Analysis of the SolarWinds Supply Chain Attack

By Tony Cook

Published: 2020-12-22 · Archived: 2026-04-02 11:12:30 UTC

Latest Update 1/8/21 at 4pm ET

The intent of this analysis is to aggregate the wide distribution of information being shared, provide insights, and recommendations. As we continue to learn more about the recent SolarWinds attack, the GuidePoint team continues to gather and distill the information for consumption. Currently our team is tracking the group as defined by FireEye as UNC2452 which is linked to the actor being tracked by the Volexity team as Dark Halo.

Ongoing Analysis of the SolarWinds Breach

Update: 1/8/21 at 4pm ET

Continuing our updates to the ever evolving SolarWinds whirlwind, CISA released updated guidance and Alert (AA20-352A) for Federal Agencies affected by the Orion Platform breach. This guidance confirms that an NSA static code review was conducted on the SolarWinds Orion Platform version 2020.2.1 HF2 update to ensure that both the vulnerabilities and the previously included malicious code had been remediated. CISA further recommends that agencies who have not seen the follow-on malicious activity to either rebuild their SolarWinds Orion server(s) to the current version or to simply update their existing SolarWinds Orion instance in accordance with their Hardening guidance. Agencies who have seen follow-on activity should keep their SolarWinds Orion infrastructure disconnected from their network while conducting an investigation.

The updated alert includes new information on initial access vectors, updated mitigation recommendations, and new indicators of compromise (IOCs). An important takeaway from the CISA alert is that during the course of several recent investigations sharing commonalities in adversarial behavior, SolarWinds was not the only intrusion vector observed. This highlights the importance of continuing to monitor and hunt for intrusion vectors not related to SolarWinds vulnerabilities – many clients may have a false sense of security if they do not have SolarWinds in their environment. The other forms of initial access detailed in the updated alert include password guessing, password spraying, and exploiting external remote access services with inappropriately secured administrative credentials. As more details continue to develop, we expect the list of initial intrusion vectors to continue to grow.

Another point CISA brings up in their Alert is the concept of Operational Security during the Incident Response process, especially when planning and implementing remediation steps. Ensuring that your incident response plan includes out of band communication methods can be the difference between a successful remediation or the adversary keeping a foothold in your environment.

Additionally, the SolarWinds Orion 0-day vulnerability which allowed for the Supernova Webshell to be installed is being tracked as CVE-2020-10148 (Thanks for the confirmation from Nick Carr @ItsReallyNick). This vulnerability could enable an attacker to bypass authentication and allow for API command execution, which may

lead to a compromise of the Orion application. While Supernova is being attributed to a different threat actor than was observed with Sunburst, this is still a potentially high impact vulnerability and we recommend implementing proactive hunting and detection measures to determine if your SolarWinds instance has been affected.

Update: 12/23/20 at 9am ET

The Volexity team discovered three incidents attributed to the same actor (Dark Halo) starting in late 2019 targeting an unnamed think tank. In the initial attack, the actor utilized a Microsoft Exchange vulnerability that allowed them to bypass multi-factor authentication (MFA) used to secure email access. Once in the environment, the actor utilized living-off-the-land binaries (LOL-BAS) in weekly operations with the intent of extracting emails from targeted individuals. Upon identification of the threat actor's activities, the actor was successfully removed from the network as a result of response efforts.

However, a short time after the remediation, the actor once again infiltrated the environment using a remote code execution vulnerability (CVE-2020-0688) targeting an on-premise Microsoft Exchange server. Utilization of this exploit allowed the threat actor further access to the environment, at which time they were able to use a "novel technique" to exploit the normal Duo MFA execution flow. Using this technique, the actor compromised the Duo integration secret key from the present OWA instance. This allowed the threat actors to pre-compute the security identifier for authentication and authorization. It's important to note that this was not a vulnerability in the Duo software itself. By simply having the privileges required to garner the key the actor was able to calculate the value of the required cookie for authentication. The actors were discovered once again and eradicated from the network.

In the third and final attack dating back to July 2020, the actors were seen utilizing the compromised SolarWinds DLL to gain access to the targeted environment. Once inside the network, the actors operated using similar tactics observed in previous intrusions. One noted objective for the actor in each of these intrusions was access to the Exchange environment.

