CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Resumen ciberataque que afectó a SolarWinds y FireEye

Santiago, 15 de Diciembre de 2020

TLP: BLANCO

Programa Red de Conectividad del Estado

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Nota

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Este informe fue clasificado como TLP BLANCO. La información puede ser distribuida sin restricciones.

Contenido

1. Resumen ejecutivo 4
2. Contexto alerta 5
3. Indicadores de Compromiso 7
4. Mitigaciones 8
5. Recomendaciones 9
6. Enlaces 9

1. Resumen ejecutivo

Este resumen de ciberataques, vulnerabilidades e incidentes de seguridad cibernética tiene como propósito destacar algunos eventos acaecidos en días pasados para que puedan ser interpretados y discutidos por las diferentes entidades que tengan acceso a su lectura.

Este informe reúne Indicadores de Compromiso asociados al incidente que afectó a la plataforma Orion de SolarWinds el pasado 13 de diciembre, donde los ciberdelincuentes insertaron el malware identificado como "SUNBURST" en el servicio de actualización del software en sus versiones 2019.4 HF 5, 2020.2. sin revisión instalada y 2020.2 HF 1

FireEye denominó al actor malicioso como "UNC2452". El presente documento entrega además recomendaciones y las mitigaciones liberadas por SolarWinds para disminuir los riesgos.

Los Indicadores de Compromiso compartidos en este informe fueron liberados por FireEye en su plataforma Github, y por Microsoft mediante su blog de Centro de Respuesta de Seguridad. La información consignada en el presente documento es catalogada como TLP BLANCO.

2. Contexto alerta

El domingo 13 de diciembre, la empresa SolarWinds informó haber sido víctima de un ataque de cadena de suministro altamente sofisticado, afectando a organizaciones públicas y privadas de todo el mundo.

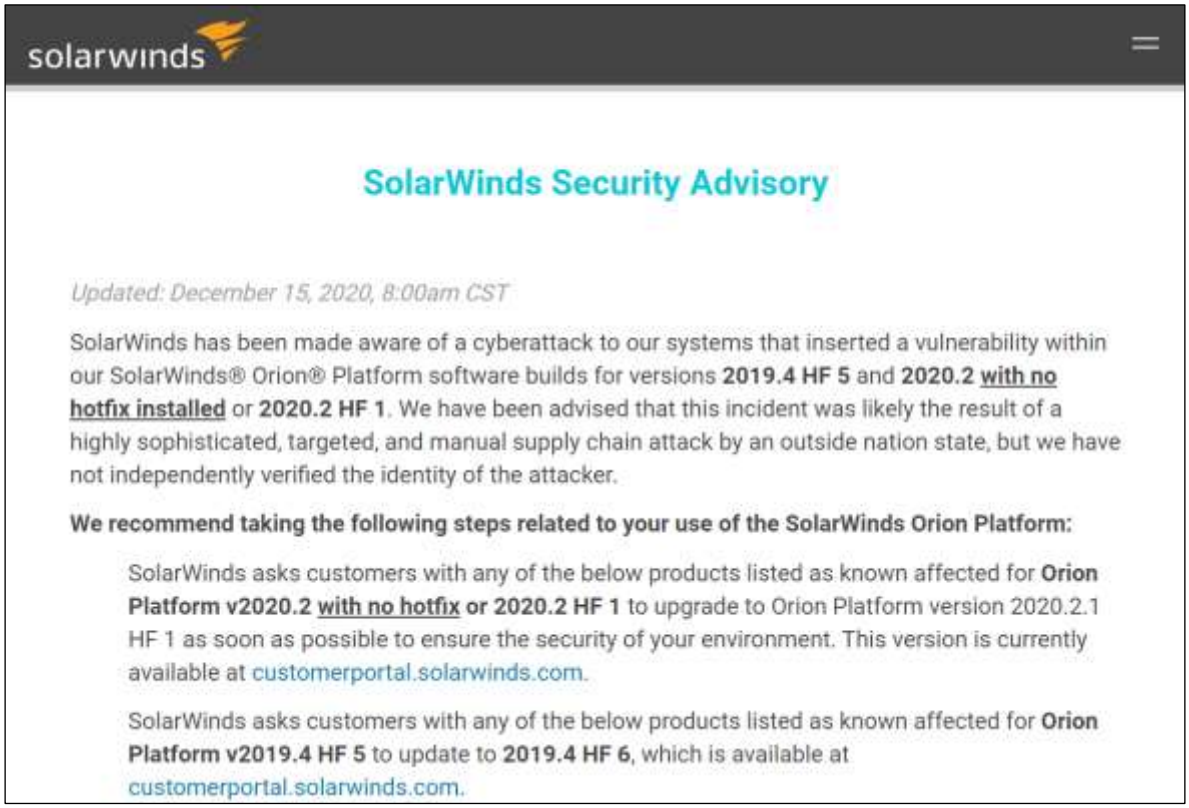
El ciberataque, confirmado por organizaciones como Microsoft, FireEye y la Agencia de Ciberseguridad e Infraestructura de EE.UU., CISA, infectó a las actualizaciones de su software de monitoreo de redes Orion publicadas entre marzo y junio de este año (versiones 2019.4 HF 5, 2020.2. sin revisión instalada y 2020.2 HF 1.), con un malware llamado “SUNBURST”.

