Lumen security research reveals threats still lurk in Windows Subsystem for Linux

Black Lotus Labs discovers evolving capabilities of Linux binaries used as loaders in WSL

DENVER, March 24, 2022 /**PRNewswire**/ -- Last fall, Black Lotus Labs, the threat intelligence team at **Lumen Technologies** (NYSE: LUMN) **discovered** what had – until then – only been theorized: Linux binaries were being used as loaders in Windows Subsystem for Linux (WSL). Since then, the team has analyzed more than 100 samples that indicate the capability is evolving.

Windows Subsystem for Linux: Threats Still Lurk Below the (Sub)Surface

---

Several of the samples leveraged custom-developed and open-source tools (OSTs) that could be used by actors to evade detection while gaining access into endpoints and computer networks.

For more details and to read the detailed report, visit https://tinyurl.com/wsl-lurks.

"This new class of WSL-based attack demonstrates the blurring boundaries between operating systems," said Michelle Lee, director of threat intelligence at Black Lotus Labs. "Because the types of users running WSL tend to have greater network privileges, organizations that use WSL as part of their day-to-day operations should take note to bolster their defenses as quickly as possible."

Tech Talk

- Given the demonstrated interest and the fact that even the samples with valid command and control (C2) infrastructure are evading general detection by AV providers, the infosec community should monitor this newly proven type of attack.
- Several samples were custom-built modules exhibiting a range of functionality that included keylogging, shellcode injection, a stager, and even a cross-platform agent that worked in both Windows and Linux.
    - The increase in custom modules suggests the WSL attack surface is a growing area of

interest.
    - While many of the samples did not yet appear to be fully functional, they demonstrate attack methods that are actively being tested and refined.

- While evaluating samples, Black Lotus Labs found several agents that were largely based on OSTs found on websites like GitHub.

    - OSTs enable actors to minimize development time by using publicly available tools rather than creating their own.
    - All the OST-based samples that leveraged the WSL also relied upon third-party services such as Discord and Telegram for command and control.
    - Black Lotus Labs suspects that by using third-party network services and operating in a nebulous subsystem space, threat actors may be trying to evade some standard detection mechanisms.

Additional Resources

- Read Black Lotus Labs' **initial report** proving that Linux executables were being deployed as stealth Windows loaders.
- To learn more about how to monitor a Windows system with WSL installed for indicators of malicious activity, read this **SANS whitepaper**.
- If your corporate environment uses WSL, Black Lotus Labs recommends that you enable **system monitoring (Sysmon)** tools to help audit commands run via the WSL terminal.
- See how Black Lotus Labs sees more, so we can stop more, at **www.lumen.com/blacklotuslabs**.

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 Black Lotus Labs

For further information: Suzanne K. Dawe, Lumen Public Relations, Connected Security | Black Lotus Labs, P: 720.217.5476, suzanne.dawe@lumen.com

---

https://news.lumen.com/2022-03-24-Lumen-security-research-reveals-threats-still-lurk-in-Windows-Subsystem-for-Linux