NEWS RELEASE

Theory confirmed: Lumen Black Lotus Labs discovers Linux executable files have been deployed as stealth Windows loaders

2021-09-16

DENVER, Sept. 16, 2021 /PRNewswire/ -- **Black Lotus Labs**, the threat intelligence arm of **Lumen Technologies** (NYSE: LUMN), has **proven** what was previously just a theory: threat actors can use a Linux binary as a loader designed for Windows Subsystem for Linux (WSL) to inject malicious files into a Windows running process.

> Black Lotus Labs proved what was previously just a theory: Linux binaries can be used as backdoors to gain access to WSL

Back in 2017, researchers **theorized** that Linux binaries could potentially be used as backdoors to gain access to WSL, but there has never been evidence of such activity in the wild until now. **Today's findings** from Black Lotus Labs proves that it is not only possible – it's actually happening – and samples have been actively developed to abuse this attack surface. This could make it a threat to any machine on which the local system administrator has already installed WSL.

"Threat actors always look for new attack surfaces," said Mike Benjamin, Lumen vice president of product security and head of Black Lotus Labs. "While the use of WSL is generally limited to power users, those users often have escalated privileges in an organization. This creates blind spots as the industry continues to remove barriers between operating systems."

Key Findings:

- Black Lotus Labs discovered several malicious files that were written primarily in Python and compiled in the Linux binary format ELF (Executable and Linkable Format) for the Debian operating system.
- These files acted as loaders running a payload that was either embedded within the sample or retrieved from a remote server and then injected into a running process using Windows API calls.

- While this approach was not particularly sophisticated, the novelty of using an ELF loader designed for the WSL environment gave the technique a detection rate of one or zero in Virus Total, depending on the sample, as of the time of the report.
- Black Lotus Labs has identified a limited number of samples with only one publicly routable IP address, indicating that this activity is limited in scope – potentially still in development – and likely the first documented instance of an actor abusing WSL to install subsequent payloads.

To combat this campaign, Black Lotus Labs null-routed the threat actor infrastructure across the Lumen global IP network.

Recommendations and Resources:

- Read the **full Black Lotus Labs blog** to learn how to identify this tradecraft, see file hashes associated with the campaign, and view the threat actor's larger activity cluster.
- System administrators who have enabled WSL should **ensure proper logging** to detect this type of tradecraft.
- Black Lotus Labs continues to follow this activity and encourages others to do the same.
- Anyone who sees similar activity in their environment can reach out via Twitter **@BlackLotusLabs**.

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 in the United States.

View original content to download multimedia:**https://www.prnewswire.com/news-releases/theory-confirmed-lumen-black-lotus-labs-discovers-linux-executable-files-have-been-deployed-as-stealth-windows-loaders-301378465.html**

SOURCE Lumen Black Lotus Labs