Por esta razón, SolarWinds solicitó, ese mismo día, a sus clientes actualizar Orion inmediatamente a su versión 2020.2.1 HF 1. De acuerdo a lo informado por la compañía, durante este martes 15 de diciembre se debería lanzar una nueva actualización de emergencia, llamada 2020.2.1 HF 2, la que reemplazará el componente comprometido y agregará nuevas funcionalidades de seguridad, el cual aún no se encuentra disponible.

El ataque está relacionado con el que afectó a la firma FireEye y que fue comunicada la semana pasada, cuando informó del robo de herramientas de Red Team y explicó que las vulnerabilidades explotadas eran todas ya conocidas.

Medios estadounidenses indican que habría varias agencias gubernamentales afectadas, como el Departamento del Tesoro y la NTIA, provocando una reunión del Consejo de Seguridad Nacional de EE.UU.

Según diversos expertos, detrás de los ataques estarían asociados al APT29, aunque FireEye decidió darle el nombre UNC2452.



solarwinds

SolarWinds Security Advisory

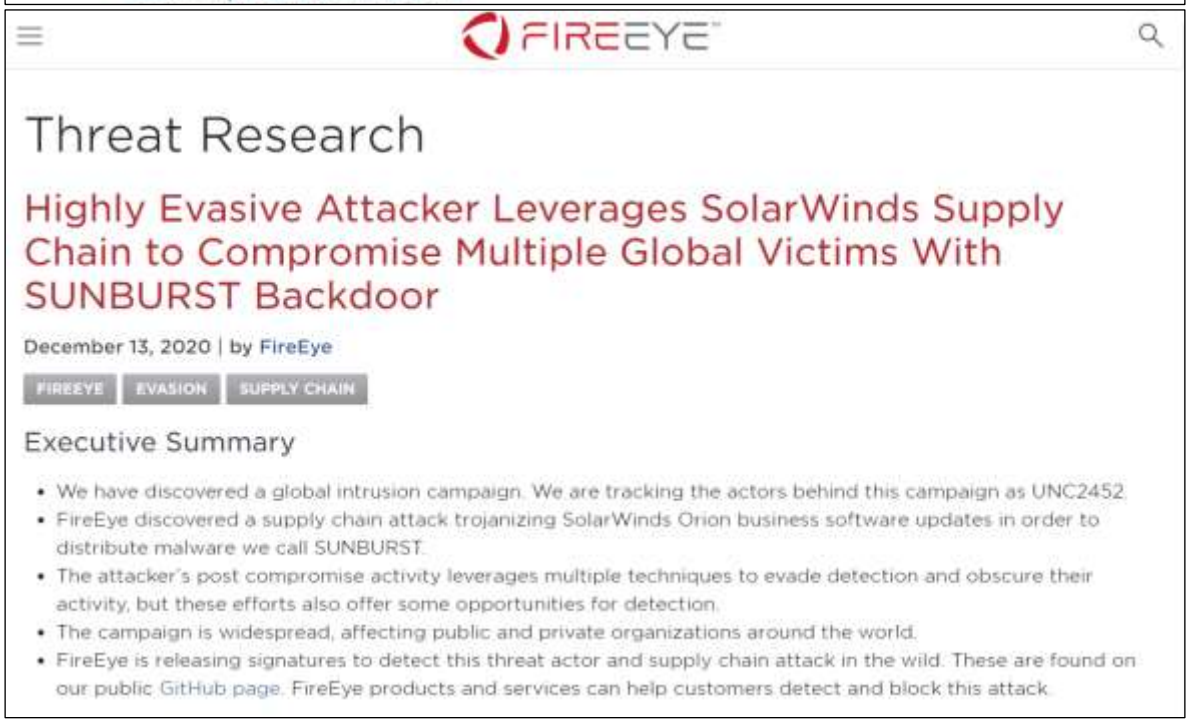
Updated: December 15, 2020, 8:00am CST

SolarWinds has been made aware of a cyberattack to our systems that inserted a vulnerability within our SolarWinds® Orion® Platform software builds for versions **2019.4 HF 5** and **2020.2 with no hotfix installed** or **2020.2 HF 1**. We have been advised that this incident was likely the result of a highly sophisticated, targeted, and manual supply chain attack by an outside nation state, but we have not independently verified the identity of the attacker.

We recommend taking the following steps related to your use of the SolarWinds Orion Platform:

