, we have no idea who the targets were.

> Want to stop targeted malware? Invest in an EDR that offers agents built natively to run on Mac architectures, both Intel and arm64 (*aka* Apple silicon).

9. Apps Downloaded from the App Store are Safe

Mac App Store apps, like those from the iOS App Store, enjoy a privileged place in Apple's ecosystem. Such apps run in sandbox environments on the user's device, are vetted by Apple, and are distributed by identified developers. The vast majority are, indeed, safe, there's no questioning that. But there are, nevertheless, questions about a small minority.

App Store apps are mostly safe, but the origin of the download doesn't guarantee that you're not getting malware. Developers of legitimate App Store apps have noticed scam apps on the App Store blatantly copying legitimate apps and being boosted with fake ratings and reviews, themselves purchased in bulk from other criminals. It's been estimated that such apps could be scamming users out of $2 million a year or more.

> If Apple's built-in defenses are not going to recognize and block scams and malware, users without other defenses are left pretty much exposed.

10. The Best Security Apps Are in the App Store

If you're thinking you want some extra security solution for your Macs, the one place *not* to look is the App Store. This has nothing to do with our previous point about the dubiousness of some App Store apps, but rather the nature of what kind of apps are allowed in the App Store.

As we already said, App Store apps must be sandboxed – that's one of Apple's conditions of entry – but a good security app by definition can't operate in a sandbox environment. A sandbox is like a container that isolates an app from other apps and other data on a device. It's one of a number of techniques that can be utilized to help make certain kinds of apps safer.

However, there's no such thing as an *effective* sandboxed security app. So-called "security apps" found in the App Store have no visibility into other processes and no capability to block or remove malware (itself almost always unsandboxed) on your device. They are, by and large, at best useless, and at worst fraudulent.

If you want effective security, you need a solution that can actually protect your device against threats and offer visibility into malicious actions; in other words, you need something that runs outside of a sandbox.

> You won't find anything like that in the App Store.

Conclusion

Macs *are* great. Let's not forget that! But we can admire our Macs as great work machines without falling into the naive belief that they are some kind of impregnable fortresses that don't need any help to keep them secure against a growing crowd of threat actors.

Computer security is a moving target, and certainly in the enterprise that requires a dedicated security solution provider who is at the forefront of keeping up with the latest threats. Help your Macs – and your Mac users – to help themselves by being aware of the reality of the macOS security threatscape and being proactive in your security posture.

If you would like to see how SentinelOne can help protect your macOS devices, 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

- XCSSET Malware Update | macOS Threat Actors Prepare for Life Without Python
- Simplify Security, Streamline Workflows and Extend Protection with Singularity XDR and Zscaler
- Dealing with Cyberattacks | A Survival Guide for C-Levels & IT Owners
- Sneaky Spies and Backdoor RATs | SysJoker and DazzleSpy Malware Target macOS
- V for Ventura | How Will Upgrading to macOS 13 Impact Organizations?
- Top 10 macOS Malware Discoveries in 2022