First Twitter-controlled Android botnet discovered

By Editor

Detected by ESET as Android/Twitoor, this malware is unique because of its resilience mechanism. Instead of being controlled by a traditional command-and-control server, it receives instructions via tweets.

24 Aug 2016 • , 2 min. read

Android/Twitoor is a backdoor capable of downloading other malware onto an infected device. It has been active for around one month. This malicious app, detected by ESET as *a variant of Android/Twitoor.A*, can't be found on any official Android app store – it probably spreads by SMS or via malicious URLs. It impersonates a porn player app or MMS application but without having their functionality.

After launching, it hides its presence on the system and checks the defined Twitter account at regular intervals for commands. Based on received commands, it can either download malicious apps or switch the C&C Twitter account to another one.

> "Using Twitter instead of command-and-control (C&C) servers is pretty innovative for an Android botnet."

"Using Twitter instead of command-and-control (C&C) servers is pretty innovative for an Android botnet," says Lukáš Štefanko, the ESET malware researcher who discovered the malicious app.

Malware that enslaves devices to form botnets needs to be able to receive updated instructions. That communication is an Achilles heel for any botnet – it may raise suspicion and, cutting the bots off is always lethal to the botnet's functioning.

Additionally, should the command-and-control (C&C) servers get seized by the authorities, it would ultimately lead to disclosing information about the entire botnet.

To make the Twitoor botnet's communication more resilient, botnet designers took various steps like encrypting their messages, using complex topologies of the C&C network – or using innovative means for communication, among them the use of social networks.

"These communication channels are hard to discover and even harder to block entirely. On the other hand, it's extremely easy for the crooks to re-direct communications to another freshly created account," explains Štefanko.

In the Windows space, Twitter, founded in 2006, was first used to control botnets as early as in 2009. Android bots have also already been found being controlled via other non-traditional means – blogs or some of the many cloud messaging systems like Google's or Baidu's – but Twitoor is the first Twitter-based bot malware, according to Štefanko.

“In the future, we can expect that the bad guys will try to make use of Facebook statuses or deploy LinkedIn and other social networks”, states ESET’s researcher.

Currently, the Twitoor trojan has been downloading several versions of mobile banking malware. However, the botnet operators can start distributing other malware, including ransomware, at any time warns Štefanko.

“Twitoor serves as another example of how cybercriminals keep on innovating their business,” Stefanko continues. “The takeaway? Internet users should keep on securing their activities with good security solutions for both computers and mobile devices.”

Hashes:

E5212D4416486AF42E7ED1F58A526AEF77BE89BE
A9891222232145581FE8D0D483EDB4B18836BCFC
AFF9F39A6CA5D68C599B30012D79DA29E2672C6E