Malware targeting Apple's M1-based computers found

February 18 2021, by Bob Yirka

Credit: CC0 Public Domain

Security researcher Patrick Wardle is claiming on his Objective-See website that he has found an instance of malware that targets Apple computers running the M1 chipset. Apple began Mac Mini, Macbook

Pro and the Macbook Air models running the new chipset late last year.

Moving to the M1 chipset was a big change for Apple—the company has been using Intel x86 based chips in its computers since 2005. When announcing the change, Apple claimed that the new chipsets would allow their computers to run faster. Unfortunately, such improvements have been slow coming. For applications to run faster on M1 based computers, they need to be rewritten—the old applications have to be run through a translator called Rosetta 2, which slows things down.

Now, it appears that malware writers are making the jump over to M1-based machines, as well. Wardle found a Safari web browser extension called GoSearch22 on an antivirus testing platform. It had been uploaded as recently as this past December. He noted that software on the platform had previously flagged x86 based-versions of the malware (all part of the Pirrit family of malware) but it had not yet discovered the M1 version. He suggests this indicates that antivirus software for the new Mac computers is likely not yet able to find and delete the malware. He also notes that the app was signed with an Apple developer ID dated to last November, which has since been revoked—without it, targeted computers would not let the malware install itself.

In looking at the malware, Wardle found it to be standard adware—once installed, it bombards the user with ads, banners, surveys and other nefarious promotions. Though not confirmed as yet, such malware also typically records IP address, search histories and site visits.

In response to the report by Wardle, *Wired* magazine is reporting that other security companies have also found malware written for M1 machines. Such reports suggest that malware developers are serious about targeting Apple computers, both old and new—a move that is not surprising, considering that Apple has increased its market share in

recent years—just 10 years ago, barely 6% of computers were from Apple. Today, that share is close to 20%.

More information: objective-see.com/blog/blog_0x62.html

Citation: Malware targeting Apple's M1-based computers found (2021, February 18) retrieved 9 April 2024 from https://techxplore.com/news/2021-02-malware-apple-m1-based.html