The Hitchhiker's Guide to SolarWinds Incident Response

zscaler.com/blogs/security-research/hitchhikers-guide-solarwinds-incident-response

On December 13, 2020, multiple security vendors in conjunction with CISA disclosed a software supply-chain attack involving the SolarWinds Orion platform. The disclosure detailed the activities of an advanced persistent threat (APT) adversary that was able to gain access to SolarWinds systems to create trojanized updates to the Orion platform between March 2020 and possibly as recently as December 2020. The trojanized updates included a custom, digitally signed backdoor called SUNBURST. SolarWinds Orion is a widely used network infrastructure monitoring and management platform with a reported customer base of over 18,000. The following versions may be affected:

- Orion Platform 2019.4 HF5, version 2019.4.5200.9083
- Orion Platform 2020.2 RC1, version 2020.2.100.12219
- Orion Platform 2020.2 RC2, version 2020.2.5200.12394
- Orion Platform 2020.2, 2020.2 HF1, version 2020.2.5300.12432

At this time, the full scope of the attack remains under investigation. What is known is that the attack was executed by a truly sophisticated adversary with a deep understanding of operational security and complex tradecraft. Based on publicly available data, this adversary demonstrated significant efforts to evade, obfuscate, and clean-up using techniques such as steganography, fingerprinting techniques to identify both target systems as well as analysis systems, rotating infrastructure with a focus on geolocation proximity, as well as executing code in memory as much as possible. These techniques, in combination with using a digitally signed component of a trusted software platform as the initial infection vector, are indicative of a highly skilled and covert adversary willing to expend resources to assure the success of their operation.

Zscaler suggests that all organizations should take several immediate actions, described below, in addition to reviewing the existing security policies and best practices available to Zscaler customers.

These actions are recommended for any organization that may be impacted by the SolarWinds event. They are not intended to be a comprehensive guide to all actions that an organization may take, and each organization should perform its own due diligence to assess impact and risk.

Investigation

Organizations should immediately identify all systems that may have SolarWinds Orion installed. Once the systems are identified, the version should be checked against the list of impacted versions. Depending on the result of the version(s) installed, additional responses may be required. Even if a version is not found on the impacted version list, it may be prudent to perform cursory checks to confirm there is no impact to the organization.

If an affected version of Orion is found, that system should be immediately taken offline and all network traffic blocked inbound and outbound. Any system or user accounts associated with the affected system should be disabled and reviewed for legitimacy as well as access. If possible, a forensics image of the affected system should also be collected.

Network activity

Based on public reporting, a SolarWinds Orion system affected by this event—meaning that the SUNBURST backdoor had been successfully installed—would begin network communication to its first stage command and control (C&C) server at avsvmcloud[.]com. While this activity does indicate that the affected system was within the target radius of the attack, it does not confirm additional compromise or post-exploitation actions. Zscaler Internet Access (ZIA) customers may be able to perform this search within the DNS Insights or Web Insights area in the portal, or within the log aggregator/SIEM of choice where ZIA logs are sent. This data will however be limited to systems that have their network traffic routed to ZIA.

The following network indicators may be used to perform a sweep for a timeframe extending back to March 2020 or further to discover possible compromised systems (note: additional indicators may be discovered as additional data is disclosed).

Domains

avsvmcloud[.]com

digitalcollege[.]org

freescanonline[.]com

deftsecurity[.]com

thedoccloud[.]com

websitetheme[.]com

highdatabase[.]com

incomeupdate[.]com

databasegalore[.]com

panhardware[.]com

zupertech[.]com

seobundlekit[.]com

lcomputers[.]com

virtualdataserver[.]com

webcodez[.]com

infinitysoftwares[.]com

ervsystem[.]com

bigtopweb[.]com - *Added 1/20/21 in relation to RainDrop*

IPs

```
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
```

All other internet-bound destinations from the Orion system should also be examined. Additionally, all network activity originating from SolarWinds Orion systems to other internal systems should be reviewed for potential lateral movement. This may prove challenging as most Orion deployments likely allow it to have privileged access across the network to a variety of systems. However, it may be possible to carve out a smaller set of data to initially analyze by suppressing known-good or expected behaviors from the potentially affected Orion system.

Endpoint

The SUNBURST backdoor is a digitally signed DLL file with a specific filename and hash. The existence of this file on an Orion server is indicative that the adversary was able to gain unauthorized access to the system. Additional post-exploitation behaviors may have been performed by the adversary, indicating a successful intrusion. The following indicators and behaviors may assist in confirming a compromise.

MD5 hashes

```
b91ce2fa41029f6955bff20079468448

d5aad0d248c237360cf39c054b654d69

2c4a910a1299cdae2a4e55988a2f102e

846e27a652a5e1bfbd0ddd38a16dc865
```

Filename

```
SolarWinds.Orion.Core.BusinessLayer.dll
```

Behaviors

- Modification of system tasks
- delete-create-execute-delete-create directory action pattern
- Newly created or unknown local user accounts
- Existence or evidence of usage of Adfind.exe
- Signs of cmd.exe or rundll32.exe spawned from solarwinds.businesslayerhost.exe
- Existence of unknown and/or very broad email forwarding/deleting rules on the email gateway

User account activity

Once SUNBURST has been deployed, the adversary will most likely begin to perform reconnaissance actions using the privileges of the Orion system and explore what is available in terms of additional assets to compromise or actions to take. The following behaviors may have been observed on the affected Orion system or other systems that have had communication with the affected system.

- Anomalous logins or repeated failed authentication to internal systems
- Logins from unknown or unrecognized external sources to internal systems
- Extremely long duration tokens, which may indicate malicious activity (examine SAML tokens for duration)

Zscaler is here to help

As described in our **ThreatLabZ blog post**, Zscaler immediately deployed protections to all customers and continues to deploy additional protections and countermeasures as more information becomes available. In addition, as we had disclosed in our **Trust Advisory**, Zscaler was not impacted by this event. This may, however, be an opportunity for organizations to reassess their security policies and confirm alignment with documented best practices and recommended policies as described within our documentation, which covers recommendations, such as:

- Enable SSL inspection where possible | SSL Best Practice Guide
- Enable Advanced Threat Protection (ATP) and its associated features | Recommended Policy
- Enable Advanced Cloud Sandbox with AI-Driven Quarantine | Recommended Policy
- Enable Advanced Cloud Firewall with Cloud IPS | Recommended Policy
- Enable Cloud Browser Isolation where possible | About Cloud Browser Isolation
- Restrict access to specific URL categories with legitimate business use cases | Recommended Policy
- Restrict access to specific file-types with legitimate business use cases | Recommended Policy
- Configure DNS Control | About DNS Control

Request your complimentary SolarWinds security assessment

Zscaler has your back. Engage with our security experts to gain insight into the SolarWinds attacks and get hands-on best practices guidance to better protect your users, applications, and systems: **zscaler.com/solarwinds-cyberattack**