Los expertos en ciberseguridad han identificado un nuevo paquete malicioso en Python que se presenta como una herramienta de comercio de criptomonedas, pero que contiene funciones diseñadas para robar información sensible y vaciar los activos de las billeteras de criptomonedas de las víctimas.

Este paquete, denominado «CryptoAITools,» se ha distribuido a través del Índice de Paquetes de Python (PyPI) y repositorios falsos en GitHub. Se registró más de 1,300 descargas antes de ser eliminado de PyPI.

> *«El malware se activa de forma automática al instalarse, dirigiéndose a sistemas operativos Windows y macOS. Se utilizó una interfaz gráfica de usuario (GUI) engañosa para distraer a las víctimas mientras el malware llevaba a cabo sus actividades maliciosas en segundo plano»,* informó Checkmarx en un nuevo reporte.

El paquete está diseñado para llevar a cabo su comportamiento dañino de inmediato tras la instalación, a través de un código insertado en su archivo «init.py,» que primero verifica si el sistema objetivo es Windows o macOS para ejecutar la versión adecuada del malware.

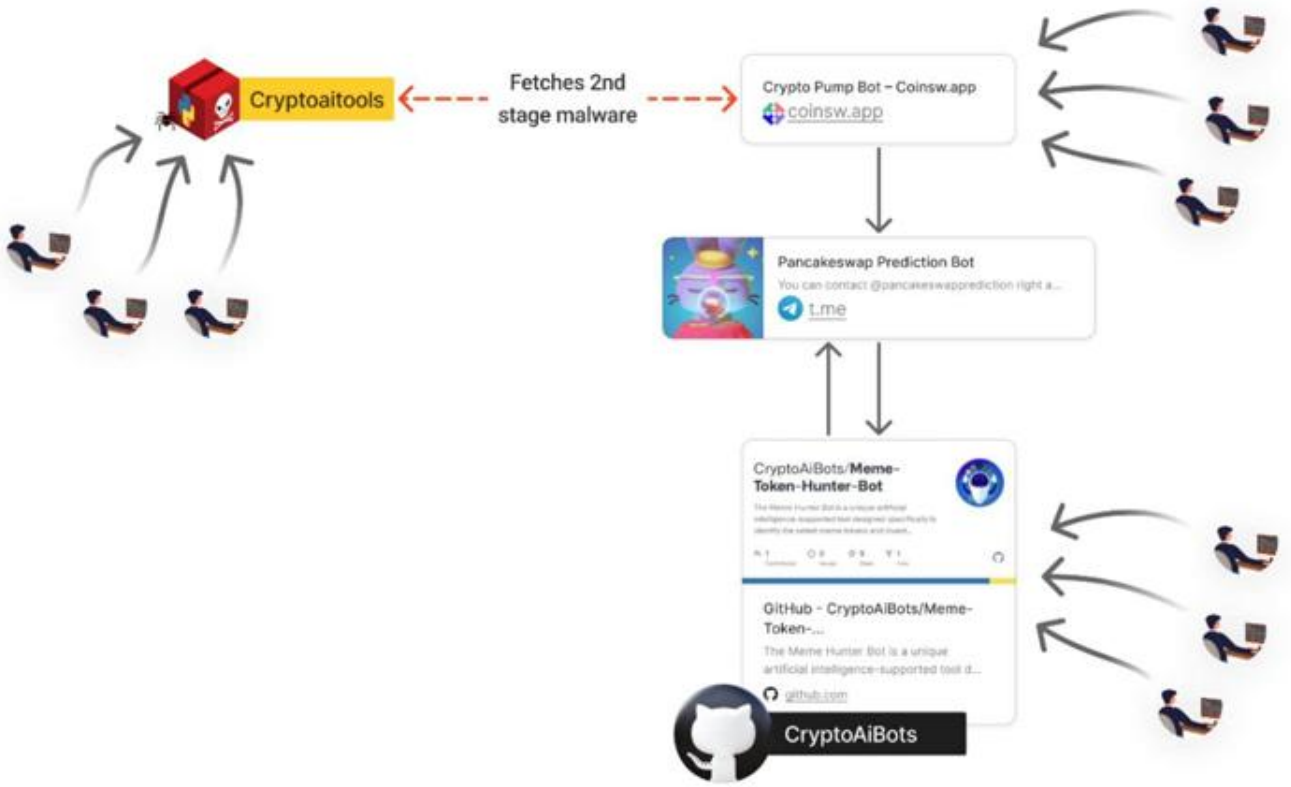
Dentro del código existe una función auxiliar que se encarga de descargar y ejecutar cargas adicionales, iniciando así un proceso de infección en varias etapas.

En particular, las cargas se descargan de un sitio web falso («coinsw[.]app«) que promociona un servicio de bot de trading de criptomonedas, pero que en realidad busca dar una apariencia de legitimidad al dominio si un desarrollador decide acceder directamente a él a través de un navegador web.

Este método no solo ayuda al atacante a evadir la detección, sino que también les permite ampliar las capacidades del malware a voluntad al simplemente modificar las cargas alojadas en el sitio que aparenta ser legítimo.

Un aspecto destacado del proceso de infección es la inclusión de un componente GUI que

distrae a las víctimas mediante un falso proceso de instalación, mientras el malware recopila de manera encubierta información sensible de los sistemas.



> *«El malware CryptoAITools realiza una operación extensa de robo de datos, dirigiéndose a una amplia variedad de información sensible en el sistema afectado. El objetivo principal es recopilar cualquier dato que pueda ayudar al atacante a robar activos de criptomonedas»,* comentó Checkmarx.

Esto incluye información de billeteras de criptomonedas (Bitcoin, Ethereum, Exodus, Atomic, Electrum, etc.), contraseñas guardadas, cookies, historial de navegación, extensiones de criptomonedas, claves SSH, y archivos almacenados en las carpetas de Descargas,

Documentos y Escritorio que hagan referencia a criptomonedas, así como contraseñas e información financiera, y Telegram.

En dispositivos Apple con macOS, el ladrón también recopila datos de las aplicaciones Apple Notes y Stickies. La información recolectada se carga al servicio de transferencia de archivos gofile[.]io, y luego se elimina la copia local.

Checkmarx también descubrió que el actor de amenazas estaba distribuyendo el mismo malware ladrón a través de un repositorio de GitHub llamado Meme Token Hunter Bot, que se presenta como *«un bot de trading impulsado por IA que lista todos los tokens meme en la red Solana y realiza transacciones en tiempo real una vez que son considerados seguros.»*

Esto indica que la campaña está apuntando también a usuarios de criptomonedas que deciden clonar y ejecutar el código directamente desde GitHub. El repositorio, que sigue activo al momento de redactar, ha sido bifurcado una vez y ha recibido 10 estrellas.

Además, los operadores gestionan un canal de Telegram que promueve el mencionado repositorio de GitHub, así como ofrece suscripciones mensuales y soporte técnico.

> *«Este enfoque multiplataforma permite al atacante extender su red, alcanzando potencialmente a víctimas que pueden ser cautelosas en una plataforma pero confiar en otra,»* declaró Checkmarx.
>
> *«La campaña de malware CryptoAITools tiene consecuencias graves para las víctimas y la comunidad de criptomonedas en general. Los usuarios que dieron estrellas o bifurcaron el repositorio malicioso 'Meme-Token-Hunter-Bot' son víctimas potenciales, lo que amplía significativamente el alcance del ataque.»*