Lumen Newsroom

Lumen discovers new malware that fueled one of the largest SOHO-router botnets ever seen

Threat discovered as CISA issues warnings about the risks posed by these vulnerable devices

DENVER, July 12, 2023 /**PRNewswire**/ -- For the third time in the past year, **Black Lotus Labs®** – the threat research arm of **Lumen Technologies** (NYSE: LUMN) – has discovered a new malware that targets small office/home office (SOHO) routers. Discovery of the malware dubbed "AVrecon" came as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued warnings about SOHO routers, including a **binding operational directive** in June and a **cybersecurity advisory** in May.

Black Lotus Labs found another new malware targeting SOHO routers -- the third such discovery in less than a year.

For detailed technical analysis of AVrecon and to see how it fits into the cybercrime ecosystem, read the full research blog.

Using Lumen's global network visibility to gather a 28-day snapshot of AVrecon, Black Lotus Labs determined the malware has infiltrated more than 70,000 machines and gained persistent hold in more than 40,000 of them in 20 countries. This makes AVrecon one of the largest SOHO router-targeting botnets ever seen.

"Our network visibility enables us to see threats other researchers cannot see, and once again we have discovered a new malware that targets SOHO routers," said Michelle Lee, director of threat intelligence for Lumen Black Lotus Labs. "This time it went undetected for two years and grew to a staggering 40,000-strong botnet."

Consumers and corporate network defenders should take action

SOHO routers pose a serious threat because these devices are not always automatically patched and updated – nor are they regularly monitored – which significantly decreases the ability to detect malicious activity. With the prevalence of remote workers, corporate network defenders should take the following precautions:

- Continue to look for attacks on weak credentials and suspicious login attempts, even when they originate from residential IP addresses.
- Be aware that threat actors can spawn a remote shell and deploy subsequent modules.
- Protect cloud assets from communicating with bots that are attempting to perform password spraying attacks and begin blocking Indicators of Compromise (IoCs) with Web Application Firewalls.

Consumers who use SOHO routers should regularly reboot their devices and install security updates and patches where available.

About AVrecon

Threat actors leverage AVrecon primarily to steal bandwidth – without impacting end users – to create a residential proxy service. This enables them to launder malicious activity, including password spraying and digital advertising fraud, and helps them avoid attracting the same level of attention from **Tor**-hidden services or commercially available VPN services.

Lee continued, "Threat actors are using AVrecon to proxy traffic and to engage in malicious activity like password spraying. This is different from the direct network targeting we saw with our other router-based malware discoveries. Defenders should be aware that such malicious activity can originate from what appears to be a residential IP address in a country other than the actual origin, and traffic from compromised IP addresses will bypass firewall rules such as geofencing and ASN-based blocking."

Read about Black Lotus Labs' previous SOHO router malware discoveries including ZuoRAT and HiatusRAT.

Black Lotus Labs' response

- Apart from a single reference to AVrecon in May 2021, the malware has been operating undetected for more than two years.
- Black Lotus Labs has null-routed the AVrecon command and control (C2) servers across the Lumen global backbone and added the Indicators of Compromise (IoCs) from this campaign into the threat intelligence feed that fuels the Lumen Connected Security portfolio.
- The team will continue to monitor new infrastructure, targeting activity, and expanding tactics, techniques and procedures (TTPs), and it will collaborate with the security research community to share findings related to this activity.

Learn about Black Lotus Labs' mission to leverage its network visibility to help protect customers and keep the internet clean.

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: Suzanne K. Dawe, Lumen Public Relations, P: 720.217.5476, suzanne.dawe@lumen.com

---

https://news.lumen.com/2023-07-12-Lumen-discovers-new-malware-that-fueled-one-of-the-largest-SOHO-router-botnets-ever-seen