Black Lotus Labs® releases threat intelligence report showing newly discovered watering hole attack that targeted Ukrainian, Canadian organizations

Attackers' tradecraft mimics that of recent hack of San Francisco International Airport websites

DENVER, April 5, 2021 /PRNewswire/ -- **Black Lotus Labs**, the threat intelligence arm of **Lumen Technologies** (NYSE: LUMN)**,** today **announced** it has uncovered a cluster of compromised websites previously used in a series of watering hole attacks. Any visitors who browsed to one of the sites would unknowingly be infected and vulnerable to the threat actor stealing a copy of their Windows authentication credentials, which could be used to impersonate them. The activity, which was only recently discovered, was identified on several Ukrainian websites and one Canadian website in 2019 and 2020.

Watering hole attacks target websites by injecting a malicious function into the site's code, which the victims' machine then executes. These types of attacks have been used for years, including in a high-profile compromise that was detected on **the San Francisco International Airport's (SFO) website** in April 2020.

In its analysis of the attacks in Ukraine and Canada, Black Lotus Labs observed malicious activity that appeared to exhibit the same tradecraft as the San Francisco airport attack. As a result, the team has clustered the activity to the same actor.

To disrupt the attacks in Ukraine and Canada, Black Lotus Labs notified the owners of the compromised websites of these findings.

How the Attacks Were Executed

In the case of the Ukranian, Canadian, and San Francisco airport websites, malicious JavaScript prompted the victims' devices to send their **New Technology LAN Manager (NTLM)** hashes to an actor-controlled server using Server Message Block (SMB), a communications protocol that enables shared access to system resources such as printers and files. In this type of attack, once the threat actor obtains the hashes they can, in some cases, be cracked offline to reveal usernames and passwords.

"Our mission is to leverage our network visibility to help protect our customers and keep the internet clean, so we will continue to monitor this actor and this type of watering hole activity," said Mike Benjamin, head of Black Lotus Labs. "To protect against this type of attack,

organizations should configure their firewalls to prevent outbound SMB-based communications from leaving the network, or consider **turning off or limiting SMB** in the corporate environment."

Additional Information:

- For more details and an in-depth analysis of this latest discovery, read the full **Black Lotus Labs Watering Hole Blog.**
- Any organization that is interested in collaborating with Black Lotus Labs should 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 of Lumen Technologies LLC in the United States. Lumen Technologies LLC is a wholly owned affiliate of Lumen Technologies Inc.

SOURCE Lumen Black Lotus Labs; Lumen Technologies

For further information: Suzanne K. Dawe, Lumen Public Relations | Connected Security | Black Lotus Labs, (318) 582-7011, suzanne.dawe@lumen.com

---

https://news.lumen.com/2021-04-05-Black-Lotus-Labs-R-releases-threat-intelligence-report-showing-newly-discovered-watering-hole-attack-that-targeted-Ukrainian-Canadian-organizations