Los atacantes maliciosos aprovecharon un proceso de actualización de contrato inteligente en el mercado OpenSea NFT para realizar un ataque de phishing contra 17 de sus usuarios que resultó en el robo de activos virtuales por un monto aproximado de 1.7 millones de dólares.

Los NFT (Tokens No Fungibles), son tokens digitales que actúan como certificados de autenticidad y, en algunos casos, representan la propiedad de activos que van desde ilustraciones costosas hasta coleccionables y bienes físicos.

La estafa de ingeniería social oportunista afectó a los usuarios utilizando el mismo correo electrónico de OpenSea notificando a los usuarios sobre la actualización, con el correo electrónico de imitación redirigiendo a las víctimas a una página web similar, incitándolos a firmar una transacción aparentemente legítima, solo para robar todos los NFT.

> *«Al firmar la transacción, se enviaría una solicitud atomic_Match_ al contrato del atacante. A partir de ahí, atomicMatch_ se reenviaría al contrato de OpenSea, lo que llevaría a la transferencia de los NFT de la víctima al atacante»,* dijeron los investigadores de Check Point.

La compañía dijo que aún está investigando la fuente exacta del ataque y dijo que las órdenes maliciosas habían sido firmadas por las víctimas antes de que OpenSea llevara a cabo su migración. *«El ataque no parece estar activo en este momento. No ha habido actividad en el contrato malicioso en más de 15 horas»,* dijo OpenSea.

> *«Firmar una transacción es similar a dar permiso a alguien para acceder a todos sus NFT y criptomonedas. Es por eso que firmar es muy peligroso. Preste especial atención a dónde y cuándo firmar una transacción»*, dijo Check Point.

El desarrollo también se produce cuando los ciberdelincuentes se encuentran explotando el

crecimiento de la popularidad de las NFT para engañar a las víctimas para que descarguen el malware troyano de acceso remoto BitRAT que es capaz de robar las credenciales del navegador, extraer criptomonedas y recopilar información confidencial.