SolarWinds advanced cyberattack: What happened and what to do now

By Mark Stockley

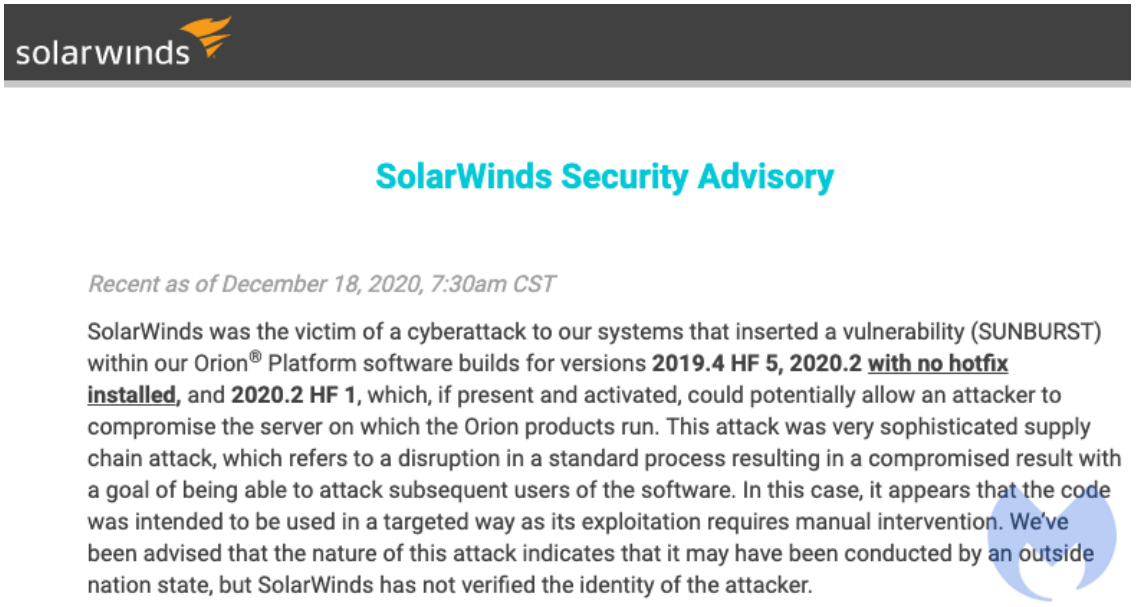
Published: 2020-12-13 · Archived: 2026-04-05 20:37:29 UTC

December 14, 2020

We learned more about the sophisticated attack first disclosed on December 8 when security firm FireEye reported it had been the victim of a state-sponsored adversary that stole Red Team assessment tools.

On December 13 there was a new development when IT company SolarWinds announced it had been hacked and that its compromised software channel was used to push out malicious updates onto 18,000 of its Orion platform customers.

This scenario, referred to as a supply-chain attack, is perhaps the most devious and difficult to detect as it relies on software that has already been trusted and that can be widely distributed at once. Among the victims who received the malicious update are FireEye, Microsoft and the US Treasury and Commerce departments, making this one of the biggest cyber incidents we have witnessed in years.



