Maker of sneaky Mac adware sends security researcher cease-and-desist letters

Home Innovation Security

"If there's code that's mining data and hiding itself on a computer without any way of removing it, that's malware, plain and simple."

Written by Zack Whittaker, Writer-editor on Dec. 13, 2017

(Image: file photo)

The maker of a sneaky adware that hijacks a user's browser to serve ads is back with a new, more advanced version -- one that can gain root privileges and spy on the user's activities.

News of the updated adware dropped Tuesday in a lengthy write-up by Amit Serper, principal security researcher at Cybereason.

The adware, dubbed OSX.Pirrit, is still highly active, infecting tens of thousands of Macs, according to Serper, who has tracked the malware and its different versions for over a year.

Serper's detailed write-up is well worth the read. The short version is that the adware, built by Israeli ad-tech firm TargetingEdge, poses as a legitimate installer, like a video player or document reader. Like other software, the installer asks for the user's password to install, tricking the user into turning over root privileges to the installer.Once it's hooked into the system, the installer uses a script to download further components from the adware's command and control server. The report said that the files used to maintain the adware's persistence on the infected Mac tries to mask themselves as legitimate macOS functions to try to hide from the victim. What's new in this version is that the adware uses macOS' native scripting language, AppleScript -- typically reserved for automation -- to inject ads directly into the browser, rather than a proxy server that can be easily removed.

TargetingEdge sent cease-and-desist letters to try to prevent Serper from publishing his research.

"We've received several letters over the past two weeks," Serper told *ZDNet*. "We decided to publish anyway because we're sick of shady 'adware' companies and their threats."

He said OSX.Pirrit is "malware with a legal team."

It's not just Serper's opinion; 28 different antivirus engines identified TargetingEdge's software as malware through VirusTotal, an online malware detector.

We contacted TargetingEdge but didn't hear back from the company directly. A lawyer representing the company provided *ZDNet* with a statement denying Serper's claims.

"Our product is not malware, it does not include any features of malware and it does not harm or damage or intend [sic] to cause any damages to the product user's device, nor 'hacks.' 'spy,' or 'takes over' the browser or uses any other 'malicious' or 'non-transparent' means," the statement said. "We highly respect the privacy of our users, take great care in protecting our users' rights and privacy, and adhere to best practices as well as applicable law and privacy related legislation."

The statement also denied any link to OSX.Pirrit.

However, as Serper notes, in his previous research he linked the adware to TargetingEdge. In his latest report, though most references to the company had been removed from the code, several domain names found in the code were registered by the company. He also noted that a former employee sent his resume to Cybereason, which linked the adware to TargetingEdge.

When asked why the company sent a cease-and-desist letter, the lawyer said it "never required Mr. Serper to not publish its report."

ZDNet independently verified the contents of the cease-and-desist letter, which contradict the company's statement.

Cybereason said it "stands by our report published yesterday."

It's rare, but not unheard of for security researchers to receive legal threats relating to their work. Last year we reported that auditing and tax giant PwC sent legal threats to security researchers try to stop them from revealing a critical flaw, even though the researchers had gone through the responsible disclosure process.

Serper said that OSX.Pirrit is a "great example" of how an ad-tech company borrows nefarious tactics found in malware to make it harder for antivirus software to detect them. "There is no difference between traditional malware that steals data from its victims and adware that spies on people's Web browsing and target them with ads, especially when those ads are for either fake antivirus programs or Apple support scams."

"If there's code that's mining data and hiding itself on a computer without any way of removing it, that's malware, plain and simple," he added.

See also

Got a tip?

You can send tips securely over Signal and WhatsApp at 646-755–8849. You can also send PGP email with the fingerprint: 4D0E 92F2 E36A EC51 DAAE 5D97 CB8C 15FA EB6C EEA5.

Read now