Microsoft advirtió sobre las amenazas emergentes en el panorama Web3, incluyendo las campañas de *«phishing de hielo»,* ya que el aumento en la adopción de las tecnologías blockchain y DeFi enfatiza la necesidad de incorporar seguridad en la web descentralizada mientras aún se encuentra en sus primeras etapas.

El equipo de investigación de Microsoft 365 Defender de la compañía, mencionó vías nuevas a través de las cuales los atacantes pueden intentar engañar a los usuarios de criptomonedas para que entreguen sus claves criptográficas privadas y realicen transferencias de fondos no autorizadas.

> *«Un aspecto que permite la cadena de bloques pública e inmutable es la transparencia total, por lo que se puede observar y estudiar un ataque después de que pase. También permite la evaluación del impacto financiero de los ataques, lo cual es un desafío en los ataques de phishing web2 tradicionales»,* dijo Christian Seifert, gerente principal de investigación del Grupo de Seguridad y Cumplimiento de Microsoft.

El robo de las claves podría llevarse a cabo de distintas formas, incluyendo la suplantación del software de la billetera, la implementación de malware en los dispositivos de las víctimas, la falsificación de las interfaces de los contratos inteligentes legítimos y la acuñación de tokens digitales no autorizados para las estafas Airdrop.

Otra técnica involucra lo que Microsoft llama *«phishing de hielo».* En lugar de robar las claves privadas de un usuario, el método funciona engañando al objetivo para que *«firme una transacción que delega la aprobación de los tokens del usuario al atacante».*

> *«Una vez que la transacción de aprobación ha sido firmada, enviada y extraída, el gastador puede acceder a los fondos. En caso de un ataque de phishing de hielo, el atacante puede acumular aprobaciones durante un período de tiempo y luego agotar todas las billeteras de la víctima rápidamente»,* dijo Seifert.

El hackeo de alto perfil de la plataforma DeFi BadgerDAO, que salió a la luz a inicios de diciembre de 2021, fue uno de esos casos de phishing de hielo, en el que un fragmento inyectado maliciosamente utilizando una clave API comprometida permitió al atacante desviar 121 millones de dólares en fondos.

> *«El atacante implementó el script de trabajo por medio de una clave API comprometida que se creó sin el conocimiento o la autorización de los ingenieros de Badger. El (los) atacante (s) usó este acceso API para inyectar periódicamente código malicioso en la aplicación Badger de modo que solo afectó a un subconjunto de la base de usuarios»,* dijo BadgerDAO.

La secuencia de comandos se programó de tal forma que interceptaría las transacciones Web3 de las billeteras con un saldo determinado e insertaría una solicitud para transferir los tokens de la víctima a una dirección elegida por los atacantes.

Para mitigar las amenazas que afectan a la tecnología blockchain, Microsoft recomienda a los usuarios que revisen y auditen los contratos inteligentes para obtener una respuesta adecuada a los incidentes o capacidades de emergencia y que reevalúen y revoquen periódicamente las asignaciones de tokens.