La Open Source Security Foundation (OpenSSF) anunció el lanzamiento del prototipo inicial de una nueva herramienta que es capaz de realizar un análisis dinámico de todos los paquetes cargados en repositorios populares de código abierto.

El proyecto, llamado Package Analysis, tiene como objetivo proteger los paquetes de código abierto al detectar y alertar a los usuarios sobre cualquier comportamiento malicioso con el objetivo de reforzar la seguridad de la cadena de suministro de software y aumentar la confianza en el software de código abierto.

> *«El proyecto de análisis de paquetes busca comprender el comportamiento y las capacidades de los paquetes disponibles en los repositorios de código abierto: a qué archivos acceden, a qué direcciones se conectan y qué comandos ejecutan»,* dijo OpenSSF.

> *«El proyecto también rastrea los cambios en el comportamiento de los paquetes a lo largo del tiempo, para identificar cuándo el software previamente seguro comienza a actuar de forma sospechosa»,* agregaron Caleb Brown y David A. Wheeler, de la fundación.

En una ejecución de prueba que duró un mes, la herramienta identificó más de 200 paquetes maliciosos cargados en PyPI y NPM, y la mayoría de las bibliotecas no autorizadas aprovecharon la confusión de dependencias y los ataques de errores tipográficos.

Google, que es miembro de OpenSSF, también demostró su apoyo para el proyecto de análisis de paquetes, al mismo tiempo que enfatiza la necesidad de *«examinar los paquetes que se publican para mantener a los usuarios seguros».*

El equipo de seguridad de código abierto de la compañía, presentó el año pasado un nuevo marco llamado Niveles de Cadena de Suministro para Artefactos de Software (SLSA) para

garantizar la integridad de los paquetes de software y evitar modificaciones no autorizadas.