MILES DE IMPLEMENTACIONES DE SOLARWINDS ORION SIGUEN EXPUESTAS A PELIGROSOS CIBERATAQUES

SECURITY OPERATION CENTER AXITY

A pesar de las desastrosas consecuencias del ataque a la cadena de suministro de SolarWinds, cientos de organizaciones en todo el mundo aún operan con sus implementaciones de SolarWinds Orion expuestas en Internet, dejando de lado cualquier mecanismo para impedir que un nuevo ataque de esta naturaleza pueda ocurrir, así lo afirma un reporte de los analistas de riesgos de RiskRecon.

Como recordará, hace unos meses un grupo de actores de amenazas presuntamente patrocinados por el gobierno de Rusia comprometieron los sistemas de SolarWinds, empleando el acceso ilegítimo para distribuir una actualización maliciosa cargada con el malware Sunburst, que fue recibido por al menos 18 mil organizaciones usando la solución de monitoreo SolarWinds Orion.

Por si no fuera suficiente, un segundo grupo cibercriminal presuntamente relacionado con el gobierno de China logró acceder a las redes informáticas de SolarWinds para entregar una variante de malware identificada como Supernova. Este ataque requirió acceso privilegiado a las redes, además de requerir de la explotación de una falla día cero en Orion, que ya ha sido corregida.

Al momento de la publicación del reporte, los expertos de RiskRecon ya habían detectado al menos 1,330 organizaciones usando una implementación de Orion expuesta en Internet. Considerando que las cifras al momento del ataque eran de 1,780 implementaciones expuestas, los especialistas consideran que aún queda mucho por hacer para mitigar posibles incidentes posteriores.

Por otra parte, un informe de Microsoft firmado por su director legal Brad Smith confirma las declaraciones de un agente de inteligencia de E.U., quien aseguraba que más de un millar de hackers rusos participaron en algún punto de este ataque: "Al analizar el problema nos preguntamos cuántos ingenieros de software podrían haber trabajado en este proyecto. Estimamos que deben haber trabajado más de mil hackers; por nuestra parte estamos trabajando con un grupo de 500 ingenieros completamente dedicados a analizar el compromiso de la cadena de suministro."

Vulnerabilidad en Windows Defender tras más de 12 años

SECURITY OPERATION CENTER AXITY

La vulnerabilidad en el antivirus Windows Defender de Microsoft, que permitiría escalar privilegios, fue corregida después de que los investigadores la detectaran el pasado otoño.

El fallo de seguridad, identificado como CVE-2021-24092 y descubierto por investigadores de la firma de seguridad SentinelOne, se encontraba en el controlador BTR.sys que forma parte del proceso de reparación dentro de Windows Defender para eliminar el sistema de archivos y los recursos de registro creados por el software malicioso desde el modo kernel. Cuando dicho controlador se carga, crea un identificador para un archivo que contiene el registro de sus operaciones. El problema residía en una falta de comprobación de si este archivo es o no un enlace. Por lo tanto, crear un enlace en C:\Windows\Temp\BootClean.log permitiría sobrescribir archivos arbitrarios, eliminar programas e incluso ejecutar código malicioso.

Los investigadores plantean la hipótesis de que el error habría permanecido sin descubrir durante tanto tiempo debido a que el controlador vulnerable no se almacena en el disco duro de una computadora a tiempo completo (como lo harían los controladores de una impresora, por poner un ejemplo), sino que forma parte de la 'biblioteca de vínculos dinámicos' de Windows. De tal modo que el antivirus Windows Defender solamente lo carga cuando es necesario y, una vez que el controlador termina de funcionar, se borra nuevamente del disco.

El equipo de SentinelOne descubrió y reportó el error a Microsoft el 16 de noviembre de 2020. Toda la información al respecto se ha mantenido en secreto hasta que la empresa de Redmond ha lanzado el parche en su ciclo de actualizaciones de seguridad del pasado martes 9 de febrero para evitar que la vulnerabilidad fuese explotada por los cibercriminales.

Guía de ciberataques

SECURITY OPERATION CENTER AXITY

¿Cómo funciona?

Consiste en el envío de grandes cantidades de mensajes o envíos publicitarios a través de Internet sin haber sido solicitados, es decir, se trata de mensajes no deseados. La mayoría tienen una finalidad comercial, aunque puede haberlos que contengan algún tipo de malware.

Spam

¿Cómo se propaga/infecta/extiende?

El canal más utilizado sigue siendo el correo electrónico, pero se sirve de cualquier medio de Internet que permita el envío de mensajes, como las aplicaciones de mensajería instantánea o las redes sociales.

¿Cuál es su objetivo?

Los objetivos son muy variados. Desde el envío masivo de mensajes publicitarios, hasta maximizar las opciones de éxito de un ataque de tipo phishing a una gran población, o tratar de infectar el mayor número posible de equipos mediante malware.

¿Cómo me protejo?

La recomendación es nunca utilizar la cuenta de correo electrónico corporativo para registrarnos en ofertas o promociones por Internet. Además, es fundamental configurar el filtro antiSpam para evitar la recepción de este tipo de mensajes. Otros medios, como las redes sociales, también cuentan con medidas de protección similares pero lo mejor es ignorar y eliminar este tipo de mensajes.

Referencias

- https://www.cibertip.com/ciberseguridad/miles-de-implementaciones-de-solarwinds-orion-siguen-expuestas-a-peligrosos-ciberataques/
- https://unaaldia.hispasec.com/2021/02/vulnerabilidad-en-windows-defender-detectada-despues-de-12-anos-o-mas.html
- https://twitter.com/colCERT/status/1316905577151430657