Expertos en ciberseguridad han detectado tres grupos de paquetes maliciosos alojados en los repositorios de npm y Python Package Index (PyPI). Estos paquetes están diseñados para robar información y, en algunos casos, eliminar datos sensibles de los sistemas comprometidos.

A continuación, se detalla la lista de paquetes identificados:

- @async-mutex/mutex, a typosquat of async-mute (npm)
- dexscreener, which masquerades as a library for accessing liquidity pool data from decentralized exchanges (DEXs) and interacting with the DEX Screener platform (npm)
- solana-transaction-toolkit (npm)
- solana-stable-web-huks (npm)

- cschokidar-next, a typosquat of chokidar (npm)
- achokidar-next, a typosquat of chokidar (npm)
- achalk-next, a typosquat of chalk (npm)
- csbchalk-next, a typosquat of chalk (npm)
- cschalk, a typosquat of chalk (npm)
- pycord-self, a typosquat of discord.py-self (PyPI)

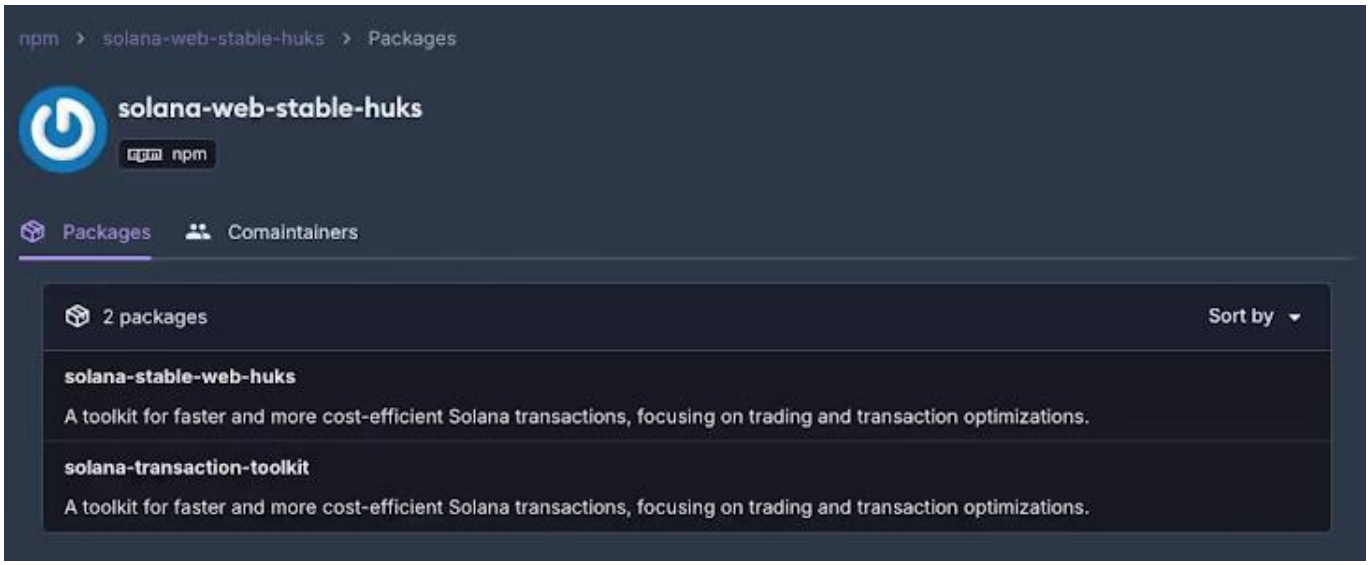
La empresa especializada en seguridad de la cadena de suministro, Socket, que descubrió estos paquetes, explicó que los cuatro primeros están diseñados para capturar claves privadas de Solana y enviarlas a través de los servidores SMTP de Gmail. El objetivo principal parece ser vaciar las billeteras de las víctimas.

En particular, los paquetes solana-transaction-toolkit y solana-stable-web-huks pueden drenar automáticamente las billeteras, transfiriendo hasta el 98% de sus fondos a una dirección de Solana controlada por los atacantes. Mientras tanto, estos paquetes se presentan como herramientas útiles para funciones específicas de Solana.

> *"Como Gmail es un servicio de correo ampliamente confiable, estos intentos de*

> *exfiltración son menos propensos a ser detectados por firewalls o sistemas de monitoreo, que consideran el tráfico hacia smtp.gmail.com como legítimo,"* explicó Kirill Boychenko, investigador en seguridad.

Además, Socket descubrió dos repositorios en GitHub vinculados con los responsables de solana-transaction-toolkit y solana-stable-web-huks, los cuales supuestamente ofrecen herramientas de desarrollo para Solana o scripts que automatizan tareas comunes en DeFi. Sin embargo, estos repositorios están diseñados para importar paquetes maliciosos de npm.



Las cuentas de GitHub relacionadas con estos repositorios, «moonshot-wif-hwan» y «Diveinprogramming,» ya no están disponibles.

> *"Un script alojado en el repositorio de GitHub del atacante, moonshot-wif-hwan/pumpfun-bump-script-bot, promocionado como un bot para operar en Raydium (un popular DEX basado en Solana), en realidad importa código malicioso desde el paquete solana-stable-web-huks,"* señaló Boychenko.

El uso de repositorios fraudulentos en GitHub evidencia los esfuerzos de los atacantes para extender su campaña más allá de npm, dirigiéndose a desarrolladores que buscan herramientas relacionadas con Solana en esta plataforma de alojamiento de código.

El segundo grupo de paquetes maliciosos de npm introduce funcionalidades más destructivas, como una *"función de apagado"* que elimina de forma recursiva todos los archivos en los directorios específicos del proyecto. En algunos casos, también exfiltran variables de entorno hacia un servidor remoto.

El paquete falso csbchalk-next imita las funciones de versiones mal escritas de chokidar, con la diferencia de que inicia el borrado de datos solo después de recibir el código "202" desde el servidor.

Por su parte, Pycord-self se dirige a desarrolladores de Python interesados en usar las APIs de Discord, capturando tokens de autenticación y conectándose a un servidor controlado por los atacantes. Esto permite establecer una puerta trasera persistente en sistemas Windows y Linux tras su instalación.