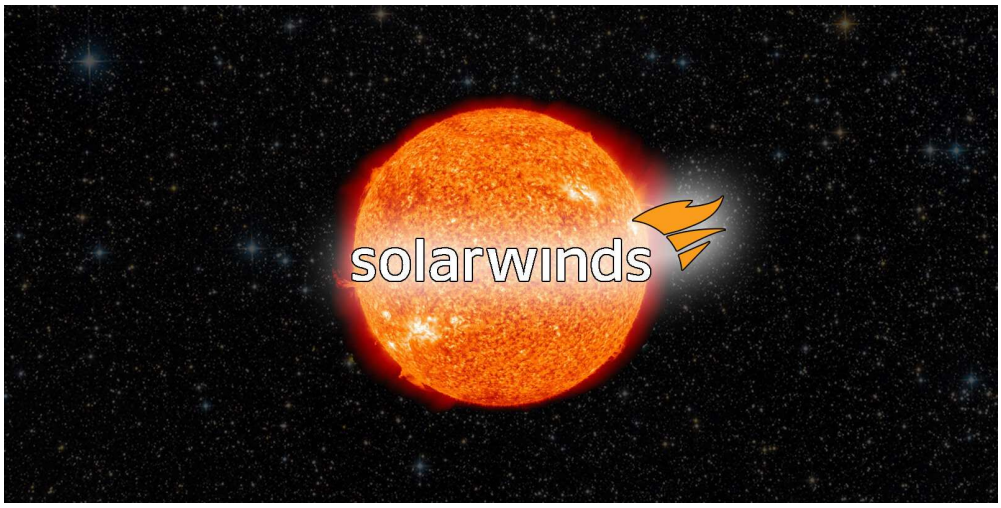
The SolarWinds cyberattack: The hack, the victims, and what we know

By
Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)

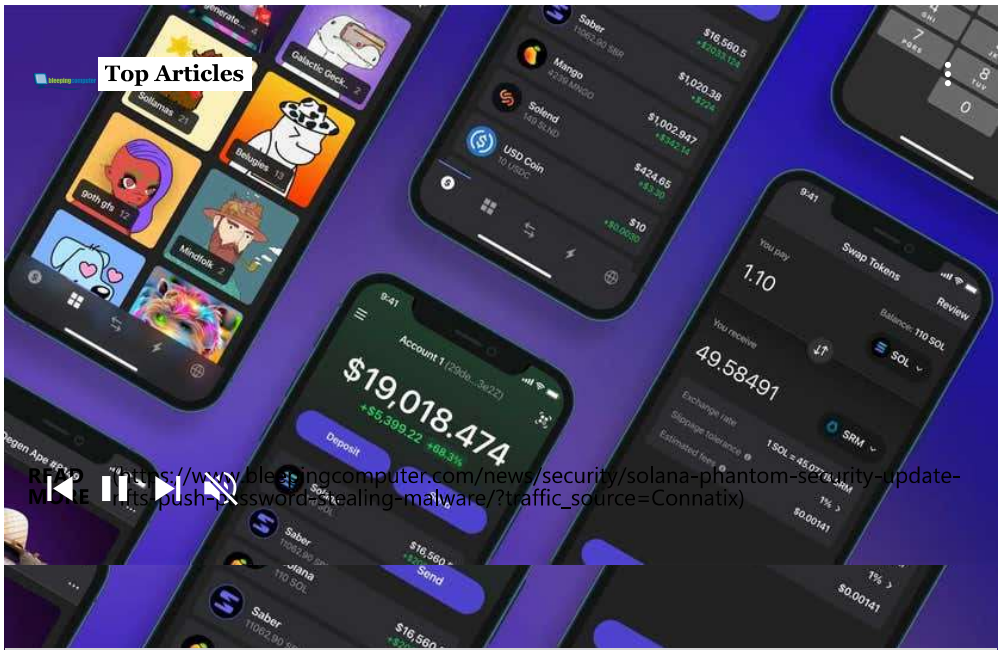
December 19, 2020 10:10 AM 13



Since the SolarWinds supply chain attack was disclosed in December, there has been a whirlwind of news, technical details, and analysis released about the hack.

Because the amount of information that was released in such a short time is definitely overwhelming, we have published this as a roundup of SolarWinds news.

The information is distilled into a format that will hopefully explain the attack, who its victims are, and what we know to this point.



