Lumen Newsroom

Lumen rediscovers malware now used in campaign to research U.S. military websites

Black Lotus Labs threat intel reveals "HiatusRat" is back, also targeting Taiwanese organizations

DENVER, Aug. 18, 2023 /PRNewswire/ -- Black Lotus Labs – the threat intelligence arm of Lumen Technologies (NYSE: LUMN) – discovered a complex campaign in March 2023 called "HiatusRAT" that infected business-grade routers globally. Continuous monitoring of HiatusRAT reveals the threat actors are back and using the malware to target Taiwanese organizations and research U.S. military websites.

> *Continuous monitoring of HiatusRAT reveals the threat actors continued their operations nearly unabated.*

Read the full analysis in Black Lotus Labs' latest blog titled, "No rest for the wicked: HiatusRAT takes little time off in a return to action."

"Black Lotus Labs' role is to keep the internet safe, so consumers and businesses stay safe," said Mark Dehus, director of threat intelligence at Lumen Black Lotus Labs. "Sophisticated threat actors, especially those sponsored by nation states, are exploiting edge routers and similar devices. They use malware like HiatusRAT to discreetly gain access to these devices and covertly run their espionage and criminal networks without the device owners' knowledge. It's a warning that businesses must act now to avoid their infrastructure becoming part of adversaries' ongoing operations."

What businesses and consumers should consider

- Lumen implemented countermeasures to help protect customers from this threat and disrupt its operations.
- Using comprehensive Secure Access Service Edge (SASE) or similar solutions that use VPN-based access can protect data and bolster their security posture.
- Enabling the latest cryptographic protocols can help protect data in transit; consider only using email services which rely upon SSL and TLS.

- Consumers with self-managed routers should follow best practices and regularly monitor, reboot, and install security updates and patches. End-of-life devices should be replaced with vendor-supported models to ensure patching against known vulnerabilities.

Why this threat is a concern

In the past year alone, Black Lotus Labs discovered three malware campaigns that utilized compromised business-grade and small office/home office (SOHO) routers, and the infosec industry has observed activity against several verticals by **China-based actors**.

Latest HiatusRAT findings and Black Lotus Labs response

- Initial HiatusRAT reporting showed the threat actor was targeting organizations in Latin America and Europe. Beginning in June 2023, however, the group's focus shifted.
- The entities targeted in the latest campaign are consistent with the **strategic interest** of the People's Republic of China according, to a 2023 ODNI threat assessment.
- Black Lotus Labs has null-routed the new Hiatus command and control (C2) servers across the Lumen global backbone. The team also added the Indicators of Compromise (IoCs) from this campaign into Rapid Threat Defense® – the automated threat detection and response capability that fuels Lumen's security product portfolio by blocking threats before they reach the customer's network.

Additional resources

- Read about Black Lotus Labs' **initial discovery** of HiatusRAT.
- See Black Lotus Labs' other router-based malware discoveries: **ZuoRAT** and **AVrecon**.
- Learn about how **Black Lotus Labs** leverages its network visibility to help protect customers and keep the internet clean.
- See how **Lumen SASE Solutions** provides simplified network access, security and management on the Lumen Platform.
- Learn how **Lumen Rapid Threat Defense** uses global threat intelligence from Black Lotus Labs as a countermeasure to block threats before they reach the customer's environment.

About Black Lotus Labs

Black Lotus Labs is the threat intelligence team at Lumen. Our mission is to leverage our visibility into the Lumen network to protect businesses and keep the internet clean. We're defenders of a clean internet, proactively disrupting ~150 C2s per month through takedowns and notifications.

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.

SOURCE Lumen Black Lotus Labs

For further information: Media Contact: Suzanne Dawe, Lumen Public Relations, P: 720-217-5476, suzanne.dawe@lumen.com

https://news.lumen.com/2023-08-18-Lumen-rediscovers-malware-now-used-in-campaign-to-research-U-S-military-websites