# Threat Advisory: SolarWinds supply chain attack

blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html



*Update 12/21:* IOC section updated to include new information and associated stage.

*Update 12/18:* We have been able to verify the name server for the DGA domain was updated as far back as late February. Compromised binaries appear to have been available on the SolarWinds website until very recently. The blog below has been amended with this informaiton. The IOC list has been modified.

*Update 12/17:* Additional IOCs added related to teardrop secondary payload.

*Update 12/16:* Based on the announcement from FireEye, Microsoft, and GoDaddy avsvmcloud[.]com has been unblocked as it is now functioning as a kill switch in an effort to help limit adversaries access. Please note that this does not imply that this is a complete protection from these attacks. Additional remediation steps will should and must be taken. Additional details here.

*Update 12/14:* We note there is a discrepancy in guidance coming from DHS and SolarWinds. The SolarWinds advisory suggests users upgrade to the latest version, Orion Platform version 2020.2.1 HF 1, while DHS guidance says 2020.2.1 HF1 is affected. However, we note that SolarWinds announced they will be releasing another hot-fix, 2020.2.1 HF 2, on December 15, which “replaces the compromised component and provides several additional security enhancements.” Talos urges customers to follow DHS guidance at this time and install 2020.2.1 HF 2 as soon as it becomes available.

Cisco Talos is monitoring yesterday's announcements by FireEye and Microsoft that a likely state-sponsored actor compromised potentially thousands of high-value government and private organizations around the world via the SolarWinds Orion product. FireEye reported on Dec. 8 that it had been compromised in a sophisticated attack in which state-sponsored actors stole sensitive red team tools. Upon investigating the breach further, FireEye and Microsoft discovered that the adversary gained access to victims' networks via trojanized updates to SolarWinds' Orion software.

## Threat activity details

In another sophisticated supply-chain attack, adversaries compromised updates to the SolarWinds Orion IT monitoring and management software, specifically a component called "SolarWinds.Orion.Core.BusinessLayer.dll" in versions 2019.4 HF 5 through 2020.2.1. The digitally signed updates were posted on the SolarWinds website until recently. This backdoor is being tracked by FireEye as SUNBURST, and it can communicate to third-party servers using HTTP. The backdoor is loaded by the actual SolarWinds executable before the legitimate code, as not to alert the victim that anything is amiss.

After a period of dormancy, which can last up to two weeks, the backdoor can execute commands to transfer and execute files, profile the system, reboot the machine and disable system services. Note that a number of SUNBURST samples have been observed along with varying payloads, including a memory-only dropper dubbed "Teardrop," which was then used to deploy Cobalt Strike beacons.

The adversaries leverage administrative privileges obtained during the on-premise compromise to access the victim's global administrator account and/or trusted SAML token-signing certificate. The adversary can forge SAML tokens that impersonate any of the organization's existing users and accounts, including highly privileged accounts, allowing them to bypass multi-factor authentication for services such as Office365 suite. Security researchers have observed that the targeted users are often key IT and security personnel. Because the SAML tokens are signed with their own trusted certificate, they can be used to log in to any on-premise resource or cloud environment, regardless of vendor.

The adversary also uses sophisticated techniques for communications. The backdoor identifies its command and control (C2) server using a domain-generated algorithm (DGA) to construct and resolve a subdomain of avsvmcloud[.]com, which it can use to deliver second-stage payloads and access or exfiltrate data. Network traffic originating from the malware appears as legitimate Orion protocol traffic and the adversaries store information in legitimate plugin configuration files, all causing it to look like normal SolarWind network traffic. The actor sets the hostnames on their C2 infrastructure to match legitimate hostnames found within the victim's environment. The adversary mainly relied on IP addresses originating from the same country as the victim — all of which are designed to evade detection.

Initial findings suggest that the campaign began in late February 2020 and lasted several months. SolarWinds and CISA issued security advisories warning of active exploitation of the SolarWinds Orion Platform software released between March and June, and Microsoft has been tracking the SUNBURST backdoor since March.