The SolarWinds supply chain attack

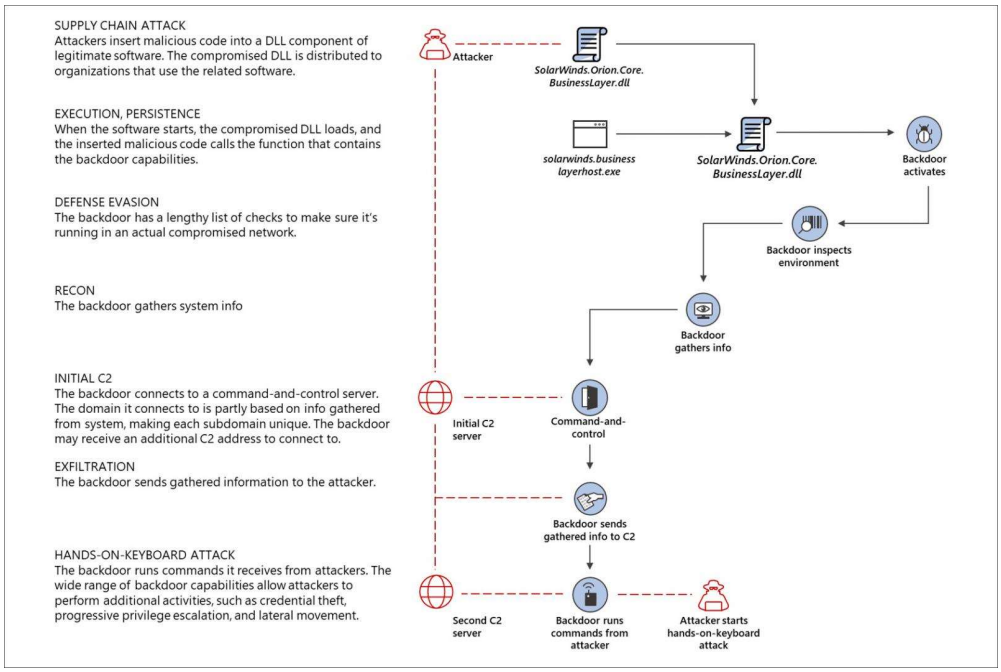
While we learned of SolarWinds' attack on December 13th, the first disclosure of its consequence was made on December 8th when leading cybersecurity firm FireEye revealed that it was hacked by a nation-state APT group (https://www.bleepingcomputer.com/news/security/fireeye-reveals-that-it-was-hacked-by-a-nation-state-apt-group/). As part of this attack, the threat actors stole Red Team assessment tools that FireEye uses to probe its customers' security.

It was not known how the hackers gained access to FireEye's network until Sunday, December 13th, 2020, when Microsoft (https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/), FireEye (https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html), SolarWinds (https://www.solarwinds.com/securityadvisory), and the

U.S. government (https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software) issued a coordinated report (https://www.bleepingcomputer.com/news/security/us-govt-fireeye-breached-after-solarwinds-supply-chain-attack/) that SolarWinds had been hacked by state-sponsored threat actors believed to be part of the Russian S.V.R.

One of SolarWinds' customers who was breached in this attack is FireEye.

As part of the attack, the threat actors gained access to the SolarWinds Orion build system and added a backdoor to the legitimate ***SolarWinds.Orion.Core.BusinessLayer.dll*** DLL file. This DLL was then distributed to SolarWinds customers in a supply chain attack via an automatic update platform used to push out new software updates.



SolarWinds supply chain attack
Source: Microsoft

This DLL backdoor is known as Sunburst (FireEye) or Solorigate (Microsoft, and is loaded by the ***SolarWinds.BusinessLayerHost.exe*** program. Once loaded, it will connect back to the remote command & control server at a subdomain of **avsvmcloud[.]com** to receive "jobs," or tasks, to execute on the infected computer.

The backdoor's command control server's DNS name is created utilizing a domain generation algorithm (DGA) to create an encoded subdomain of **avsvmcloud[.]com**. FireEye states that the subdomain is created by "concatenating a victim userId with a reversible encoding of the victims local machine domain name," and then hashed. For example, a subdomain used in this attack is '1btcr12b62me0buden60ceud01uv2f0i.appsync-api.us-east-2[.]avsvmcloud.com.'

It is unknown what tasks were executed, but it could be anything from giving remote access to the threat actors, downloading and installing further malware, or stealing data.

Microsoft published a technical writeup (https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/) on Friday for those interested in the technical aspects of the Sunburst backdoor.

