Expertos en ciberseguridad identificaron dos paquetes maliciosos en el repositorio Python Package Index (PyPI) que se hacían pasar por modelos reconocidos de inteligencia artificial, como OpenAI ChatGPT y Anthropic Claude, para distribuir un malware conocido como JarkaStealer.

Los paquetes, llamados gptplus y claudeai-eng, fueron publicados en noviembre de 2023 por un usuario con el alias «Xeroline» y lograron 1,748 y 1,826 descargas, respectivamente. Actualmente, ya no están disponibles en PyPI.

> *«Ambos paquetes fueron subidos por el mismo autor y solo se diferenciaban en el nombre y la descripción»,* explicó Kaspersky en un informe.

Los desarrolladores de los paquetes afirmaban ofrecer acceso a las API de GPT-4 Turbo y Claude AI, pero en realidad incluían código dañino que activaba el despliegue del malware al ser instalado.

En particular, el archivo «init.py» contenía datos codificados en Base64 diseñados para descargar un archivo Java («JavaUpdater.jar») desde un repositorio de GitHub («github[.]com/imystorage/storage»). Si el sistema no contaba con el entorno de ejecución de Java (JRE), también se descargaba automáticamente desde un enlace de Dropbox antes de ejecutar el archivo JAR.

Este archivo JAR contenía JarkaStealer, un malware especializado en robar información confidencial como datos de navegadores web, detalles del sistema, capturas de pantalla y tokens de sesión de aplicaciones como Telegram, Discord y Steam.

El proceso final del ataque incluía archivar la información obtenida, enviarla a un servidor controlado por los atacantes y luego eliminar cualquier rastro del dispositivo afectado. JarkaStealer se ha comercializado en un modelo de malware como servicio (MaaS) a través de un canal de Telegram, con precios entre $20 y $50, aunque su código fuente se filtró en GitHub.

Según datos de ClickPy, los paquetes fueron descargados principalmente por usuarios de países como Estados Unidos, China, India, Francia, Alemania y Rusia, como parte de una campaña de ataques a la cadena de suministro que se extendió durante un año.

«Este caso pone de manifiesto los riesgos constantes de los ataques a la cadena de suministro de software y enfatiza la importancia de mantener una estricta vigilancia al incorporar componentes de código abierto en los procesos de desarrollo», señaló Leonid Bezvershenko, investigador de Kaspersky.