Recent information on the SolarWinds DLL, tracked as SUNBURST (FireEye) and Solorigate (Microsoft), has shown that the actors behind the compromise may have had access to the Orion codebase as far back as October 10th, 2019. It's been determined that SolarWinds Orion 2019.4 HF 5 through 2020.2.1 were affected with the following hotfixes released to fix the issues:

- 2020.2.1 HF 1
- 2020.2.1 HF 2

Additional analysis by various teams has determined that SUPERNOVA webshell discovered during initial analysis by FireEye may not be related to UNC2452/Dark Halo. Researchers have concluded that due to the unsigned nature of the binary that it is likely not as sophisticated as the Sunburst/Solorigate attack and potentially a second actor. Further research is being conducted to determine the attribution of the webshell.

Initial Analysis of the SolarWinds Breach

Posted on 12/14/20

Recent disclosure and documentation by FireEye, beginning on 14 December, reported that FireEye was the victim of a highly sophisticated, state-sponsored attack. As more and more details are released about the attack, it has been confirmed this was part of a much larger campaign affecting numerous organizations and government agencies globally. This attack, which may have started as early as March 2020, was executed through the use of a supply chain compromise originating out of the SolarWinds Orion product. While full details around the compromise of the SolarWinds product are not currently known, we do know that a legitimate DLL used to support the product was modified to allow the actors remote access into SolarWinds customer environments. This access could allow for actors to deliver second-stage payloads, move laterally, and ultimately achieve their attack objectives.

What has been reported thus far is that actors compromised a version of SolarWinds Orion, which was deployed to SolarWinds Clients through legitimate software updates. Once successfully deployed, the actors achieved initial access to the environment, which was then followed by attempts to achieve persistent access through compromising privileged accounts or by forging SAML tokens to allow for specific level of access. The primary goal for the actors appears to be establishing a legitimate and persistent access mechanism into the environment that can be used as the primary method of ingress. After they have established this access method, the actor subsequently utilizes known tools such as Cobalt Strike's BEACON module to move laterally and perform environment-specific actions-on-objective, as well as ensure they have foothold access into Exchange email environments.

It is important to note that while this particular attack focuses on SolarWinds as the initial access point through a supply chain vector, this could easily be applied to other products or services being widely used in customer environments. This solidifies and reiterates the need to fully understand your network and follow best-practices for hygiene, proactive defense measures, threat hunting, and response. Also, we highly recommended threat modeling similar attack scenarios, followed by threat hunts to determine the likelihood an organization has been affected.

Tactical Information & Recommendations

In order to provide customers with a solid strategy to identify and respond to this attack, as well as to ensure protection against similar types of attacks, GuidePoint Security's DFIR team has developed the following tactical information and recommendations based on details collected from FireEye, Microsoft and SolarWinds reports.

The following information can be used agnostic of any specific toolset while vendors continue to develop product-specific detection capabilities.

Below are the high-level steps that GuidePoint recommends for anyone using SolarWinds Orion, along with supporting technical details.

Isolate

- Ensure that the SolarWinds Orion appliance is isolated from the network until a patch can be deployed. If any evidence of compromise is found it should be further isolated from the internal network.

Patch / Stay Up to Date

- **SolarWinds:** Organizations leveraging SolarWinds Orion Platform v2020.2 without a hotfix or 2020.2 HF 1 should upgrade ASAP to Orion Platform version 2020.2.1 HF 2 as soon as possible. For more information on SolarWinds' guidance, go to https://www.solarwinds.com/securityadvisory.
- **Security Products:** As security vendors release additional content related to this attack, it is important to remain up to date and vigilant on what the content detects/protects.

Hunt / Validate

- Multiple Indicators of Compromise (IOCs) have been released thus far in the investigation. Confirm not only whether you were vulnerable, but also leverage the indicators provided here, as well as those distributed by the various vendors, to validate that you haven't been further impacted. GuidePoint recommends that organizations perform threat hunting activities in order to identify if any IOCs are present in their environment.

Behavioral Indicators

The primary communication mechanisms reported are HTTP with domain name fields matching the domains listed in the FireEye IOCs, and HTTP communications containing XML responses containing control codes embedded in various locations in the XML tree.