SolarWinds asks customers with any of the below products listed as known affected for **Orion Platform v2020.2 with no hotfix or 2020.2 HF 1** to upgrade to Orion Platform version 2020.2.1 HF 1 as soon as possible to ensure the security of your environment. This version is currently available at customerportal.solarwinds.com.

SolarWinds asks customers with any of the below products listed as known affected for **Orion Platform v2019.4 HF 5** to update to **2019.4 HF 6**, which is available at customerportal.solarwinds.com.



FIREEYE

Threat Research

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

December 13, 2020 | by FireEye

FIREEYE EVASION SUPPLY CHAIN

Executive Summary

- We have discovered a global intrusion campaign. We are tracking the actors behind this campaign as UNC2452.
- FireEye discovered a supply chain attack trojanizing SolarWinds Orion business software updates in order to distribute malware we call SUNBURST.
- The attacker's post compromise activity leverages multiple techniques to evade detection and obscure their activity, but these efforts also offer some opportunities for detection.
- The campaign is widespread, affecting public and private organizations around the world.
- FireEye is releasing signatures to detect this threat actor and supply chain attack in the wild. These are found on our public GitHub page. FireEye products and services can help customers detect and block this attack.

3. Indicadores de Compromiso

Los siguientes IoC fueron liberados por las empresas SolarWinds y Microsoft. El CSIRT de Gobierno recomienda tener en consideración los siguientes Indicadores de Compromiso, monitorear y/o bloquear las IP's y Hash, además de revisar el repositorio GitHub que compartió FireEye con reglas en múltiples lenguajes para sus respectivas plataformas: Snort, Yara, IOC, ClamAV, disponibles en el siguiente enlace: https://github.com/fireeye/sunburst_countermeasures

