LUMEN

NEWS RELEASE

Lumen research reveals 60% growth of a known, preventable DDoS attack vector

2022-10-25

Q3 DDoS report details attack trends, including the expanding base of CLDAP reflectors

DENVER, Oct. 25, 2022 /PRNewswire/ -- With October's focus on cybersecurity awareness, **Lumen Technologies®** (NYSE: LUMN) and its threat research team, **Black Lotus Labs®**, today released a pair of research reports including:

- New **intelligence from Black Lotus Labs** regarding the proliferation of Connectionless Lightweight Directory Access Protocol (CLDAP) reflectors – a known attack vector that is easily prevented with well-documented best practices.
- The Q3 2022 Distributed Denial of Service **(DDoS) report**, which provides the latest data and trends from the Lumen DDoS mitigation platform.

Black Lotus Labs discovered more than 12,000 CLDAP services are open to the internet – a 60% increase over the past year.

Read the Black Lotus Labs blog titled **"CLDAP Reflectors on the Rise Despite Best Practices"** and the **Lumen Q3 DDoS report**.

CLDAP Research:

Background:

- CLDAP is an essential service in Microsoft environments. When improperly configured to expose the service to the internet, CLDAP can carry a bandwidth amplification factor of up to 70 times the volume of traffic sent. This makes it an enticing target for cybercriminals launching DDoS attacks.
- As soon as the CLDAP vulnerability was discovered in 2016, best practices for mitigating the threat were published; and yet, six years later, the number of exposed CLDAP reflectors is on the rise.
- Using Lumen's global network visibility, Black Lotus Labs tracks CLDAP reflectors with a proprietary validator

that registers distinct IPs that are open to reflection. This is a more precise assessment of the breadth of reflectors than has previously been available to the industry.

Notable findings:

- Black Lotus Labs discovered more than 12,000 CLDAP services are open to the internet – a 60% increase over the past year.
- One of the observed reflectors recently emitted 17 Gbps of traffic. At this level, just 100 CLDAP reflectors could be leveraged to wage an attack greater than 1 Tbps.

"It is alarming that CLDAP continues to be prolific and capable of generating large, impactful attacks – especially when we have well-documented best practices for prevention," said Mark Dehus, director of threat intelligence for Lumen Black Lotus Labs. "Organizations running Active Directory should understand the risks of publicly exposing CLDAP, and we strongly recommend they restrict access to only the hosts and networks that need access."

Lumen response

Black Lotus Labs is continuing to track and analyze vulnerable CLDAP reflectors and feed the intelligence into the Lumen Connected Security portfolio. The team is also expanding efforts to notify legitimate, third-party hosts of CLDAP reflection activity, and blocking long-lived CLDAP reflector traffic from traversing the Lumen global backbone.

Notable findings from the Lumen Q3 2022 DDoS report:

- Lumen mitigated 5,547 attacks in Q3 – a 21% increase over Q2 – and the largest bandwidth attack scrubbed was 493 Gbps. This is nearly half the size of the largest mitigation in Q2 which, at **1.06 Tbps**, was Lumen's largest to date.
- Although Session Initiation Protocol (SIP) attacks only accounted for 3% of all mitigations, this attack vector – which targets VoIP infrastructure – remains of interest due to a dramatic upward trend over the past year. This quarter saw a 59% increase over Q2.
- The top five targeted industries were Telecommunications, Gaming, Software and Technology, Government and Finance.
- Of the 5,500+ attacks Lumen mitigated in Q3, nearly 40% targeted a single government customer. Despite the bombardment and a concentrated effort around July 4, the customer experienced no downtime.

"The combined research from Black Lotus Labs and the Lumen DDoS mitigation platform underscores an important reality for businesses today," said Peter Brecl, director of security product management for Lumen. "Cyber criminals are always looking for new ways to achieve their goals, and attacks have become more complex. This means organizations need to consider a holistic security solution that includes DDoS mitigation to protect the availability of infrastructure and applications, Web Application and API Protection (WAAP) to protect against application-layer attacks, and bot management services to protect from malicious or unwanted bots. As organizations navigate through their digital transformation, this type of multi-layered approach is more important than ever."

Additional Resources:

- Read the full **CLDAP blog** and **Q3 2022 DDoS report.**
- See the Black Lotus Labs' previous reporting on UDP reflectors: **Tracking UDP Reflectors For A Safer Internet**.
- Learn more about Black Lotus Labs and the latest threats they're tracking – including CLDAP – in the new **IDG webinar**.
- Visit the Lumen Quarterly DDoS report **archive**.
- Learn about Lumen's comprehensive **DDoS mitigation** and **Next-gen WAF/WAAP** services.
- See why Frost and Sullivan recognized Lumen with the **2021 Global New Product Innovation Award** for its Holistic Web Protection Solutions.

About Lumen Technologies and the People of Lumen:
Lumen is guided by our belief that humanity is at its best when technology advances the way we live and work. With approximately 400,000 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: /lumentechnologies, Twitter: @lumentechco, Facebook: /lumentechnologies, Instagram: @lumentechnologies and YouTube: /lumentechnologies. Lumen and Lumen Technologies are registered trademarks in the United States.

View original content to download multimedia:**https://www.prnewswire.com/news-releases/lumen-research-reveals-60-growth-of-a-known-preventable-ddos-attack-vector-301657915.html**

SOURCE Lumen Technologies