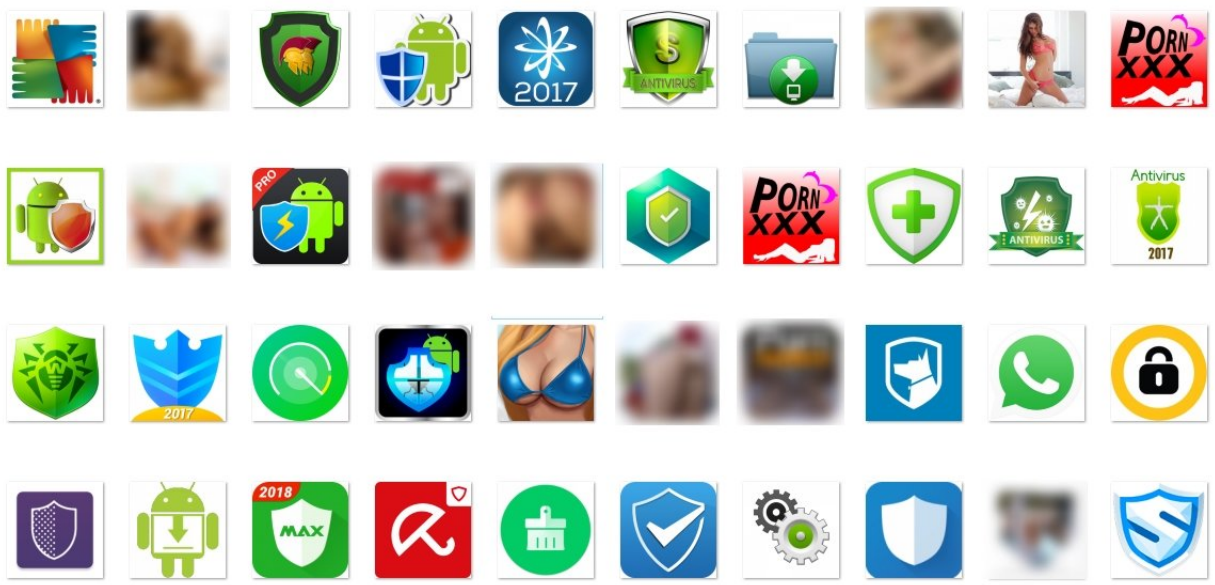
Mobile Trojan Loapi is one powerful nuisance

December 21 2017, by Nancy Owano



Credit: Kaspersky

A newly discovered malware by Kaspersky Lab researchers is so aggressive it can harm phones physically.

Numerous tech watching sites got busy this week sending signals that the malware was ruining phones, causing the phones to deform. How can that be? *Silicon UK* reported that the malware runs processor-intensive scams —running a number of different scams at once – that can cause

overheating and a deformed case.

Ashley King in *Phandroid* said after installing it on a test device the researchers saw the extra load from running a phone at 100% nearly all the time created "a warped frame and battery bulge in the infected device."

Kaspersky Lab had released a report on Trojan.AndroidOS.Loapi.

As if that feature was not enough to raise eyebrows, there was something else about Laopi.

"According to the security firm, this malware is something that it has never seen before, due to its overall capabilities, being a jack of all trades," said *Neowin*.

Ryan Whitwam, *ExtremeTech*, noticed that the malware, "has modules for just about everything, from serving up ads to mining cryptocurrency."

Kaspersky Lab: "Because of Loapi's modular structure, it can switch functions on the fly at a remote server's command, downloading and installing the necessary add-ons all by itself."

Dan Goodin, *Ars Technica*, did not find this one at all pretty. He described the malware as sending off "a litany of malicious activities, including showing an almost unending series of ads, participating in distributed denial-of-service attacks, sending text messages to any number, and silently subscribing to paid services," along with the cryptocurrency miner.

As for the cryptocurrency activity, the fact that hackers were surreptitiously mining on hijacked computers threw open-source Monero

, a type of digital currency, into the spotlight.

Why Monero?

Goodin described Monero as "less resource intensive than Bitcoin and most other cryptocurrencies." He said the module allows the malware creators to generate new coins "by leaching the electricity and hardware of infected phone owners."

"Like all cryptocurrency, networks of machines mining Monero are necessary to keep the currency functional. It takes a lot of computing power to mine Monero, but with enough phones linked together, the malware authors could earn some real cash," said Ryan Whitwam, *ExtremeTech*.

(Monero is not based on Bitcoin. It is based on the CryptoNote protocol.)

Timi Cantisano in *Neowin*: "The fact that this malware specifically mines Monero is of particular interest as it is somewhat less demanding in terms of required processing power to turn a profit compared to other cryptocurrencies."

According to a Kaspersky Lab post on Dec. 18, users might pick up the Loapi Trojan by clicking on an ad banner and downloading a fake AV or adult-content app.

"After installation, Loapi demands administrator rights—and it doesn't take no for an answer; notification after notification appears on the screen until the desperate user finally gives in and taps OK."

Advice from Kaspersky Lab included installing apps only from official stores. "Google Play has a dedicated team responsible for catching

mobile malware. Trojans do occasionally infiltrate official stores, but the chances of encountering one there are far lower than on dubious sites. Disable the installation of apps from unknown sources for added security."

More information: securelist.com/jack-of-all-trades/83470/

www.kaspersky.com/blog/loapi-trojan/20510/