El Departamento de Justicia de Estados Unidos admitió este miércoles, que es la última agencia gubernamental confirmada del país que se vio afectada por el ataque a la cadena de suministro de SolarWinds.

> *«El 24 de diciembre de 2020, la Oficina del Director de Información (OCIO) del Departamento de Justicia, se enteró de una actividad maliciosa previamente desconocida relacionada con el incidente global de SolarWinds que ha afectado a múltiples agencias federales y contratistas de tecnología, entre otros. Esta actividad implicó el acceso al entorno de correo electrónico de Microsoft Office 365»*, dijo Marc Raimondi en un comunicado.

Al llamarlo un *«incidente importante»*, el Departamento de Justicia dijo que los actores de amenazas que espiaron las redes gubernamentales a través del software SolarWinds potencialmente accedieron a aproximadamente el 3% de las cuentas de correo electrónico del Departamento de Justicia, pero agregó que no hay indicios de que hayan accedido a sistemas clasificados.

La divulgación ocurrió un día después de que la Oficina Federal de Investigaciones (FBI), la Agencia de Seguridad e Infraestructura y Ciberseguridad (CISA), la Oficina del Director de Inteligencia Nacional (ODNI) y la Agencia de Seguridad Nacional (NSA), emitieron una declaración conjunta formalmente acusando a un adversario *«probablemente de origen ruso»* por organizar el ataque a SolarWinds.

Las agencias describieron toda la operación de SolarWinds como *«un esfuerzo de recopilación de inteligencia».*

La campaña de espionaje, que se originó en marzo de 2020, funcionó mediante la entrega de código malicioso que se incorporó al software de administración de red SolarWinds a 18,000 de sus clientes, aunque se cree que se ha realizado actividad intrusiva adicional contra objetivos seleccionados.

JetBrains niega su participación en el hackeo de SolarWinds

En un desarrollo separado, The New York Times, Reuters y The Wall Street Journal, informaron que las oficinas de inteligencia están investigando la posibilidad de que el sistema de distribución de software TeamCity de JetBrains haya sido violado y *«utilizado como una vía para que los hackers inserten puertas traseras en el software de un incontable número de empresas de tecnología».*

TeamCity es un servidor de gestión de construcción e integración continua ofrecido por la empresa de desarrollo de software checa. JetBrains cuenta con 79 de las 100 empresas de Fortune como sus clientes, incluyendo SolarWinds.

En una publicación de blog publicada por el CEO Maxim Shafirov, la compañía negó estar involucrada en el ataque de alguna manera, o que fue contactada por algún gobierno o agencia de seguridad con respecto a su papel en el incidente de seguridad.

> *«SolarWinds es uno de nuestros clientes y utiliza TeamCity, que es un sistema de implementación e integración continua, que se utiliza como parte del software de construcción. SolarWinds no se ha puesto en contacto con nosotros con ningún detalle sobre la infracción y la única información que tenemos es la que se ha puesto a disposición del público»*, dijo Shafirov.

Shafirov enfatizó que en el caso de que TeamCity se hubiera utilizado para comprometer SolarWinds, podría deberse a una mala configuración y no a una vulnerabilidad específica.