La compañía de seguridad cibernética CrowdStrike, que se ha involucrado en la investigación del ataque a la cadena de suministro de SolarWinds, informó hoy que identificó una tercera cepa de malware directamente involucrada en el ataque cibernético.

Sunspot es el nombre que la compañía le dio al malware, que se suma a Sunburst (Solorigate) y Teardrop, descubiertas anteriormente.

Sin embargo, aunque Sunspot es el último descubrimiento en el hackeo a SolarWinds, CrowdStrike dijo que en realidad es el primer malware que se utilizó.

En un informe publicado este lunes, CrowdStrike dijo que Sunspot se implementó en septiembre de 2019, cuando los hackers violaron por primera vez la red interna de SolarWinds.

El malware Sunspot se instaló en el servidor de compilación SolarWinds, un tipo de software utilizado por los desarrolladores para ensamblar componentes más pequeños en aplicaciones de software grandes.

CrowdStrike informó que Sunspot tenía un propósito singular: vigilar el servidor de compilación en busca de comandos de compilación que ensamblaron Orion, uno de los principales productos de SolarWinds, una plataforma de monitoreo de recursos de TI utilizada por más de 33 mil clientes en todo el mundo.

Una vez que se detectaba un comando de compilación, el malware reemplazaba de forma silenciosa los archivos de código fuente dentro de la aplicación Orion con archivos que cargaban el malware Sunburst, lo que resultaba en versiones de la aplicación Orion que también instalaban el malware Sunburst.

Los clientes de Orion troyanizados, finalmente se abrieron camino en los servidores de actualización oficiales de SolarWinds y se instalaron en las redes de muchos clientes de la compañía.

Una vez que ocurre esto, el malware Sunburst se activaría dentro de las redes internas de empresas y agencias gubernamentales, donde recopilaría datos sobre sus víctimas y luego enviaría la información a los hackers de SolarWinds.

Los hackers entonces, podrían decidir si una víctima era lo suficientemente importante como para comprometerse y desplegaría el troyano de puerta trasera Teardrop más poderoso en estos sistemas, mientras que al mismo tiempo, instruirían Sunburst para que se borrara de las redes que consideraba insignificantes o de alto riesgo.

Sin embargo, la revelación acerca del descubrimiento de una tercera cepa de malware en el ataque a SolarWinds es una de las tres actualizaciones principales que hoy salieron a la luz.

En un anuncio separado, SolarWinds publicó en su blog una línea de tiempo del hackeo. El proveedor de software con sede en Texas dijo que antes de que el malware Sunburst se implementara en los clientes entre marzo y junio de 2020, los hackers también ejecutaron una prueba entre septiembre y noviembre de 2019.

> *«La versión posterior de octubre de 2019 del lanzamiento de la plataforma Orion parece haber contenido modificaciones diseñadas para probar la capacidad de los perpetradores para insertar código en nuestras compilaciones»*, dijo el director ejecutivo de SolarWinds, Sudhakar Ramakrishna.

Además, la compañía de seguridad Kaspersky, también publicó sus hallazgos en un informe separado.

Kaspersky, que no formó parte de la investigación formal sobre el ataque a SolarWinds, analizó el malware e informó que el código fuente de Sunburst tiene superposiciones de código entre Sunburst y Kazuar, una cepa de malware vinculada al grupo Turla, de Rusia.