xataka.com

Un sofisticado ciberataque contra SolarWinds enciende las alarmas: el proveedor del Pentágono y decenas...

Enrique Pérez

4-5 minutos

Las empresas tecnológicas están en alarma por el último ciberataque. El proveedor informático SolarWinds anuncia "que sus sistemas sufrieron un ataque manual altamente sofisticado a la cadena de suministros de su software Orion". Un **ciberataque "extremadamente dirigido" que habría estado realizado por "un estado nacional externo"**.

No es un objetivo baladí, pues entre los clientes de SolarWinds se encuentran la gran mayoría de grandes empresas de los EE.UU, además de **organizaciones gubernamentales** como la NASA, las fuerzas aéreas o el Pentágono.

Un importante ciberataque pone en jaque a la industria

El ciberataque se cree relacionado con la intrusión a la firma FireEye, donde desde el Washington Post **se apunta a Rusia como origen**. La confirmación del ataque llega al mismo tiempo que la inteligencia de los Estados Unidos se encuentra investigando varios ataques al Departamento de Comercio y el Tesoro.

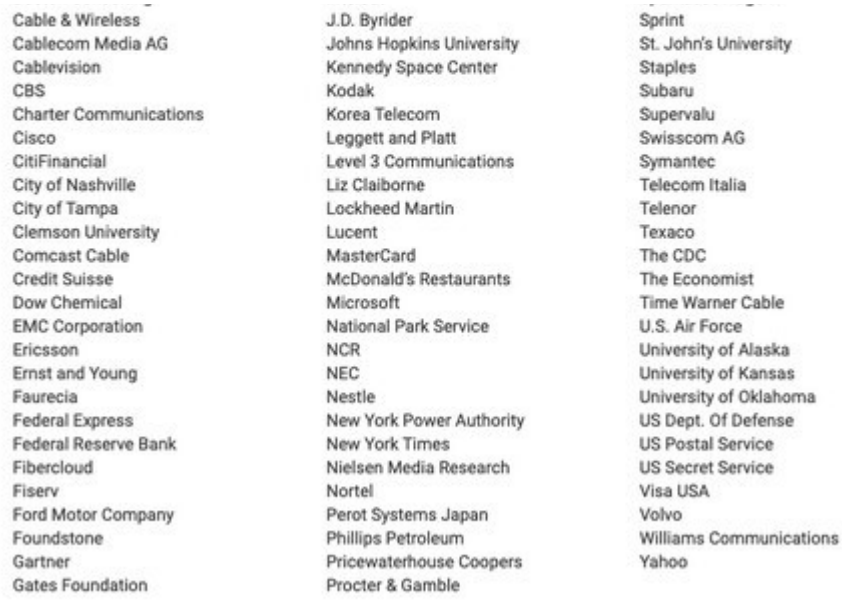
En respuesta a Reuters, desde SolarWinds explican que están "actuando en estrecha coordinación con FireEye, la Oficina Federal de Investigaciones, la comunidad de inteligencia y otras fuerzas del orden para investigar estos asuntos".

> SolarWinds asks all customers to upgrade immediately to Orion Platform version 2020.2.1 HF 1 to address a security vulnerability. More information is available at https://t.co/scsUhZJCk8
>
> — SolarWinds (@solarwinds) December 14, 2020

El sistema **Orion es una herramienta de monitorización y administración de redes, utilizado por múltiples grandes empresas**. Se cree 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.

Comprometer los sistemas de SolarWinds significa atacar potencialmente al enorme listado de grandes empresas que colaboran con ellos. De la lista Fortune 500, 425 empresas están incluida: desde las 10 mayores empresas de telecomunicaciones hasta las cinco agencias militares de los EE.UU.

Acxiom	General Dynamics	Sabre
Ameritrade	Gillette Deutschland GmbH	Saks
AT&T	GTE	San Francisco Intl. Airport
Bellsouth Telecommunications	H&R Block	Siemens
Best Western Intl.	Harvard University	Smart City Networks
Blue Cross Blue Shield	Hertz Corporation	Smith Barney
Booz Allen Hamilton	ING Direct	Smithsonian Institute
Boston Consulting	IntelSat	Sparkasse Hagen



Cable & Wireless
Cablecom Media AG
Cablevision
CBS
Charter Communications
Cisco
CitiFinancial
City of Nashville
City of Tampa
Clemson University
Comcast Cable
Credit Suisse
Dow Chemical
EMC Corporation
Ericsson
Ernst and Young
Faurecia
Federal Express
Federal Reserve Bank
Fibercloud
Fiserv
Ford Motor Company
Foundstone
Gartner
Gates Foundation
J.D. Byrider
Johns Hopkins University
Kennedy Space Center
Kodak
Korea Telecom
Leggett and Platt
Level 3 Communications
Liz Claiborne
Lockheed Martin
Lucent
MasterCard
McDonald's Restaurants
Microsoft
National Park Service
NCR
NEC
Nestle
New York Power Authority
New York Times
Nielsen Media Research
Nortel
Perot Systems Japan
Phillips Petroleum
Pricewaterhouse Coopers
Procter & Gamble
Sprint
St. John's University
Staples
Subaru
Supervalu
Swisscom AG
Symantec
Telecom Italia
Telenor
Texaco
The CDC
The Economist
Time Warner Cable
U.S. Air Force
University of Alaska
University of Kansas
University of Oklahoma
US Dept. Of Defense
US Postal Service
US Secret Service
Visa USA
Volvo
Williams Communications
Yahoo

Entre los clientes de SolarWinds encontramos empresas como Ford, MasterCard, AT&T o las fuerzas aéreas de los EE.UU.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) ha publicado una nota informativa de emergencia donde alerta del "**riesgo inaceptable**" de este ciberataque que tendría como objetivo monitorizar el tráfico de los sistemas federales y podría suponer un "grave impacto en caso de un compromiso exitoso".

> Last night we issued an emergency directive to mitigate the compromise involving SolarWinds Orion products: https://t.co/VFZ81W2Ow7. We urge all our partners—in the public & private sectors—to assess their exposure to this compromise and to secure their networks.
>
> — Cybersecurity and Infrastructure Security Agency (@CISAgov) December 14, 2020

Por parte de Microsoft también se ha confirmado el ataque a Orion. La compañía de Redmond cree que "se trata de una actividad de estado-nación a una escala significativa, dirigida tanto al gobierno como al sector privado".

Debido a la sofisticación del ataque, Microsoft urge a un

escrutinio general por parte de la comunidad. La compañía explica que como resultado del ataque, los atacantes podrían obtener credenciales para acceder a la red de las empresas y **acceder a cuentas certificadas de los usuarios de la empresa**.

Por el momento **no hay confirmación de qué empresas ni agencias se han visto afectadas**. Previsiblemente, las consecuencias de este complejo ciberataque no se irán mostrando hasta pasado un tiempo. Según explica SolarWinds, menos de 18.000 clientes se han visto afectados. Desde Google, niegan que el incidente de esta mañana haya sido causado por un ciberataque.

Vía | ZDnet