En otro hallazgo que podría exponer a los desarrolladores a un mayor riesgo de un ataque a la cadena de suministro, se descubrió que casi un tercio de los paquetes en PyPI, el índice de paquetes de Python, activan la ejecución automática de código al descargarlos.

> *«Una característica preocupante en pip/PyPI permite que el código se ejecute automáticamente cuando los desarrolladores simplemente descargan un paquete»,* dijo el investigador de Checkmarx, Yehuda Gelb.

> *«Además, esta función es alarmante debido al hecho de que una gran cantidad de paquetes maliciosos que encontramos en la naturaleza usan esta función de ejecución de código durante la instalación para lograr tasas de infección más altas».*

Una de las formas en que se pueden instalar paquetes para Python es ejecutando el comando «*pip install*«, que a su vez, invoca un archivo llamada «setup.py» que viene incluido en el módulo.

«setup.py», como su nombre lo indica, es un script de configuración que se usa para especificar los metadatos asociados con el paquete, incluyendo sus dependencias.

Aunque los atacantes recurrieron a la incorporación de código malicioso en el archivo setup.py, Checkmarx descubrió que los adversarios podrían lograr los mismos objetivos ejecutando lo que se llama un comando de *«pip download».*

> *«pip download hace la misma resolución y descarga que pip install, pero en lugar de instalar las dependencias, recopila las distribuciones descargadas en el directorio proporcionado (el directorio actual es el predeterminado»*, dice la documentación.

En otras palabras, el comando se puede usar para descargar un paquete de Python sin tener

que instalarlo en el sistema. Pero resulta que, al ejecutar el comando de descarga, también se ejecuta el script «setup.py» antes mencionado, lo que da como resultado la ejecución del código malicioso que contiene.

Sin embargo, el problema ocurre solo cuando el paquete contiene un archivo tar.gz en lugar de un archivo de rue (.whl), que *«elimina la ejecución de 'setup.py' de la ecuación».*

> *«Los desarrolladores que optan por descargar, en lugar de instalar paquetes, esperan razonablemente que no se ejecute ningún código en la máquina al descargar los archivos»,* dijo Gelb, caracterizándolo como un problema de diseño en lugar de un error.

Aunque pip usa de forma predeterminada ruedas en lugar de archivos tar.gz, un atacante podría aprovechar este comportamiento para publicar de forma intencional paquetes de python sin un archivo .whl, lo que llevaría a la ejecución del código malicioso presente en el script de instalación.

> *«Cuando un usuario descarga un paquete de python desde PyPI, pip utilizará preferentemente el archivo .whl, pero recurrirá al archivo tar.gz sin falta el archivo .whl»,* dijo Gelb.

Los hallazgos se producen cuando la Agencia de Seguridad Nacional de Estados Unidos (NSA), junto con la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) y la Oficina del Director de Inteligencia Nacional (ODNI), publicaron una guía para asegurar la cadena de suministro de software.

> *«A medida que la amenaza cibernética sigue volviéndose más sofisticada, los adversarios comenzaron a atacar la cadena de suministro de software, en lugar de*

> *confiar en las vulnerabilidades conocidas públicamente. Hasta que todos los DevOps sean DevSecOps, el ciclo de vida del desarrollo de software estará en riesgo»*, dijo la agencia.