SUNBURST SolarWinds Orion Backdoor

The SUNBURST malware communicates over an HTTP C2 channel with callouts delayed by a configurable timeframe. The default value for this delay is one minute between callouts. This communication channel uses a separate set of HTTP methods for requesting data from and sending data to the C2 server. The HTTP GET or HEAD methods are used when the malware is requesting data from the C2 server, and the HTTP PUT or POST methods are used when the malware needs to send data to the C2 server. The malware will use the PUT method to send data when the payload (HTTP body length) is less than 10,000 bytes. Any payloads larger than 10,000 bytes will use the POST method. The payload format being sent to the C2 server for both the PUT and POST requests is JSON containing the following schema:

```
{
      "userid": value,
      "sessionid": value,
      "steps": [
         {
            "Timestamp": integer,
            "Index": value,
            "EventType": "Orion",
            "EventName": "EventManager",
            "DurationMs": integer,
            "Succeeded": value,
            "Message": string
         }
      ]
}
```

Each HTTP Request contains the 'If-None-Match' HTTP header, with a XOR encoded value. Methods of hunting for this activity are as follows:

- Outbound HTTP PUT Requests with Content-Length < 10000 and 'If-None-Match' HTTP Header
- Outbound HTTP POST Requests with Content-Length > 10000 and 'If-None-Match' HTTP Header
- Outbound HTTP PUT or POST Requests with HTTP Request Content-Type Header value of 'application/json'

Analysis conducted by FireEye and Microsoft determined that the SUNBURST backdoor used DNS resolutions of avsvmcloud[.]com as a built in killswitch depending on the IP address returned during the DNS query. FireEye and Microsoft worked together with GoDaddy to take over the malicious domain and modify the IP address returned during DNS resolution to mitigate the effectiveness of the SUNBURST backdoor.

TEARDROP Dropper

During FireEye's analysis of the SolarWinds Supply Chain Compromise, they discovered a previously unobserved dropper that they have dubbed TEARDROP. This dropper has been found to run as a service and is responsible for loading additional executable code into memory with no on-disk presence. Based on details from FireEye, it appears that the TEARDROP dropper is associated with the file "C:\Windows\SYSWOW64\netsetupsvc.dll."

Additionally, FireEye observed TEARDROP's loading process which reads from the file "gracious_truth.jpg," which contains the obfuscated payload, uses a fake JPG file header, and uses a rolling XOR algorithm to decode the payload before executing it in memory. According to FireEye's analysis of TEARDROP, this dropper could load any executable code into memory for execution, but was likely used to execute a customized Cobalt Strike BEACON.

FireEye created YARA signatures that can be used to detect TEARDROP on impacted systems which can be found here.

SUPERNOVA .NET SolarWinds Service Webshell

GuidePoint recently released a blog regarding the SUPERNOVA .NET webshell backdoor masquerading as a legitimate SolarWinds web service handler. This .NET module inspects inbound HTTP requests and responds to HTTP requests sent with specific query strings, cookies, or HTML form values. The .NET webshell is located under the filename 'app_web_logoimagehandler.ashx.<8 alphanumeric chars>.dll'. The request will also contain values for the following parameters that are used to compile anonymous code for execution by the webshell:

- codes: This parameter stores compiler codes to be passed to the webshell during compilation
- clazz: The C# Class name to compile as module for execution by the webshell
- method: The C# Class Method to be called within the C# Class listed by the 'clazz' parameter
- args: Newline-delimited list of arguments to pass as parameters to the C# Method listed by the 'method' parameter

The result of the memory execution of this compiled code will be written directly to the HTTP Response body, and the HTTP Response Content-Type Header will have the value of 'text/plain'. Methods to identify this activity

are as follows:

- Inbound HTTP GET Requests with:
    - URI file ending with logoimagehandler.ashx AND
    - HTTP body parameters of ‘codes’, ‘clazz’, ‘method’, or ‘args’ AND
    - HTTP Response Status Code of 200, AND
    - HTTP Response Content-Type Header Value of text/plain
- Inbound HTTP POST Requests with:
    - URI file ending with logoimagehandler.ashx AND
    - HTTP Response Status Code of 200, AND/OR
    - HTTP Response Content-Type Header Value of text/plain

Cobalt Strike BEACON

One method of lateral movement was reported as remote scheduled tasks implementing Cobalt Strike BEACON via %COMSPEC% or PowerShell encoded command executions. For each Cobalt Strike BEACON Scheduled Task, there would be a network communication occurring commensurate with the execution of the Scheduled Task. One method of identifying this activity is to review Scheduled Task execution in the environment, specifically Task Names and their associated binary/command executions. Since these actors have been reported to execute the malicious Task in-between a remove-and-restore cycle of a legitimate Schedule Task, analysts will want to review:

- Any Scheduled Task modifications conducted in rapid succession
- Multiple Scheduled Task executions of the same Task Name with differing binaries/command executions on the same host
- Scheduled Task executions in which there is a network connection outbound to TCP/443 by the Task binary
- Scheduled Task executions with a Command Line value containing ‘%COMSPEC%’, ‘cmd’, or ‘powershell’, or with cmd.exe or powershell.exe executions associated with the Scheduled Task execution