solarwinds

SolarWinds Security Advisory

Recent as of December 18, 2020, 7:30am CST

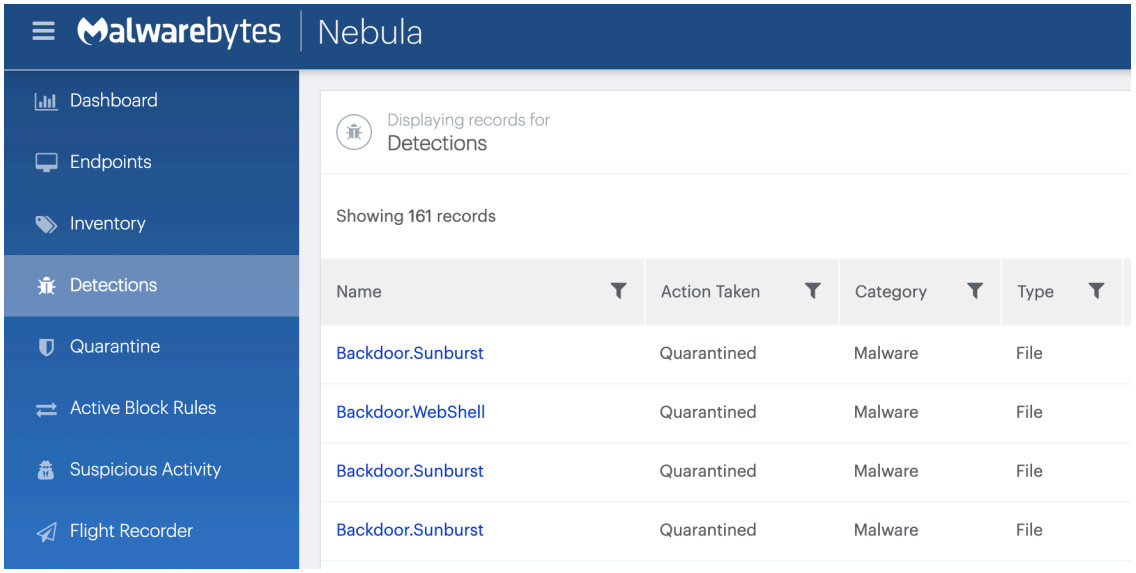
SolarWinds was the victim of a cyberattack to our systems that inserted a vulnerability (SUNBURST) within our Orion® Platform software builds for versions **2019.4 HF 5, 2020.2 with no hotfix installed,** and **2020.2 HF 1**, which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run. This attack was very sophisticated supply chain attack, which refers to a disruption in a standard process resulting in a compromised result with a goal of being able to attack subsequent users of the software. In this case, it appears that the code was intended to be used in a targeted way as its exploitation requires manual intervention. We've been advised that the nature of this attack indicates that it may have been conducted by an outside nation state, but SolarWinds has not verified the identity of the attacker.

The Department of Homeland Security has issued an emergency directive to order all federal agencies to take immediate steps in putting affected SolarWinds Orion products offline and reporting back any incident by Monday.

We do know that the threat actors were in for a much bigger prize than the offensive tools stolen from security firm FireEye, although this incident helped to uncover a very advanced operation with deep ramifications. As this story is still unfolding we will keep our customers informed of any newer developments.

Call to action

- Immediately isolate any systems running the Orion platform **versions 2019.4 HF 5 through 2020.2.1**, released between March 2020 and June 2020.
- Scan your premises using Malwarebytes and look for any detection, and in particular **Backdoor.Sunburst** and **Backdoor.WebShell**.
- Use the Indicators of Compromise at the end of this blog to hunt within your logs, telemetry and other SIEM data to give a timeline perspective to any potential intrusion.
- Perform a comprehensive security sweep to review and harden your physical and cloud infrastructure.
- Upgrade to Orion Platform version **2020.2.1 HF 2** and restore systems once you feel confident with the previous steps.



Further reading

- **SolarWinds**: SolarWinds Security Advisory
- **FireEye**: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor
- **Microsoft**: Customer Guidance on Recent Nation-State Cyber Attacks
- **Volexity**: Dark Halo Leverages SolarWinds Compromise to Breach Organizations
- **CISA**: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
- **Microsoft**: Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect

Indicators of Compromise (IOCs)

This list has been put together from several sources. Kudos to FireEye and Microsoft for sharing IOCs and TTPs so quickly.

SolarWinds.Orion.Core.BusinessLayer.dll

32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589
6e4050c6a2d2e5e49606d96dd2922da480f2e0c70082cc7e54449a7dc0d20f8d

CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp
d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600

appweblogoimagehandler.ashx.b6031896.dll
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71

Additional DLLs
e0b9eda35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d
20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9
2b3445e42d64c85a5475bdbc88a50ba8c013febb53ea97119a11604b7595e53d
a3efbc07068606ba1c19a7ef21f4de15d15b41ef680832d7bcba485143668f2d
92bd1c3d2a11fc4aba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690
a58d02465e26bdd3a839fd90e4b317eece431d28cab203bbdde569e11247d9e2
cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70e01dc69048e6

TEARDROP
b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07
1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c

Raindrop (Source)
f2d38a29f6727f4ade62d88d8a68de0d52a0695930b8c92437a2f9e4de92e418
be9dbbec6937dfe0a652c0603d4972ba354e83c06b8397d6555fd1847da36725
955609cf0b4ea38b409d523a0f675d8404fee55c458ad079b4031e02433fdbf3
240ef5b8392b8c7a5a025c36a7e5b0e03e5bb0d0d1a28703bb22e6159a4fd10e
f2d38a29f6727f4ade62d88d8a68de0d52a0695930b8c92437a2f9e4de92e418
955609cf0b4ea38b409d523a0f675d8404fee55c458ad079b4031e02433fdbf3
be9dbbec6937dfe0a652c0603d4972ba354e83c06b8397d6555fd1847da36725

Network indicators

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

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

Additional hunting rules: https://github.com/fireeye/sunburst_countermeasures/tree/main/rules

---