A report by Kim Zetter released Friday night (https://news.yahoo.com/hackers-last-year-conducted-a-dry-run-of-solar-winds-breach-215232815.html) indicates that the threat actors may have performed a dry run of the distribution method as early as October 2019. During this dry run, the DLL was distributed without the malicious Sunburst backdoor.

After the threat actors began distributing the backdoor in March 2020, researchers believe that the attackers have been silently sitting in some of the compromised networks for months while harvesting information or performing other malicious activity.

Zetter's report stated that FireEye eventually detected they were hacked after the threat actors registered a device to the company's multi-factor authentication (MFA) system using stolen credentials. After the system alerted the employee and the security team of this unknown device, FireEye realized that they had been compromised.

Additional malware discovered

After performing investigations of SolarWinds supply chain victims, researchers have begun to get a better idea of the different malware used in the attack.

According to CrowdStrike, a malware named SunSpot (https://www.bleepingcomputer.com/news/security/new-sunspot-malware-found-while-investigating-solarwinds-hack/) was first executed in the SolarWinds network to monitor for and automatically inject the Sunburst backdoor in the SolarWinds development builds.

The Sunburst backdoor would then be transferred to victims via automatic updates for the SolarWinds Orion platform. Once executed, it would routinely connect to a remote command and control server for commands to execute on the infected device.

FireEye discovered that the Sunburst backdoor would drop a malware named Teardrop (https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html), which is a previously unknown memory-only dropper and a post-exploitation tool used to deploy customized Cobalt Strike beacons.

Finally, Symantec discovered the RainDrop malware (https://www.bleepingcomputer.com/news/security/solarwinds-hackers-used-7-zip-code-to-hide-raindrop-cobalt-strike-loader/), which was also used to deploy Cobalt Strike beacons on other hosts in an already compromised network.

The hackers behind the SolarWinds attack

FireEye is currently tracking the threat actor behind this campaign as UNC2452 (https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html), while Washington-based cybersecurity firm Volexity has linked this activity to a hacking group known under the Dark Halo (https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/) moniker.

Volexity says that Dark Halo actors have coordinated malicious campaigns between late 2019 and July 2020, targeting and successfully compromising the same US-based think tank three times in a row (https://www.bleepingcomputer.com/news/security/nation-state-hackers-breached-us-think-tank-thrice-in-a-row/).

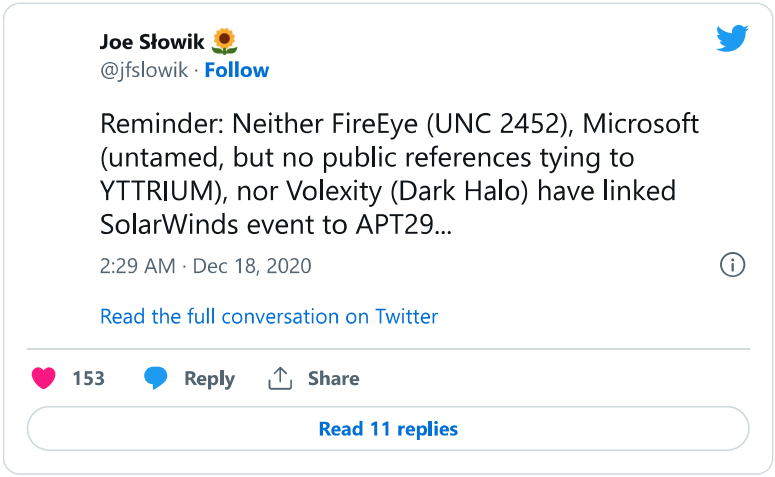
“In the initial incident, Volexity found multiple tools, backdoors, and malware implants that had allowed the attacker to remain undetected for several years,” the company said.

In the second attack, after being cast out from the victim’s network, Dark Halo leveraged a newly disclosed Microsoft Exchange server bug that helped them to circumvent Duo multi-factor authentication (MFA) defenses for unauthorized email access via the Outlook Web App (OWA) service.

During the third attack targeting the same think tank, the threat actor used the SolarWinds supply chain attack to deploy the same backdoor Dark Halo used to breach FireEye's networks and several U.S. government agencies.

Unconfirmed media reports have also cited sources linking the attacks to APT29 (aka Cozy Bear) (https://www.bleepingcomputer.com/news/security/us-govt-fireeye-breached-after-solarwinds-supply-chain-attack/), a state-sponsored hacking group associated with the Russian Foreign Intelligence Service (SVR).

