El fabricante de monederos de hardware para criptomonedas, Ledger, lanzó una nueva edición de su módulo npm «@ledgerhq/connect-kit» después de que actores de amenazas no identificados insertaran código malicioso, provocando el robo de más de $600,000 en activos virtuales.

La vulnerabilidad surgió porque un antiguo empleado cayó víctima de un ataque de phishing, según explicó la compañía en un comunicado.

Este incidente permitió a los atacantes acceder a la cuenta npm de Ledger y cargar tres versiones maliciosas del módulo: 1.1.5, 1.1.6 y 1.1.7, propagando malware de criptoextracción a otras aplicaciones que dependen del módulo, resultando en una violación de la cadena de suministro de software.

> *«El código malicioso utilizó un proyecto falso de WalletConnect para redirigir fondos a una billetera controlada por un hacker»,* informó Ledger.

Como su nombre indica, Connect Kit posibilita la conexión de aplicaciones descentralizadas (DApps) con los monederos de hardware de Ledger.

De acuerdo con la firma de seguridad Sonatype, la versión 1.1.7 incorporó directamente una carga útil de extracción de monedero para ejecutar transacciones no autorizadas con el propósito de transferir activos digitales a una billetera controlada por un actor.

Mientras que las versiones 1.1.5 y 1.1.6, aunque carecían de un componente de extracción integrado, fueron modificadas para descargar un paquete secundario de npm, identificado como 2e6d5f64604be31, que actuaba como un programa de criptoextracción.

> *«Una vez instalado en su software, el malware presenta a los usuarios una falsa ventana de diálogo modal que los invita a conectar billeteras. Una vez que los usuarios hacen clic en esta ventana, el malware comienza a extraer fondos de las billeteras conectadas»,* explicó el investigador de Sonatype, Ilkka Turunen.

Se estima que el archivo malicioso estuvo activo durante aproximadamente cinco horas, aunque el periodo de explotación activa durante el cual se extrajeron los fondos se limitó a menos de dos horas.

Revoke.cash, una de las compañías afectadas por el incidente, señaló que Ledger carecía de protecciones de autenticación de dos factores (2FA) para sus sistemas de implementación, lo que permitió que un atacante utilizara la cuenta comprometida del desarrollador para publicar una versión maliciosa del software.

Desde entonces, Ledger ha eliminado las tres versiones maliciosas de Connect Kit de npm y ha lanzado la versión 1.1.8 para mitigar el problema. También ha informado sobre las direcciones de billetera del actor de amenazas y ha indicado que Tether, el emisor de la stablecoin, ha bloqueado los fondos robados.

En cualquier caso, este suceso destaca la continua focalización de los ecosistemas de código abierto, con registros de software como PyPI y npm utilizados cada vez más como vectores

para instalar malware mediante ataques a la cadena de suministro.

El módulo npm fraudulento en cuestión, 2e6d5f64604be31, ha sido eliminado del repositorio de paquetes por el equipo de seguridad debido a la presencia de *«código malicioso».*