New research looks at DDoS attacks that passed through Lumen scrubbing centers

Report includes a new blog that tracks attack methods recently used against Belgian government network

DENVER, May 19, 2021 /**PRNewswire**/ -- Distributed Denial of Service (DDoS) attacks continue to evolve in complexity, frequency and scale. **Lumen Technologies** (NYSE: LUMN) tracks and mitigates these threats – including the Gafgyt and Mirai botnet families – and today the company released its quarterly DDoS report for Q1 2021. This research provides a view of the DDoS landscape with findings that both reinforce and expand on these trends.

Experience the interactive Multichannel News Release here: **https://www.multivu.com/players/English/85243512-lumen-quarterly-ddos-report-q1-2021/**

To create the report, the security team at Lumen looked at intelligence from **Black Lotus Labs** – the company's threat research arm – and attack trends from the **Lumen DDoS Mitigation Service** platform, which integrates countermeasures directly into the company's extensive and deeply peered global network.

"As organizations' dependency on applications to generate revenue deepens, many are realizing they can no longer risk foregoing essential DDoS defenses. The information in this report is more evidence of that," said Mike Benjamin, Lumen vice president of security and Black Lotus Labs. "As IoT DDoS botnets continue to evolve, Lumen is focused on leveraging our visibility to identify and disrupt malicious infrastructure."

Key Findings:

The attack sizes in the DDoS report convey the largest attacks scrubbed by Lumen global DDoS scrubbing infrastructure, rather than the largest attacks observed transiting the Lumen network.

IoT Botnets:

- Well-known IoT botnets like Gafgyt and Mirai remain serious DDoS threats, with 700 active Command and Control servers (C2s) attacking 28,000 unique victims combined.
- Lumen tracked nearly 3,000 DDoS C2s globally in Q1. The most were hosted in Serbia (1,260), followed by the United States (380) and China (373).
- Of the most active global C2s that Lumen observed issuing attack commands, the United

States had the most (163), followed by the Netherlands (73) and Germany (70).
- Lumen tracked more than 160,000 global DDoS botnet hosts. Nearly 42,000 were in the United States – the most of any country.

DDoS Attack Trends

- The largest attack Lumen measured by bandwidth scrubbed was 268 Gbps; the largest attack measured by packet rate scrubbed was 26 Mpps.
- The longest DDoS attack period Lumen mitigated for an individual customer lasted almost two weeks.
- Multi-vector mitigations represented 41% of all DDoS mitigations, with the most common using a DNS query flood combined with a TCP SYN flood.
- The top three industries targeted in the 500 largest attacks in 1Q21 were: Finance, Software and Technology, and Government.

Tracking User Diagram Protocol (UDP) Reflectors

- One of the key tools in the hands of cybercriminals seeking to increase the bandwidth of their attacks is UDP-based reflection leveraging services such as Memcached, CLDAP and DNS.
- Through this process, an attacker spoofs a source IP, then uses an intermediary server – a reflector – to send massive response packets to the victim's IP rather than back to the attacker.
- Black Lotus Labs leverages the visibility from its extensive global network to identify services potentially being leveraged to launch these types of attacks.
- Based on data from 1Q21, Black Lotus Labs sees Memcached, CLDAP and DNS services being actively exploited today.
- For a more detailed look at UDP reflectors, read the latest Black Lotus Labs blog: **Tracking UDP Reflectors for a Safer Internet**.

Additional Resources:

- Read the full **Q1 2021 DDoS report**.
- See a summary of the DDoS report data in **this infographic**.
- Go deeper into **UPD-based reflectors** in the latest blog from Black Lotus Labs.
- Read more about Lumen **DDoS Mitigation Service**.
- Learn how organizations currently under attack can **turn up DDoS mitigation** in minutes with Lumen DDoS Hyper.

About Lumen Technologies:

Lumen is guided by our belief that humanity is at its best when technology advances the way we

live and work. With approximately 450,000 route fiber miles and serving customers in more than 60 countries, we deliver the fastest, most secure platform for applications and data to help businesses, government and communities deliver amazing experiences. Learn more about the Lumen network, edge cloud, security, communication and collaboration solutions and our purpose to further human progress through technology at **news.lumen.com/home**, LinkedIn: /lumentechnologies, Twitter: @lumentechco, Facebook: /lumentechnologies, Instagram: @lumentechnologies and YouTube: /lumentechnologies. Lumen and Lumen Technologies are registered trademarks of Lumen Technologies LLC in the United States. Lumen Technologies LLC is a wholly owned affiliate of Lumen Technologies Inc.

SOURCE Lumen Technologies

For further information: Suzanne K. Dawe, Lumen Public Relations, Connected Security | Black Lotus Labs, 720.217.5476, suzanne.dawe@lumen.com

---

Additional assets available online: **Photos (3)** **Video (1)**

https://news.lumen.com/2021-05-19-New-research-looks-at-DDoS-attacks-that-passed-through-Lumen-scrubbing-centers