Microsoft engineer eyeballs Android botnet

July 4 2012, by Nancy Owano

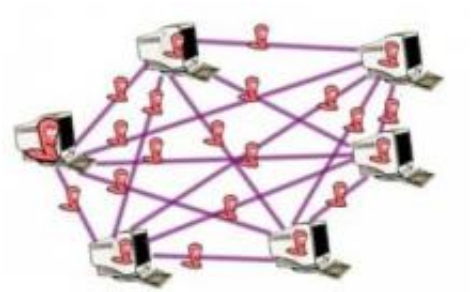

Image credit: Security Networks

(Phys.org) -- A Microsoft engineer has spotted a botnet that targets Yahoo! Mail users using Android devices. Terry Zink , who also writes an Internet security blog, said he has evidence of a botnet running on Android devices where spam e-mail messages are being sent from Yahoo mail servers on Android devices, logging into Yahoo! mail accounts and sending off spam. Zink, embarking on a tracking expedition, reported how all the messages coming from compromised Yahoo! accounts and sent through Yahoo! Mail servers, seemed to finish with “Sent from Yahoo! Mail on Android” signatures.

Zink was able to look up where the IPs were located: Chile, Indonesia, Lebanon, Oman, Philippines, Russia, Saudi Arabia, Thailand, Ukraine, and Venezuela.

Zink’s theory is that the users of those phones had downloaded a malicious Android app in order to avoid paying for a legitimate version

but they got more than they expected. “Either that or they acquired a rogue Yahoo Mail app,” he said.

A botnet is a large number of compromised computers used to generate spam, and spread viruses. The spam samples he examined from compromised Yahoo accounts all had the Message-ID:
Message-ID:
1341147286.19774.androidMobile@web140302.mail.bf1.yahoo.com

He also said they all had the same message at the bottom of their spam: “Sent from Yahoo! Mail on Android.”

Android malware is a well-known fact of digital life, and last year security firms like McAfee spoke about sharp rises in Android malware. One reason given for Android’s vulnerability is that the platform simply provides, like Windows, a big marketplace and in turn serves as a big target for intruders. Like other security bloggers offering advice, where they suggest the user takes care to use trusted application stores and avoid unknown sources for apps, Zink said, “Your odds of downloading and installing a malicious Android app is pretty low if you get it from the Android Marketplace. But if you get it from some guy in a back alley on the Internet, the odds go way up.”

Those minimizing the July 3 posting perhaps would not want to recall the news release one day earlier, on July 2, where Trend Micro said Android malware levels were rising at an alarming rate. In the first three months of the year the team identified 5,000 malicious applications designed to infect Android phones, a number which spiked more than fourfold over subsequent months. “Consumers need to use care when downloading and installing apps and should be considering installing antimalware on their mobile devices," said the release.

Last month, the Defense Advanced Research Projects Agency

(DARPA) awarded a $21.4 million contract to security firm Invincea to build security Android devices for the U.S. Army. The contract focus is to be protection of the devices against cyber-threats.

More information: blogs.msdn.com/b/tzink/archive … -android-botnet.aspx