Se han eliminado del portal PyPI hasta ocho paquetes de Python que contenían código malicioso y fueron descargados más de 30 mil veces, lo que destaca una vez más cómo los repositorios de paquetes de software se están convirtiendo en un objetivo popular para los ataques a la cadena de suministro.

> *«La falta de moderación y los controles de seguridad automatizados en los repositorios de software públicos permiten que incluso los atacantes sin experiencia los utilicen como una plataforma para difundir malware, ya sea a través de typosquatting, confusión de dependencias o simples ataques de ingeniería social»,* dijeron los investigadores de JFrog, Andrey Polkovnichenko, Omer Kaspi y Shachar Menashe.

PyPI, abreviatura de Python Package Index, es el repositorio oficial de software de terceros para Python, con utilidades del administrador de paquetes como pip que se basan en él como fuente predeterminada para los paquetes y sus dependencias.

Los paquetes de Python en cuestión, que se encontraron ofuscados utilizando la codificación Base64, se enumeran a continuación:

- Pytagora (subido por leonora123)
- Pytagora2 (subido por leonora123)
- noblesse (subido por xin1111)
- genesisbot (subido por xin1111)
- are (subido por xin1111)
- suffer (subido por suffer)
- noblesse2 (subido por suffer)
- noblessev2 (subido por suffer)

Se podría abusar de los paquetes mencionados para convertirse en un punto de entrada para amenazas más sofisticadas, lo que permitiría al atacante ejecutar código remoto en la máquina de destino, acumular información del sistema, saquear información de tarjetas de

crédito y contraseñas guardadas de forma automática en los navegadores Chrome y Edge, e incluso robar Tokens de autenticación de Discord para hacerse pasar por la víctima.

PyPI no está solo entre los repositorios de paquetes de software que han surgido como una superficie de ataque potencial para intrusos, con paquetes maliciosos descubiertos en npm y RubyGems equipados con capacidades que podrían potencialmente interrumpir todo un sistema o servir como un valioso punto de partida para excavar más profundamente en la red de una víctima.

El mes pasado, Sonatype y Vdoo revelaron paquetes con errores tipográficos en PyPI que se descubrió que descargaban y ejecutaban un script de shell de carga útil que, a su vez, recuperaba un criptominer de terceros como T-Rex, ubqminer o PhoenixMiner para extraer Ethereum y Ubiq en los sistemas de las víctimas.

> *«El descubrimiento continuo de paquetes de software malicioso en repositorios populares como PyPI es una tendencia alarmante que puede llevar a ataques generalizados a la cadena de suministro. La capacidad de los atacantes de utilizar técnicas simples de ocultación para introducir malware significa que los desarrolladores deben estar preocupados y vigilantes. Se trata de una amenaza sistémica y debe abordarse activamente en varias capas, tanto por los encargados de mantenimiento de los repositorios de software como por los desarrolladores»*, dijo Asaf Karas, CTO de JFrog.

> *«Por parte de los desarrolladores, las medidas preventivas, como la verificación de las firmas de la biblioteca y el empleo de herramientas de seguridad de aplicaciones automatizadas que escanean en busca de indicios de código sospechoso incluido en el proyecto, deben ser una parte integral de cualquier canal de CI/CD. Herramientas automatizadas como estas pueden alertar cuando se están utilizando paradigmas de códigos maliciosos»*, agregó Karas.