Black Lotus Labs Identifies Tiering Structure of Pervasive Botnet

How Spam Botnet Emotet Hides and Spreads

MONROE, La., June 18, 2019 /PRNewswire/ -- New intelligence from Black Lotus Labs reveals undocumented tactics spam botnet Emotet uses to hide and spread, while its operators have shifted their focus to offering its botnet as a service to other bad actors.

Read the Black Lotus Labs Emotet Blog:
http://www.centurylink.com/business/enterprise/blog/thinkgig/emotet-illuminated-mapping-a-tiered-botnet-using-global-network-forensics/

Through a complex and tiered command and control (C2) infrastructure, this globally distributed botnet is one of the most prolific spam botnets in operation today. Emotet demonstrates the ongoing evolution of botnet operators and the network of infected devices they rely on to conduct criminal activities on the internet. Black Lotus Labs is the threat and research operations arm of CenturyLink, Inc. (NYSE: CTL).

Part of the danger of Emotet is how pervasive it is. "Over the past six months, we have, on average, identified 40,000 unique Emotet bots daily," said Mike Benjamin, Head of Black Lotus Labs. Through our network visibility and advanced analysis, CenturyLink can identify and respond to sophisticated threats like Emotet.

Key Takeaways:

- Emotet's command structure has evolved to using infected endpoints (bots) as another layer of hierarchy. These Bot C2s have represented 80% of C2s in 2019.
- Over the last 30 days, more than 17,000 unique bot IP addresses associated with Emotet C2s were also associated with Trickbot C2s.
- Using network analysis, Black Lotus Labs can observe as Emotet botnets change to new C2s, sometimes even before they are distributed.
- During the month of May 2019 alone, Black Lotus Labs identified and validated 310 unique C2 IP addresses.
- By emulating the protocol to validate the Emotet C2, Black Lotus labs identified Emotet C2s seven days faster than other sources.
- Due to Emotet's rapidly changing and complex infrastructure, Black Lotus Labs continues to work with industry peers to keep up to date with and protect our customers from this threat.

Additional Resources

- Learn more about Black Lotus Labs: https://centurylink.com/blacklotuslabs
- See how Black Lotus Labs cast light on the Necurs shadow: https://netformation.com/our-pov/casting-light-on-the-necurs-shadow/
- Explore why CenturyLink was positioned in the Visionaries Quadrant in the 2019 Gartner Magic Quadrant for Managed Security Services, Worldwide https://www.msspalert.com/cybersecurity-research/gartner-magic-quadrant-managed-security-services-list/

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.

SOURCE CenturyLink, Inc.

For further information: Kerry Zimmer, Kerry.zimmer@centurylink.com, (509) 720-4441

Additional assets available online: Photos (1)

http://news.centurylink.com/2019-06-18-Black-Lotus-Labs-identifies-tiering-structure-of-pervasive-botnet