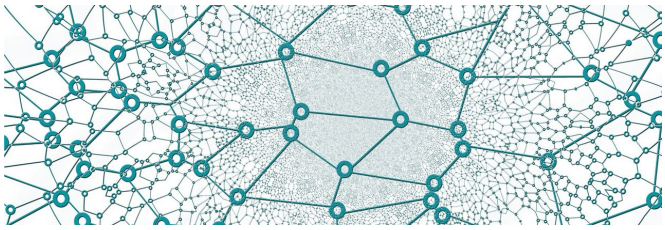
Torii makes botnet watchers look twice and think plenty about IoT security

2 October 2018, by Nancy Owano



Credit: CC0 Public Domain

A botnet of a special nature is alive and well. Type of damage? Exfiltration of information; commands and executables via "multiple layers of encrypted communication."

It is not easily comparable to other strains, and security watchers seem rather unsettled. Taking the center of attention is Torii. The botnet was spotted by Bulgarian researcher Vesselin Bontchev on September 19.

Torii is designed to work on a number of hardware systems.

Avast, a security company, had the much-quoted blog that had the details about Torii. The blog stated that it was *not* another run-of-the-mill Mirai variant. (*BleepingComputer* said it was actually "in a league superior to" Marai variants.)

Jakub Kroustek, Vladislav Iliushin, Anna Shirokova, Jan Neduchal and Martin Hron said in the blog that this was a new malware strain. Unlike other botnets, this one used techniques that they characterized as advanced and, compared against other botnets, more stealthy and persistent.

"It uses at least six methods to make sure the file remains on the device and always runs," said Ionut Ilascu in *BleepingComputer*. As the researchers discovered, the report added, "not just one method is executed – it runs all of them."

Other descriptions were on sites including *The Parallax*. The latter said hackers were caught lashing together Internet connected devices —and playing with techniques not seen before, wrote Seth Rosenblatt. They are (1) intercepting and stealing data and (2) they are using Tor and its network of anonymously linked computers for obscuring Internet traffic, he added.

Wait, what is the Tor connection? Jai Vijayan in *Dark Reading* said, "the telnet attacks through which it is being propagated have been coming from Tor exit nodes."

The blog's authors said the investigation was continuing. They said it was clear that Torii was "an example of the evolution of IoT malware." Torii could become a modular platform for future use.

The blog authors: "Even though our investigation is continuing, it is clear that Torii is an example of the evolution of IoT malware, and that its sophistication is a level above anything we have seen before. Once it infects a device, not only does it send quite a lot of information about the machine it resides on to the CnC, but by communicating with the CnC, it allows Torii authors to execute any code or deliver any payload to the infected device."

Vijayan in *Dark Reading* similarly told readers what it was optimized to do—steal data from IoT devices.

Bradley Barth, SC Media, shared email comments with his readers from Rod Soto, director of security research at JASK. Soto said poor security practices in the IoT space open the door to campaigns such as this. "As long as there are millions of these devices without strong security protections in place, there will continue to be many versions of Mirai and Torii-like botnets."

Dark Reading's article said "Torii's support for a

large number of common architectures gives it the ability to infect anything with open telnet, which includes millions of IoT devices. Worryingly, it is likely the malware authors have other attack vectors as well, but telnet is the only vector that has been used so far, Hron notes."

More information:
blog.avast.com/new-torii-botnet-threat-research

APA citation: Torii makes botnet watchers look twice and think plenty about IoT security (2018, October 2) retrieved 18 September 2021 from https://techxplore.com/news/2018-10-torii-botnet-watchers-plenty-iot.html