## Impact

SolarWinds confirmed that less than 18,000 of its 300,000 customers have downloaded the compromised update. Still, the effects of this campaign are potentially staggering, with the company's products being used by several high-value entities. Victims reportedly include government agencies and consulting, technology, telecom, and oil and gas companies in North America, Europe, Asia and the Middle East, according to FireEye. Several reports also indicate that the U.S. Treasury and Commerce departments were also targeted in what is likely related to the same activity.

## Response

SolarWinds issued a security advisory recommending users upgrade to the latest version, Orion Platform version 2020.2.1 HF 1, as soon as possible. In response to this activity, on Dec. 13, 2020 the U.S. Department of Homeland Security (DHS) and CISA issued an

emergency alert calling on all U.S. federal civilian agencies to review their networks for indicators of compromise (IOCs) and advising them to disconnect SolarWinds Orion products immediately. Microsoft has named this attack "Solorigate" in Windows Defender and, along with other industry partners, has published guidance and timelines for this activity. CISA and DHS provided required actions and mitigations in their advisories:

- Reimage system memory and/or host operating systems hosting all instances of SolarWinds Orion versions 2019.4 through 2020.2.1 HF1, and analyze for new user or service accounts.
- Disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from their network.
- Identify the existence of "SolarWinds.Orion.Core.BusinessLayer.dll" and "C:\WINDOWS\SysWOW64\netsetupsvc.dll".
- Block all traffic to and from hosts where any version of SolarWinds Orion software has been installed.
- Identify and remove threat-actor controlled accounts and persistence mechanisms.
- Reset all credentials used by SolarWinds software and implement a rotation policy for these accounts. Require long and complex passwords.
- See Microsoft's guidance and documentation on kerberoasting.

We urge all organizations that use the SolarWinds Orion IT monitoring and management software to carefully follow the guidance from DHS and CISA. We also note that Cobalt Strike was observed being leveraged in these attacks. Cisco Talos released a research paper detailing the large amount of coverage for the Cobalt Strike framework. Our pre-existing coverage is still applicable and can reliably detect FireEye red team beacons and other activity.

## Incident Response

Cisco Talos Incident Response (CTIR) is currently supporting retainer customers in regard to the SolarWinds Orion Sunburst backdoor. CTIR recommends organizations update incident response plans, playbooks, or a tabletop exercise (TTX) to test the organization's ability to respond to a supply-chain attack. Finally, once mitigation efforts have been successfully put in place, CTIR recommends a targeted threat hunt leveraging indicators and adversary TTPs.

## Coverage

Ways our customers can detect and block this threat are listed below.

Snort:

SIDs 56660-56668

AMP:

- Trojan.Sunburst.[A-Z]
- Trojan.Teardrop.[A-Z]

ClamAV:

- Win.Countermeasure.Sunburst-9816012-0
- Win.Countermeasure.Sunburst-9809153-0
- Win.Countermeasure.Sunburst-9816013-0
- Win.Countermeasure.Sunburst-9809152-0
- Win.Dropper.Teardrop-9808996-3
- PUA.Tool.Countermeasure.DropperRaw64TEARDROP-9808998-0

| Product | Protection |
|---|---|
| AMP | ✓ |
| Cloudlock | N/A |
| CWS | ✓ |
| Email Security | N/A |
| Network Security | ✓ |
| Secure Network Analytics | See Below |
| Secure Cloud Analytics | See Below |
| Secure Workload | See Below |
| Threat Grid | ✓ |
| Umbrella | ✓ |
| WSA | ✓ |

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware detailed in this post. Below is a screenshot showing how AMP can protect customers from this threat. Try AMP for free here.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), Cisco ISR, and Meraki MX can detect malicious activity associated with this threat.

Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Secure Cloud Analytics uses a variety of analytical processes to identify anomalous and malicious behavior occurring on the network. This particular threat can have some heuristic indicators to identify potential SolarWinds Orion servers, including SNMP traffic, scanning activity, and anomalous DNS traffic.

- “New SNMP sweep” alert will have fired if a server has been attempting to reach a large number of hosts using SNMP. Start a search in Monitor-> Alerts using the name of alert, and search over the last month (including closed alerts).
- “IP scanner” observation triggers when a device is seen on the network scanning a large number of entities. It can be included in “New SNMP sweep” as evidence, among other alerts (like “Outbound SMB spike”or “NetBios connection spike”). Look for this type of observation in your network.
- “Domain Generation Algorithm Successful Lookup” is an alert that will trigger when a device succeeds in resolving an algorithmically generated domain (e.g., rgkte-hdvj.cc) to an IP address. This alert uses the Domain Generation Algorithm Success observation and may indicate a malware infection or botnet activity.

