NEWS RELEASE

Black Lotus Labs uncovers another new malware that targets compromised routers

2023-03-06

HiatusRAT has been targeting business-grade routers to covertly spy on victims since July 2022

DENVER, March 6, 2023 /PRNewswire/ -- For the second time in nine months, Black Lotus Labs® – the threat research team at **Lumen Technologies** (NYSE: LUMN) – has uncovered a complex new malware campaign that has been exploiting compromised routers. The latest research delves into a complex, never-before-seen campaign called "Hiatus," which has been targeting business-grade routers since June 2022. It comes on the heels of the team's other recent discovery– a novel malware called **ZuoRAT** – which targeted SOHO (small office/home office) routers. Black Lotus Labs does not currently believe the two campaigns are related.

> For the second time, Black Lotus Lab has uncovered a new malware campaign that exploits compromised routers.

Some of the industries targeted in the Hiatus campaign include pharmaceuticals, and IT services and consulting firms. Researchers suspect the IT firms were chosen to give the threat actor downstream access to the victims' customers' environments.

Read the full research report: New HiatusRAT router malware covertly spies on victims

"The rise of hybrid work has led to increased dependency on relatively low-cost routers that enable VPN access – especially for many small- and medium-sized businesses." said Mark Dehus, director of threat intelligence for Lumen Black Lotus Labs. "These devices typically live outside the traditional security perimeter, which means they usually are not monitored or updated. This helps the actor establish and maintain long-term persistence without detection."

HiatusRAT research findings:

- The threat actors behind the Hiatus campaign primarily target DrayTek Vigor router models 2960 and 3900 that are at their end of life.
- As of mid-February 2023, approximately 4,100 DrayTek models 2960 and 3900 were exposed on the internet, and Hiatus had compromised approximately 100 of them in Latin America, Europe and North America.
- Upon infection, the malware intercepts data transiting the infected router. It does this by deploying a binary that captures network packets from the compromised device and sends them to actor-controlled infrastructure.
- At the same time, the malware deploys a Remote Access Trojan (RAT) dubbed "HiatusRAT" which displays a highly unusual feature: it converts the compromised machine into a bot that can proxy malicious traffic transmitted by the adversary to victims on additional networks.

Dehus continued, "The discovery of Hiatus confirms that actors are continuing to pursue router exploitation. These campaigns demonstrate the need to secure the router ecosystem, and routers should be regularly monitored, rebooted, and updated, while end-of-life devices should be replaced."

Black Lotus Labs' response:

- Black Lotus Labs has null-routed Hiatus C2s across the Lumen global backbone and 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.
- The team will continue to monitor for new Hiatus infrastructure, targeting activity, and expanding tactics, techniques and procedures (TTPs), and share this information with the security research community.

Recommendations:

- 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.
- Businesses should consider comprehensive Secure Access Service Edge (SASE) or similar solutions that utilize VPN-based access to protect data and bolster their security posture.
- Users should only use secure email services that help protect data in transit.

Additional Resources:

- Read the full HiatusRAT blog titled: **New HiatusRAT router malware covertly spies on victims**.
- See Black Lotus Labs' ZuoRAT research: **ZuoRAT hijacks SOHO routers to silently stalk networks**.
- For more Black Lotus Labs research, visit the **blog archive**.
- See how Black Lotus Labs **sees more, so we can stop more**.

- Learn how to simplify network access, security and management with **SASE solutions** on the Lumen Platform.

About Lumen Technologies:

Lumen is guided by our belief that humanity is at its best when technology advances the way we live and work. With approximately 400,000 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.

View original content to download multimedia:**https://www.prnewswire.com/news-releases/black-lotus-labs-uncovers-another-new-malware-that-targets-compromised-routers-301762772.html**

SOURCE Lumen Black Lotus Labs