La compañía alemanda de software detrás de TeamViewer, uno de los programas más populares del mundo para compartir escritorio de forma remota, tuvo una brecha de seguridad en 2016, según el diario alemán Der Spiegel.

TeamViewer es un software popular de soporte remoto que permite compartir tu computadora de forma segura o tomar el control total de la computadora de otros por medio de Internet desde cualquier parte del mundo. El software siempre ha sido blanco de interés por parte de los hackers, en parte por sus millones de usuarios.

Según el reportaje, el ataque cibernético fue lanzado por piratas informáticos chinos que utilizaron el troyano Winnti, cuyas actividades fueron encontradas vinculadas al sistema de inteligencia estatal chino.

Winnti, formado por un grupo de amenazas persistentes avanzadas (APT), activo desde 2010, lanzó una serie de ataques financieros contra software y organizaciones de juegos principalmente en Estados Unidos, Japón y Corea del Sur.

El grupo es conocido por utilizar ataques en la cadena de suministro al infectar software o servidores legítimos con actualizaciones maliciosas para instalar malware en los sistemas de usuarios finales.

Una vez infectado, Winnti descarga una carga de puerta trasera en las computadoras comprometidas, lo que brinda a los atacantes la capacidad de controlar de forma remota las computadoras de las víctimas sin su consentimiento.

Der Spiegel criticó a la compañía TeamViwer por no revelar la intrusión al público para informar lo sucedido a sus clientes, muchos de los cuales utilizan el software específico en empresas.

Sin embargo, la compañía informó a The Hacker News que descubrió el ataque cibernético *«a tiempo»*, poco después de detectar actividades sospechosas, por lo que tomó las medidas necesarias e inmediatas para *«evitar cualquier daño importante».*

TeamViewer también informó que tanto su equipo como las autoridades responsables en ese momento no encontraron pruebas de que los datos de los clientes fueran robados o que los sistemas informáticos de sus clientes estuvieran infectados.

> *«Al igual que muchos líderes tecnológicos, TeamViewer se enfrente con frecuencia a los ataques de los delincuentes cibernéticos. Por este motivo, invertimos constantemente en el avance de nuestra tecnología de TI y cooperamos estrechamente con instituciones de renombre mundial en este campo.*
>
> *En otoño de 2016, TeamViewer fue objeto de un ciberataque. Nuestros sistemas detectaron las actividades sospechosas a tiempo para evitar daños mayores. Un equipo de expertos de investigadores de seguridad cibernética internos y externos, que trabajaron en estrecha colaboración con las autoridades responsables, se defendieron con éxito y con todos los medios forenses de TI disponibles no encontraron evidencia de que los datos del cliente u otra información confidencial hayan sido robados, que los sistemas informáticos de los clientes hayan sido infectados o que el código fuente de TemViewer haya sido manipulado, robado o utilizado de otra forma»,* dijo la compañía en un comunicado.

TeamViewer también confirmó a THN que la infracción informada no está relacionada de ningún modo con otro evento de piratería ocurrido en mayo de 2016 cuando los usuarios de TeamViewer afirmaron que los piratas informáticos vaciaban sus cuentas bancarias al explotar una falla en el software.

Además, en un comunicado de prensa publicado en ese momento, TemViewer afirmó que ni la compañía había sido pirateada ni que había un agujero de seguridad, en cambio, culpó a los usuarios por el uso descuidado del software.