Los mantenedores del paquete PyTorch advirtieron a los usuarios que instalaron las compilaciones nocturnas de la biblioteca entre el 25 de diciembre de 2022 y el 30 de diciembre del mismo año, que desinstalen y descarguen las últimas versiones después de un ataque de confusión de dependencia.

> *«Los paquetes PyTorch-nightly Linux instalados a través de pip durante ese tiempo instalaron una dependencia, torchtriton, que se comprometió en el repositorio de código Python Package Index (PyPI) y ejecutó un binario malicioso»,* dijo el equipo de PyTorch en una alerta durante el fin de semana.

PyTorch, similar a Keras y TensorFlow, es un marco de aprendizaje automático basado en Python de código abierto, que fue desarrollado originalmente por Meta Platforms.

El equipo de PyTorch dijo que se dio cuenta de la dependencia maliciosa el 30 de diciembre a las 4:40 pm GMT. El ataque a la cadena de suministro implicó cargar la copia con malware de una dependencia legítima llamada torchtriton al repositorio de código Python Package Index (PyPI).

Debido a que los administradores de paquetes como pip verifican los registros de códigos públicos como PyPI para un paquete antes que los registros privados, permitió que el módulo fraudulento se instalara en los sistemas de los usuarios en lugar de la versión real extraída del índice de terceros.

La versión no autorizada, por su parte, está diseñada para extraer información del sistema, incluidas las variables de entorno, el directorio de trabajo actual y el nombre del host, además de acceder a los siguientes archivos:

- /etc/hosts
- /etc/password
- Los primeros 1000 archivos en $HOME/*
- $INICIO/.gitconfig

- $INICIO/.ssh/*

En una declaración compartida con Bleeping Computer, el propietario del dominio al que se transmitieron los datos robados, afirmó que era parte de un ejercicio de investigación ético y que todos los datos se eliminaron desde entonces.

Como medidas de mitigación, torchtriton se eliminó como dependencia y se reemplazó con pytorch-triton. También se registró un paquete ficticio en PyPI como marcador de posición para evitar más abusos.

> *«Este no es el paquete de torchtriton real, pero se cargó aquí para descubrir vulnerabilidades de confusión de dependencias. Puede obtener el torchtriton real en https://download.pytorch[.]org/whl/nightly/torchtriton/»,* dice un mensaje en la página de PyPI para torchtriton.

El desarrollo también se produce cuando JFrog reveló detalles de otro paquete conocido como cookiezlog que se ha observado usando técnicas anti-depuración para resistir el análisis, lo que marca la primera vez que tales mecanismos se incorporan en el malware PyPI.