Los investigadores de ciberseguridad han descubierto un paquete malicioso de Python en el repositorio Python Package Index (PyPI) diseñado para robar las claves privadas de Ethereum de sus víctimas al hacerse pasar por bibliotecas populares.

El paquete en cuestión es set-utils, que ha sido descargado 1,077 veces hasta la fecha. Actualmente, ya no está disponible para su descarga desde el registro oficial.

> *«Disfrazado como una simple utilidad para conjuntos en Python, el paquete imita bibliotecas ampliamente utilizadas como python-utils (más de 712 millones de descargas) y utils (más de 23.5 millones de descargas)»,* señaló la empresa de seguridad en la cadena de suministro de software Socket.
>
> *«Este engaño hace que los desarrolladores desprevenidos instalen el paquete comprometido, otorgando a los atacantes acceso no autorizado a monederos de Ethereum».*

El paquete tiene como objetivo atacar a desarrolladores de Ethereum y organizaciones que trabajan con aplicaciones blockchain basadas en Python, especialmente aquellas que gestionan monederos con bibliotecas como eth-account.

Además de incrustar la clave pública RSA del atacante para cifrar los datos robados y una cuenta de remitente de Ethereum bajo su control, la biblioteca se engancha en funciones de creación de monederos como «from_key()» y «from_mnemonic()», interceptando las claves privadas a medida que se generan en la máquina comprometida.

En un giro interesante, las claves privadas son exfiltradas a través de transacciones en la blockchain mediante el endpoint RPC de Polygon «rpc-amoy.polygon.technology», en un intento por evadir los métodos tradicionales de detección que monitorean solicitudes HTTP sospechosas.

> *«Esto garantiza que, incluso cuando un usuario crea con éxito una cuenta de Ethereum, su clave privada sea robada y transmitida al atacante. La función maliciosa se ejecuta en un hilo en segundo plano, lo que hace que su detección sea aún más difícil»*, explicó Socket.