NEWS RELEASE

Lumen Q3 DDoS report: Banking was the most targeted industry for the first time

2023-10-26

After mitigating targeted DDoS attacks against a major bank, Lumen urges implementation of comprehensive DDoS mitigation

DENVER, Oct. 26, 2023 /PRNewswire/ -- New data from the **Lumen Technologies** (NYSE: LUMN) Distributed Denial of Service (DDoS) mitigation platform landed the banking industry in the unenviable position of being the most targeted vertical of Q3 2023. This is the first time the banking industry topped Lumen's "most targeted verticals" list and was largely due to the events of a single day: Sept. 21, 2023.

> For the first time ever, banking was the most-targeted industry for both DDoS and application-layer attacks in Q3 2023.

On that day, a single banking customer was targeted with more than 230 DDoS attacks – a whopping 4,500% increase over the daily average for that industry – yet it experienced no downtime. Had the attackers been successful, they could have caused significant damage in the form of lost business, remediation costs and reputational damage.

"The successful mitigations for this banking customer can be traced back to Lumen's multi-layered approach to DDoS mitigation," said Brett Lemarinel, director of unified threat management for Lumen. "It starts at our network, where countermeasures are built in, and our intelligent routing technology, which sends excess traffic through our 500+ scrubbing locations. Our DDoS customers have an added layer of protection from Rapid Threat Defense, our proprietary capability that utilizes threat intelligence from Lumen Black Lotus Labs® to block DDoS botnet traffic before it reaches the customer's environment."

Read the Lumen Q3 2023 DDoS and Application Threat Report for the latest stats.

Lemarinel continued, "This should be a warning to all other businesses. More than 230 mitigations in a single day

suggests the threat actor was determined to wreak havoc on this customer. Even though the attacker failed, the activity we saw on Sept. 21 is a potent reminder that any business can be in an attacker's crosshairs on any given day."

Other notable findings in the report include:

- A never-before-seen, four-vector combination was attempted during the Sept. 21 event.
    - The four-vector combination included DNS Amplification, IP Fragmentation, Invalid Packets and Static Filtering. Cyber attackers frequently modify their vector combinations as they attempt to defeat mitigation strategies, but the Lumen DDoS mitigation platform has the flexibility required to recognize and stop these attacks before they impact the targeted customers.
- The total number of attacks decreased in Q3 2023.
    - Attackers frequently run their operations like a business and, as with any business, cyberattacks have seasonal ups and downs. In Q3 2023, Lumen mitigated 4,217 attacks, which was a 23% quarter-over-quarter decrease and a 24% annual decrease.
- The banking industry was also the most-targeted vertical for application threats, according to Lumen's application protection partner, ThreatX.
    - Among all industries, the highest percentage of blocked traffic (25.5%) came from programmatic access, which are suspicious, automated attempts to access a web application. This number is up 89% from the previous quarter.
    - The banking sector experienced a significant percentage of "Attacks Against Authentication" (nearly 25%), which are used to gain unauthorized access to financial data.
    - Financial institutions are attractive to attackers, as evidenced by the high attack ratio and combination of brute-force attacks that targeted banks in Q3. Protecting financial data is paramount, but robust web application and API protection solutions can help protect the industry.

"The Q3 ThreatX application attack analysis underscores the critical importance of bot protection and the need for awareness of industry-specific threats," said Neil Weitzel, director, Security Operations Center at ThreatX. "The especially high number of programmatic access threats this quarter underscores the prevalence of bots in API and application attacks. In addition, our findings reveal variations in threats across industries, so businesses must stay vigilant and proactive to safeguard their applications and APIs."

Additional resources

- Read the full **Q3 2023 DDoS and Application Threat Report**.
- See how Lumen and ThreatX **combine** to offer API and Application Protection.

- Calculate the potential cost of a DDoS attack using the **Lumen DDoS Calculator**.
- See how **Lumen Rapid Threat Defense** uses global threat intelligence from **Black Lotus Labs®** as a countermeasure to block DDoS bots on the network as traffic hits a scrubbing center.
- Visit the Lumen Quarterly DDoS report **archive**.
- Learn about Lumen's comprehensive **DDoS mitigation** and **Next-gen WAF/WAAP** services.

About Lumen Technologies

Lumen connects the world. We are igniting business growth by connecting people, data, and applications – quickly, securely, and effortlessly. Everything we do at Lumen takes advantage of our network strength. From metro connectivity to long-haul data transport to our edge cloud, security, and managed service capabilities, we meet our customers' needs today and as they build for tomorrow. For news and insights visit **news.lumen.com**, LinkedIn: /lumentechnologies, Twitter: @lumentechco, Facebook: /lumentechnologies, Instagram: @lumentechnologies, and YouTube: /lumentechnologies.

About ThreatX

ThreatX is managed API and application protection that lets you secure them with confidence, not complexity. It blocks botnets and advanced attacks in real time, letting enterprises keep attackers at bay without lifting a finger. Trusted by companies in every industry across the globe, ThreatX profiles attackers and blocks advanced risks to protect APIs and applications 24/7. Learn more at **https://www.threatx.com**.

View original content to download multimedia:**https://www.prnewswire.com/news-releases/lumen-q3-ddos-report-banking-was-the-most-targeted-industry-for-the-first-time-301968096.html**

SOURCE Lumen Technologies