NEWS RELEASE

Lumen research reveals threat actors are modifying tactics to disrupt businesses

2023-08-08

Robust DDoS mitigation is the best defense to maintain availability of critical business applications

DENVER, Aug. 8, 2023 /PRNewswire/ -- Cyber attackers will never stop trying to overwhelm network defenders, and they constantly change their tactics to make Distributed Denial of Service (DDoS) and application attacks more difficult to stop. New data from **Lumen Technologies** (NYSE: LUMN), however, indicate the company's DDoS mitigation service continues to stop these complex attacks.

> Cyber attackers constantly change their tactics to make DDoS and application attacks more difficult to stop.

Earlier today, Lumen released a report detailing the DDoS mitigations and Application Programming Interface (API) protection measures the company deployed in Q2 2023. It shows complex, multi-vector attacks continue to rise, but Lumen® DDoS Mitigation and Application Protection services are helping mitigate them.

"As attackers modify their tactics, it's critical for businesses to have highly available, dynamic, high-performing and secure applications," said Peter Brecl, Lumen's director of product management for DDoS mitigation and application protection. "Companies need the best mitigation controls to protect their customers and their business from DDoS and application-layer attacks without decreasing performance."

Read the Lumen Q2 2023 DDoS and Application Threat Report for the latest stats.

Notable findings in the report include:

- Threat actors are mixing things up.
    - Forty-four percent of Lumen's Q2 DDoS mitigations were multi-vector in nature, meaning the threat

actors combined two or more attack techniques.
    - Lumen's quarter-over-quarter data indicate that attackers are continuously attempting to defeat the company's countermeasures by changing the number and types of vector combinations they deploy.
    - Multi-vector attacks are significantly more complex than single vector and require sophisticated countermeasures like Lumen's to mitigate. When threat actors deploy multi-vector attacks, they are targeting victims who are unprepared for the new vector combinations.
- Government and Telecom continue to be major targets.
    - Among the top 1,000 largest DDoS attacks mitigated in Q2 2023, telecommunications customers and the government sector were the most targeted. These data are consistent with previous quarters.
- API traffic is growing.
    - As businesses continue to adopt APIs, there has been a significant risen API traffic. ThreatX, Lumen's API and Application Protection partner, expects this trend to continue.
    - Robust API protection solutions should be implemented to safeguard against attacks that exploit API vulnerabilities.

Brecl continued, "Because threat actors are always and aggressively looking for new, more complex attack strategies, these mitigation controls should also leverage and integrate with threat intelligence capabilities, like those available with Lumen® Rapid Threat Defense. These enable us to discover unique DDoS threats because we have visibility into the network that others do not have. The system then automatically integrates mitigation controls in near-real time, and in conjunction with other mitigating controls effectively blocks the threats before they reach the customer's environment."

"ThreatX has seen a steadily increase growth in traffic associated with APIs, as well as threat actors attempting to exploit this growing attack surface," said Neil Weitzel, director, Security Operations Center at ThreatX. "In addition, we are seeing a range of industries that play critical roles in peoples' lives - banking, telecommunications, education and insurance, for example - turn to APIs as a means of delivering new services and greater value. As the developers in these organizations turn to APIs, however, it is very important that security teams are building long-term strategies to identify APIs and to protect them against complex threats."

Additional resources

- Read the full **Q2 2023 DDoS and Application Threat Report**.
- 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**.
- See how Lumen and ThreatX **combine** to offer API and Application Protection.

- Learn about Lumen's comprehensive **DDoS mitigation** and **Next-gen WAF/WAAP** services.

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, 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-research-reveals-threat-actors-are-modifying-tactics-to-disrupt-businesses-301895315.html**

SOURCE Lumen Technologies