

# Machine Learning is Helping to Combat Cyberthreats

## CenturyLink's Black Lotus Labs Shows Importance of DNS Monitoring

MONROE, La., Sept. 5, 2019 /[PRNewswire](#)/ -- Domain Name Server (DNS) tunneling remains a popular method used for cyberattacks because too many organizations allow DNS traffic to go unmonitored. In a new blog, technology leader CenturyLink (NYSE: CTL) shares insights from its threat research and operations team, [Black Lotus Labs](#), about the security risk posed by lax attitudes toward DNS monitoring.

Among the dangers of DNS tunneling is it can be used to encode data in subdomains of a DNS query or response, allowing unabated network access to extract data, subvert security controls or send arbitrary traffic. On average, Black Lotus Labs monitors 771 million DNS queries globally each day for tunneling activity and other potentially malicious behavior. The team uses machine learning techniques to flag suspicious domains, evaluate them and protect CenturyLink and its customers against them. Left undetected, this covert channel for communication can cause significant impact to businesses.

**Read the blog: [Ismdoor Malware Continues to Make Use of DNS Tunneling](#)**

"CenturyLink operates one of the largest DNS resolution services on the internet. This gives us the unique ability to identify and enumerate malicious infrastructure changes as they propagate," said Mike Benjamin, head, Black Lotus Labs. "The concern is, not enough is being done to monitor DNS queries so we hope this information helps to bring awareness of the risk to more people."

### Steps to Subvert This Popular Attack Method:

- Implement protocols to monitor DNS traffic and logs for anomalies that may indicate malicious use of DNS
- Embed security in the network and leverage an agile threat environment that includes the ability to automatically terminate malicious queries
- Evaluate what constitutes a trusted network environment and practice good cyber hygiene

### Additional Resources:

- [7 Questions to Ask a Potential DDoS Mitigation Provider](#)
- [Putting Your Security in the Right Hands](#)

## 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/>.

### Media Relations Contact:

D. Nikki Wheeler

[Nikki.Wheeler@CenturyLink.com](mailto:Nikki.Wheeler@CenturyLink.com)

+1 720-888-0560

### Investor Relations Contact:

Mark Stoutenberg

[Mark.Stoutenberg@CenturyLink.com](mailto:Mark.Stoutenberg@CenturyLink.com)

+1 720-888-1662

SOURCE CenturyLink, Inc.

---

<https://news.lumen.com/2019-09-05-Machine-Learning-is-Helping-to-Combat-Cyberthreats>