

Apple bans cryptocurrency mining apps on iOS to protect mobile users

Using an iPad or iPhone to mine bitcoin or other cryptocurrencies would be hard to do, as the CPU power available to complete the task would be a drop in the bucket compared to what's needed.

But using a portion of the CPU power from thousands of iPads or iPhones to mine cryptocurrency makes more sense – and that's exactly what some malware has been doing.

Apple is now moving to stop the practice.

Computerworld's Facebook page.]

[Further reading: The way blockchain-based cryptocurrencies are governed could soon change]

The company released several rules changes for developers at WWDC last week, but rolled out the modifications with no fanfare. This week, however, Apple Insider discovered a section of the company's developer guidelines under the heading Hardware Compatibility specific to the malware issue; it states that any apps, "including third party advertisements displayed within them, may not run unrelated background processes, such as cryptocurrency mining."

Though some might question the Apple edict, the decision still makes sense, according to Martha Bennett, a principal analyst at Forrester Research.

"Just like with all the cryptocurrency mining utilities you get for PCs (in the shape of apps or browser plug-ins, most of which are malware), they thrash your CPU, and if you're running on battery, which you almost invariably are on a

mobile device, they drain your battery,” Bennett said via email. “Plus, Apple won’t want to be associated with all the shady stuff that’s going on in relation to cryptocurrencies.”

Take this mobile device management course from PluralSight and learn how to secure devices in your company without degrading the user experience.]

Apple may not be the only taking that tack. While there has been no similar change yet on the Android side of things, Google is keeping the door open to the same kind of move. The company updates its user policies on a monthly basis, a spokesperson said, when asked about the possibility of a cryptocurrency mining ban.

The problem with malware that siphons CPU cycles from desktops and mobile devices for the purpose of cryptocurrency mining is relatively new but growing quickly. For example, cryptocurrency mining service Coinhive has been cited as one of the top offenders for spreading malware for its own purposes.

Coinhive uses a small piece of JavaScript that installs on websites and in advertisements; the code then hijacks a portion of the compute power of any device using a browser to visit that site. Essentially, it unwittingly enlists a device to mine Monero cryptocurrency. The practice is known as cryptojacking.

Not surprisingly, the rise of “cryptomining” malware over the past year seems to reflect the rise of cryptocurrency itself, according to antivirus vendor Trend Micro.

Trend Micro’s research data showed cryptocurrency mining has overtaken ransomware in North America. The first quarter of 2018 saw information theft malware being the most detected event in end user devices, with cryptocurrency mining close behind, a report stated.

Trend Micro

Cryptojacking malware was second only to information theft malware.

“Cryptocurrency mining presents a more furtive and passive alternative to ransomware,” a Trend Micro spokesperson wrote in an email reply. “Due to the nature of cryptocurrency mining, a single infection might not provide cybercriminals as much profit as they would from other types of malware. However, a cryptocurrency miner’s stealth and longer infection time mean less work on the attacker’s end.”

Cryptocurrencies are created through a process known as Proof of Work (PoW). PoW algorithms force computers to expend CPU power to solve complex cryptographic-based equations before they’re authorized to add data to a blockchain-based, distributed ledger; those computer nodes that complete the equations the fastest are rewarded with a portion of digital coins, such as bitcoin. The process of earning cryptocurrency through PoW is known as “mining” – as in mining bitcoin.

Garnering valuable cryptocurrencies has become so popular that people, groups and even companies have set up mining rigs and data centers with thousands of servers for the express purpose of generating bitcoin or other cryptocurrencies.

The purchase price of GPUs and ASICs has shot up as a result and some nations and cities have even restricted mining operations because of the amount of electrical power they’re using.

For a single iPhone or iPad, the CPU drain from mining could be significant, even as part of a hive mining cryptocurrencies.

“I’m not sure many users would be sophisticated enough to understand that mining takes up all of the resources on the device. And if it’s a third party installing it on devices in secret, that’s even worse for the end user and the ramifications it could have with Apple support, not to mention

all the negative social media posts,” said Jack Gold, principal analyst with J. Gold Associates.

“It makes sense to me that Apple be proactive and make sure this doesn’t become a real problem,” he said. “It will be interesting to see if others go down the same path.”