Lumen Black Lotus Labs discovers an expanding, multipurpose botnet called Chaos

Research suggests criminal actor is cultivating a network of infected devices to launch Distributed Denial of Service (DDoS) attacks and crypto mining

DENVER, Sept. 28, 2022 /**PRNewswire**/ -- Black Lotus Labs®, the threat intelligence team at **Lumen Technologies** (NYSE: LUMN), has discovered a new, rapidly growing, multipurpose malware written in the Go programming language. Dubbed "Chaos" by the author, the malware was developed for Windows, Linux, and a wide array of consumer devices, small office/home office (SOHO) routers and enterprise servers.

> *We are seeing a complex malware that has quadrupled in just two months and is well-positioned to continue accelerating.*

"We are seeing a complex malware that has quadrupled in size in just two months, and it is well-positioned to continue accelerating," said Mark Dehus, director of threat intelligence for Lumen Black Lotus Labs. "Chaos poses a threat to a variety of consumer and enterprise devices and hosts. We strongly recommend organizations bolster their security postures by deploying services like Secure Access Service Edge (SASE) and DDoS mitigation."

Key Findings:

- The Chaos malware exploits known vulnerabilities and enables the actor to:
    - Scan the target system to profile it for future commands.
    - Automatically initiate lateral movement and propagation through Secure Shell (SSH) private keys that are either stolen or obtained using brute force.
    - Launch DDoS attacks and initiate crypto mining.
- Beginning in June, analysts discovered several distinct Chaos clusters that were written in Chinese. The clusters leveraged China-based command and control (C2) infrastructure that grew rapidly in August and September.
- The actor compromised at least one GitLab server and launched numerous DDoS attacks on organizations in the gaming, financial services and technology, media/entertainment,

cryptocurrency, and even DDoS-as-a-Service industries.
- Black Lotus Labs believes this malware is not related to the Chaos ransomware builder **discovered** in 2021; rather, the overlapping code and functions suggest it is likely the evolution of **Kaiji**, a DDoS malware discovered in 2020.

Read the full research report at https://tinyurl.com/BlackLotusLabsChaosMalware

"The Chaos malware targets known vulnerabilities," Dehus added, "we recommend network administrators practice rigorous patch management, and use the IoCs (Indicators of Compromise) outlined in our report to monitor for infection or connections to suspicious infrastructure. Consumers and remote workers should enable automatic software updates, and regularly update passwords and reboot hardware."

Why it Matters:

- The prevalence of malware written in Go has increased dramatically in recent years due to its flexibility, low antivirus detection rates and difficulty to reverse-engineer.
- The Chaos malware is potent because it works across a variety of architectures, targets devices and systems (e.g., SOHO routers and FreeBDS OS) that are not routinely monitored as part of an enterprise security model, and propagates through known vulnerabilities and SSH keys that are either stolen or obtained through brute force.

Black Lotus Labs' Response:

- Black Lotus Labs has null-routed Chaos C2s across the Lumen global backbone and added the IoCs from this campaign into Rapid Threat Defense® – the automated threat detection and response capability that fuels the Lumen Connected Security portfolio by blocking threats before they reach the customer's network.
- The team will continue to monitor for new infrastructure, targeting activity, and expanding Tactics, Techniques and Procedures (TTPs), and share this information with the security research community.

Additional Resources:

- Read about Black Lotus Labs' recent **discovery of ZuoRAT**, which targets SOHO routers.
- See how **Black Lotus Labs** leverages its network visibility to help protect Lumen customers and keep the internet clean.
- For additional Black Lotus Labs research, visit our **blog archive**.
- Learn more about how **SASE** and **DDoS Mitigation** services can protect your business.

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 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 in the United States.

SOURCE Lumen Technologies; Black Lotus Labs

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/2022-09-28-Lumen-Black-Lotus-Labs-discovers-an-expanding,-multipurpose-botnet-called-Chaos