Lumen Newsroom

Black Lotus Labs reveals global distribution, hiding technique of multitool botnet Necurs

MONROE, Louisiana, Feb. 28, 2019 /**PRNewswire**/ -- Furthering its dedication to helping protect the internet from malicious actors, **CenturyLink, Inc.** (NYSE:CTL) is sharing intelligence on the Necurs botnet uncovered by its new threat research and operations division, **Black Lotus Labs**.

Experience the interactive Multichannel News Release here: **https://www.multivu.com/players/English/8238355-centurylink-black-lotus-labs/**

The mission of Black Lotus Labs is to leverage CenturyLink's network visibility to help protect customers and keep the internet clean. Among the ways Black Lotus Labs does this is by tracking and disrupting botnets like Necurs, a prolific and globally dispersed spam and malware distribution botnet which has recently demonstrated a hiding technique to both avoid detection and quietly amass more bots.

Read the Black Lotus Labs report on Necurs: https://www.netformation.com/our-pov/casting-light-on-the-necurs-shadow/.

"Necurs is the multitool of botnets, evolving from operating as a spam botnet delivering banking trojans and ransomware to developing a proxy service, as well as cryptomining and DDoS capabilities," said Mike Benjamin, head of Black Lotus Labs. "What's particularly interesting is Necurs' regular cadence of going dark to avoid detection, reemerging to send new commands to infected hosts and then going dark again. This technique is one of many the reasons Necurs has been able to expand to more than half a million bots around the world."

Key Takeaways

- Beginning in May of 2018, Black Lotus Labs observed regular, sustained downtime of roughly two weeks, followed by roughly three weeks of activity for the three most active groups of bots comprising Necurs.
- Necurs' roughly 570,000 bots are distributed globally, with about half located in the following countries, in order of prevalence: India, Indonesia, Vietnam, Turkey and Iran.
- Necurs uses a domain generation algorithm (DGA) to obfuscate its operations and avoid takedown. However, DGA is a double-edged sword: because the DGA domains Necurs will use are known in advance, security researchers can use methods like sinkholing DGA domains and analyzing DNS and network traffic to enumerate bots and command and control (C2) infrastructure.
- CenturyLink took steps to mitigate the risk of Necurs to customers, in addition to notifying other network owners of potentially infected devices to help protect the internet.

Additional Resources

- Discover how TheMoon has evolved into a proxy as a service: **http://news.centurylink.com/2019-01-31-TheMoon-Illustrates-Evolving-Threat-of-IoT-Botnets**.
- 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**.

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.

Logo - **https://mma.prnewswire.com/media/134213/centurylink_logo.jpg**

For further information: Stephanie Walkenshaw, +1 720-888-3084, stephanie.walkenshaw@centurylink.com

---

Additional assets available online: **(1)**

https://news.lumen.com/2019-02-28-CenturyLink-Announces-New-Threat-Research-and-Operations-Arm-Black-Lotus-Labs,2