Lumen discovers new malware that targeted home-office routers for two years

Black Lotus Labs' global visibility led to the discovery of a remote access trojan and sophisticated campaign that aligns with nation-state activity

DENVER, June 28, 2022 /**PRNewswire**/ -- Black Lotus Labs, the threat intelligence arm of **Lumen Technologies** (NYSE: LUMN), today announced that it discovered a new remote access trojan (RAT) called ZuoRAT, which targets remote workers via their small office/home office (SOHO) devices. It is part of a complex campaign that went undetected for nearly two years. The tactics, techniques and procedures (TTPs) that analysts observed are highly sophisticated and bear the markings of what is likely a nation-state threat actor.

ZuoRAT targets remote workers via their home routers and is part of a complex, potentially nation-state campaign.

Read the full report here: https://blog.lumen.com/zuorat-hijacks-soho-routers-to-silently-stalk-networks/?utm_source=referral&utm_medium=press+release

When the pandemic forced offices to close, the rapid shift to remote work expanded security concerns as millions of employees began accessing corporate networks from home. This gave threat actors a fresh opportunity to leverage at-home devices such as SOHO routers – which are widely used but rarely monitored or patched – to collect data in transit, hijack connections, and compromise devices in adjacent networks.

"Router malware campaigns pose a grave threat to organizations because routers exist outside of the conventional security perimeter and can often have weaknesses that make compromise relatively simple to achieve," said Mark Dehus, director of threat intelligence for Lumen Black Lotus Labs. "In this campaign, we have observed a threat actor's capability to exploit SOHO routers, covertly access and modify internet traffic in ways difficult to detect and gain additional footholds in the compromised network."

Dehus continued, "Organizations should keep a close watch on SOHO devices and look for any signs of activity outlined in this research. This level of sophistication leads us to believe this campaign might not be limited to the small number of victims observed. To help mitigate the

threat, they should ensure patch planning includes routers, and confirm these devices are running the latest software available."

Overview and Analysis of Malware Campaign

- Black Lotus Labs recently discovered the highly targeted, sophisticated campaign which has been active in North America and Europe for nearly two years beginning in October 2020.
- The campaign included ZuoRAT – a multi-stage RAT developed for SOHO routers leveraging known vulnerabilities – which allowed the threat actor to enumerate the adjacent home network, collect data in transit, and hijack home users' DNS/HTTP internet traffic. The actor was able to remain undetected by living on devices rarely monitored, and by hijacking DNS and HTTP traffic.
- The hijacking capability allowed the threat actor to pivot from the router to workstations in the network where they likely deployed two additional custom-built RATs – one of which allowed for cross-platform functionality (i.e. Windows, Linux and MacOs). These additional RATs allowed the actor to upload/download files, run commands and persist on the workstation.
- Black Lotus Labs also identified two distinct sets of command-and-control (C2) infrastructure. The first was developed for the custom workstation RAT and relied upon third-party services from Chinese companies. The second set of C2s was developed for the routers.
- Using proprietary telemetry from the Lumen global IP backbone, Black Lotus Labs identified that, once infected, the routers communicated with other compromised routers to further obfuscate malicious activity.
- A complete list of affected routers is included in the **ZuoRAT blog**.

Additional Resources:

- See how Black Lotus Labs leverages its network visibility to protect businesses and help keep the internet clean: **www.lumen.com/blacklotuslabs**.
- To see our most recent research into suspected nation-state activity with **Konni**, **ReverseRAT** and **ReverseRAT 2.0**.
- For more Black Lotus Labs blogs, visit the **archive**.

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 500,000 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.

SOURCE Lumen Technologies

For further information: Suzanne Kernes Dawe, Lumen Public Relations, P: 720.217.5476, suzanne.dawe@lumen.com

---

Additional assets available online: **Photos (1**

https://news.lumen.com/2022-06-28-Lumen-discovers-new-malware-that-targeted-home-office-routers-for-two-years