Un actor amenazante de identidad desconocida ha sido detectado difundiendo paquetes de typosquat en el repositorio Python Package Index (PyPI) durante aproximadamente seis meses, con la intención de desplegar malware capaz de establecer persistencia, robar datos confidenciales y acceder a billeteras de criptomonedas con el fin de obtener ganancias financieras.

Según un reciente informe de Checkmarx, los 27 paquetes, camuflados como conocidas y legítimas bibliotecas de Python, han atraído a miles de descargas. La mayoría de estas descargas provinieron de usuarios en Estados Unidos, China, Francia, Hong Kong, Alemania, Rusia, Irlanda, Singapur, el Reino Unido y Japón.

> *«Una característica distintiva de este ataque fue la utilización de la esteganografía para ocultar una carga maliciosa dentro de un archivo de imagen aparentemente inofensivo, lo que aumentó la furtividad del ataque»*, destacó la empresa especializada en seguridad de la cadena de suministro de software.

Entre los paquetes se encuentran nombres como pyefflorer, pyminor, pyowler, pystallerer, pystob y pywool, siendo este último implantado el 13 de mayo de 2023.

Un elemento común en estos paquetes es el uso del script setup.py para incluir referencias a otros paquetes maliciosos (por ejemplo, pystob y pywool) que utilizan un Visual Basic Script (VBScript) para descargar y ejecutar un archivo llamado «Runtime.exe» con el fin de lograr persistencia en el sistema afectado.

Dentro del binario se encuentra un archivo compilado capaz de recopilar información de navegadores web, billeteras de criptomonedas y otras aplicaciones.

Checkmarx también identificó una cadena de ataque alternativa en la que el código ejecutable se oculta dentro de una imagen PNG («uwu.png»), que luego se descodifica y ejecuta para extraer la dirección IP pública y el identificador único universal (UUID) del sistema comprometido.

En particular, Pystob y Pywool se presentaron como herramientas para la gestión de API, solo para exfiltrar los datos a un webhook de Discord e intentar mantener la persistencia mediante la colocación del archivo VBS en la carpeta de inicio de Windows.

> *«Esta campaña sirve como otro recordatorio impactante de las amenazas siempre presentes en el panorama digital actual, especialmente en áreas donde la colaboración y el intercambio abierto de código son fundamentales»,* advirtió Checkmarx.

Este desarrollo se produce mientras ReversingLabs revela una nueva ola de paquetes npm de protesta que *«ocultan scripts que difunden mensajes de paz relacionados con los conflictos en Ucrania y en Israel y la Franja de Gaza».*

Uno de estos paquetes, denominado @snyk/sweater-comb (versión 2.1.1), determina la ubicación geográfica del host y, si se identifica como Rusia, muestra un mensaje criticando la «invasión injustificada» de Ucrania a través de otro módulo llamado «es5-ext«.

Otro paquete, e2eakarev, con la descripción *«paquete de protesta por la libertad de Palestina»* en el archivo package.json, realiza comprobaciones similares para ver si la dirección IP se resuelve en Israel, y en ese caso, registra un *«mensaje de protesta inofensivo»* que insta a los desarrolladores a concienciar sobre la lucha palestina.

No solo son los actores de amenazas los que infiltran los ecosistemas de código abierto. A principios de esta semana, GitGuardian reveló la presencia de 3,938 secretos únicos en un total de 2,922 proyectos de PyPI, de los cuales 768 secretos únicos fueron considerados válidos.

Esto incluye claves AWS, claves de la API de Azure Active Directory, claves de la aplicación OAuth de GitHub, claves de Dropbox, claves SSH y credenciales asociadas con MongoDB, MySQL, PostgreSQL, Coinbase y Twilio.

Adicionalmente, se observa que muchos de estos secretos se filtraron en más de una ocasión, abarcando varias versiones de lanzamiento y elevando la cantidad total de incidentes a 56,866.

> Tom Forbes de GitGuardian señaló: *«La revelación de secretos en paquetes de código abierto conlleva riesgos significativos tanto para los desarrolladores como para los usuarios. Los atacantes pueden aprovechar esta información para obtener acceso no autorizado, hacerse pasar por los responsables del mantenimiento de los paquetes o manipular a los usuarios mediante tácticas de ingeniería social».*

La constante oleada de ataques dirigidos a la cadena de suministro de software también ha motivado al gobierno de Estados Unidos a emitir nuevas pautas este mes para que los desarrolladores de software y los proveedores mantengan y promuevan la conciencia sobre la seguridad del software.

La Agencia de Ciberseguridad e Infraestructura (CISA), la Agencia de Seguridad Nacional (NSA) y la Oficina del Director de Inteligencia Nacional (ODNI) expresaron: *«Se recomienda que las organizaciones de adquisiciones integren evaluaciones de riesgo de la cadena de suministro en sus decisiones de compra, dado los recientes incidentes de alto perfil en la cadena de suministro de software».*

> *«Los desarrolladores y proveedores de software deben perfeccionar sus procesos de desarrollo de software y reducir el riesgo de perjuicio, no solo para sus empleados y accionistas, sino también para sus usuarios».*