NEWS RELEASE

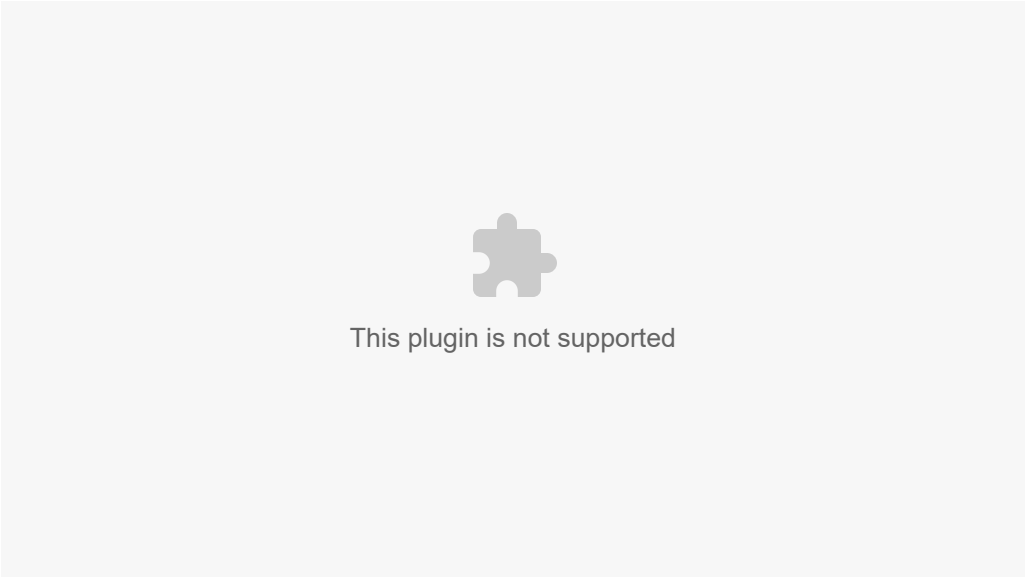
The Army of Network-Based Threats Continues to Advance

2019-09-12

CenturyLink Threat Report Reveals Top Attacks and How to Protect Your Network

MONROE, La., Sept. 12, 2019 /PRNewswire/ -- Cyberthreats are escalating faster than many organizations can identify, block and mitigate them. Visibility into the expanding threat landscape is imperative, but according to a new threat report released by CenturyLink, Inc. (NYSE: CTL), it is even more essential to act.

Experience the interactive Multichannel News Release here: **https://www.multivu.com/players/English/8524352-centurylink-2019-threat-report/**



Read the 2019 Threat Report: https://www.centurylink.com/asset/business/enterprise/report/2019-threat-research-report.pdf

"As companies focus on digital innovation, they are entering a world of unprecedented threat and risk," said Mike

Benjamin, head of CenturyLink's threat research and operations division, **Black Lotus Labs**. "Threats continue to evolve, as do bad actors. Well-financed nation-states and focused criminal groups have replaced the lone-wolf troublemaker and less sophisticated attackers motivated by chatroom fame. Thankfully, through our actionable insights, we can defend our network and those of our customers against these evolving threats."

Observations:

- **Botnets:** These rogue networks of infected computers continue to be successful because of the ease with which they compromise their targets and their ability to be operated remotely and covertly. Botnets like Necurs, Emotet and TheMoon have demonstrated evolutions in both complexity and resiliency. Malware families like Gafgyt and Mirai are also ongoing concerns given their target of IoT devices.
- **DNS:** Domain Name Server (DNS) is often overlooked as a potential attack vector. However, we have seen a rise in DNS-based attacks, such as DNS tunneling. A DNS tunneling attack can be used to encode data in the sub domains of a DNS query or response, allowing unabated network access to extract data, subvert security controls or send arbitrary traffic. Over one recent multi-week period, Black Lotus Labs detected an average of 250 domains per day being abused, representing over 70,000 lookups to each domain.
- **DDoS:** Distributed Denial of Service (DDoS) attacks continue to cause service delays and take businesses offline. While we observed ongoing progressions in attack sizes, we also detected an increase in burst attacks, lasting a minute or less. Over the first half of the year, CenturyLink's Security Operations Center (SOC) mitigated over 14,000 DDoS attacks against customers. A point of interest to note, of the top 100 largest attacks, in the first half of the year, 89 percent were multi-vector.
- **Geography:** Geographies with growing IT networks and infrastructure continue to be the primary source for cybercriminal activity. The top five countries most under attack in the first half of 2019 were: The United States, China, India, Russia and Vietnam. While the United States, China and Russia have appeared on the list year-over-year, India and Vietnam are new to the top five. Most C2 attacks in the first half of 2019 targeted the United States, China, Russia, Netherlands and Mexico. Netherlands and Mexico are new additions to the top five.

Facts:

Daily, over 139 billion NetFlow sessions and 771 million DNS queries are ingested by various machine learning threat intelligence models developed by Black Lotus Labs. From January to June 2019, Black Lotus Labs:

- Monitored for 1.2 million unique threats daily, representing 15 million distinct malicious hosts.
- Validated 4,120 new C2s, which equates to about 686 C2s per month.
- Tracked 3.8 million unique threats per month. These threats are correlated against CenturyLink NetFlow and DNS metadata to alert customers to a potential compromise.

CenturyLink is serious about doing its part to help protect the internet, including disrupting the work of bad actors and providing insights and recommendations for enterprise defenders to safeguard their networks. Here are some things to consider:

- Embed security directly into network layers to help create more agile threat mitigation.
- Identify the right solution for your business, taking into consideration where you can expertly architect security controls and where you need an outside partner.
- Close the gap, collaborate on ways to build security into every product and solution so security is not an afterthought.
- Evaluate what constitutes a trusted network environment and practice good cyber hygiene.

About CenturyLink

CenturyLink (NYSE: CTL) is a technology leader delivering hybrid networking, cloud connectivity, and security solutions to customers around the world. Through its extensive global fiber network, CenturyLink provides secure and reliable services to meet the growing digital demands of businesses and consumers. CenturyLink strives to be the trusted connection to the networked world and is focused on delivering technology that enhances the customer experience. Learn more at **http://news.centurylink.com/**.

View original content:**http://www.prnewswire.com/news-releases/the-army-of-network-based-threats-continues-to-advance-300916558.html**

SOURCE CenturyLink, Inc.