Mac Attack: Why macOS is not as secure as you think

To attackers, whether your organization uses PCs or Macs is irrelevant. All operating systems are vulnerable and motivated attackers will eventually find a way to infiltrate. Macs, contrary to popular opinion, are not immune to malware, ransomware and other nasty threats.

While more threats may target Windows machines, adversaries have not forgotten about Macs. Look at KeRanger, the first ransomware program targeting Macs, which was detected in 2016. More recently, in May 2017 attackers hacked the popular DVD-ripping app HandBrake to spread a variant of the Proton malware. These developments come as more Macs turn up in the workplace.

Younger employees who grew up with Apple products want to use a MacBook at the office while many workers have started using their personal Macs for work tasks as part of the BYOD movement. Meanwhile, Apple has been trying to capture enterprise users by teaming up with IBM to offer business-focused iOS apps. Apple's success with enterprise mobility could make other Mac hardware, like MacBooks, an easier sell to businesses.

In reality, correlations exist between how to attack Mac and Windows machines. The same exploits that attackers use to take over Windows machines can also be used against Macs. Meanwhile, the overall macOS security landscape is still maturing. In this white paper, we'll look at the state of Mac security, explore how attackers can infiltrate Macs and talk about what this means for enterprise security.

The state of Mac security

Whether you're looking at security features included with macOS or the programs offered by outside vendors, Mac security is a work in progress. The OS contains some built-in security components, like an anti-malware tool called XProtect that uses hashes to alert users if a binary they downloaded is bad. But like all products that use hashes and signatures to detect malicious programs, attackers can easily evade XProtect. They just need to change the malware's hash (a quick and easy procedure that some applications do automatically) to make the program appear new, allowing it to slip past XProtect.

Another anti-malware tool included in macOS is GateKeeper, which carries out code signing on third-party applications before they run. In theory, GateKeeper decreases the chances that a user will run a malicious program. But GateKeeper doesn't require a binary to be signed before it executes if the execution is done from a shell. While that prevents a user from accidentally running a malicious program by executing it, it does little to stop attackers with a shell. They're capable of running whatever programs they chose.

Judging by the programs available in the App Store, Mac security is on the radar of security vendors. The top 30 paid apps include a handful of adware and malware tools. While these apps are from vendors whose names may sound unfamiliar, well-known vendors like Kaspersky are also selling Mac security tools in the store. Consumers just aren't buying them, considering that no traditional

security vendor appears in the top 100 most popular paid apps. The lack of a leading security vendor in the eyes of Mac users could mean that people have yet to hear a convincing argument on why Mac security matters.

From an attacker's perspective, these factors make Macs an appealing target. There's an OS with a growing user base that likely includes executives given the rise of Mac usage in organizations. And that user base may include people who don't think Macs require the same security protections as Windows machines, giving adversaries a sizeable, soft attack surface. Plus, the security features included in a Mac can be circumvented.

Attacking the Mac

Options abound for delivering a payload to a Mac, especially when people are factored into the security equation. As long as there are people sitting at a keyboard, there are ways for the bad guys to access a Mac. People fall for phishing emails, visit compromised websites and plug USB drives into their computers.

Attackers have multiple tools at their disposal for weaponizing the attack. Apple's decision to use Intel chips in Macs allowed hackers to port code for Windows malware to macOS, giving these programs cross-platform functionality. While this feature hasn't been leveraged as much as anticipated, Cybereason Labs discovered a Mac port of Windows adware that included functions like the ability to execute scripts and obtain root access. Called OSX.Pirrit, the adware is a Windows binary that was recompiled to be able to run on a Mac. The people behind OSX.Pirrit didn't use it to conduct malicious activity, but the incident should serve as a reminder that attackers can modify Windows threats and use them against Macs.

Third-party applications offer attackers a clear pathway into all computers, whether they're running Windows or macOS. Looking at the US-CERT's list of the top 30 CVEs used in targeted attacks shows that there are several Windows vulnerabilities that can also be used against Macs, including many in Office. For example, the JavaScript vulnerabilities and Office macro exploits that have been used against Windows machines can also impact Macs. Weaponized Office documents (opened by

unsuspecting users on their Macs) containing payloads like JavaScript or Python that run across platforms have permitted attackers to infiltrate Macs that they weren't targeting. And the Adobe Flash and the Java Runtime Environment flaws that attackers use to exploit PCs also work against Macs.

Note to enterprises: Remember that Mac security matters

The immediate takeaway for enterprises is to remember that Mac security matters. While this point may seem obvious, organizations sometimes treat their Macs as the second most vulnerable attack surface after Windows machines. In reality, all machines, regardless of what OS they run, are vulnerable. Make sure that your company's Mac users know not to click a suspicious link because a MacBook can't protect the network from ransomware. And that phishing emails land in the inboxes of both Mac and Window users.

As defenders, learn from the mistakes that were made when attempting to secure Windows endpoints and don't repeat them with Mac security. For example, remember to protect your users since they're typically the most vulnerable part of your company. But don't roll out security tools that prevent them from doing their jobs.

Next, remember that security is meant to enable business, a point that was lost in when developing Windows security programs. Security will likely take a backseat if it prevents a company from carrying out its core business. Your security program needs to reflect this principle and include Macs.

Finally, be prepared for an evolution of attacks on Macs. The tactics, techniques and procedures used to pop Windows machines are just starting to be applied to Macs. Expect more of this activity in the future as Macs make further strides in the enterprise and become a bigger target.

Having complete endpoint visibility can help counter this development. Knowing what's happening on your Macs and proactively looking for threats allows defenders to detect malicious activity as soon as it starts and prevent more serious damage from occurring.

cybereason

About Cybereason

Cybereason is the leader in endpoint protection, offering endpoint detection and response, next-generation antivirus, and managed monitoring services. Cybereason gives enterprises the upper hand over cyber adversaries. The Cybereason platform is powered by a custom-built in-memory graph, the only truly automated hunting engine anywhere. It detects behavioral patterns across every endpoint and surfaces malicious operations in an exceptionally user-friendly interface. Cybereason is privately held and headquartered in Boston with offices in London, Tel Aviv, and Tokyo.