# Apple error approves MacOS malware

September 1 2020, by Peter Grad

Credit: CC0 Public Domain

Oops. Apple, which recently stepped up efforts to guarantee malware is tracked and blocked before it can infect its Macs, has acknowledged the first breach of its notarization process.

A trojan Adobe Flash downloader made it past Apple's automated

security system designed to scan new programs for malicious content and potentially harmful code.

The malware was detected by a college student who inadvertently typed the wrong web address while working on an open source online Mac development tool. He wound up being surreptitiously redirected to a fake Adobe Flash update page. Exploring the curious misdirection, the student, Peter Dantini, downloaded the phony installer. When he ran the program, instead of its being blocked as malware by Mac defenses, the standard Mac Gatekeeper notification screen popped up, asking only if the user was sure he or she wanted to proceed with installation. Installation of third party software on a Mac always triggers Gatekeeper as a precaution. Dantini clicked yes and proceeded with installation.

The malware, Shlayer, is not new. It in fact is the most common threat to Macs, according to cybersecurity firm Kaspersky, and is believed to have infected one out of 10 Mac machines over the past two years. This is the first time Shlayer was confirmed to have bypassed Macs' notarization system.

Shlayer hides in a user's machine and can be activated by hackers to accept and execute future spyware and malware programs.

Dantini notified Patrick Wardle, a macOS security researcher, of his findings.

"I had been expecting that if someone were to abuse the notarization system it would be something more sophisticated or complex," Wardle said after confirming the malware activity. "But in a way I'm not surprised that it was adware that did it first. Adware developers are very innovative and constantly evolving, because they stand to lose a ton of money if they can't get around new defenses. And notarization is a death knell for a lot of these standard ad campaigns, because even if the users

are tricked into clicking and trying to run the software, macOS will block it now."

In its earliest years, Macs were seen as nearly invulnerable. In a well-known ad campaign Apple once boasted that a Mac computer "doesn't get PC viruses. A Mac isn't susceptible to the thousands of viruses plaguing Windows-based computers. That's thanks to built-in defenses in Mac OS X that keep you safe without any work on your part."

But those days are long gone. In fact, it was reported earlier this year that for the first time the number of malware infections on Macs is greater than on PCs.

Security specialists warn that complacency by Mac users could be risky.

"There is a rising tide of Mac threats hitting a population that still believes that 'Macs don't get viruses,'" said Thomas Reed, a contributor to Malwarebytes February security report revealing Mac malware problems are getting worse. "I still frequently encounter people who firmly believe this, and who believe that using any kind of security software is not necessary, or even harmful. This makes macOS a fertile ground for the influx of new threats, whereas it's common knowledge that Windows PCs need security software."

After Wardle contacted Apple developers, they immediately revoked programs carrying the Shlayer code. However, a new version of the trojan was detected days later. Apple again acted promptly to block the new malware, but it's clear the battle will continue.

Mac users are advised to install updates routinely and to use anti-malware programs.

**More information:** objective-see.com/blog/blog_0x4E.html