Threat Advisory Report: SolarWinds Supply Chain Attack (Solorigate/SUNBURST)

Published: 12/13/2020
Updated: 3/18/2021 10:15 AM ET

Contents

Summary 3
Threat Details 3
Technique Timeline & Detection 3
Resource Development 3
Initial Access 4
Execution 4
Persistence 4
Defense Evasion 5
Discovery 6
Privilege Escalation 6
Collection 7
Command and Control 7
ReliaQuest Response 7
Recommendation 8
References 8

Summary

SolarWinds – an IT software development company – has been compromised and the subsequent supply chain attack is believed to affect multiple public and private sector customers. Attackers implanted backdoors in legitimate, signed DLL files contained in update packages for SolarWinds Orion from March until June of 2020 that were then used to breach customers who upgraded to the affected versions (versions **2019.4 HF 5** through **2020.2 HF 1**).

Threat Details

The actors behind this campaign were able to gain access to SolarWinds software and create a backdoor in a legitimate DLL – **SolarWinds.Orion.Core.BusinessLayer.dll**. Although the details of the initial SolarWinds compromise are not yet known, these updates were digitally signed and made available to SolarWinds customers between March and June of 2020.

Once the SolarWinds application is updated to an affected version, the embedded backdoor code loads and remains dormant for up to two weeks before establishing command-and-control (C2) communication. Once activated, the implant receives commands to perform post-exploitation activities, including conducting reconnaissance, exfiltrating files, and disabling security controls. The malware traffic imitates the SolarWinds Orion Improvement Program (OIP) protocol and stores information in SolarWinds configuration files to disguise itself as normal activity. The backdoor can also identify and block anti-virus and forensic tools to evade detection.

FireEye noted that the threat actors kept a "light malware footprint" by using legitimate credentials and remote access tools for network access and lateral movement. As SolarWinds products typically run with elevated privileges, the attackers were able to use their initial foothold to move laterally and gain additional administrative credentials within the target environments. The attacker's infrastructure was configured to match legitimate target hostnames within the environment and new authentications were typically executed in the same geographic region of the target using virtual private networks. When authenticating remotely to the network, a different set of stolen credentials was used for the authentication than was used for lateral movement.

Technique Timeline & Detection

This section details the MITRE tactics and techniques used by the attackers in their campaign. Detections in GreyMatter that are relevant to the tactics are also listed. ReliaQuest will continue to monitor the situation as new details emerge and update or create new detections to address this threat.

Resource Development

T1584 – Compromise Infrastructure

Although the details of the initial compromise of SolarWinds are unknown, we do know that it led to eventual compromise of their internal software build or distribution system.

Initial Access

T1195.002 – Supply Chain Compromise: Compromise Software Supply Chain

With access to the SolarWinds development system, the threat actor embedded a backdoor in **SolarWinds.Orion.Core.BusinessLayer.dll** – a legitimate component of the Orion software framework present in multiple updates available through the SolarWinds website. SolarWinds customers who installed these malicious updates unknowingly installed this backdoor in their environment.

Execution

T1059 – Command and Scripting Interpreter

SolarWinds.Orion.Core.BusinessLayer.dll contained an obfuscated backdoor that communicated to C2 servers. It utilized "Jobs" to execute commands on an affected host.

T1569.002 – System Services: Service Execution

The backdoor deployed the malware dropper TEARDROP that runs as a service.

GreyMatter Detections

- RQ-000110-04 - Recon Commands
- RQ-000073 - Service Installations - Critical Host
- RQ-SM-000237-07 - Suspicious Service Installation
- RQ-SH-000238-02 - Service Installation in Suspicious Directory
- RQ-SL-000234-02 - PowerShell Remote Execution

Persistence

T1543.003 – Create or Modify System Process: Windows Service

The backdoor deployed the malware dropper TEARDROP that runs as a service.

T1053 – Scheduled Task/Job

Manipulation of scheduled tasks by updating an existing legitimate task to execute their tools and then returning the scheduled task to its original configuration.

GreyMatter Detections

- RQ-000073 - Service Installations - Critical Host
- RQ-SM-000237-07 - Suspicious Service Installation
- RQ-SH-000238-02 - Service Installation in Suspicious Directory
- RQ-SM-000149-02 - Suspicious Scheduled Task Created
- RQ-SM-000233-02 - PowerShell Scheduled Task Creation
- RQ-000771-01 - Task Scheduled via Command Line

Command and Control

T1071.001 – Application Layer Protocol: Web Protocols

HTTP requests were used for C2 beacons and transferring data out of the network.

T1001.003 – Data Obfuscation: Protocol Impersonation

The network traffic was designed to impersonate the Orion Improvement Program protocol, which normally sends usage information back to SolarWinds.

T1071.004 – Application Layer Protocol: DNS

The attackers used DNS CNAME records to store the domain names of its C2 servers. Once the backdoor was initialized, it would resolve the CNAME record for **avsvmcloud[.]com** to retrieve the C2 server domains.

T1105 – Ingress Tool Transfer

The backdoor has the capability to transfer files and download additional tools. The dropper TEARDROP is used to download additional malware.

T1132.001 – Data Encoding: Standard Encoding

The C2 beacon and response traffic are both encoded and compressed with multiple algorithms.

T1568.002 – Dynamic Resolution: Domain Generation Algorithms

The backdoor used a Domain Generation Algorithm (DGA) to create and resolve subdomains of **avsvmcloud[.]com**.

