Los investigadores en ciberseguridad han alertado sobre un nuevo paquete malicioso de Python que ha sido descubierto en el repositorio de Python Package Index (PyPI) y que está diseñado para facilitar el robo de criptomonedas como parte de una campaña más amplia.

El paquete en cuestión se llama pytoileur y, hasta el momento de redactar este informe, ha sido descargado 316 veces. De manera interesante, el autor del paquete, conocido como PhilipsPY, ha subido una nueva versión del paquete (1.0.2) con la misma funcionalidad después de que la versión anterior (1.0.1) fuera retirada por los mantenedores de PyPI el 28 de mayo de 2024.

Según un análisis realizado por Sonatype, el código malicioso está incrustado en el script setup.py del paquete, permitiendo la ejecución de una carga útil codificada en Base64 que se encarga de descargar un binario de Windows desde un servidor externo.

> *«El binario descargado, 'Runtime.exe', se ejecuta utilizando comandos de Windows PowerShell y VBScript en el sistema,»* explicó el investigador de seguridad Ax Sharma.

Una vez instalado, el binario establece persistencia y descarga cargas útiles adicionales, incluyendo spyware y un malware ladrón capaz de recopilar datos de navegadores web y servicios de criptomonedas.

Sonatype también identificó una cuenta recién creada en StackOverflow llamada «EstAYA G» que respondía a las preguntas de los usuarios en la plataforma de preguntas y respuestas, dirigiéndolos a instalar el paquete malicioso pytoileur como una supuesta solución a sus problemas.

> *«Aunque es difícil atribuir con certeza cuando se trata de cuentas de usuario seudónimas en plataformas de internet sin acceso a los registros, la reciente creación de ambas cuentas de usuario y su único propósito de publicar y*

> *promocionar el paquete malicioso de Python nos indica que están vinculadas al mismo actor o actores de amenaza detrás de esta campaña,»* dijo Sharma a The Hacker News.

Este desarrollo representa una nueva escalada, ya que abusa de una plataforma confiable como vector de propagación de malware.

> *«El abuso abierto e inédito de una plataforma tan confiable, utilizándola como un terreno fértil para campañas maliciosas, es una gran señal de advertencia para los desarrolladores en todo el mundo,»* comentó Sonatype en una declaración.
>
> *«El compromiso de Stack Overflow es especialmente preocupante dado el gran número de desarrolladores novatos que tiene, quienes están aprendiendo, haciendo preguntas y pueden caer en consejos maliciosos.»*

Cuando se les solicitó un comentario, Stack Overflow informó a The Hacker News que tomó medidas para suspender la cuenta.

> *«El equipo de Confianza y Seguridad de Stack Overflow ha investigado la reclamación. El equipo descubrió cierto contenido que viola las políticas de la red de Stack Overflow, lo eliminó de la red y tomó acciones adicionales de acuerdo con los procedimientos estándar de respuesta a incidentes»,* dijo un portavoz de la compañía a la publicación.

Un examen más detallado de los metadatos del paquete y su historial de autoría ha revelado coincidencias con una campaña anterior que involucraba paquetes falsos de Python como Pystob y Pywool, que fue divulgada por Checkmarx en noviembre de 2023.

Estos hallazgos son otro ejemplo de por qué los ecosistemas de código abierto continúan siendo un objetivo atractivo para los actores malintencionados que buscan comprometer múltiples objetivos al mismo tiempo con ladrones de información como Bladeroid y otros tipos de malware a través de lo que se conoce como un ataque a la cadena de suministro.

(La historia se actualizó después de la publicación para incluir una respuesta de Stack Overflow sobre la suspensión de la cuenta).