En un nuevo caso de paquetes maliciosos que ingresan de forma sigilosa a los repositorios de códigos públicos, se eliminaron 10 módulos del índice de paquetes de Python (PyPi) por su capacidad para recopilar puntos de datos críticos, como contraseñas y tokens API.

Los paquetes *«instalan ladrones de información que permiten a los atacantes robar los datos privados y las credenciales personales del desarrollador»,* dijo la compañía de ciberseguridad Check Point.

Los paquetes maliciosos son:

- Ascii2text – Descarga un script malicioso que recopila contraseñas almacenadas en navegadores web como Google Chrome, Microsoft Edge, Brave, Opera y Yandex Browser.
- Pyg-utils, Pymocks y PyProto2 – Están diseñados para robar las credenciales de AWS de los usuarios.
- Test-async y Zlibsrc – Descargan y ejecutan código malicioso durante la instalación.
- Free-net-vpn, Free-net-vpn2 y WINRPCexploit – Roban las credenciales de usuario y las variables de entorno.
- Browserdiv – Recopila credenciales y otra información guardada en la carpeta de almacenamiento local del navegador web.

La divulgación es la última de una lista que crece rápidamente de casos recientes en los que los atacantes publican software no autorizado en repositorios de software ampliamente utilizados, como PyPI y Node Package Manager (NPM), con el objetivo de interrumpir la cadena de suministro de software.

Los paquetes NPM maliciosos roban tokens de Discord y datos de tarjetas bancarias

El riesgo que muestran los incidentes aumenta la necesidad de revisar y ejercer la diligencia debida antes de descargar software de código abierto y de terceros de repositorios públicos.

El mes pasado, Kaspersky reveló cuatro bibliotecas, small-sm, pern-valids, lifeculer y proc-title, en el registro del paquete NPM que contenía código malicioso de Python y JavaScript altamente ofuscado diseñado para robar tokens de Discord e información de tarjetas de crédito vinculadas.

La campaña, denominada LofyLife, demuestra cómo dichos servicios demostraron ser un vector de ataque lucrativo para que los atacantes lleguen a un número significativo de usuarios intermedios disfrazando el malware como bibliotecas aparentemente útiles.

> *«Los ataques a la cadena de suministro están diseñadas para explotar las relaciones de confianza entre una organización y partes externas. Estas relaciones podrían incluir asociaciones, relaciones con proveedores o el uso de software de terceros»,* dijeron los investigadores.

> *«Los actores de amenazas cibernéticas comprometerán a una organización y luego ascenderán en la cadena de suministro, aprovechando estas relaciones confiables para obtener acceso a los entornos de otras organizaciones».*