El Reino Unido atribuyó formalmente este jueves el ataque a la cadena de suministro de la compañía de gestión de infraestructura de TI, SolarWinds, con una *«alta confianza»* a los agentes del gobierno que trabajan para el Servicio de Inteligencia Exterior de Rusia (SVR).

> *«Patrón de comportamiento maligno en todo el mundo de Rusia, ya sea en el ciberespacio, en la elección o en las operaciones agresivas de sus servicios de inteligencia, demuestra que Rusia sigue siendo la amenaza más grave para la seguridad nacional y colectiva del Reino Unido»,* dijo el gobierno del Reino Unido en una declaración.

Ante esto, el Departamento del Tesoro de Estados Unidos ha impuesto grandes sanciones contra Rusia por *«socavar la realización de elecciones libres y justas y las intrusiones democráticas»* en Estados Unidos, y por su papel en facilitar el extenso ataque a SolarWinds, al mismo tiempo que prohíbe a seis empresas de tecnología en el país que brinden apoyo al programa cibernético dirigido por los servicios de inteligencia de Rusia.

La empresas incluyen ERA Technopolis, Pasit, Instituto de Investigación Científica del Establecimiento Científico Autónomo del Estado Federal, Dispositivos y Automatización de Computación de Seguridad Especializados (SVA), Neobit, Advanced System Technology y Pozitiv Teknolodzhiz (Positive Technologies), las tres últimas de las cuales son empresas de seguridad de TI cuyps clientes inluyen agencias de inteligencia rusas.

Además, la administración Biden también está expulsando a diez miembros de la misión diplomática de Rusia en Washington DC, incluidos los representantes de sus servicios de inteligencia.

> *«El alcance y la escala de este compromiso se combina con la historia de llevar a*

> *cabo operaciones cibernéticas imprudentes y perturbadoras de Rusia, hace que sea un problema de seguridad nacional. SVR ha puesto en riesgo la cadena de suministro de tecnología global al permitir que se instale malware en las máquinas de decenas de miles de clientes de SolarWinds»*, dijo el Departamento de Tesoro.

Por su parte, Moscú negó previamente su participación en la campaña SolarWinds de amplio alcance, afirmando que *«no realiza operaciones ofensivas en el dominios cibernético»*.

Las intrusiones salieron a la luz en diciembre de 2020, cuando FireEye y otras compañías de seguridad cibernética revelaron que los operadores detrás de la campaña de espionaje lograron comprometer la construcción de software y la infraestructura de firma de código de la plataforma SolarWinds Orion ya en octubre de 2019, con el fin de entregar la backdoor Sunburst con el objetivo de recopilación de información sensible.

Se cree que hasta 18 mil clientes de SolarWinds recibieron la actualización de Orion con troyanos, aunque los atacantes seleccionaron cuidadosamente sus objetivos, optando por escalar los ataques solo en algunos casos mediante la implementación de malware Teardrop, basado en un reconocimiento inicial del entorno de destino para cuentas de valor y activos.

Al parecer, el compromiso del adversario con la cadena de suministro de software de SolarWinds le dio la capacidad de espiar remotamente o potencialmente interrumpir más de 16,000 sistemas informáticos en todo el mundo, según la orden ejecutiva emitida por el gobierno de Estados Unidos.

Además de infiltrarse en las redes de Microsoft, FireEye, Malwarebytes y Mimecast, se dice que los atacantes también utilizaron SolarWinds como un trampolín para violar varias agencias estadounidenses, como la Administración Nacional de Aeronáutica y del Espacio (NASA), la Administración Federal de Aviación (FAA) y los Departamentos de Estado, Justicia, Comercio, Seguridad Nacional, Energía, Tesoro y los Institutos Nacionales de Salud.

El actor de SVR también es conocido por otros nombres, como APT29, Cozy Bear y The

Dukes, y el grupo de amenazas se rastrea con distintos apodos, como UNC2452 (FireEye), SolarStorm (Palo Alto Unit 42), StellarParticle (CrowdStrike), Dark Halo (Volexity) y Nobelium (Microsoft).

Además, la Agencia de Seguridad NAcional (NSA), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) y la Oficina Federal de Investigaciones (FBI), publicaron en conjunto un aviso, advirtiendo a las compañías de la explotación activa de cinco vulnerabilidades conocidas públicamente por ATP29 para obtener una ventaja inicial.

Entre las vulnerabilidades reveladas se encuentran:

- CVE-2018-13379 – Fortinet FortiGate VPN
- CVE-2019-9670 – Paquete de colaboración Synacor Zimbra
- CVE-2019-11510 – Pulse Secure Connect VPN
- CVE-2019-19781 – Puerta de enlace y controlador de entrega de aplicaciones Citrix
- CVE-2020-4006 – Acceso a VMware Workspace ONE

> *«Vemos lo que Rusia está haciendo para socavar nuestras democracias. El Reino Unido y Estados Unidos están denunciando el comportamiento malicioso de Rusia, para emitir que nuestros socios internacionales y empresas en casa se defiendan mejor y se preparen contra este tipo de acción»*, dijo el secretario de Relaciones Exteriores del Reino Unido, Dominic Raab.