

Lumen Q3 DDoS research reveals increases in quantity, size and complexity of attacks

2021-11-16

Latest report includes troubling insights, plus strategies for mitigating attacks

DENVER, Nov. 16, 2021 /PRNewswire/ -- Data from the Lumen Technologies **Q3 DDoS Report**, released today, reveals that three fundamental metrics – quantity, size and complexity of DDoS attacks – all increased in the third quarter of 2021.

Attacks are evolving to use more complex methods, and to target atypical services such as voice.

Key Findings from the Report

To compile these findings, the security team at Lumen analyzed 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.

To read the full report, visit: tinyurl.com/ykmm2dsz

DDoS Attack Trends

- Lumen mitigated 35% more attacks in **Q3** than in **Q2**.
- The largest bandwidth attack scrubbed in Q3 was 612 Gbps – a 49% increase over Q2 – and the largest packet rate-based attack scrubbed was 252 Mpps – a 91% increase.
- The longest DDoS attack period Lumen mitigated for an individual customer lasted 14 days.
- For the first time, 28% of multi-vector mitigations involved a complex combination of four different attack types, including DNS amplification, TCP RST, TCP SYN-ACK amplification and UDP amplification.
- Like Q2, the top two verticals targeted in the 500 largest attacks in Q3 were Telecom and Software/Technology; the Retail vertical, which did not make the top 3 in Q2, was the third most attacked

industry in Q3.

IoT DDoS Botnets

- Although Lumen observed a 26% decrease in unique C2s for Gafgyt and Mirai – two predominant IoT botnet families it continually monitors – the company observed more than 217,000 DDoS botnet hosts globally. This represents a 45% increase over Q2 and the most seen all year.
- Lumen tracked more than 2,100 C2s globally. The countries with the most C2s were (in order): China, United States and, tied for third, Taiwan and the Netherlands.

Mark Dehus, Lumen director of information security and threat intelligence, shares what companies can do to protect themselves. "DDoS attacks are rampant, and the frequency doesn't seem to be slowing down," Dehus said. "If anything, attacks are evolving to use more complex methods, and are being aimed at services such as voice that have not typically been targets in recent years."

"At Lumen, we partner with industry trust groups to track attacks back to their original sources and proactively block nefarious traffic whenever possible. We want businesses to join the fight to protect themselves," Dehus added. "First, have a solid strategy in place to address all potential security issues. Second, work with an established DDoS mitigation partner – particularly one that has an ability to track DDoS botnets and find new sources before they launch an attack. Also look for a provider that offers application security services like Web Application Firewall and Botnet Management. And finally, if you find yourself under attack, look for a solution like Lumen DDoS Hyper, which enables you to turn up service in about 15 minutes and be in a position to enable mitigation."

Attack sizes in the Lumen Q3 DDoS Report convey the largest attacks scrubbed by Lumen global DDoS scrubbing infrastructure, rather than the largest attacks observed transiting or being scrubbed by the Lumen network. To learn more about Lumen's methodology and the detailed data used to create this report, please see the full **Q3 DDoS Report**.

Additional Resources: _

- Read the **full Q3 DDoS report**.
- For results from previous quarters, see the reports from **Q2 2021** and **Q1 2021**.
- Take a deeper dive into **Ransom DDoS** and the tracking of reflectors used in DDoS attacks.
- Read more about Lumen **DDoS Mitigation and Application Security Services**.
- 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: /lumentechologies, Twitter: @lumentechco, Facebook: /lumentechologies, Instagram: @lumentechologies and YouTube: /lumentechologies. Lumen and Lumen Technologies are registered trademarks.

View original content to download multimedia:<https://www.prnewswire.com/news-releases/lumen-q3-ddos-research-reveals-increases-in-quantity-size-and-complexity-of-attacks-301424765.html>

SOURCE Lumen Technologies