Microsoft reveló el jueves que los hackers detrás del ataque a la cadena de suministro de SolarWinds, pudieron obtener acceso a una pequeña cantidad de cuentas internas y escalar el acceso dentro de su red interna.

El *«actor de estado-nación muy sofisticado»* utilizó el acceso no autorizado para ver, pero no modificar, el código fuente presente en sus repositorios, dijo Microsoft.

> *«Detectamos actividad inusual con una pequeña cantidad de cuentas internas y, tras la revisión, descubrimos que una cuenta se había utilizado para ver el código fuente en varios repositorios de código fuente»,* reveló la compañía.
>
> *«La cuenta no tenía permisos para modificar ningún código o sistema de ingeniería y nuestra investigación confirmó además que no se realizaron cambios. Estas cuentas fueron investigadas y remediadas».*

El desarrollo es el último de la saga de espionaje de gran alcance que salió a la luz a inicios de diciembre, luego de las revelaciones de la compañía de seguridad FireEye acerca de que los atacantes comprometieron sus sistemas a través de una actualización de SolarWinds troyanizada para robar sus herramientas de prueba de penetración Red Team.

Durante el curso de la investigación sobre el ataque, Microsoft admitió previamente haber detectado binarios de SolarWinds maliciosos en su propio entorno, pero negó que sus sistemas se usaran para atacar a otros o que los atacantes tuvieran acceso a servicios de producción o datos de clientes.

Otras empresas, incluyendo Cisco, VMware, Intel, NVIDIA y agencias gubernamentales de Estados Unidos, descubrieron desde entonces marcadores del malware Sunburst (o Solorigate) en sus redes, plantados a través de actualizaciones de Orion contaminadas.

La compañía con sede en Redmond, dijo que su investigación aún está en curso, pero restó

importancia al incidente y agregó que *«ver el código fuente no está vinculado a la elevación del riesgo»* y que había encontrado evidencia de intentos de actividades que fueron neutralizadas por sus protecciones.

En un análisis separado publicado por Microsoft el 28 de diciembre, la compañía calificó el ataque como un *«compromiso entre dominios»* que permitió al adversario introducir el código malicioso en los archivos binarios firmados de SolarWinds Orion Platform y aprovechar este punto de apoyo generalizado para seguir operando sin ser detectado y acceder a los recursos en la nube, que culminan con la exfiltración de datos confidenciales.

Sin embargo, el software Orion de SolarWinds no fue el único vector de infección inicial, ya que la Agencia de Seguridad e Infraestructura y Ciberseguridad de Estados Unidos (CISA), dijo que los atacantes también utilizaron otros métodos, que aún no se divulgan de forma pública.

La agencia también publicó una guía complementaria instando a todas las agencias federales de Estados Unidos que aún ejecutan el software SolarWinds Orion a actualizar a la última versión 2020.2.1 HF2.

> *«La Agencia de Seguridad Nacional (NSA) examinó esta versión y verificó que elimina el código malicioso previamente identificado»*, dijo la agencia.