Indicadores entregados por FireEye	
Hash 256	Nombre Archivo
d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600	CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp
53f8dfc65169ccda021b72a62e0c22a4db7c4077f002fa742717d41b3c40f2c7	Solarwinds Worldwide, LLC
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134	SolarWinds.Orion.Core.BusinessLayer.dll
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6	SolarWinds.Orion.Core.BusinessLayer.dll
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77	SolarWinds.Orion.Core.BusinessLayer.dll
292327e5c94afa352cc5a02ca273df543f2020d0e76368ff96c84f4e90778712	OrionImprovementBusinessLayer.2.cs
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71	app_web_logoimagehandler.ashx.b6031896.dll

Indicadores entregados por Microsoft	
Hash 256	Versión del archivo
519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77	2019.4.5200.9083
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b	2020.2.100.12219
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed	2020.2.100.11831
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77	No disponible
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c	2020.4.100.478
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134	2020.2.5200.12394
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6	2020.2.5300.12432
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc	2019.4.5200.8890
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af	2019.4.5200.8890

Dominios
.avsvmcloud[.]com
deftsecurity[.]com
freescanonline[.]com
thedoccloud[.]com
websitetheme[.]com
highdatabase[.]com
incomeupdate[.]com
databasegalore[.]com
panhardware[.]com
zupertech[.]com

zupertech[.]com

IP
13.59.205.66
54.193.127.66
54.215.192.52
34.203.203.23
139.99.115.204
5.252.177.25
5.252.177.21
204.188.205.176
51.89.125.18
167.114.213.199

4. Mitigaciones

SolarWinds disponibilizó dos actualizaciones de emergencia (2019.4 HF 6 y 2020.2.1 HF 1) para la mitigación de la vulnerabilidad, además de agregar múltiples funcionalidades de seguridad, por lo que se recomienda realizar las actualizaciones a la brevedad para mitigar las vulnerabilidades.

Si no es posible aplicar las actualizaciones de seguridad de forma inmediata, FireEye publicó una serie de recomendaciones que permiten mitigar la amenaza:

- Asegurarse de que los servidores SolarWinds estén aislados/contenidos hasta que se lleve a cabo una revisión e investigación adicionales. Esto debería incluir el bloqueo de todas las salidas de Internet de los servidores SolarWinds.
- Si la infraestructura de SolarWinds no está aislada, realizar los siguientes pasos:
  - Restringir el alcance de la conectividad a los puntos finales de los servidores de SolarWinds, especialmente aquellos que se considerarían activos de capa 0.
  - Restringir el alcance de las cuentas que tienen privilegios de administrador local en los servidores SolarWinds.
  - Bloquear la salida de Internet desde servidores u otros puntos finales con el software SolarWinds.
- Considerar, como mínimo, cambiar las contraseñas de las cuentas que tienen acceso a los servidores/infraestructura de SolarWinds. En base a una revisión/investigación adicional, es posible que se requieran medidas de mitigación adicionales.

Para obtener más información sobre este incidente, pueden ingresar al sitio web: https://www.solarwinds.com/securityadvisory

En caso de emergencia es posible contactarse directamente con la empresa en https://www.solarwinds.com/company/contact-us

5. Recomendaciones

Junto con las mitigaciones y recomendaciones obtenidas por SolarWinds, el CSIRT de Gobierno solicita considerar otras medidas preventivas, como:

- Actualizar plataformas de seguridad de antivirus y EDR para tener las últimas actualizaciones de detección de bibliotecas y comportamientos de procesos anómalos.
- Desactivar SolarWinds en su entorno hasta tener la versión confiable y recomendada por el fabricante.
- Bloquear y monitorear los Indicadores de Compromiso compartidos en este informe.
- Disminuir la cantidad de usuarios con privilegios elevados, como administradores globales, administradores de aplicaciones y administradores de aplicaciones en la nube de Active Directory de Microsoft.
- Monitorear inicios de sesión en estaciones de trabajo y servidores.
- Revisar dispositivos para detectar modificaciones no autorizadas.

6. Enlaces

https://github.com/fireeye/sunburst_countermeasures

https://www.solarwinds.com/securityadvisory

https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software

https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

CSIRT
Gobierno de
Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.12.15 23:03:48 -03'00'