Roban 1,7 millones US$ en NFT en OpenSea

El mercado estadounidense de tokens no fungibles (NFT) OpenSea registró un ataque de 'phishing' el pasado fin de semana, que tuvo como resultado un robo valorado en casi dos millones de dólares en NFT en tan solo tres horas.

El cofundador y CEO de OpenSea, Devin Finzer, ha explicado a través de Twitter que los ataques a estas cuentas personales en OpenSea fueron ajenos a la plataforma y que no se originaron internamente.

«Por lo que sabemos, se trata de un ataque de 'phishing'. No creemos que esté relacionado con la web de OpenSea. Parece que, hasta ahora, 32 usuarios firmaron una carga maliciosa de un atacante y algunos de sus NFT fueron robados», ha indicado en la red social.

Para detallar el modo en que se ha procedido al ataque, el directivo ha compartido un hilo de tuits en el que otro usuario detalla cómo se produjo el saqueo de las cuentas este sábado.

En este caso, el atacante violó el protocolo wyvern, un estándar de código abierto que utilizan diferentes plataformas -entre ellas, este mercado de NFT- para respaldar los contratos de comercio de estos activos.

Eso indica que habría modificado estos acuerdos para hacerse pasar por la plataforma y engañar a las víctimas, a quienes instó a compartir información y aprobar contratos parciales de sus cuentas. De ese modo, una parte del contrato quedaba firmada por la víctima y, la otra, por el atacante haciéndose pasar por OpenSea.

Una vez firmados, completó los datos que faltaban con los NFT que querían robar de los usuarios originales y los vinculó con su propio contrato para proceder a la transferencia de tokens no fungibles.

«Los datos de los NFT y las transferencias se guardan cuando se envían las órdenes firmadas [por las víctimas] al contrato wyvern, que verifica que son válidas y que las firmas son correctas», menciona este usuario, conocido como Neso.

Una vez se valida el pedido, se conecta con el servidor proxy, que alberga todos los permisos del sistema operativo (SO) y este

reclama al emisor (atacante) la orden de transferencia junto «con los datos de llamada, que en la mayoría de estas órdenes es el NFT que se está comprando o vendiendo», ha añadido este usuario.

Finalmente, el atacante modifica las direcciones y los tokens de transferencia previamente guardadas en el contrato proxy que cuenta con la aprobación del usuario original y las revierte, como si se tratase de una operación validada por las víctimas.

Según ha señalado la compañía de seguridad 'blockchain' y análisis de datos PeckShield, durante el ataque se requisaron 254 tokens de diferentes colecciones, causando un robo valorado en 1,7 millones de dólares (cerca de 1,5 millones de euros). Entre las cuentas que figuran en este listado se encuentran algunas de las más valiosas actualmente, como Bored Ape Yacht Club.

Conviene recordar que tan solo unos días antes, el pasado viernes 18 de febrero, la compañía presentó un nuevo contrato inteligente y solicitó a los usuarios una migración de sus activos.
Por ese motivo, y mientras continúa la investigación para conocer con mayor profundidad el caso de robo, Finzer ha asegurado que «la interacción con un correo electrónico [para proceder a esta migración] de OpenSea no es un vector de ataque».

Con ello, ha descartado otros vectores de ataque, como hacer clic en el banner de la web, el uso de la herramienta de migración en OpenSea para mover listados al nuevo contrato Wyvern 2.3 o acuñar, comprar, vender o listar elementos en la plataforma.

Con información de PortalTic.