Los administradores del repositorio Python Package Index (PyPI) han aislado el paquete «aiocpa» tras identificar una actualización reciente que incluía código malicioso diseñado para extraer claves privadas mediante Telegram.

Este paquete, descrito como un cliente API de Crypto Pay que funciona tanto de forma síncrona como asíncrona, fue lanzado originalmente en septiembre de 2024 y acumula 12,100 descargas hasta la fecha.

El aislamiento de la biblioteca por parte de PyPI evita que nuevos usuarios puedan instalarla y bloquea cualquier modificación por parte de los desarrolladores responsables.

La firma de ciberseguridad Phylum, que reveló detalles sobre este ataque a la cadena de suministro de software la semana pasada, indicó que el creador del paquete subió la actualización maliciosa al repositorio de PyPI, mientras mantenía limpio el repositorio del proyecto en GitHub, intentando así pasar desapercibido.

No se ha confirmado aún si la modificación maliciosa fue realizada por el desarrollador original o si sus credenciales fueron comprometidas por un tercero.

El comportamiento sospechoso se detectó por primera vez en la versión 0.1.13 del paquete, que contenía cambios en el archivo «sync.py». Este archivo estaba diseñado para descodificar y ejecutar un fragmento de código ofuscado inmediatamente después de que el paquete fuera instalado.

«Este código en particular está codificado y comprimido en un proceso recursivo 50 veces», explicó Phylum, añadiendo que su propósito era capturar y enviar el token de la API de Crypto Pay de la víctima a través de un bot de Telegram.

Crypto Pay es una plataforma de pagos que utiliza Crypto Bot (@CryptoBot) para permitir a los usuarios aceptar pagos en criptomonedas y transferir fondos mediante una API.

El incidente es notable porque pone de manifiesto la importancia de analizar el código fuente

de los paquetes antes de instalarlos, en lugar de confiar únicamente en la revisión de sus repositorios asociados.

«Como demuestra este caso, los atacantes pueden mantener repositorios fuente limpios mientras distribuyen paquetes maliciosos en los ecosistemas», afirmó Phylum, añadiendo que este ataque *«es un recordatorio de que el historial de seguridad de un paquete no garantiza su protección futura».*