New Ttint IoT botnet caught exploiting two zero-days in Tenda routers

Ttint is a new form of IoT botnet that also includes remote access tools-like (RAT) features, rarely seen in these types of botnets before.

For almost a year, a threat actor has been using zero-day vulnerabilities to install malware on Tenda routers and build a so-called IoT (Internet of Things) botnet.

Named Ttint, this botnet was first detailed in a report published on Friday by Netlab, the network security division of Chinese tech giant Qihoo 360.

But unlike the myriad of IoT botnets of its kind spotted in the past, Netlab researchers said Ttint was different on several levels.

It didn't just infect devices to perform DDoS attacks, but also implemented 12 different remote access methods to the infected routers, used the routers as proxies to relay traffic, tampered with the router's firewall and DNS settings, and even gave attackers the ability to execute remote commands on the infected devices.

"Two zero-days, 12 remote access functions for the router, encrypted traffic protocol, and infrastructure [...] that that moves around. This botnet does not seem to be a very typical player," Netlab said on Friday.

Two zero-days, neither patched

According to the company's report, the botnet appears to have been deployed last year, in November 2019, when Netlab said it detected Ttint abusing its first Tenda zero-day to take over vulnerable routers.

The botnet continued to exploit this zero-day (tracked as CVE-2020-10987) until July 2020, when Sanjana Sarda, a Junior Security Analyst at Independent Security Evaluators, published a detailed report about the vulnerability and four others.

Tenda didn't release a firmware patch to address Sarda's findings, but Ttint operators didn't wait around to find out if the vendor was going to patch its bug later on.

Just a few weeks later, Netlab said it detected Ttint abusing a second zero-day in the same Tenda routers.

Netlab didn't publish details about this zero-day, fearing that other botnets would start reporting it as well; however, this wasn't patched either, even if Netlab researchers said they reached out to Tenda to inform the company.

Netlab said that any Tenda router running a firmware version between AC9 to AC18 are to be considered vulnerable. Since Ttint has been seen altering DNS settings on infected routers, most likely to redirect users to malicious sites, using one of these routers is not recommended.

Tenda routers owners who'd like to know if they're using a vulnerable router can find firmware version information in the routers' administration panel.

Based on Mirai, but also expanded

But IoT botnets that abuse zero-days and vendors that delay patches aren't a novelty, at this point, in 2020. There are other details about Ttint that caught Netlab's eye, but also the interest of Radware researchers, which ZDNet asked to review the report.

Under the hood, Ttint was built on Mirai, an IoT malware family that was leaked online in 2016. Since it was leaked online, there have been countless of botnets that have been offshoots of this original codebase.

Each botnet operator tried to innovate and add something different, but Ttint appears to have borrowed something from each to build a Mirai version more complex than anything before.

"There is nothing really new that was used by this bot that we haven't seen in other IoT or Linux malware yet," said Pascal Geenens, cybersecurity evangelist at Radware.

"That said, combining its features in new ways and introducing a C2 protocol to adapt and reconfigure the bot to create a flexible remote access tool is new for IoT malware."

"Windows RAT tools that are real Swiss Army knives have been in existence for a while. IoT never really caught up with the breadth and depth of Windows malware, except for VPNfilter and now Ttint," Geenens said.

"Ttint could mark the beginning of the maturing of general IoT malware and broader leverage in more sophisticated campaigns," the Radware security evangelist told ZDNet.

References:

- https://www.zdnet.com/article/new-ttint-iot-botnet-caught-exploiting-two-zero-days-in-tenda-routers/?&web_view=true
- https://www.cybersecurity-help.cz/blog/1610.html
- https://worldbestnews.info/new-ttint-iot-botnet-caught-exploiting-two-zero-days-in-tenda-routers/