GreyMatter Detections

- RQ-SM-000050-05 - Domain Generation Algorithm HTTP(S) Request Pattern
- RQ-SM-000044-05 - DNS Request to DGA Domain
- RQ-SM-000046-03 - DNS CNAME Request Beaconing

Defense Evasion

T1027 – Obfuscated Files or Information

The legitimate file **SolarWinds.Orion.Core.BusinessLayer.dll.config** is used by the malware to store persistence settings.

T1070.004 – Indicator Removal on Host: File Deletion

The attackers removed their tools and backdoors once other remote access vectors were secured. They also replaced legitimate executables with malicious ones, executed them, then removed their files and restored the originals.

T1553.002 – Subvert Trust Controls: Code Signing

As the attackers compromised the software build system, the file that was backdoored was then signed – giving it additional legitimacy and further reducing chances of detection.

T1562.001 - Impair Defenses: Disable or Modify Tools / T1112 - Modify Registry

Attackers stopped services associated with security and monitoring tools by setting the value of the **HKLM\SYSTEM\CurrentControlSet\services\{SERVICE_NAME}\Start** key in the Windows registry to “4”.

T1134.003 – Access Token Manipulation: Make and Impersonate Token

In the Microsoft cloud, attackers used compromised SAML token signing certificates to forge SAML tokens to access administrative privileges.

T1036.005 – Masquerading: Match Legitimate Name or Location

Attackers replaced legitimate files with malicious ones that used the same name to avoid detection. The malicious files were then deleted and the original

GreyMatter Detections

- RQ-SM-002340-01 - Security Tool Service Disabled

Discovery

T1012 – Query Registry

Attackers queried the Windows registry for the value of the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid** key to be used in an identifier for compromised hosts.

T1057 – Process Discovery

SolarWinds.Orion.Core.BusinessLayer.dll contained an obfuscated backdoor that communicated to C2 servers. It utilized "Jobs" to execute commands for discovering processes on an affected host.

T1083 – File and Directory Discovery

SolarWinds.Orion.Core.BusinessLayer.dll contained an obfuscated backdoor that communicated to C2 servers. It utilized "Jobs" to execute commands for file and directory discovery on an affected host.

T1518 – Software Discovery

SolarWinds.Orion.Core.BusinessLayer.dll contained an obfuscated backdoor that communicated to C2 servers. It utilized "Jobs" to execute commands for software discovery on an affected host.

T1518.001 - Software Discovery: Security Software Discovery

SolarWinds.Orion.Core.BusinessLayer.dll contained an obfuscated backdoor that communicated to C2 servers. It utilized "Jobs" to execute commands for security software discovery on an affected host.

GreyMatter Detections

- RQ-000110-04 - Recon Commands
- RQ-SH-000706-01 - Credential Harvesting

Privilege Escalation

T1543.003 – Create or Modify System Process: Windows Service

The backdoor deployed the malware dropper TEARDROP that runs as a service.

T1053 – Scheduled Task/Job

Manipulation of scheduled tasks by updating an existing legitimate task to execute their tools and then returning the scheduled task to its original configuration.

GreyMatter Detections

- RQ-000073 - Service Installations - Critical Host
- RQ-SM-000237-07 - Suspicious Service Installation
- RQ-SH-000238-02 - Service Installation in Suspicious Directory
- RQ-SM-000149-02 - Suspicious Scheduled Task Created
- RQ-SM-000233-02 - PowerShell Scheduled Task Creation
- RQ-000771-01 - Task Scheduled via Command Line

Collection

T1114.002 – Email Collection: Remote Email Collection

There are several instances of the attackers adding mail read permissions to their compromised accounts in order to collect and monitor the target's emails.

ReliaQuest Response

ReliaQuest has ingested all currently identified IOCs related to this attack into GreyMatter Intel for rapid detection capabilities and will continue to monitor for additional IOCs. Countermeasures and IOCs identified by FireEye can be found in their GitHub repository referenced at the end of the document.

We are also leveraging GreyMatter Hunt to perform a retroactive IOC hunt for all customers integrated with the GreyMatter Platform. For questions related to the ReliaQuest response, please reach out to your Delivery Manager or the SOC at (813) 518-6565.

ReliaQuest will continue to research the threat actor's behavior to identify new detection opportunities that can be deployed to customers through GreyMatter Detect.

If IOC activity has been detected within your environment, the following responses are recommended:

- Investigate any hosts associated with IOC hits for evidence of the techniques listed above around or after the time in which the first IOC hit was seen.
- Isolate/disable SolarWinds servers until confident there is a trustworthy build to update to.
- Block known IOCs on network/security infrastructure and monitor for these IOCs in logs as a sign of infection. Hosts associated with these indicators should be isolated and re-imaged before being redeployed in the environment. Any account credentials found to have been used by the attackers should be reset.
- Change passwords for administrator and service accounts.
- Ensure default passwords are changed.
- Remove or disable unused/unnecessary applications and users, especially those with significant privilege (domain administrators, for example).
- Limit user/service account privilege to the least amount necessary.
- Restrict scope of connectivity as appropriate between network segments (in particular, from SolarWinds to other areas of the network).
- Verify backups for critical data and servers are available and stored securely.

Recommendation

SolarWinds has advised customers with Orion Platform version **2020.2** or **2020.2 HF 1** to update to the **2020.2.1 HF 2** hotfix and customers with version **2019.4 HF 5** to update to **2019.4 HF 6**. We recommend performing these updates as soon as possible. If you are not able to do so immediately, consider disconnecting or otherwise isolating SolarWinds hosts in your environment until they can be patched.

References

FireEye Threat Research

- https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- https://github.com/fireeye/sunburst_countermeasures

Microsoft Security Response Center

- https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

SolarWinds Security Advisory

- https://www.solarwinds.com/securityadvisory

Volexity Threat Research

- https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/