Se descubrió que un paquete malicioso, ya eliminado, enviado al repositorio oficial de software de terceros para Python, implementa criptomineros en sistemas Linux.

El módulo, llamado «secretslib» y que ha sido descargado 93 veces antes de su eliminación, se lanzó al índice de paquetes de Python (PyPI) el 6 de agosto de 2022, y se describe como *«comparación y verificación de secretos simplificada».*

> *«Sin embargo, en una inspección más cercana, el paquete ejecuta criptomineros de forma encubierta en la memoria de su máquina Linux (directamente desde su RAM), una técnica empleada en gran medida por el malware y los encriptadores sin archivos»,* dijo el investigador de Sonartype Ax Sharma.

Lo logra mediante la ejecución de un archivo ejecutable de Linux reuperado de un servidor remoto luego de la instalación, cuya tarea principal es colocar un archivo ELF («memfd«) directamente en la memoria, que funciona como un criptominero de Monero, después de lo cual es eliminado por el paquete «secretslib».

> *«La actividad maliciosa deja poca o ninguna huella y es bastante 'invisible' en un sentido forense»*, dijo Sharma.

Además, el atacante detrás del paquete abusó de la identidad y la información de contacto de un ingeniero de software legítimo que trabajaba para el Laboratorio Nacional de Argonne, un laboratorio financiado por el Departamento de Energía de Estados Unidos, para dar credibilidad al malware.

La idea, en pocas palabras, es engañar a los usuarios para que descarguen bibliotecas envenenadas asignándolas a mantenedores populares y confiables sin su conocimiento o consentimiento: una amenaza en la cadena de suministro llamada plantación de paquetes.

El desarrollo se produce cuando PyPi tomó medidas para purgar 10 paquetes maliciosos que fueron orquestados para recolectar puntos de datos críticos, como contraseñas y tokens API.