Este martes, el gobierno de Estados Unidos acusó formalmente al gobierno ruso por orquestar el ataque masivo a la cadena de suministro de SolarWinds, que salió a la luz a inicios del mes pasado.

> *«Este trabajo indica que un actor de Advanced Persisten Threat (APT), probablemente de origen ruso, es responsable de la mayoría o de todos los ciberataques en curso recientemente descubiertos de las redes gubernamentales y no gubernamentales»*, dijeron el FBI, CISA, ODNI y NSA en un comunicado.

Sin embargo, Rusia negó cualquier participación en la operación del 13 de diciembre, afirmando que *«no realiza operaciones ofensivas en el dominio cibernético».*

El FBI, CISA, ODNI y NSA son miembros del Cyber Unified Coordination Group (UCG), un grupo de trabajo recién formado establecido por el Consejo de Seguridad Nacional de la Casa Blanca para investigar y liderar los esfuerzos de respuesta para remediar la brecha de SolarWinds.

Calificando la campaña como un *«esfuerzo de recopilación de inteligencia»,* las oficinas de inteligencia dijeron que actualmente están trabajando para comprender el alcance total del ataque y dijeron que menos de 10 agencias gubernamentales de Estados Unidos se vieron afectadas por el compromiso.

Los nombres de las agencias afectadas no fueron revelados, aunque los informes anteriores señalaron al Tesoro, Comercio, Estado y los Departamentos de Energía y Seguridad Nacional de Estados Unidos, entre los que han detectado instalaciones de software de administración de red de SolarWinds contaminadas, por no mencionar algunas entidades privadas en todo el mundo.

Se cree que unos 18000 clientes de SolarWinds descargaron la actualización de software con la puerta trasera, pero la UGC dijo que solo un número menor había sido objetivo de actividad intrusiva de *«seguimiento»* en sus redes internas.

El análisis de Microsoft sobre el modus operandi de Solorigate el mes pasado, encontró que el malware de segunda etapa denominado Teardrop, se implementó de forma selectiva contra objetivos basados en información acumulada durante un reconocimiento inicial del entorno de la víctima para cuentas y activos de alto valor.

La declaración conjunta también confirma especulaciones anteriores que vinculaban la operación de espionaje con APT29 (o CozyBear), un grupo de hackers patrocinados por el estado asociados con el Servicio de Inteligencia Exterior de Rusia (SVR).

La campaña de piratería se destacó por su escala y sigilo, y los atacantes aprovecharon la confianza asociada con el software SolarWinds Orion para espiar a las agencias gubernamentales y otras empresas durante al menos nueve meses, incluida la visualización del código fuente y el robo de herramientas de seguridad.

Demanda colectiva

SolarWinds está enfrentando más problemas luego de que un accionista de la compañía presentó una demanda colectiva en el Tribunal de Distrito de Estados Unidos para el Distrito Oeste de Texas este lunes contra su presidente, Kevin Thompson, y el director financiero, J. Barton Kalsu, alegando que los ejecutivos violaron las leyes de valores federales bajo la Ley de Bolsa de Valores de 1934.

La denuncia afirma que SolarWinds no reveló que *«desde mediados de 2020, los productos de monitoreo SolarWinds Orion tenían una vulnerabilidad que permitía a los hackers comprometer el servidor en el que se ejecutaban los productos y que el servidor de actualización de SolarWinds tenía una contraseña de fácil acceso 'solarwinds123' dando como resultado que la empresa sufriría un daño significativo a su reputación».*