Nuevas pruebas en medio de una investigación en curso sobre la campaña de espionaje dirigida a SolarWinds, descubrió un intento fallido de comprometer a la empresa de seguridad cibernética Crowdstrike y acceder al correo electrónico de la compañía.

El 15 de diciembre, el Centro de Inteligencia de Amenazas de Microsoft informó a la empresa del intento de piratería, que identificó que la cuenta de Microsoft Azure de un revendedor externo estaba haciendo «*llamadas anormales*» a las API de la nube de Microsoft durante un período de 17 horas hace varios meses.

La cuenta de Azure del revendedor afectado no revelada maneja las licencias de Microsoft Office para sus clientes de Azure, incluido CrowdStrike.

Aunque hubo un intento por parte de actores de amenazas no identificados de leer los correos electrónicos, finalmente fue frustrado porque la empresa no usa el servicio de correo electrónico Office 365 de Microsoft, dijo CrowdStrike.

El incidente se produce a raíz del ataque a la cadena de suministro de SolarWinds revelado a inicios de este mes, lo que resultó en el despliegue de una puerta trasera encubierta (también conocida como Sunburst) a través de actualizaciones maliciosas de un software de monitoreo de red llamado SolarWinds Orion.

Desde la divulgación, Microsoft, Cisco, VMware, Intel, NVIDIA y varias agencias gubernamentales de Estados Unidos confirmaron haber encontrado instalaciones de Orion contaminadas en sus entornos.

El desarrollo se produce una semana después de que Microsoft, un cliente de SolarWinds, negara que los piratas informáticos se hubieran infiltrado en sus sistemas de producción para realizar más ataques contra sus usuarios y encontrara evidencia de un grupo de hackers separado que abusaba del software Orion para instalar una puerta trasera separada llamada Supernova.

También coincide con un nuevo informe de The Washington Post del 25 de diciembre, que

alega que piratas informáticos del gobierno ruso atacaron a los clientes de la nube de Microsoft y robaron correos electrónicos de al menos una empresa del sector privado aprovechando un revendedor de Microsoft que administra servicios de acceso a la nube.

> *«Nuestra investigación de ataques recientes encontró incidentes relacionados con el abuso de credenciales para obtener acceso, que pueden presentarse en distintas formas. No hemos identificado ninguna vulnerabilidad o compromiso de los productos o servicios en la nube de Microsoft»,* dijo el director senior de Microsoft, Jeff Jones.

CrowdStrike también lanzó CrowdStrike Reporting Tool para Azure (CRT), una herramienta gratuita que tiene como objetivo ayudar a las organizaciones a revisar los permisos excesivos en sus entornos de Azure Active Directory, así como en Office 365 y ayudar a determinar las debilidades de configuración.

Además, la Agencia de Seguridad e Infraestructura de Ciberseguridad de Estados Unidos (CISA), creó por separado una utilidad de código abierto similar llamada Sparrow para ayudar a detectar posibles cuentas y aplicaciones comprometidas en entornos Azure y Office 365.

> *«La herramienta está pensada para que la utilicen los responsables de incidentes y se centra estrictamente en la actividad endémica de los recientes ataques basados en identidad y autenticación que se han visto en múltiples sectores»,* dijo CISA.

Por su parte, SolarWinds ha actualizado su aviso de seguridad, instando a los clientes a actualizar el software Orion Platform a la versión 2020.2.1 HF 2 o 2019.4 HF 6, para mitigar los riesgos asociados con las vulnerabilidades Sunburst y Supernova.