Brace yourselves: New variant of Mirai takes aim at a new crop of IoT devices

reader comments

31 with 27 posters participating

Share this story

Mirai, the virulent Internet of Things malware that delivered record-setting denial-of-service attacks in 2016, has been updated to target a new crop of devices, including two found inside enterprise networks, where bandwidth is often plentiful, researchers said on Monday.

The malware infects webcams, routers, DVRs, and other Internet-connected devices, which typically ship with default credentials and run woefully outdated versions of Linux that are rarely, if ever, updated. The rapidly spreading Mirai first made a name for itself in 2016, when it helped achieve record-setting DDoS attacks against KrebsOnSecurity and French Web host OVH.

A newly discovered variant contains a total of 27 exploits, 11 of which are new to Mirai, researchers with security firm Palo Alto Networks reported in a blog post Monday. Besides demonstrating an attempt to reinvigorate Mirai's place among powerful botnets, the new exploits signal an attempt to penetrate an arena that's largely new to Mirai. One of the 11 new exploits targets the WePresent WiPG-1000 Wireless Presentation systems, and another exploit targets LG Supersign

TVs. Both of these devices are intended for use by businesses, which typically have networks that offer larger amounts of bandwidth than Mirai's more traditional target of home consumers.

"These new features afford the botnet a large attack surface," Palo Alto Networks researcher Ruchna Nigam wrote in Monday's post, referring to the 11 new exploits. "In particular, targeting enterprise links also grants it access to larger bandwidth, ultimately resulting in greater firepower for the botnet for DDoS attacks."

Attack code exploiting a WePresent command-injection vulnerability was published in 2017, while a remote code execution exploit for LG Supersign TVs has been available since last September. By being packaged in a new Mirai variant, the exploits become much easier to be actively used to compromise vulnerable devices.

Not the first time

It's not the first time Mirai has attempted to move into enterprise networks. Last September, Palo Alto Networks reported, Mirai was found targeting the same Apache Struts vulnerability hackers exploited to breach Equifax.

"These developments underscore the importance for enterprises to be aware of the IoT devices on their network, change default passwords, [and] ensure that devices are fully up-to-date on patches," Nigam wrote. "And in the case of devices that cannot be patched, to remove those devices from the network as a last resort."

The nine other new exploits targeted vulnerabilities in a range of devices from Netgear, DLink, and Zyxel. The new variant also targets new default administrator credentials including the following previously unseen user-password combinations:

- admin:huigu309
- root:huigu309
- CRAFTSPERSON:ALC#FGU
- root:videoflow

Once the variant successfully compromises a device, the device is infected with a Mirai payload that’s unique for the hardware. The device is then made part of a botnet that can force devices to send out HTTP-based DDoS floods in lockstep. At the time Monday’s post went live, the shell script for the payload remained live, ironically on the compromised website of an unnamed “electronic security, integration, and alarm monitoring” service in Colombia.

The takeaway is that, like many botnet platforms, Mirai continues to try to increase its foothold, both by infecting a larger number of devices and moving into networks with more available bandwidth.

“IoT/Linux botnets continue to expand their attack surface, either by the incorporation of multiple exploits targeting a plethora of devices, or by adding to the list of default credentials they brute force, or both,” Nigam wrote. “In addition, targeting enterprise vulnerabilities allows them access to links with potentially larger bandwidth than consumer device links, affording them greater firepower for DDoS attacks.”

https://arstechnica.com/?p=1475511