Additional behavioral indications of usage of modules present within Cobalt Strike BEACON and reported lateral movement are as follows:

- Windows Service (Event ID 7045) or Scheduled Task (EventID 4698, 4700) creations with 7-character pseudo-random alphanumeric character Service or Task Names
- Windows Services (Event ID 7045) or Scheduled Tasks (EventID 4698, 4700) with Service Filename or Command containing UNC ADMIN$ share path references, beginning with either the loopback IP address or RFC1918 localhost IP address (ex: ‘\\127.0.0.1\ADMIN$\<7-character>.exe’)
- PowerShell (Event ID 400) with the following values:
    - HostName: ConsoleHost
    - HostApplication contains ‘rundll32.exe’
    - HostVersion and EngineVersion with different version numbers
        - Ex: HostVersion:1.0 and EngineVersion: 5.1.17763.1
- PowerShell (Event ID 400) with Base64 encoded value in HostApplication field

- Recent changes in NTFS FileName Creation Time for Scheduled Task or at job files located in C:\Windows\System32\Tasks or C:\Windows\Tasks. Each Scheduled Task and at job should be reviewed for any outlying recent NTFS Creation timestamps or unauthorized commands.

Atomic Indicators

Domains

Domain	Association
aysymcloud[.]com	SUNBURST
databasegalore[.]com	SUNBURST/BEACON
deftsecurity[.]com	SUNBURST
digitalcollege[.]org	SUNBURST
ervsystem[.]com	TEARDROP
freescanonline[.]com	SUNBURST
globalnetworkissues[.]com	SUNBURST
highdatabase[.]com	SUNBURST
incomeupdate[.]org	BEACON
infinitysoftwares[.]com	TEARDROP
kubecloud[.]com	BEACON
lcomputers[.]com	BEACON
mobilnweb[.]com	Unknown Association
panhardware[.]com	SUNBURST/BEACON
seobundlekit[.]com	SUNBURST
solartrackingsystem[.]net	BEACON
thedoccloud[.]com	SUNBURST
virtualdataserver[.]com	SUNBURST
virtualwebdata[.]com	SUNBURST
webcodez[.]com	BEACON
websitetheme[.]com	SUNBURST

zupertech[.]com	SUNBURST/BEACON

IP Addresses

IP Address	Association
162.223.31[.]184	BEACON
173.237.190[.]2	BEACON
3.87.182[.]149	BEACON
34.219.234[.]134	BEACON
45.141.152[.]18	BEACON
13.57.184[.]217	SUNBURST
13.59.205[.]66	SUNBURST
139.99.115[.]204	SUNBURST
18.220.219[.]143	SUNBURST
18.253.52[.]187	SUNBURST
204.188.205[.]176	SUNBURST
3.16.81[.]254	SUNBURST
34.203.203[.]23	SUNBURST
5.252.177[.]21	SUNBURST
5.252.177[.]25	SUNBURST
51.89.125[.]18	SUNBURST
54.193.127[.]66	SUNBURST
54.215.192[.]52	SUNBURST
107.152.35[.]77	SUNBURST
167.114.213[.]199	Unknown Association
18.217.225[.]111	Unknown Association
184.72.1[.]3	Unknown Association
184.72.101[.]22	Unknown Association

184.72.113[.]55	Unknown Association
184.72.145[.]34	Unknown Association
184.72.209[.]33	Unknown Association
184.72.21[.]54	Unknown Association
184.72.212[.]52	Unknown Association
184.72.224[.]3	Unknown Association
184.72.229[.]1	Unknown Association
184.72.240[.]3	Unknown Association
184.72.245[.]1	Unknown Association
184.72.48[.]22	Unknown Association
196.203.11[.]89	Unknown Association
198.12.75[.]112	Unknown Association
20.141.48[.]154	Unknown Association
8.18.144[.]11	Unknown Association
8.18.144[.]12	Unknown Association
8.18.144[.]130	Unknown Association
8.18.144[.]135	Unknown Association
8.18.144[.]136	Unknown Association
8.18.144[.]149	Unknown Association
8.18.144[.]156	Unknown Association

File Hashes: SUNBURST

Microsoft published a list of nineteen malicious SolarWinds.Orion.Core.BusinessLayer.dll DLL files spotted in the wild. We have listed them below with the file version and date first seen.