Researchers, including FireEye, Microsoft, or Volexity, have not attributed these attacks to APT29 at this time.



The Russian Embassy in the USA reacted [1 (https://www.facebook.com/RusEmbUSA/posts/1488755328001519), 2 (https://twitter.com/RusEmbUSA/status/1338330751067172866)] to these media reports saying that they were an “unfounded attempt of the U.S. media to blame Russia for hacker attacks on U.S. governmental bodies.”

"*Russia does not conduct offensive operations in the cyber domain*," the Embassy added.

While Russia continues to deny these attacks, Secretary of State Mike Pompeo stated in an interview (https://www.politico.com/news/2020/12/19/pompeo-russia-behind-cyberhack-of-us-agencies-448625) released Friday night that it is "pretty clear" that Russia was behind that attack.

"This was a very significant effort, and I think it's the case that now we can say pretty clearly that it was the Russians that engaged in this activity," Pompeo told radio host Mark Levin.

Microsoft believes that the ultimate goal of these attacks was to gain access to victims' cloud assets (https://www.bleepingcomputer.com/news/security/microsoft-solarwinds-hackers-goal-was-the-victims-cloud-data/) after deploying the Sunburst/Solorigate backdoor on their local networks.

The victims of the attack

Researchers believe that the malicious DLL was pushed out to approximately 18,000 customers as part of this attack.

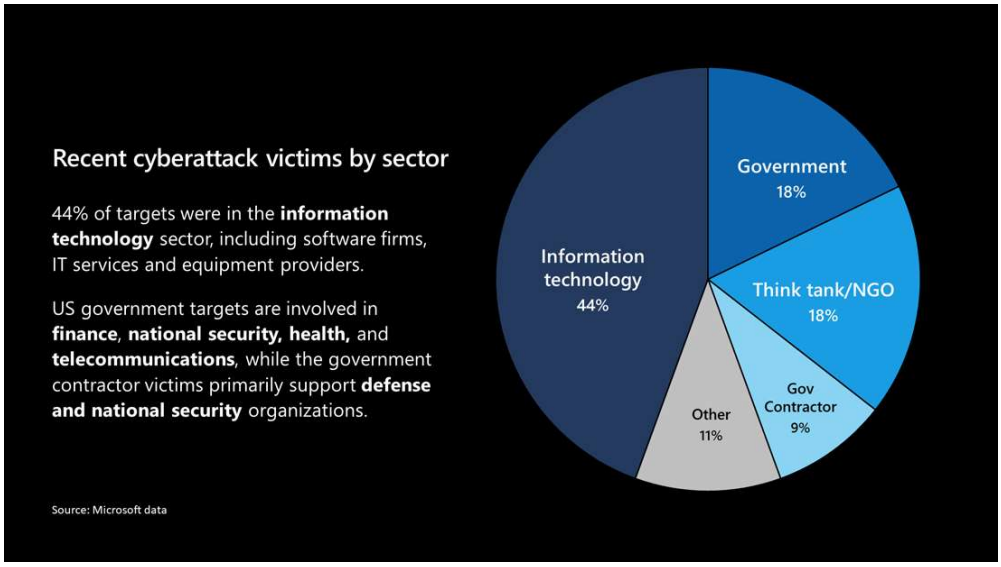
The threat actors, though, only targeted organizations that they perceived as 'high value,' so even though some of these customers may have received the DLL, it is unknown if they were actively targeted in further attacks.

The currently known list of organizations that were hit by the SolarWinds supply chain attack include:

- FireEye (https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html)
- U.S. Department of the Treasury (https://www.reuters.com/article/BigStory12/idUSKBN28N0PG)
- U.S. National Telecommunications and Information Administration (https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html) (NTIA)
- U.S. Department of State (https://www.washingtonpost.com/national-security/dhs-is-third-federal-agency-hacked-in-major-russian-cyberespionage-campaign/2020/12/14/41f8fc98-3e3c-11eb-8bc0-ae155bee4aff_story.html)
- The National Institutes of Health (https://www.washingtonpost.com/national-security/dhs-is-third-federal-agency-hacked-in-major-russian-cyberespionage-campaign/2020/12/14/41f8fc98-3e3c-11eb-8bc0-ae155bee4aff_story.html) (NIH) (Part of the U.S. Department of Health)
- U.S. Department of Homeland Security (https://www.washingtonpost.com/national-security/dhs-is-third-federal-agency-hacked-in-major-russian-cyberespionage-campaign/2020/12/14/41f8fc98-3e3c-11eb-8bc0-ae155bee4aff_story.html) (DHS)
- U.S. Department of Energy (https://www.bleepingcomputer.com/news/security/solarwinds-hackers-breach-us-nuclear-weapons-agency/) (DOE)
- U.S. National Nuclear Security Administration (https://www.bleepingcomputer.com/news/security/solarwinds-hackers-breach-us-nuclear-weapons-agency/) (NNSA)
- Some US states (https://www.bloomberg.com/news/articles/2020-12-17/u-s-states-were-also-hacked-in-suspected-russian-attack) (Specific states are undisclosed)
- Microsoft (https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-breach-in-solarwinds-hack-denies-infecting-others/)

