Issued 12/19/17

Loapi Malware Capable of Destroying Android Phones

A new strain of malware targeting Android phones is capable of performing a plethora of malicious activities, from mining cryptocurrencies to launching DDoS attacks — and so many more malicious functions in between those extremes that it can cause the battery to bulge and destroy the phone within two days.

This malware, dubbed Loapi, has such a complicated modular architecture that Kaspersky Lab researchers called it a “jack of all trades” and unlike any malware they had seen before. It has an advertisement module, a texting module, a web crawling module, a proxy module and a module for mining Monero. Loapi also aggressively fights to protect itself. After the malicious files are downloaded and installed, the app obtains device administrator permissions by using popups. Kaspersky showed an example of a supposed security app needing the user to activate administrator permissions. After acquiring admin privileges, the app either hides its icon or pretends to do what it is supposed to be doing, such as running an antivirus scan.

When it comes to self-protection, Loapi “aggressively fights any attempts to revoke device manager permissions,” including receiving a list of apps from the C&C server that endanger the malware. If that app is installed or launched, then Loapi displays a fake message claiming to have detected malware and asks the victim to uninstall it.

The researchers showed the test Android used while analyzing the malware. It was completely trashed after two days of testing. They noted, “Because of the constant load caused by the mining module and generated traffic, the battery bulged and deformed the phone cover.”