Collaborative Takedown Kills IoT Worm ‘Satori’

eweek.com/security/collaborative-takedown-kills-iot-worm-satori

December 19, 2017

Cybersecurity

By

Robert Lemos

-

December 19, 2017

In early December, a new version of Mirai—the internet of things malware responsible for creating a massive botnet that took down internet services in October 2016—started infecting home routers.

Unlike Mirai, the latest version—dubbed Satori by security researchers—used two exploits in popular routers to compromise IoT devices and build a 700,000-node botnet in less than four days, according to Dale Drew, chief security strategist at internet infrastructure firm Level 3 Communications, now owned by CenturyLink. The attack, which mainly affected devices in Egypt and Latin America, where the specific routers were in widespread use, could have led to another major denial-of-service campaign, he said.

Instead, security researchers worked with the two largest internet service providers (ISPs) in the areas affected to block traffic to the server managing infected devices—known as a command-and-control (C2) server—and begin patching customers' routers.

"We were able to cooperate with the security research community very quickly, we got the command-and-control systems shut down very fast, and we pushed out notices to the two largest ISPs who have those modems," Drew said. "So the good news is—in very, very quick order—we were able to block scanning on our backbone."

The quick reaction and shutdown of the botnet is significant because the Satori malware automatically used any compromised router to scan and infect new systems, which qualifies the code to be a worm, according to **an analysis posted by Chinese security firm 360 Netlab** on Dec. 5. The company stated that the scanning from the worm had "gotten more intense" and noted the existence of the two exploits, one of which appeared to be a zero-day attack for a previously unknown vulnerability.

Following the ISPs blocking the command-and-control traffic, 360 Netlab noticed that the scanning dropped off significantly.

"[W]e observed the C2 sending kill scan command to the bots, and that explains why the scan activities on the two ports started to drop on a global scale," the company wrote.

Malware targeting vulnerabilities in the IoT will increasingly be a concern, said CenturyLink's Drew, because a single vulnerability can be exploited globally.

"Unlike any other device, a single exposure can be exploited across the entire vendor platform," he said. "With Windows devices, the attacker is hindered by how each individual person has customized their environment."

While the Satori attacker can no longer connect to the compromised devices, the battle between malware authors and security researchers is not over, Drew said. The creator of the Satori malware has shown a quickness to adapt, so Drew warned that the similar attacks will likely continue. Prior to Satori, the attacker created another Mirai variant that similarly exploited Huawei routers, but—taking a page from Mirai's playbook—used brute-force password guessing as another vector to exploit devices.

Yet, the system of information exchange and research collaboration worked well and holds out hope that such attacks in the future can be quickly blunted, Drew said.

"This is one of the few times that we were able to make an event a non-event," he said. "I'm very proud of the collaborative effort."