- Cisco (https://www.bloomberg.com/news/articles/2020-12-18/cisco-latest-victim-of-russian-cyber-attack-using-solarwinds)

Microsoft has also identified and notified more than 40 of its customers affected by this attack but has not disclosed their names. They state that 80% of the victims were from the U.S., and 44% were in the IT sector.



Sunburst victims by sector

Based on the decoding of subdomains (http://twitter.com/RedDrip7/status/1339168187619790848) generated by the malware domain generation algorithm (DGA), many well-known companies may disclose targeted attacks at a later date.

Decoded backdoor command & control server subdomains
Source: RedDrip Team (http://twitter.com/RedDrip7/status/1339168187619790848)

What are security firms doing to protect victims

Since the cyberattack has been disclosed, security firms have been adding the malicious Sunburst backdoor binaries to their detections.

While Microsoft was already detecting and alerting customers of malicious SolarWinds binaries, they were not quarantining them out of concern it could affect an organization's network management services. On December 16th, at 8:00 AM PST, Microsoft Defender began quarantining detected binaries (https://www.bleepingcomputer.com/news/security/microsoft-to-quarantine-compromised-solarwinds-binaries-tomorrow/) even if the process is running.

Microsoft, FireEye, and GoDaddy also collaborated to create a kill switch (https://www.bleepingcomputer.com/news/security/fireeye-microsoft-create-kill-switch-for-solarwinds-backdoor/) for the Sunburst backdoor distributed in the SolarWinds hack.

When the malicious binaries attempt to contact the command & control servers, they will perform DNS resolution to get the IP address. If this IP address is part of certain IP ranges, including ones owned by Microsoft, the backdoor will terminate and prevent itself from executing again.

To create the kill switch, GoDaddy created a wildcard DNS resolution so that any subdomain of avsvmcloud[.]com resolves to the IP address 20.140.0.1, which belongs to Microsoft and is on the malware's blocklist. This wildcard resolution is illustrated by a DNS lookup for a made-up subdomain, as shown below.

Wildcard DNS resolution

As this IP address is part of the malware's blocklist, when it connects to any subdomain of avsvmcloud[.]com, it will unload and no longer execute.

While this kill switch will disable Sunburst backdoor deployments connecting the command & control servers, FireEye has stated the threat actors may have deployed other backdoors.

"However, in the intrusions FireEye has seen, this actor moved quickly to establish additional persistent mechanisms to access to victim networks beyond the Sunburst backdoor. This killswitch will not remove the actor from victim networks where they have established other backdoors. However, it will make it more difficult to for the actor to leverage the previously distributed versions of Sunburst," FireEye warned about the kill switch," FireEye told BleepingComputer in a statement.

How to check if you were compromised

If you are a user of SolarWinds products, you should immediately consult their advisory (https://www.solarwinds.com/securityadvisory) and Frequently Asked Questions (https://www.solarwinds.com/securityadvisory/faq) as it contains necessary information about upgrading to the latest 'clean' version of their software.

Microsoft has also published a list (http://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/) of nineteen malicious SolarWinds.Orion.Core.BusinessLayer.dll DLL files spotted in the wild.

This list, shown below, contains a file's SHA256 hash, the file version, and when it was first seen.