Once you have identified the mentioned alert or observation, you can investigate all the servers related to them, as they are potentially SolarWinds Orion servers.

These types of detections and others can be applied to a variety of different threats through Secure Cloud Analytics to identify behavior not directly associated with existing IOCs or TTPs, like: C&C connections, lateral movement and data exfiltration.

Secure Workload can be used to identify compromised or affected assets and can be leveraged to apply primary mitigations as recommended by CISA including restricting network traffic to least privilege.

Additional protections with context to your specific environment and threat data are available from the Firepower Management Center.
Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

For Cisco customers that are concerned about potential impacts to Cisco products, please see the PSIRT advisory available here.

## Indicators of compromise (IOCs)

Domains:
avsvmcloud[.]com (SUNBURST) - Killswitch domain/currently unblocked

zupertech[.]com (SUNBURST)
panhardware[.]com (SUNBURST)
databasegalore[.]com (SUNBURST)
incomeupdate[.]com (SUNBURST)
highdatabase[.]com (SUNBURST)
websitetheme[.]com (SUNBURST)
freescanonline[.]com (SUNBURST)
virtualdataserver[.]com (SUNBURST)
deftsecurity[.]com (SUNBURST)
thedoccloud[.]com (SUNBURST)
digitalcollege[.]org (SUNBURST)
globalnetworkissues[.]com (SUNBURST)
seobundlekit[.]com (SUNBURST)
virtualwebdata[.]com (SUNBURST)
kubecloud[.]com (BEACON)
lcomputers[.]com (BEACON)
solartrackingsystem[.]net (BEACON)
webcodez[.]com (BEACON)
ervsystem[.]com (TEARDROP)
infinitysoftwares[.]com (TEARDROP)

IP Addresses:
13.59.205[.]66 (SUNBURST)
54.193.127[.]66 (SUNBURST)
3.87.182[.]149 (BEACON)
3.16.81[.]254 (SUNBURST)
54.215.192[.]52 (SUNBURST)
18.253.52[.]187 (SUNBURST)
34.203.203[.]23 (SUNBURST)
54.215.192[.]52 (SUNBURST)
18.220.219[.]143 (SUNBURST)
139.99.115[.]204 (SUNBURST)
13.57.184[.]217 (SUNBURST)
34.219.234[.]134 (BEACON)
5.252.177[.]25 (SUNBURST)
5.252.177[.]21 (SUNBURST)
204.188.205[.]176 (SUNBURST)
51.89.125[.]18 (SUNBURST)
162.223.31[.]184 (BEACON)
173.237.190[.]2 (BEACON)
45.141.152[.]18 (BEACON)

Hashes (SHA256):

019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134 (SUNBURST)
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77 (SUNBURST)
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c (SUNBURST)
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77 (SUNBURST)
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71 (SUPERNOVA)
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6 (SUNBURST)
d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600 (SUNBURST)
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b (SUNBURST)
1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c (TEARDROP)
b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07 (TEARDROP)
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589 (SUNBURST)
db9e63337dacf0c0f1baa06145fd5f1007002c63124f99180f520ac11d551420 (SUNBURST)
118189f90da3788362fe85eafa555298423e21ec37f147f3bf88c61d4cd46c51 (TEARDROP)
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed (SUNBURST)
abe22cf0d78836c3ea072daeaf4c5eeaf9c29b6feb597741651979fc8fbd2417 (SUNBURST)
20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9 (SUNBURST)
2ade1ac8911ad6a23498230a5e119516db47f6e76687f804e2512cc9bcfda2b0 (SUNBURST)
6e4050c6a2d2e5e49606d96dd2922da480f2e0c70082cc7e54449a7dc0d20f8d (TEARDROP)

The follow hashes reference files that contain incomplete portions of modified code - not enough to permit remote code execution. As a result we are not convicting the files as removing them may create additional issues by breaking existing SolarWinds installations.

a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af