Lumen Disrupts Cybercriminals Targeting Home and Office Routers

Black Lotus Labs reveals how TheMoon malware used end-of-life routers to power a notorious cybercrime service called Faceless, urges consumers to secure devices

DENVER, March 26, 2024 /**PRNewswire**/ -- **Black Lotus Labs**, Lumen Technologies' (NYSE: LUMN) threat intelligence team, has identified a new multi-year campaign targeting end-of-life, or outdated small office/home office (SOHO) routers and IoT devices. An updated version of **TheMoon** malware has reemerged and is fueling a cybercriminal anonymity service called **Faceless**. Lumen has stopped all traffic to and from the infrastructures associated with TheMoon and Faceless across its global network. Small office routers continue to be a key target for cybercriminals. In less than two years, Black Lotus Labs has discovered six large malware campaigns using compromised SOHO routers.

*For detailed technical analysis of TheMoon and Faceless, read our latest blog, **"The Darkside of TheMoon"**.*

Cybercriminals join forces

Lumen first reported on TheMoon in 2019. It reemerged in 2023 and quietly operated while growing to over 40,000 web robots (bots) from 88 countries in the first two months of 2024. Black Lotus Labs discovered that most of these bots are used as the foundation of a notorious, cybercriminal-focused proxy service known as Faceless. TheMoon allowed Faceless operators to anonymously send malicious traffic through outdated routers and devices owned by consumers and small businesses.

"Black Lotus Labs' advanced network visibility allows us to uncover threats other researchers can't see. TheMoon botnet quietly returned with its criminal operations, but we were able to see it and stop the attacks across our network," said Mark Dehus, senior director of threat intelligence at Lumen Black Lotus Labs. "The attackers behind Faceless are using the botnets from this malware to create an anonymous proxy network by abusing outdated and unsupported routers to run their criminal networks. We believe these cybercriminals are using these networks to steal data and information from their victims, including the financial sector."

How it works

Black Lotus Labs believes TheMoon is the main or sole provider of bots to Faceless. This proxy service gives its users the chance to impersonate a legitimate user in a chosen country. Faceless doesn't require customer identification. This allows users to stay anonymous as they send malicious traffic through the routers attempting to steal valuable data.

"TheMoon malware is a serious threat not only to the owners of the compromised SOHO devices, but also the victims exploited through this anonymous proxy network," continued Dehus. "We urge consumers to update and secure their devices to prevent them from becoming part of these malicious networks."

Stopping the threat

Consumers and businesses should take steps to protect their routers from cybercriminals.

- **Reboot**: Consumers who use SOHO routers should regularly reboot their devices and install security updates and patches when available.
- **Update old routers**: Consumers and business should replace end-of-life devices with vendor-supported models to help ensure security updates are in place.

IT professionals:

- **Install protection**: Remote workers can invite threats to a company network. Install Web Application Firewalls to protect company assets from communicating with bots.
- **Monitor activity**: Look for suspicious login attempts, even those that come from residential IP addresses.
- **Encrypt data**: Use the latest cryptographic protocols, such as TLS (Transport Layer Security) to encrypt data sent over the internet. This helps secure email and website services.

Cybersecurity threats are growing and putting organizations at risk. Lumen will soon offer a new proactive defense solution that spots and isolates threats before they reach business networks and applications. This provides protection against advanced cyberattacks and malicious activity. Businesses can also turn to **Lumen® Rapid Threat Defense**, powered by Lumen Black Lotus Labs threat intelligence. The team uses global network data from the Lumen network, one of the world's largest and most deeply peered networks. Experienced researchers use their expertise to create machine learning algorithms that detect, classify, and validate threats.

For more tips on best practices for securing routers, visit **Canadian Centre for Cyber Security**.

Threat protection continues

Black Lotus Labs has added the threat intelligence from this campaign into the Lumen security portfolio to help quickly detect these threats in the future. The team continues to monitor new infrastructure to identify and stop suspicious behaviors and attacks. To help protect the larger cybercrime ecosystem, Lumen shares its research with experts in the broader security research community so they can also identify and act on these threats.

Additional information

- Read how Black Lotus Labs disrupted **Chinese nation state cyber actors supporting recent Volt Typhoon attacks**.
- Read about Black Lotus Labs' previous SOHO router malware discoveries including **ZuoRAT**, **HiatusRAT**, and **AVrecon**.
- Learn more about Lumen **DDoS mitigation**, **DDoS Hyper®**, and **Lumen® SASE solutions**.

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.

SOURCE Lumen Technologies

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

---

https://news.lumen.com/2024-03-26-Lumen-Disrupts-Cybercriminals-Targeting-Home-and-Office-Routers