Lumen Newsroom

Government Sector is Top Targeted Industry for DDoS Attacks in Q4 2023

Lumen Quarterly DDoS & Application Threat Report reveals the latest trends and insights on cyberattacks and AI threats

DENVER, Feb. 8, 2024 /**PRNewswire**/ -- The government sector experienced a surge of DDoS attacks in Q4 according to **Lumen Technologies** (NYSE: LUMN), a global leader in integrated network and cybersecurity solutions. The Lumen **Quarterly DDoS & Application Threat Report for Q4 2023** analyzes data from its DDoS mitigation platform and application protection partner, ThreatX, to provide an overview of the DDoS and application-layer attacks that targeted organizations in the last quarter of 2023.

According to the report, the government sector was hit hard:

- 66% of the 1,000 largest attacks Lumen mitigated were targeting the government.
- Government attacks increased 163% from Q3 and a staggering 4,025% year over year.
- One government customer accounted for 1,759 attacks of the 1,953 government attacks in Q4, showing a persistent and focused campaign by cybercriminals.

"The government sector holds extremely sensitive data, so you can understand why it is a prime target for cyberattacks," said Sharada Achanta, Lumen VP of Product, Cybersecurity and AI. "Espionage, extortion, and disruptions are the reasons behind these attacks, and the attackers are not deterred by the increased security measures. The good news is that Lumen, through our Black Lotus Labs threat intelligence, can stop the attacks that cross our network before they become destructive. Lumen's threat intelligence and DDoS mitigation, powered by AI and machine learning, offer customers a distinctive and comprehensive cybersecurity solution."

Lumen's report also reveals that its largest DDoS attack of 2023 happened in Q4, reaching a peak of 903 Gbps. This attack targeted a telecom customer, which is part of a trend of telecom being a frequent target of attacks because it carries traffic for all other industries.

The Two Sides of AI

Artificial intelligence (AI) is a double-edged sword for cybersecurity, as attackers and defenders use it to enhance their skills. Attackers use AI to hide, automate, and craft sophisticated attacks, while defenders, like Black Lotus Labs, use AI to monitor, detect, predict, and respond to threats.

One growing concern in the AI space is how it might leverage devices on the network edge. Those include IoT devices, smartphones, and laptops.

- AI at the edge could increase the potential for AI-driven attacks, such as DDoS attacks using compromised IoT devices, or deepfake attacks using manipulated audio and video.
- AI can enable attacks that are faster, smarter, and more powerful, such as self-learning malware, botnets that adjust to defenses, and targeted social engineering.

AI can also be a powerful tool for defenders of the network.

- By using more analytics from edge devices, defenders can improve AI models for detection, prediction, and response.
- AI at the edge can boost the defense capabilities by giving more data and insights from edge devices and allowing quicker and more customized responses.

Application Threats on the Rise

The report shows that applications owned by ThreatX customers received more than 84 billion requests in Q4, with 1.7 billion of those blocked in real time. Almost 37% of the blocked traffic was from web bots. The attackers tried to access confidential information, change the structure of the websites, and steal passwords.

"Cyber miscreants span a broad spectrum, from activists to criminals to nation-state sponsored cyberwarfare groups. But DDoS remains a common link between all these groups, as the ability to disrupt the digital experience is a crude but effective cudgel against any modern business," said IDC Cybersecurity research director Chris Rodriguez. "With the security implications of GenAI only just now being explored, the most prudent way to prepare for the unpredictable is to focus on security basics, including a robust DDoS detection and response strategy."

"Application security is a critical component of any organization's cybersecurity strategy," said Achanta. "Attackers are after that critical data, constantly probing and testing applications for vulnerabilities and weaknesses using a variety of techniques and tools. Organizations need to have comprehensive and tailored protection against network- and application-layer attacks."

Protecting Businesses from DDoS Attacks

Although people believe identifying a DDoS attack is simple, tactics are becoming more complex and discreet. Businesses need to protect themselves.

- If a company uses applications to interact with customers, employees, or other stakeholders, they need holistic protection against network- and application-layer attacks. This will keep critical business functions up and running—even if they are under an active attack.
- Businesses should consider deploying additional application-layer defenses using Web Application Firewalls, API protections and Bot Risk Management solutions, and pair those with application acceleration solutions to make applications more responsive for their customers.

- Having DDoS mitigation in place, such as **Lumen® DDoS Hyper®** can prevent attackers from successfully launching large campaigns against an organization.
- This guide can help businesses **find out if they're under an active DDoS attack**.

Additional Information:

- For more insights and recommendations on how organizations can improve their security posture and defend against cyberattacks, read the full report **here**.
- Lumen has one of the largest DDoS mitigation deployments in the industry, backed by 170 Tbps of network-based mitigation capacity in more than 500 multi-tiered scrubbing locations.
- Learn more about Lumen DDoS Mitigation Services: **DDoS Mitigation | Web Application Security | Lumen**
- Learn more about Lumen application protection services**:** **Web Application Firewall | Lumen**
- Read how Lumen DDoS protection backed Texas Rangers' World Series triumph: **Texas Rangers' World Series triumph backed by Lumen DDoS protection - Nov 27, 2023**

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**. 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: Stephanie Meisse, Lumen Technologies, P: 419-610-3142, stephanie.n.meisse@lumen.com

---

Additional assets available online: **Photos (1**

https://news.lumen.com/2024-02-08-Government-Sector-is-Top-Targeted-Industry-for-DDoS-Attacks-in-Q4-2023