In The Wild: Mobile Malware Implements New Features

blog.checkpoint.com/2016/06/17/in-the-wild-mobile-malware-implements-new-features/

June 17, 2016

Malware developers just won't stand still. They continue developing malware as they go, sometimes to adapt to the changing threat landscape, and sometimes simply to improve their capabilities. Recently, two examples of such advancements presented themselves, one in Triada's code and one in Viking Horde's.

Triada's Trident is Getting Stronger

As if the original malware wasn't bad enough, Triada has now received a dangerous update. Triada's main purpose is to steal money transferred over SMS messages as part of in-app purchases. The malware does so by leveraging its system level malicious compromise to highjack the raw SMS data (PDU) and send it directly to its C&C servers.

The new module introduced by the latest strain of Triada uses a similar concept to target incoming URLs. The malware is capable of leveraging root access to inject code into four browsers, including Android's default browser. Once the malware detects an incoming URL, it postpones it, and if the URL meets certain terms set by Triada it will replace it with any URL the attackers choose. The user could enter credentials in a fraudulent page, or even download additional malware, without knowing he is visiting a malicious site.

Meet the Horde: Part FOUR

No matter how far we delve into the Viking Horde malware, we find new, innovative features. Viking Horde is malware discovered last month on Google Play by the Check Point research team. It's the first of its kind malware in many areas including its primary goal of creating a botnet through which it conducts fraud.

Viking Horde’s newest technique is its ability to check running processes on Android’s latest versions (Lollipop and Marshmallow) to bypass Google’s security measures. In the past, this feature was used mainly by banker malware to monitor any activation of a banking app, upon which the malware would pop a fake overlay page.

Google has invested some efforts in preventing such activity and blocked apps from calling the getRunningTasks() API. Viking Horde manages to bypass this security measure by reading the “/proc/” file system, which displays running processes, from which the malware can find the current running processes.

Everywhere Computing Means Everywhere, Including Your Smart TV

Recently, the Flocker mobile ransomware managed to infect smart TVs as well. This is additional evidence to the ever widening phenomenon of everywhere computing. Malware is capable of propagating throughout every possible location in your network, no matter what connection you might use.

In the ransomware’s case, this is even truer. Ransomware attempts to encrypt any data it can reach. While in this case it was merely a TV set (which can be a devastating concept for some), it demonstrates how malware can cross boundaries, using your mobile device as a starting point.

Malware on your mobile device endangers not only everything on it but everything on you entire network, including computers. Users should make sure they close all possible breaches in their security, including those on mobile.

Saudi Government Job Seekers Under Attack

A recent malware campaign targets a particular sector – Saudi governmental job seekers, through a job site. The malware itself is a full-grown surveillance tool, with vast capabilities, including stealing contacts, SMS messages, and voice calls from infected devices and forwards them to the attacker’s server.

Usually, such malware is not widely spread, and target specific users through spear phishing attacks. The motive for the attack remains unclear, but the malware displays once again the full potential that exists in mobile malware.

Users face an increasing number of attacks from more and different types of malware. Malware continuously evolves and upgrades its capabilities. To stay protected, users must use security solutions that can keep them one step ahead of malware at all times.

Learn more:
Check Point Mobile Threat Prevention

See it in action:
Schedule a demo of Mobile Threat Prevention

Oren Koriat is a Mobile Information Security Analyst in the Check Point Mobile Threat Prevention Research Group. He is a technology enthusiast and a polyglot, whose expertise is in the field of Asian mobile software markets. Koriat holds a degree in linguistics from Bar Ilan University.