SHA256	File Version	Date First Seen
e0b9eda35f01c1540134ab	2020.2.100.11713	February 2020

a9195e7e6393286dde3e0 01fce36fb661cc346b91d		
a58d02465e26bdd3a839fd 90e4b317eece431d28cab2 03bbdde569e11247d9e2	2020.2.100.11784	March 2020
32519b85c0b422e4656de6 e6c41878e95fd95026267d aab4215ee59c107d6c77	2019.4.5200.9083	March 2020
dab758bf98d9b36fa057a66 cd0284737abf89857b73ca8 9280267ee7caf62f3b	2020.2.100.12219	March 2020
eb6fab5a2964c5817fb239a 7a5079cabca0a00464fb3e0 7155f28b0a57a2c0ed	2020.2.100.11831	March 2020
c09040d35630d75dfef0f80 4f320f8b3d16a481071076 918e9b236a321c1ea77	N/A	March 2020
ffdbdd460420972fd2926a7 f460c198523480bc6279dd 6cca177230db18748e8	2019.4.5200.9065	March 2020
b8a05cc492f70ffa4adcd446 b693d5aa2b71dc4fa2bf502 2bf60d7b13884f666	2019.4.5200.9068	March 2020
20e35055113dac104d2bb0 2d4e7e33413fae0e5a426e 0eea0dfd2c1dce692fd9	2019.4.5200.9078	March 2020
0f5d7e6dfdd62c83eb096ba 193b5ae394001bac036745 495674156ead6557589	2019.4.5200.9078	March 2020
cc082d21b9e880ceb6c96d b1c48a0375aaf06a5f444cb 0144b70e01dc69048e6	2019.4.5200.9083	March 2020
ac1b2b89e60707a20e9eb1 ca480bc3410ead40643b38 6d624c5d21b47c02917c	2020.4.100.478	April 2020

019085a76ba7126fff22770 d71bd901c325fc68ac55aa7 43327984e89f4b0134	2020.2.5200.12394	April 2020
ce77d116a074dab7a22a0fd 4f2c1ab475f16eec42e1ded3 c0b0aa8211fe858d6	2020.2.5300.12432	May 2020
2b3445e42d64c85a5475bdb c88a50ba8c013febb53ea971 19a11604b7595e53d	2019.4.5200.9078	May 2020
92bd1c3d2a11fc4aba2735d9 547bd0261560fb20f36a0e7c a2f2d451f1b62690	2020.4.100.751	May 2020
a3efbc07068606ba1c19a7ef 21f4de15d15b41ef680832d7 bcba485143668f2d	N/A	N/A
a25cadd48d70f6ea0c4a241d 99c5241269e6faccb4054e62 d16784640f8e53bc	2019.4.5200.8890	October 2019
d3c6785e18fba3749fb785bc3 13cf8346182f532c59172b69 adfb31b96a5d0af	2019.4.5200.8890	October 2019

File Hashes: SUPERNOVA and TEARDROP

SHA256 Hash	**Association**
c15abaf51e78ca56c0376522d699c97821 7bf041a3bd3c71d09193efa5717c71	SUPERNOVA
118189f90da3788362fe85eafa55529842 3e21ec37f147f3bf88c61d4cd46c51	TEARDROP
1817a5bf9c01035bcf8a975c9f1d94b0ce7 f6a200339485d8f93859f8f6d730c	TEARDROP

Resources

While we've collected some general guidance and recommendations regarding this threat, our partnering solution providers should be developing specific content unique to their technologies as more information is becoming

available. Further details on the attack and recommendations can also be found in the following posts by Microsoft, SolarWinds & FireEye who are currently working to overcome these attacks.

- https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
- https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/
- https://www.fireeye.com/blog/threat-research/2020/12/evasive-actor-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- https://github.com/fireeye/sunburst_countermeasures
- https://www.solarwinds.com/securityadvisory
- https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/
- https://community.riskiq.com/article/c98949a2
- https://www.bleepingcomputer.com/news/security/us-govt-fireeye-breached-after-solarwinds-supply-chain-attack/
- https://www.bleepingcomputer.com/news/security/new-supernova-backdoor-found-in-solarwinds-cyberattack-analysis/
- https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-breach-in-solarwinds-hack-denies-infecting-others/
- https://www.bleepingcomputer.com/news/security/microsoft-identifies-40-plus-victims-of-solarwinds-hack-80-percent-from-us/
- https://www.bleepingcomputer.com/news/security/us-think-tank-breached-three-times-in-a-row-by-solarwinds-hackers/
- https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/
- https://www.bleepingcomputer.com/news/security/fireeye-microsoft-create-kill-switch-for-solarwinds-backdoor/
- https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
- https://www.guidepointsecurity.com/supernova-solarwinds-net-webshell-analysis/
- https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html

---