Hackers target smartphones to mine cryptocurrencies

August 22 2018, by Hélène Masquelier

Apps that surreptitiously mine cryptocurrencies can cause smartphones to overheat to the point they are damaged or destroyed, experts say

Has your smartphone suddenly slowed down, warmed up and the battery drained down for no apparent reason? If so, it may have been hijacked

to mine cryptocurrencies.

This new type of cyberattack is called "cryptojacking" by security experts.

It "consists of entrapping an internet server, a personal computer or a smartphone to install malware to mine cryptocurrencies," said Gerome Billois, an expert at the IT service management company Wavestone.

Mining is basically the process of helping verify and process transactions in a given virtual currency. In exchange miners are now and then rewarded with some of the currency themselves.

Legitimate mining operations link thousands of processors together to increase the computing power available to earn cryptocurrencies.

Mining bitcoin, ethereum, monero and other cryptocurrencies may be very profitable, but it does require considerable investments and generates huge electricity bills.

But hackers have found a cheaper option: surreptitiously exploiting the processors in smartphones.

To lure victims, hackers turn to the digital world's equivalent of the Trojan horse subterfuge of Greek mythology: inside an innocuous-looking app or programme hides a malicious one.

The popularity of games makes them attractive for hackers.

"Recently, we have discovered that a version of the popular game Bug Smasher, installed from Google Play between one and five million times, has been secretly mining the cryptocurrency monero on users' devices," said researchers at IT security firm ESET.

The phenomenon is apparently growing.

"More and more mobile applications hiding Trojan horses associated to a cryptocurrency mining programme have appeared on the platforms in the last 12 months," said David Emm, a security researcher at Kaspersky Lab, a leading supplier of computer security and anti-virus software.

"On mobiles the processing power available to criminals is less," but "there is a lot more of these devices, and therefore taking in total, they offer a greater potential," he added.

Google cleans house

But for smartphone owners, the mining is at best a nuisance, slowing down the operation of the phone and making it warm to the touch as the processor struggles to unlock cryptocurrency and accomplish other tasks.

At worst, it can damage the phone.

"On Android devices, the computational load can even lead to 'bloating' of the battery and thus to physical damage to, or destruction of, the device," said ESET.

However, "users are generally unaware" they have been cryptojacked, said Emm.

Cryptojacking affects mostly smartphones running Google's Android operating system.

Apple exercises more control over apps that can be installed on its phones, so hackers have targetted iPhones less.

But Google recently cleaned up its app store, Google Play, telling

developers that it will no longer accept apps that mine cryptocurrencies on its platform.

'Cat and mouse game'

"It is difficult to know which applications to block," said Pascal Le Digol, the country manager in France for US IT security firm WatchGuard, given that "there are new ones every day."

Moreover, as the miners try to "be as discreet as possible" the apps do not stand out immediately, he added.

There are steps to take to protect one's phone.

Besides installing an antivirus programme, it is important "to update your Android phone" to the latest version of the operating system available to it, said online fraud expert Laurent Petroque at F5 Networks.

He also noted that "people who decide to download apps from non-official sources are at more risk of inadvertantly downloading a malicious app".

Defending against cyberattacks of all kinds is "a game of cat and mouse", said Le Digol at WatchGuard.

"You need to constantly adapt to the evolution of threats."

In this case he said "the mouse made a large leap", said Le Digol, adding cryptojacking could evolve to other forms in the future to include all types of connected objects.