Se han encontrado cuatro paquetes no autorizados distintos en el índice de paquetes de Python (PyPI) para llevar a cabo una serie de acciones maliciosas, incluyendo la adición de malware, la eliminación de la utilidad netstar y la manipulación del archivo de claves autorizadas SSH.

Los paquetes en cuestión son aptx, bingchilling2, httops y tkint3rs, todos los cuales se descargaron de forma colectiva unas 450 veces antes de que se eliminaran. Mientras que aptx es un intento de hacerse pasar por el popular códec de audio del mismo nombre de Qualcomm, httops y tkint3rs son typosquats de https y tkinter, respectivamente.

> *«La mayoría de estos paquetes tenían nombres bien pensados para confundir a la gente a propósito»*, dijo el periodista e investigador de seguridad Ax Sharma.

Un análisis del código malicioso inyectado en el script de instalación revela la presencia de una carga útil ofuscada de Meterpreter, que está disfrazada como «pip«, un instalador de paquetes legítimo para Python, y puede aprovecharse para obtener acceso de shell al host infectado.

También se llevan a cabo pasos para eliminar la utilidad de línea de comandos netsat que se usa para monitorear la configuración y la actividad de la red, así como para modificar el archivo .ssh/authorized_keys para configurar una puerta trasera SSH para el acceso remoto.

> *«Ahora bien, este es un ejemplo elegante pero del mundo real de malware dañino que se abrió paso con éxito en el ecosistema de código abierto»,* dijo Sharma.

Pero como señal de que el malware que se infiltra en los repositorios de software es una amenaza recurrente, Fortinet FortiGuard Labs descubrió cinco paquetes distintos: web3-essential, 3m-promo-gen-api, ai-solver-gen, hypixel-coins, httpxrequesterv2 y httpxrequester, que están diseñados para recolectar y exfiltrar información confidencial.

Las revelaciones se producen cuando ReversingLabs arrojó luz sobre un módulo npm malicioso llamado aabquerys que está diseñado para hacerse pasar por el paquete abquery legítimo para engañar a los desarrolladores para que lo descarguen.

El código JavaScript ofuscado, por su parte, cuenta con capacidades para recuperar un ejecutable de segunda etapa desde un servidor remoto que, a su vez, contiene un proxy binario de Avast (wsc_proxy.exe) que se sabe que es vulnerable a los ataques de carga lateral de DLL.

Esto permite que el atacante invoque una biblioteca maliciosa que está diseñada para obtener un componente de tercera etapa, Demon.bin, desde un servidor de comando y control (C2).

> *«Demon.bin es un agente malicioso con funcionalidades típicas de RAT (Troyano de Acceso Remoto) que se generó usando un marco de comando y control de código abierto, posterior a la explotación llamado Havoc»,* dijo Lucija Valentic, investigadora de Reversing Labs.

Además, se dice que el autor de aabquerys publicó múltiples versiones de otros dos paquetes llamados bbbquery y nvm_jquery que se sospecha que son las primeras iteraciones de aabquerys.

Havoc está lejos de ser el único marco de explotación de C2 detectado en la naturaleza, ya que los hackers aprovechan suites personalizadas como Manjusaka, Covenant, Merlin y Empire en campañas de malware.

Los hallazgos también subrayan al creciente riesgo de paquetes maliciosos que acechan en los repositorios de código abierto como npm y PyPi, que pueden tener un impacto severo en

la cadena de suministro de software.