Black Lotus Labs® lanza un informe sobre inteligencia de amenazas que muestra un ataque de watering hole descubierto recientemente, dirigido a organizaciones ucranianas y canadienses

Las tácticas operativas de los atacantes imitan a las del ataque reciente a los sitios web del Aeropuerto Internacional de San Francisco.

5 de abril de 2021, DENVER – Black Lotus Labs, la división de inteligencia de amenazas de **Lumen Technologies** (NYSE: LUMN)**,** anunció hoy que ha descubierto un clúster de sitios web comprometidos utilizado previamente en una serie de ataques de watering hole. Cualquier visitante que navegara por uno de estos sitios sin saberlo estaría infectado y sería vulnerable a que el actor de la amenaza sustrajera una copia de sus credenciales de autenticación de Windows, que podría usarse para hacerse pasar por ellos. La actividad, que se descubrió recientemente, se identificó en varios sitios web ucranianos y en un sitio web canadiense en 2019 y 2020.

Los ataques de watering hole apuntan a sitios web mediante la inyección de una función maliciosa en el código del sitio, que luego es ejecutada por la máquina de la víctima. Estos tipos de ataques han sido utilizados durante años, incluido un compromiso de alto perfil que fue detectado en **el sitio web del Aeropuerto internacional de San Francisco (SFO)** en abril de 2020.

En su análisis de los ataques en Ucrania y Canadá, Black Lotus Labs observó una actividad maliciosa que parecía exhibir la misma táctica operativa que la del ataque al aeropuerto de San Francisco. Como resultado, el equipo ha agrupado la actividad en el mismo actor.

Para interrumpir los ataques en Ucrania y Canadá, Black Lotus Labs notificó a los propietarios de los sitios web comprometidos sobre estos hallazgos.

Cómo se llevaron a cabo los ataques

En el caso de los sitios web ucranianos, canadiense y del aeropuerto de San Francisco, un JavaScript malicioso preparaba a los dispositivos de las víctimas para que enviaran sus hashes de **New Technology LAN Manager (NTLM)** a un servidor controlado por el actor, usando Server Message Block (SMB), un protocolo de comunicaciones que permite el acceso compartido a recursos tales como impresoras y archivos. En este tipo de ataque, una vez que el actor de la amenaza obtiene los hashes, puede en algunos casos descifrarlos fuera de línea para obtener los

nombres de usuario y contraseñas.

“Nuestra misión consiste en aprovechar la visibilidad de nuestra red para ayudar a proteger a nuestros clientes y mantener la internet limpia, de modo que seguiremos monitoreando a este actor y este tipo de actividad de watering hole”, comentó Mike Benjamin, director de Black Lotus Labs. “Para protegerse de este tipo de ataques, las organizaciones deberían configurar sus firewalls para evitar que las comunicaciones salientes basadas en SMB salgan de la red, o considerar **desactivar o limitar SMB** en el entorno corporativo.”

Información adicional:

- Para más información y un análisis profundo de este reciente descubrimiento, lea el blog completo de **Black Lotus Labs sobre ataque de watering hole**
- Cualquier organización interesada en colaborar con Black Lotus Labs puede contactarnos por Twitter a **@BlackLotusLabs**.

Acerca de Lumen Technologies:

Lumen se guía por la convicción de que la humanidad está en su mejor estado cuando la tecnología mejora nuestra forma de vivir y trabajar. Con aproximadamente 720.000 km de rutas de fibra y prestando servicios a clientes en más de 60 países, entregamos la plataforma más rápida y segura para aplicaciones y datos, para ayudar a empresas, gobiernos y comunidades a entregar experiencias increíbles. Conozca más sobre las soluciones de red, seguridad, comunicación y colaboración de Lumen y nuestro propósito de promover el progreso humano a través de la tecnología en **news.lumen.com**/home, LinkedIn: /lumentechnologies, Twitter: @lumentechco, Facebook: /lumentechnologies, Instagram: @lumentechnologies y YouTube: /lumentechnologies. Lumen y Lumen Technologies son marcas registradas de Lumen Technologies LLC en los Estados Unidos. Lumen Technologies LLC es una filial de propiedad absoluta de Lumen Technologies, Inc.

Síganos en nuestras redes sociales de LATAM:

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

---

https://news.lumen.com/black-lotus-lab-watering-hole-attack-sp