xataka.com

# El ataque a SolarWinds, explicado: por qué un ataque a esta empresa desconocida trae de cabeza a grandes...

*Bárbara Bécares*

6-7 minutos

---

El ataque a SolarWinds que se dio a conocer el 13 de diciembre podría haber quedado como un ataque más a una empresa, si no fuera por la relevancia de los clientes que tiene. Lo que empezó como un ciberataque a un software hace casi un mes, **ha derivado en el acceso a un código fuente** de software de Microsoft, como la compañía anunció.

La **información de unas 18.000 empresas de todo el mundo, también de España,** y de las mayores agencias de gobierno de Estados Unidos podría estar ahora en manos de un "una nación extranjera", según SolarWinds. ¿Qué tiene esta empresa y su software que han causado tanto revuelo?


- **Qué es SolarWinds y cuál es su mayor activo**. Además de ser una empresa nacida en 1999 en Oklahoma, SolarWinds es

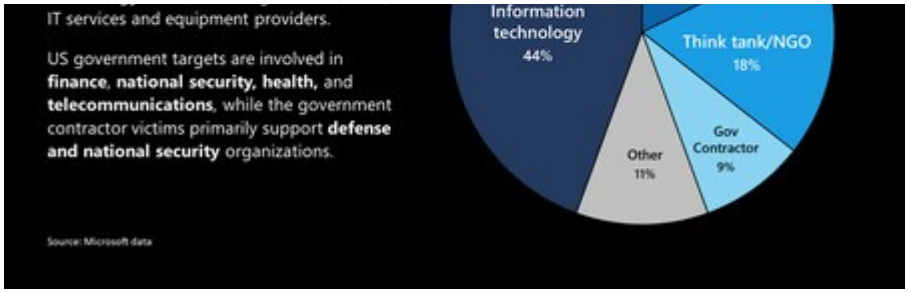
la empresa fabricante de Orion, un software que es usado por unos 33.000 clientes entre los que se incluyen casi todas las empresas que integran la lista de Fortune 500 y organizaciones gubernamentales de Estados Unidos **como la NASA, las fuerzas aéreas o el Pentágono**. La misma empresa describe Orion como "una plataforma de administración y monitorización están de la infraestructura diseñada para simplificar la administración de TI en entornos locales, híbridos y de software como servicio (SaaS) en un solo panel".

- **Cómo y cuándo fue el ataque a SolarWinds**. El anuncio llegó el 13 de diciembre pero las informaciones apuntan a que en la actualización del pasado mes de marzo se habría introducido una puerta trasera, comprometiendo la herramienta Orion y de paso toda la infraestructura de las empresas que lo utilizan. Esta vulnerabilidad se conoce como Sunburst o **Solorigate.** Cuando está presente y activada permite al atacante acceder a la cadena de suministro. Es decir, los atacantes comprometen la seguridad de un tercero, en este caso SolarWinds, y consiguen con ello infiltrarse en compañías y entidades públicas que usan sus servicios, como Microsoft, la NASA o Cisco (y casi todas las compañías que integran la lista de Fortune 500). El 21 de diciembre se descubrió otro malware que se ha bautizado como Supernova, un malware que puede desplegar código malicioso. Con la información que hay hasta ahora, **Supernova tiene menor relevancia**.

- **Quién atacó a SolarWinds y a su larga lista de clientes**.

Sobre Sunburst dice SolarWinds en su web que "se nos ha informado de que la naturaleza de este ataque indica que puede **haber sido llevado a cabo por un estado nación exterior**". La empresa se muestra muy cauta ante una información muy relevante que ha levantado mucha polémica. El 18 de diciembre, Mike Pompeo, actual secretario de estado de Estados Unidos, dijo públicamente que "podemos decir que está bastante claro que los rusos están relacionados con esta actividad". Microsoft, como una de las empresas afectadas, habló de "un actor estatal muy sofisticado".

- **Qué tiene que ver esto con el código fuente de Microsoft.** La investigación del centro de respuestas de Microsoft descubrió que más allá de la presencia de código malicioso en los programas de SolarWinds, también se habían detectado intentos por acceder a sus programas por parte de un hacker. "Descubrimos que **una cuenta había sido utilizada para ver el código fuente**", afirmó la de Redmond. Desde la firma dicen que ese problema está solucionado y no ha afectado a sus clientes, pero la polémica saltó. Para CNBC esto muestra una señal preocupante de las ambiciones de los espías, puesto que el código fuente no deja de ser una de las tecnologías más guardadas y protegidas de una empresa. Microsoft no ha detallado qué tipo de código fuente fue visto ni qué software está afectado por esto. Según el presidente de esta empresa, ver el código fuente no quiere decir que los hackers hayan podido acceder a información de mayor importancia y que no hay indicios de que sus sistemas hayan sido usados para atacar a terceros.




- **Por qué nos importa el ataque de seguridad a SolarWinds**. Ahora toca saber qué tiene que ver SolarWinds con una empresa española o con una europea. La firma tiene 33.000 clientes (o tenía en el momento del ataque), de acuerdo con The Verge. De esos, las investigaciones de Microsoft, **hablan de más de 18.000 clientes que tendrían instalada la actualización de Orion afectada por el ataque** y 40 entidades públicas. De acuerdo con un texto firmado por Brad Smith, presidente de Microsoft, un 20% de las empresas afectadas están repartidos en siete países fuera de Estados Unidos. Estos países son: Canadá, México, Bélgica, Reino Unido, España e Israel. Y "está claro que el número de víctimas y ubicaciones va a seguir creciendo", concluyó. SolarWinds eliminó la lista concreta de sus clientes, que estaba en su web.

- **Solución conocida a esta brecha de seguridad**. El secretismo continúa alrededor del ataque a SolarWinds y aún no se sabe el alcance de este evento que lleva tres semanas copando titulares. SolarWinds pidió a sus clientes que **se asegurasen de haber eliminado de sus sistemas las versiones de su software** que se sabe que están afectadas por la vulnerabilidad de Sunburst. Por su parte, Microsoft tomó la decisión de poner en cuarentena las versiones de SolarWinds

Orion Platform afectadas desde el día 16 de diciembre.

- **A qué han podido tener acceso los atacantes**. Esa es la pregunta que aún no tiene una respuesta clara. La investigación se está llevando a cabo de una forma muy discreta. De hecho, Mike Pompeo dijo en la mencionada entrevista que la investigación estaba aún trabajando por esclarecer dudas y que probablemente **mucha de la información se vaya a mantener clasificada**. SolarWinds ha hablado poco sobre el alcance total del ataque. Aparte de Microsoft, las empresas clientes de este software no se han pronunciado al respecto.