New Lumen research reveals previously unseen Qakbot infrastructure

Black Lotus Labs' discovery gives insight into the pervasive botnet's resiliency

DENVER, June 1, 2023 /**PRNewswire**/ -- Black Lotus Labs, the threat research arm of **Lumen Technologies** (NYSE: LUMN), has used Lumen's proprietary global telemetry to monitor Qakbot – a potent malware/ransomware distribution network – for years. Today the team announced new research into the advanced techniques the botnet uses to propagate and evade detection.

> *We discovered sophisticated infrastructure indicating Qakbot has reached a concerning level of maturity.*

"Qakbot remains a pervasive threat that continues to leverage its infected hosts in previously unknown ways," said Mark Dehus, director of threat intelligence for Lumen Black Lotus Labs. "Our team discovered previously unseen infrastructure used to reallocate existing bots for additional functions. The discovery of this sophisticated backend control infrastructure shows that Qakbot has reached a very concerning level of maturity."

As a result of this research, Black Lotus Labs null-routed the higher-tier infrastructure, limiting Qakbot's ability to impact Lumen's customers and the internet as a whole.

For more information, visit https://blog.lumen.com/qakbot-retool-reinfect-recycle/

Key findings

- Black Lotus Labs noticed the lifespan of Qakbot's command and control (C2) infrastructure was brief; however, Qakbot retains resiliency by repurposing victim machines into C2s.
    - Over a given seven-day period, the team could see 70-90 new C2s emerge during the botnet spamming cycle.
    - Black Lotus Labs observed that more than 25% of C2s do not remain active for more than a day; 50% don't remain active for more than a week.
- Black Lotus Labs discovered a new backconnect server – which is traditionally used for backup communications – that appears to exist only to provide new instructions to bots

within the botnet. Additional discoveries related to this backconnect server include:

- Several hours after bots became infected, a significant number began reaching out to the backconnect server. While its complete functionality is currently unknown, it was often seen turning bots into proxies that could be used or sold for different purposes.
- The way the bots communicated with the backconnect server led us to believe we were looking at bots that had been converted into C2s and could simultaneously maintain bot functionality.

Advantages of Black Lotus Labs' unique visibility

Due to their high turnover rate, Qakbot must continually replace its C2 nodes. Black Lotus Labs can detect this replacement by leveraging Lumen's global IP backbone telemetry. Through machine learning and by emulating the protocol to validate the nodes, Black Lotus Labs can potentially identify – and null-route – as many as 35% of Qakbot C2s before they are used in spam campaigns.

Response and recommendations

Because Qakbot is primarily spread through email hijacking and spamming malicious email attachments and embedded URLs, Lumen customers and other businesses are advised to bolster defenses against phishing as an initial access vector. This should be done by fully monitoring network resources, ensuring proper patch management, and conducting ongoing phishing and social engineering training for employees.

In addition to null-routing all higher-tier infrastructure prior to publication of our research, Black Lotus Labs will continue to collaborate with the community to detect and disrupt Qakbot as this and other botnets rise and fall in activity. The team encourages other organizations to alert on these and similar indicators in their environment.

Additional resources

- For more research from Black Lotus Labs, visit the **blog archive**.
- To see how Black Lotus Labs sees more and stops more, visit their **website**.

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/2023-06-01-New-Lumen-research-reveals-previously-unseen-Qakbot-infrastructure