SHA256	File Version	Date first seen
e0b9eda35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d	2020.2.100.11713	February 2020

a58d02465e26bdd3a839fd90e4b317eece431d28cab203bbdde569e11247d9e2	2020.2.100.11784	March 2020
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77	2019.4.5200.9083	March 2020
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b	2020.2.100.12219	March 2020
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed	2020.2.100.11831	March 2020
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77	Not available	March 2020
ffdbdd460420972fd2926a7f460c198523480bc6279dd6cca177230db18748e8	2019.4.5200.9065	March 2020
b8a05cc492f70ffa4adcd446b693d5aa2b71dc4fa2bf5022bf60d7b13884f666	2019.4.5200.9068	March 2020
20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9	2019.4.5200.9078	March 2020
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589	2019.4.5200.9078	March 2020
cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70e01dc69048e6	2019.4.5200.9083	March 2020
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c	2020.4.100.478	April 2020
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134	2020.2.5200.12394	April 2020
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6	2020.2.5300.12432	May 2020
2b3445e42d64c85a5475bdbc88a50ba8c013febb53ea97119a11604b7595e53d	2019.4.5200.9078	May 2020
92bd1c3d2a11fc4aba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690	2020.4.100.751	May 2020
a3efbc07068606ba1c19a7ef21f4de15d15b41ef680832d7bcba485143668f2d	Not available	Not available
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc	2019.4.5200.8890	October 2019
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af	2019.4.5200.8890	October 2019

Finally, security researchers have released various tools that allow you to check if you were compromised or what credentials were stored in your SolarWinds Orion installation.

- SolarFlare Release: Password Dumper for SolarWinds Orion (https://malicious.link/post/2020/solarflare-release-password-dumper-for-solarwinds-orion/)

- SpearTip's SolarWinds' Orion Vulnerability Tool SunScreen – SPF 10 (https://www.speartip.com/resources/sunscreen-spf10/)

The source code for both projects is published to GitHub. You are strongly encouraged to review the source code, if available, of any program you plan to run on your network.

Security researcher Cory Kennedy (https://twitter.com/CoryKennedy) has also released a python tool to help you find the Sunburst malware on your network.

This tool is called Sunburst hunter and can be downloaded from the project's GitHub page (https://github.com/NoDataFound/RiskIQ.SunBurst.Hunter/tree/MISP).

SolarWinds Orion abused in other supply chain attacks

During the investigation into the SolarWinds hack, Palo Alto Networks and Microsoft found an additional malware named SUPERNOVA (https://www.bleepingcomputer.com/news/security/new-supernova-backdoor-found-in-solarwinds-cyberattack-analysis/) distributed using the ***App_Web_logoimagehandler.ashx.b6031896.dll*** DLL file.

This malware is a backdoor that allowed the threat actors to send C# code that would be compiled and executed by the malware.

SUPERNOVA code

This malware is not believed to be related to the ***SolarWinds.Orion.Core.BusinessLayer.dll*** supply chain attack. It does, though, indicate that the SolarWinds Orion platform was used in two different attacks, and possibly by different groups, to distribute malware.

Last week, SolarWinds released an update advisory (https://www.bleepingcomputer.com/news/security/solarwinds-releases-updated-advisory-for-new-supernova-malware/) that advises all Orion Platform customers to

upgrade to the latest versions to be protected from not only the SUNBURST vulnerability but the SUPERNOVA malware as well.

Additional reporting by Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/) and Ionut Ilascu (https://www.bleepingcomputer.com/author/ionut-ilascu/).

Update 12/19/20: Added Cisco to the victim list.
Update 12/27/20: Added information about second SUPERNOVA malware.
Update 01/20/20: Added information about further malware

Related Articles:

ADATA denies RansomHouse cyberattack, says leaked data from 2021 breach (https://www.bleepingcomputer.com/news/security/adata-denies-ransomhouse-cyberattack-says-leaked-data-from-2021-breach/)

Hacker shares how they allegedly breached Fast Company's site (https://www.bleepingcomputer.com/news/security/hacker-shares-how-they-allegedly-breached-fast-company-s-site/)

npm packages used by crypto exchanges compromised (https://www.bleepingcomputer.com/news/security/npm-packages-used-by-crypto-exchanges-compromised/)

MFA Fatigue: Hackers' new favorite tactic in high-profile breaches (https://www.bleepingcomputer.com/news/security/mfa-fatigue-hackers-new-favorite-tactic-in-high-profile-breaches/)

GTA 6 source code and videos leaked after Rockstar Games hack (https://www.bleepingcomputer.com/news/security/gta-6-source-code-and-videos-leaked-after-rockstar-games-hack/)

CYBERATTACK (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CYBERATTACK/)

SOLARWINDS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SOLARWINDS/)

SOLORIGATE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SOLORIGATE/)

SUNBURST (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SUNBURST/)

SUPPLY-CHAIN ATTACK (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SUPPLY-CHAIN-ATTACK/)