Mylobot botnet delivers one-two punch with Khalesi malware

CenturyLink Threat Research Labs identifies new infection tactic by globally distributed malware

MONROE, La., Nov. 14, 2018 /**PRNewswire**/ -- With the ability to download other types of malware after infecting a computer, the Mylobot botnet is demonstrating the capability of information stealing, according to a new report from **CenturyLink, Inc.** (NYSE: CTL). Mylobot contains sophisticated anti-virtual machine and anti-sandboxing techniques to avoid detection and analysis, such as lying dormant for 14 days before attempting to contact the command and control server (C2). However, since being identified in June 2018, CenturyLink Threat Research Labs has observed Mylobot downloading Khalesi, a pervasive information-stealing malware family, as a second stage attack on infected hosts.

Read the CenturyLink Threat Research Labs report on Mylobot: https://blog.lumen.com/mylobot-continues-global-infections/.

"What makes Mylobot so dangerous is its ability to download and execute any other type of payload the attacker wants, and we now have evidence one of those payloads is Khalesi," said Mike Benjamin, head of CenturyLink's Threat Research Labs. "By analyzing global botnet attack trends and methods, CenturyLink is better able to anticipate and respond to evolving threats like Mylobot in defense of our own network and those of our customers."

Key Takeaways

- CenturyLink Threat Research Labs observed approximately 18,000 unique IPs communicating with Mylobot C2s.
- The top 10 countries where the infected IPs originated were Iraq, Iran, Argentina, Russia, Vietnam, China, India, Saudi Arabia, Chile and Egypt.
- CenturyLink blocked the Mylobot infrastructure on its network to mitigate risk to its customers and notified the providers of infected devices to help mitigate Mylobot infections.
- For enterprises that are monitoring DNS, Mylobot can be detected through the up to 60,000 domain name system (DNS) queries infected hosts perform while attempting to contact the C2.

Additional Resources

- 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=cPmySkMoHRI**.

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.

---

https://news.lumen.com/2018-11-14-Mylobot-botnet-delivers-one-two-punch-with-Khalesi-malware