TheMoon Illustrates Evolving Threat of IoT Botnets

CenturyLink Threat Research Labs uncovers new module of botnet targeting ISPs

MONROE, La., Jan. 31, 2019 /PRNewswire/ -- Botnets continue to find new ways to exploit the growing cache of internet-connected devices. According to new threat intelligence from CenturyLink, Inc. (NYSE: CTL), TheMoon is one of the latest examples of how far these threats have evolved. TheMoon is a modular botnet that targets vulnerabilities in routers within broadband networks. In recent months, CenturyLink Threat Research Labs discovered an undocumented module of TheMoon designed to allow the botnet to be leveraged as a service by other malicious actors.

Read the CenturyLink Threat Research Labs report on TheMoon: https://www.netformation.com/our-pov/a-new-phase-of-themoon/.

"TheMoon is a stark reminder that the threat from IoT botnets continues to evolve," said Mike Benjamin, head of CenturyLink's Threat Research Labs. "Not only does TheMoon demonstrate the ability to distribute malicious modules of differing functionality, but it's designed to function like a botnet as a service, enabling other malicious actors to use it for credential brute forcing, video advertisement fraud and general traffic obfuscation, among other uses."

Key Takeaways

- CenturyLink Threat Research Labs identified an undocumented module of TheMoon that is only deployed on MIPS devices, a common microprocessor architecture typically found in residential gateways and modems.
- TheMoon's new module turns an infected device into a SOCKS proxy, a service that can be used maliciously to circumnavigate internet filtering or obscure the source of internet traffic, allowing the botnet author to sell its proxy network as a service to others.
- CenturyLink Threat Research Labs observed a video ad fraud operator leveraging TheMoon as a proxy service, impacting 19,000 unique URLs on 2,700 unique domains from a single server over a six-hour period.
- CenturyLink blocked TheMoon infrastructure on its network to mitigate the risk to customers, in addition to notifying other network owners of potentially infected devices to help protect the internet.
- As many recent exploits have used known vulnerabilities that only worked on machines or devices that were not patched in a timely manner, CenturyLink encourages consumers to regularly update their home router firmware and to check with their ISPs to determine when their routers should be replaced.

Additional Resources

- Learn more about Mylobot's second stage attack: http://news.centurylink.com/2018-11-14-Mylobot-botnet-delivers-one-two-punch-with-Khalesi-malware.
- Find out how the Satori botnet is resurfacing with new targets: http://news.centurylink.com/2018-10-29-Satori-botnet-resurfaces-with-new-targets.
- Read the CenturyLink 2018 Threat Report: https://www.multivu.com/players/English/8085056-centurylink-2018-threat-report/.
- Discover the depth and breadth of CenturyLink's Security Services: https://www.youtube.com/watch?v=LXY1rkM7RTA.

About CenturyLink

CenturyLink (NYSE: CTL) is the second largest U.S. communications provider to global enterprise customers. With customers in more than 60 countries and an intense focus on the customer experience, CenturyLink strives to be the world's best networking company by solving customers' increased demand for reliable and secure connections. The company also serves as its customers' trusted partner, helping them manage increased network and IT complexity and providing managed network and cyber security solutions that help protect their business.

Media Contact:
Stephanie Walkenshaw
+1 720-888-3084
stephanie.walkenshaw@centurylink.com

SOURCE CenturyLink, Inc.
