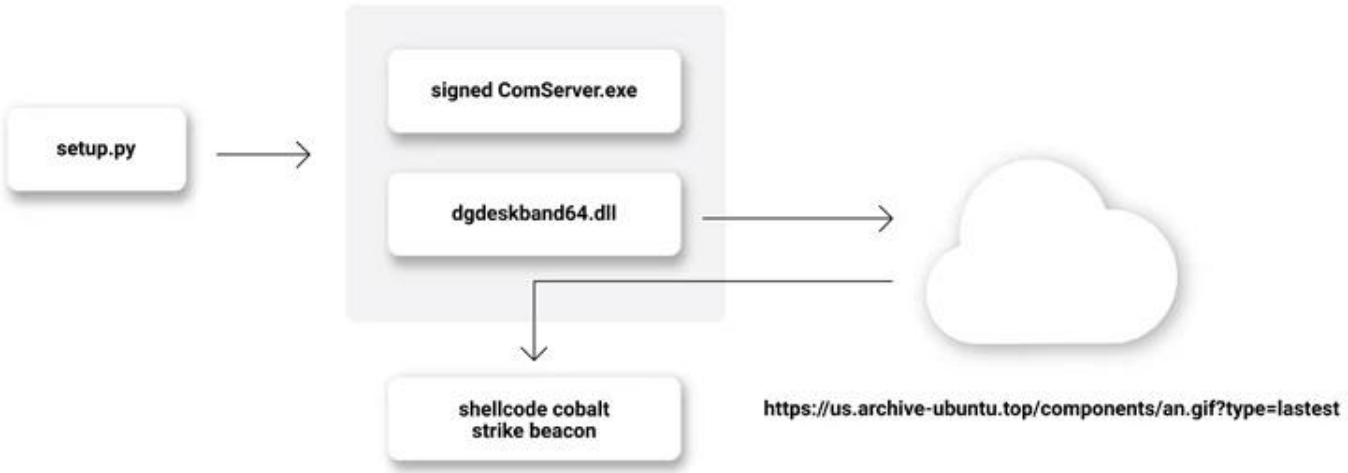
Investigadores de ciberseguridad han identificado dos paquetes maliciosos en el repositorio del Índice de Paquetes de Python (PyPI) que empleaban una táctica conocida como «*DLL side-loading*» para evadir la detección por parte del software de seguridad y ejecutar código perjudicial.

Estos paquetes, denominados NP6HelperHttptest y NP6HelperHttper, fueron descargados 537 y 166 veces, respectivamente, antes de ser retirados.

En un informe, el investigador de ReversingLabs, Petar Kirhmajer, señaló que este último hallazgo representa un caso de «*DLL side-loading*» llevado a cabo por un paquete de código abierto, indicando así que las amenazas en la cadena de suministro de software están en aumento.

Es importante destacar que el nombre NP6 hace referencia a una solución legítima de automatización de marketing desarrollada por ChapsVision. Específicamente, los paquetes falsos son versiones con errores tipográficos de NP6HelperHttp y NP6HelperConfig, que son herramientas auxiliares publicadas por un empleado de ChapsVision en PyPI.

En otras palabras, el propósito es engañar a los desarrolladores que buscan NP6HelperHttp y NP6HelperConfig para que descarguen versiones maliciosas.



Dentro de las dos bibliotecas se encuentra un script setup.py diseñado para descargar dos archivos: un ejecutable legítimo de la empresa Kingsoft Corporation con sede en Beijing («ComServer.exe») vulnerable al «side-loading» de DLL, y la DLL maliciosa que se debe cargar («dgdeskband64.dll»).

Al cargar la DLL, el objetivo es evitar la detección del código malicioso, tal como se observó previamente en el caso de un paquete npm llamado aabquerys, que también utilizó la misma técnica para ejecutar código capaz de desplegar un troyano de acceso remoto.

En cuanto a la DLL, se conecta a un dominio controlado por el atacante («us.archive-ubuntu[.]top») para obtener un archivo GIF que, en realidad, es un fragmento de código de shell destinado a un Beacon de Cobalt Strike, una herramienta de post-explotación utilizada en simulaciones de seguridad (red teaming).

Hay indicios que sugieren que estos paquetes forman parte de una campaña más amplia que implica la distribución de ejecutables similares susceptibles al *«side-loading»* de DLL.

Karlo Zanki, investigador de seguridad, subrayó la importancia de que las organizaciones de desarrollo estén conscientes de las amenazas vinculadas a la seguridad de la cadena de suministro y a los repositorios de paquetes de código abierto.

> *«Incluso si no están utilizando repositorios de paquetes de código abierto, esto no significa que los actores maliciosos no los exploren para suplantar a empresas y sus productos y herramientas de software»,* advirtió Zanki.