Conforme avanza la investigación sobre el ataque cibernético a la cadena de suministro de SolarWinds, nueva evidencia forense digital ha mostrado que un actor de amenazas separado puede haber estado abusando del software Orion del proveedor de infraestructura de TI para colocar una puerta trasera persistente similar en los sistemas de destino.

> *«La investigación de todo el compromiso de SolarWinds llevó al descubrimiento de un malware adicional que también afecta al producto SolarWinds Orion, pero se ha determinado que probablemente no esté relacionado con este compromiso y que sea utilizado por un actor de amenaza diferente»,* dijo el viernes el equipo de investigación de Microsoft 365.

Lo que hace diferente al malware recientemente revelado, denominado *«Supernova»*, es que, a diferencia de Sunburst DLL, Supernova (*«app_web_logoimagehandler.ashx.b6031896.dll»*) no está firmado con un certificado digital legítimo de SolarWinds, lo que indica que el compromiso puede no estar relacionado con el ataque a la cadena de suministro previamente revelado.

En un artículo independiente, los investigadores de Palo Alto Networks dijeron que el malware Supernova se compila y ejecuta en la memoria, lo que permite al atacante pasar por alto los sistemas de detección y respuesta de puntos finales (EDR) e *«implementar .NET con todas las funciones y, presumiblemente, sofisticados programas de reconocimiento, movimiento lateral y otras fases de ataque».*

Funcionamiento de la backdoor Sunburst

Los atacantes utilizaron lo que se denomina un ataque a la cadena de suministro, explotando las actualizaciones del software de administración de red SolarWinds Orion que la compañía distribuyó entre marzo y junio de este año para plantar código malicioso en un archivo DLL (también conocido como Sunburst o Solorigate) en los servidores de los objetivos, que es capaz de recopilar de forma sigilosa información crítica, ejecutar comandos remotos y filtrar

los resultados a un servidor controlado por el atacante.

El análisis del modus operandi de Solorigate también ha revelado que la compañía eligió robar datos solo de unas pocas de las miles de víctimas seleccionadas, optando por escalar sus ataques en función de la información obtenida durante un reconocimiento inicial del entorno objetivo para cuentas y activos de alto valor.

La escalada involucra al servidor de comando y control (C2) predefinido, un dominio ahora dividido llamado «*avsvmcloud[.]com*«, que responde al sistema infectado con un segundo servidor C2 que permite que la puerta trasera Sunburst ejecute comandos específicos para obtener privilegios, exploración de escalada, robo de credenciales y movimiento lateral.

El hecho de que el archivo DLL comprometido esté firmado digitalmente implica un compromiso del desarrollo de software de la compañía o del proceso de distribución, con evidencia que sugiere que los atacantes han estado realizando una prueba de la campaña desde octubre de 2019.

Los archivos de octubre no tenían una puerta trasera incorporada en la forma en que lo hicieron las actualizaciones de software posteriores que los clientes de SolarWinds Orion descargaron en la primavera de 2020. Lo que se sugiere que es se utilizó principalmente para probar si las modificaciones aparecían en las actualizaciones recién lanzadas como se esperaba.

La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), en una alerta la semana pasada, dijo que encontró evidencia de vectores de infección inicial utilizando fallas distintas del software SolarWinds.

Cisco, VMware y Deloitte confirman instalaciones de Orion maliciosas

Las compañías de seguridad cibernética Kaspersky y Symatec dijeron que cada una identificó

a 100 clientes que descargaron el paquete troyanizado que contiene la puerta trasera Sunburst, y este último encontró rastros de una carga útil de segunda etapa llamada Teardrop en un pequeño número de organizaciones.

El número específico de víctimas infectadas sigue siendo desconocido en este momento, pero aumenta constantemente desde que la firma de seguridad cibernética FireEye reveló que había sido violada a través del software de SolarWinds a inicios del mes. Hasta ahora, varias agencias gubernamentales y empresas privadas de Estados Unidos, incluidas Microsoft, Cisco, Equifax, General Electric, Inte, NVIDIA, Deloitte y VMware, informaron que encontraron el malware en sus servidores.

> *«Tras el anuncio del ataque de SolarWinds, Cisco Security inició inmediatamente nuestros procesos de respuesta a incidentes establecidos»*, dijo Cisco en un comunicado.
>
> *«Hemos aislado y eliminado las instalaciones de Orion de una pequeña cantidad de entornos de laboratorio y terminales de empleados. En este momento, no se conoce ningún impacto en los productos, servicios o datos de los clientes de Cisco. Seguimos investigando todos los aspectos de esta situación en evolución con la máxima prioridad».*

FireEye fue el primero en exponer la amplia campaña de espionaje el 8 de diciembre después de descubrir que el actor de la amenaza había robado su arsenal de herramientas de prueba de penetración del Red Team, lo que lo convierte en el único caso en el que los atacantes escalaron el acceso hasta el momento. Ningún gobierno extranjero ha anunciado compromisos de sus propios sistemas.

Aunque los informes de los medios lo citan como obra de APT29, Rusia ha negado su participación en la campaña de piratería. Las empresas de ciberseguridad y los investigadores de FireEye, Microsoft y Volexity tampoco atribuyeron estos ataques al actor

de la amenaza.