NEWS RELEASE

Black Lotus Labs uncovers hacktivist campaign that used a misconfigured router to spread an anti-government manifesto

2021-06-04

More than 18,000 devices worldwide are still exposed to the potential abuse

DENVER, June 4, 2021 /PRNewswire/ -- **Black Lotus Labs®**, the threat intelligence arm of **Lumen** Technologies (NYSE: LUMN), recently uncovered a hacktivist campaign that leveraged misconfigured routers and switches to distribute an anti-government manifesto.

More than 18,000 devices worldwide are still exposed to the potential abuse.

Details of the research findings are contained in the latest **Black Lotus Labs blog**.

Overview of the Attack

- On and around May 13, 2021, the attacker gained access to the victims' routers and switches due to a misconfiguration that exposed control of the devices to the internet.
- This external exposure allowed the threat actor to remotely alter the victims' configuration files, which rendered the routers unusable.
- Victims who attempted to fix the compromised file found that it had been replaced with approximately six pages of an anti-government manifesto.

Additional Key Findings

- Abusing the misconfigured router to gain access to the victims' configurations is not a new tactic, and recommendations for properly configuration the routers and switches were published in 2017.
- Despite this, more than **18,000 devices around the world are still exposed**,1 and Black Lotus Labs has identified more than 800 unique scanners looking for the misconfigured equipment– and potential victims.

The Black Lotus Labs Response and Recommendations
Black Lotus Labs null-routed the malicious IP address across the Lumen global network and added it to a block list for its security customers.

The company also offered recommendations for organizations that had already been attacked, and those that have misconfigured routers. "Victims can recover from this attack by rebuilding their router configuration, and either disabling or limiting the ability to manage the device remotely," said Mike Benjamin, Lumen vice president of product security and head of Black Lotus Labs. "In the meantime, we will continue to look for attackers abusing this protocol."

More information about Black Lotus Labs can be found at **www.lumen.com/blacklotuslabs**.

Other Recent Threat Intelligence Blogs from Black Lotus Labs

- **Tracking UDP Reflectors for a Safer Internet**
- **Newly Discovered Watering Hole Attack Targets Ukrainian, Canadian Organizations**
- **The Reemergence of Ransom-Based Distributed Denial of Service (RDDoS) Attacks**

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 450,000 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 of Lumen Technologies LLC in the United States. Lumen Technologies LLC is a wholly owned affiliate of Lumen Technologies Inc.

1 According to ShadowServer, a foundation that scans the internet for publicly accessible devices that are running this vulnerability. **https://scan.shadowserver.org/smartinstall/**

View original content to download multimedia:**http://www.prnewswire.com/news-releases/black-lotus-labs-uncovers-hacktivist-campaign-that-used-a-misconfigured-router-to-spread-an-anti-government-manifesto-**

301306120.html

SOURCE Lumen Black Lotus Labs