NEWS RELEASE

Lumen finds and disrupts malicious botnet targeting critical networks in U.S. and Asia

2023-12-13

Lumen's Black Lotus Labs exposes Chinese cyber actor behind Volt Typhoon's attacks on telecoms, government, and green energy sectors

DENVER, Dec. 13, 2023 /PRNewswire/ -- In a major win for national security, Black Lotus Labs, the threat research and intelligence arm of **Lumen Technologies** (NYSE: LUMN), discovered and stopped a malicious botnet used by Chinese nation state cyber actors supporting Volt Typhoon operations. The KV-botnet targeted critical infrastructure providers and municipal governments in Guam and other regions creating a serious threat to U.S. businesses and strategic interests.

To learn more about how Black Lotus Labs uncovered the KV-botnet, traced the activities aligned with the People's Republic of China, and disrupted their operational infrastructure, read **Routers Roasting on an Open Firewall: The KV-botnet Investigation.**

"KV-botnet is a new discovery signaling an escalation in the abuse of network and security devices to hide secret operations against some of our nation's most vital networks," said Mark Dehus, senior director of threat intelligence at Lumen Black Lotus Labs. "Blocking the threat actor's infrastructure across Lumen's network disrupts the botnet's ability to operate and helps combat dangerous and highly skilled nation state threats like Volt Typhoon. Black Lotus Labs is releasing the information about the threat's operations so critical infrastructure providers, the defense industrial base, commercial businesses, and even end consumers can be aware of this activity and take steps to defend against it."

How it works:

The botnet, discovered and named KV-botnet by Black Lotus Labs, uses sophisticated malware to create hidden channels on infected small office/home office (SOHO) routers and firewalls, forming a secret network for data

transmission. Black Lotus Labs detected KV-botnet activity on its global backbone and traced it to the control servers run by threat actors aligned with China. The team then null routed, or dropped, the malicious IP addresses, blocking access to the compromised devices and stopping further attacks on critical infrastructure.

Why it matters:
Since the beginning of 2022, a sophisticated and secretive group of cyber actors has been running the KV-botnet, which has connections to Volt Typhoon. Microsoft and other security researchers have attributed this network to the Chinese government.

By using the KV-botnet, Volt Typhoon could send secret communication channels that avoided security barriers and firewalls and merged with normal network traffic. This botnet was essential for their strategic intelligence collection operations, helping them accomplish their long-term goals. The campaign targeted devices outside the reach of traditional security detection teams, an intentional layer of obfuscation for covert operations.

Black Lotus Labs also shared its findings and evidence with the broader security research community, to help them protect their networks from the threat posed by these kinds of hidden networks.

Tips for businesses and consumers:
Businesses:

- Watch out for substantial amounts of data leaving your network, even if they appear to go to nearby locations. Geofencing will not protect you from these activities.
- Use an advanced security solution such as Secure Access Service Edge (SASE) to detect and stop suspicious network activity.

Consumers:

- Regularly restart your routers and install the latest security updates and patches.
- Use reliable and updated security software on your devices and install updates when they are available.

Additional resources:

- This is the fourth malware campaign Black Lotus Labs has found this year using compromised small office/home office (SOHO) routers. The infosec industry has observed activity against several verticals by **China-based actors**.
- Learn more about **Black Lotus Labs®**, defenders of a clean internet.
- See how **Lumen Rapid Threat Defense** uses global threat intelligence to block DDoS bots on the network.
- Read how **Lumen SASE Solutions** provides simplified network access, security, and management on the

Lumen Platform.

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.

View original content to download multimedia:**https://www.prnewswire.com/news-releases/lumen-finds-and-disrupts-malicious-botnet-targeting-critical-networks-in-us-and-asia-302014128.html**

SOURCE Lumen Technologies