Lumen research reveals a rise in sophisticated, complex DDoS attacks in Q1 2023

Quarterly DDoS report expanded to include data from API and application protection partner ThreatX

DENVER, April 25, 2023 /**PRNewswire**/ -- **Lumen Technologies**® (NYSE: LUMN) today released its latest **report** detailing Distributed Denial of Service (DDoS) mitigations in Q1 2023. For the first time, the report also includes Q1 data from Lumen's API and application protection partner, **ThreatX**. The combined report – which examines DDoS attacks that Lumen mitigated for its customers and application requests that ThreatX blocked for its customers – provides a more holistic view of the overall threat landscape.

Read the Lumen Q1 2023 DDoS and Application Threat Report, and visit us at RSA (booth 2145-S) to hear Lumen experts talk about research findings during an in-booth "lightning talk."

"The pace at which companies and other organizations have been expanding their digital footprints has increased over the past few years," said Peter Brecl, Lumen's director of product management for DDoS mitigation and application protection. "The larger attack surface creates more opportunities for threat actors to launch attacks. The only way to protect that digital presence is to deploy a holistic solution that includes network protection, application-layer protection, and application acceleration capabilities. This type of comprehensive coverage – including DDoS mitigation, API protections, Web Application Firewalls and Bot Risk Management – helps ensure that critical business functions stay up and running – even when under an active attack."

Notable Findings: Complex Attacks on the Rise

- **Domain Name System (DNS) water torture attacks**
  - Twenty six percent of all single-vector attacks in Q1 utilized DNS amplification – a 417% increase over the same quarter last year. Of these, a sophisticated form of DNS amplification known as a "DNS water torture attack" was the most common.
  - DNS water torture is a complex attack vector designed to overwhelm the resources of an authoritative DNS server and prevent it from responding to valid DNS queries. A comprehensive DDoS mitigation solution is necessary to defend against DNS water torture attacks.

- **Complex, multi-vector mitigations**
    - Multi-vector attacks are not new, and threat actors deploy different combinations of vectors because they are more difficult to mitigate. In Q1, Lumen mitigated an attack that utilized a record *six different vectors* including DNS Amplification, ICMP, TCP RST, TCP SYN/ACK Amplification and UDP amplification. Because each vector targets specific ports, protocols and systems, these complex attacks are significantly more difficult to mitigate.

Other Highlights

- **The volume of DDoS attacks continues to be high.** Lumen mitigated more than 8,600 DDoS attacks in Q1 – a 40% increase year-over-year and the second-busiest quarter in two years.
- **Consistent with previous observations, DDoS attack activity increased around U.S. holidays.** In Q1, the busiest holiday for threat actors was Martin Luther King, Jr. Day. Lumen researchers theorize that attackers focus their efforts on or around holidays because staffing levels are typically lower.
- **Real-time bot protection**. ThreatX blocked 25 billion application requests in Q1, representing 42% of all its customers' traffic. Of the blocked traffic, more than 30% came from bots. This volume underscores the need for real-time API and application protection and tightly integrated bot mitigations solutions as part of a comprehensive security strategy.
- **The telecommunications industry continues to be highly targeted.** Eighty-five percent of the largest 1,000 DDoS attacks that Lumen mitigated in Q1 targeted the telecommunications industry. In addition, more than 700,000 of the application requests that ThreatX blocked targeted telecom customers – the third most-targeted industry after banking and advertising.

"As we monitor our customers for attacks targeting their APIs and applications, we have seen a consistent increase in both the volume and complexity of attacks. More and more, these attacks are powered by very large botnets and leverage a combination of techniques," said Jeremy Ventura, director of security strategy and field CISO at ThreatX. "Threat actors increasingly go after both APIs and web applications, often with the goal of obfuscating the intended target. Having a complete view of the attacker and their tactics helps us clearly identify threats that must be blocked in real-time."

Additional resources

- Read the full **Q1 2023 DDoS and Application Threat Report**.
- Visit the Lumen Quarterly DDoS report **archive**.

- See how Lumen and ThreatX **combine** to offer API and Web Application Protection.
- Learn about Lumen's comprehensive **DDoS mitigation** and **Next-gen WAF/WAAP** services.
- 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.

About Lumen Technologies

Lumen connects the world. We are dedicated to furthering human progress through technology 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, ThreatXprofiles attackers and blocks advanced risks to protect APIs and applications 24/7. Learn more at **https://www.threatx.com**.

SOURCE Lumen Technologies

For further information: Suzanne Kernes Dawe, Lumen Public Relations, P: 720.217.5476, suzanne.dawe@lumen.com

---

https://news.lumen.com/2023-04-25-Lumen-research-reveals-a-rise-in-sophisticated,-complex-DDoS-attacks-in-Q1-2023