Un paquete inactivo que estaba disponible en el Repositorio del Índice de Paquetes de Python (PyPI) fue actualizado después de casi dos años para difundir un malware de robo de información llamado Nova Sentinel.

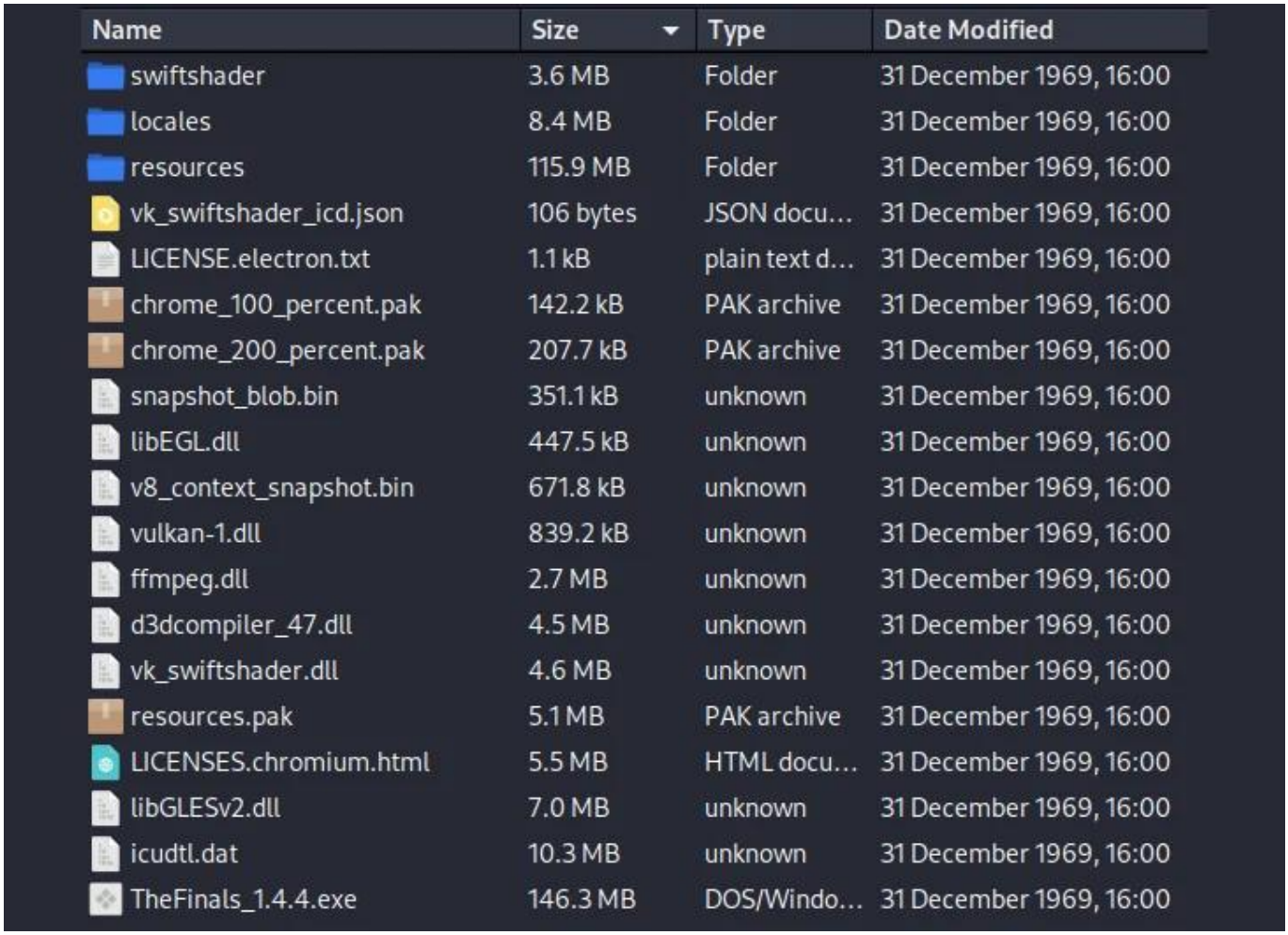
El paquete en cuestión, denominado django-log-tracker, se subió por primera vez a PyPI en abril de 2022, según la empresa de seguridad de la cadena de suministro de software Phylum, que identificó una actualización inusual en la biblioteca el 21 de febrero de 2024.

A pesar de que el repositorio enlazado en GitHub no ha tenido modificaciones desde el 10 de abril de 2022, la introducción de una actualización maliciosa sugiere una probable intrusión de la cuenta de PyPI perteneciente al desarrollador.

Hasta la fecha, django-log-tracker ha sido descargado 3,866 veces, siendo que la versión falsificada (1.0.4) se descargó 107 veces en la fecha de su publicación. El paquete ya no está disponible para su descarga desde PyPI.

> *«En la actualización maliciosa, el atacante eliminó la mayoría del contenido original del paquete, dejando únicamente un archivo init.py y example.py»,* informó la compañía.

Los cambios, que son sencillos y autoexplicativos, implican la recuperación de un archivo ejecutable llamado «Updater_1.4.4_x64.exe» desde un servidor remoto («45.88.180[.]54»), seguido por su ejecución mediante la función os.startfile() de Python.



Name	Size	Type	Date Modified
swiftshader	3.6 MB	Folder	31 December 1969, 16:00
locales	8.4 MB	Folder	31 December 1969, 16:00
resources	115.9 MB	Folder	31 December 1969, 16:00
vk_swiftshader_icd.json	106 bytes	JSON docu…	31 December 1969, 16:00
LICENSE.electron.txt	1.1 kB	plain text d…	31 December 1969, 16:00
chrome_100_percent.pak	142.2 kB	PAK archive	31 December 1969, 16:00
chrome_200_percent.pak	207.7 kB	PAK archive	31 December 1969, 16:00
snapshot_blob.bin	351.1 kB	unknown	31 December 1969, 16:00
libEGL.dll	447.5 kB	unknown	31 December 1969, 16:00
v8_context_snapshot.bin	671.8 kB	unknown	31 December 1969, 16:00
vulkan-1.dll	839.2 kB	unknown	31 December 1969, 16:00
ffmpeg.dll	2.7 MB	unknown	31 December 1969, 16:00
d3dcompiler_47.dll	4.5 MB	unknown	31 December 1969, 16:00
vk_swiftshader.dll	4.6 MB	unknown	31 December 1969, 16:00
resources.pak	5.1 MB	PAK archive	31 December 1969, 16:00
LICENSES.chromium.html	5.5 MB	HTML docu…	31 December 1969, 16:00
libGLESv2.dll	7.0 MB	unknown	31 December 1969, 16:00
icudtl.dat	10.3 MB	unknown	31 December 1969, 16:00
TheFinals_1.4.4.exe	146.3 MB	DOS/Windo…	31 December 1969, 16:00

El binario, por su parte, está integrado con Nova Sentinel, un malware de robo que fue documentado por Sekoia en noviembre de 2023 como una amenaza distribuida en forma de aplicaciones Electron fraudulentas en sitios web ficticios que ofrecen descargas de videojuegos.

> *«Lo que resulta intrigante en este caso en particular […] es que el vector de ataque parece haber sido un intento de ataque a la cadena de suministro mediante el compromiso de la cuenta de PyPI»,* destacó Phylum.

> *«Si este paquete hubiera sido muy popular, cualquier proyecto que tuviera este paquete enlistado como una dependencia sin una versión específica o con una versión flexible especificada en su archivo de dependencias habría descargado la última versión maliciosa de este paquete».*