Se descubrió que un paquete malicioso de Python en el repositorio Python Package Index (PyPI) usa Unicode como un truco para evadir la detección e implementar un malware que roba información.

El paquete en cuestión, llamado onyxproxy, se cargó en PyPI el 15 de marzo de 2023 y cuenta con capacidades para recolectar y filtrar credenciales y otros datos valiosos. Desde entonces ha sido eliminado, pero no antes de atraer un total de 183 descargas.

Según la compañía de seguridad de la cadena de suministro de software Phylum, el paquete incorpora su comportamiento malicioso en un script de instalación que contiene miles de cadenas de código aparentemente legítimas.

Estas cadenas incluyen una combinación de fuentes en negrita y cursiva y aún son legibles y pueden ser analizadas por el intérprete de Python, solo para activar la ejecución del malware ladrón al instalar el paquete.

> *«Un beneficio obvio e inmediato de este extraño esquema es la legibilidad. Además, estas diferencias visibles ni impiden que el código se ejecute»,* dijo la compañía.

Esto es posible gracias al uso de variantes Unicode de lo que parece ser el mismo carácter (también conocido como homoglifos) para camuflar sus verdaderos colores entre funciones y variables de aspecto inocuo.

El uso de Unicode para inyectar vulnerabilidades en el código fuente fue revelado previamente por los investigadores de la Universidad de Cambridge, Nicholas Boucher y Ross Anderson, en una técnica de ataque denominada Trojan Source.

Cabe mencionar que el método crea una nueva pieza de código ofuscado, a pesar de mostrar signos reveladores de esfuerzos de copiar y pegar de otras fuentes.

El desarrollo destaca los intentos continuos por parte de los hackers para encontrar nuevas

formas de pasar a través de las defensas basadas en la coincidencia de cadenas, aprovechando *«cómo el intérprete de Python maneja Unicode para ofuscar su malware».*

En una nota relacionada, la empresa canadiense de seguridad cibernética PyUp detalló el descubrimiento de tres nuevos paquetes fraudulentos de Python (aiotoolbox, asyncio-proxy y pycolorz) que se descargaron acumulativamente más de 1000 veces y se diseñaron para recuperar código ofuscado de un servidor remoto.