Nobelium, el actor de amenazas detrás del compromiso de SolarWinds en diciembre de 2020, ha estado detrás de una ola continua de ataques que comprometieron a 14 clientes intermedios de múltiples proveedores de servicios en la nube (CSP), proveedores de servicios administrados (MSP) y otras organizaciones de servicios de TI, lo que ilustra el interés continuo del adversario en apuntar a la cadena de suministro a través del enfoque de *«compromise-one-to-compromise-many».*

Microsoft, que reveló los detalles de esta campaña el lunes, dijo que notificó a más de 140 revendedores y proveedores de servicios de tecnología desde mayo. Entre el 1 de julio y el 19 de octubre de 2021, se dice que Nobelium destacó a 609 clientes, que fueron atacados de forma colectiva un total de 22,868 veces.

> *«Esta actividad reciente es otro indicador de que Rusia está tratando de obtener acceso sistemático a largo plazo a una variedad de puntos en la cadena de suministro de tecnología y establecer un mecanismo para vigilar, ahora o en el futuro, los objetivos de interés para el gobierno ruso»,* dijo Tom Burt, vicepresidente corporativo de seguridad y confianza del cliente de Microsoft.

Los ataques recientemente revelados no explotan ninguna debilidad de seguridad específica en el software, sino que aprovechan una amplia gama de técnicas como la propagación de contraseñas, el robo de tokens, el abuso de API y el spear-phishing para desviar las credenciales asociadas con cuentas privilegiadas de proveedores de servicios, lo que permite a los atacantes moverse lateralmente en entornos de nube y montar más intrusiones.

Según Microsoft, el objetivo es que *«Nobelium espera aprovechar cualquier acceso directo que puedan tener los revendedores a los sistemas de TI de sus clientes y hacerse pasar más fácilmente por el socio tecnológico de confianza de una organización para obtener acceso a sus clientes intermedios».*

En todo caso, los ataques son otra manifestación de las tácticas frecuentemente repetidas de Nobelium, que se ha descubierto que abusan de las relaciones de confianza de las que disfrutan los proveedores de servicios para meterse en múltiples víctimas de interés para obtener inteligencia.

Como mitigaciones, la empresa recomienda a las compañías que habiliten la autenticación multifactor (MFA) y los privilegios administrativos delegados de auditoría (DAP) para evitar cualquier posible uso indebido de los permisos elevados.

El desarrollo también llega menos de un mes después de que el gigante tecnológico revelara una nueva puerta trasera pasiva y altamente especificada denominada *«FoggyWeb»* implementada por el grupo de piratería para entregar cargas útiles adicionales y robar información confidencial de los servidores de Active Directory Federation Services (AD FS).