Tactics, Techniques, and Procedures (TTPs) Used in the SolarWinds Breach

By Suleyman Ozarslan, PhD

Published: 2020-12-15 · Archived: 2026-04-05 17:11:37 UTC

EXECUTIVE SUMMARY

SolarWinds announced on Sunday that the SolarWinds Orion Platform network monitoring product had been modified by a state-sponsored threat actor via embedding backdoor code into a legitimate SolarWinds library. This leads to the attacker having remote access into the victim's environment and a foothold in the network, which can be used by the attacker to obtain privileged credentials. SolarWinds breach is also connected to the FireEye breach. In this article, we analyzed tactics, techniques, and procedures utilized by threat actors of the SolarWinds incident to understand their attack methods and the impact of this breach.

Key Findings

- It is a global attack campaign that started in March 2020 and is ongoing.
- The attack campaign has the potential to affect thousands of public and private organizations.
- The attack started with a software supply chain compromise attack.
- Threat actors trojanized a component of the SolarWinds Orion Platform software, dubbed as SUNBURST by FireEye [1].
- The backdoored version of the software was distributed via its automatic update mechanism.
- Attackers heavily used various defense evasion techniques such as masquerading, code signing, obfuscated files or information, indicator removal on host, and virtualization/sandbox evasion.
- The threat actor leverages ten different MITRE ATT&CK tactics, including Lateral Movement, Command and Control, and Data Exfiltration.
- Used techniques indicate that the threat actors are highly skilled.

Tactic, Techniques and Procedures used in SolarWinds Breach (Mapped to MITRE ATT&CK Framework)

Our analysis uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 8.1 framework. See the ATT&CK for Enterprise version 8.1 for all referenced threat actor tactics and techniques.

1. Resource Development

1.1. T1587.001 Develop Capabilities: Malware

Adversaries create malware and malware components before compromising a victim, such as payloads, droppers, backdoors, and post-compromise tools [2]. They may create malware from scratch or use publicly available tools.

In the SolarWinds incident, attackers embedded their malicious payload on a legitimate component of the SolarWinds Orion Platform software. This component is a DLL library, SolarWinds.Orion.Core.BusinessLayer.dll. FireEye named the backdoored version of the DLL file as SUNBURST [1]. The SUNBURST backdoor delivers different payloads, such as a previously unseen memory-only dropper dubbed TEARDROP by FireEye [1]. The TEARDROP dropper deploys an infamous post-compromise tool, Cobalt Strike Beacon. Apparently, attackers used Beacon in the FireEye breach and stole FireEye's Red Team tools that include Beacon.

1.2. T1583.003 Acquire Infrastructure: Virtual Private Server

In this MITRE ATT&CK technique, adversaries rent Virtual Private Servers (VPSs) that can be used during the attack campaign [3]. According to the FireEye research, the threat actor leverages VPSs to use only IP addresses originating from the same country as the victim [1]. FireEye has provided two Yara rules to detect TEARDROP available on GitHub [4].

2. Initial Access

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

In the software supply chain compromise attack technique, adversaries modify software prior to receipt by a final user by manipulating the software's:

- source code
- source code repositories (public or private)
- open-source dependencies' source code
- build & distribution systems
- update mechanism
- development environment, or
- compiled release [5]

In the SolarWinds Orion breach, adversaries embedded malicious code into a SolarWinds library file, SolarWinds.Orion.Core.BusinessLayer.dll. According to SolarWinds security advisory, attackers backdoored three versions of the Orion Platform software: 2019.4 HF 5, 2020.2 with no hotfix, and 2020.2 HF 1 [6].

However, it is not clear how attackers could tamper this file. According to Microsoft's research, adversaries might have compromised and manipulated **build or distribution systems** and embedded malicious code [7]. Another claim is that attackers might have uploaded the malicious DLL file to the **source code repository** of SolarWinds using leaked FTP credentials [8].

The backdoored SolarWinds Orion Platform software update file that includes the malicious DLL file was distributed via its automatic update mechanism.

As a countermeasure, check whether the manipulated SolarWinds.Orion.Core.BusinessLayer.dll file exists in the following locations:

- %PROGRAMFILES%\SolarWinds\Orion\
- %WINDIR%\System32\config\systemprofile\AppData\Local\assembly\tmp\<random>\

If the DLL has one of the following SHA256 hashes, it is a manipulated and malicious version [7]:

- 32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
- dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
- eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed
- c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77
- ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
- 019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
- ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
- a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc

Then, scan the above folders with up-to-date antivirus products, and run EDRs to detect maliciously tampered SolarWinds files and their (potentially) anomalous behavior.

3. Execution

3.1. T1569.002 System Services: Service Execution

In this MITRE ATT&CK technique, adversaries execute their malware as a Windows service [6]. During the installation of the SolarWinds application or update, the tampered DLL file is loaded by the legitimate SolarWinds.BusinessLayerHost.exe or SolarWinds.BusinessLayerHostx64.exe and installed as a Windows service.

4. Persistence

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

As part of persistence, adversaries can create or change Windows services to repeatedly execute malicious payloads [4], [9]. When Windows boots up, the malicious code starts as a service. The TEARDROP malware loaded by the modified DLL runs as a service in the background.

5. Privilege Escalation

5.1. T1078 Valid Accounts

According to this MITRE ATT&CK technique, adversaries may obtain and abuse legitimate credentials to gain Initial Access, Persistence, Privilege Escalation, Defense Evasion, or Lateral Movement [10]. Threat actors use multiple valid accounts for lateral movement in this attack campaign [1].

6. Defense Evasion

6.1. T1553.002 Subvert Trust Controls: Code Signing

To bypass application control technologies, adversaries sign their malware with valid signatures by creating, acquiring, or stealing code-signing materials [11].

In the SolarWinds incident, attackers have compromised digital certificates of SolarWinds.

Remove compromised SolarWinds certificates:

"Signer": "Solarwinds Worldwide LLC"
"SignerHash": "47d92d49e6f7f296260da1af355f941eb25360c4"

6.2. T1036.005 Masquerading: Match Legitimate Name or Location

As a defense evasion technique, adversaries change features of their malicious artifacts with legitimate and trusted ones. Code signatures, names and location of malware files, names of tasks and services are some examples of these features. After masquerading, malicious artifacts of adversaries such as malware files appear legitimate to users and security controls [12]. You can read our blog post to find out more information about the masquerading technique.

According to the FireEye report, the threat actor of the SolarWinds breach uses a legitimate hostname found within the victim's environment as the hostname on their Command and Control (C2) infrastructure to avoid detection [1]. Moreover, the malware masquerades its C2 traffic as the Orion Improvement Program (OIP) protocol [1].

6.3. T1036.003 Masquerading: Rename System Utilities

To avoid name-based detection, adversaries may rename system utilities. Moreover, the threat actor replaces a legitimate utility with theirs, executes their payload, and then restores the legitimate original file [1].

6.4. T1036.004 Masquerading: Masquerade Task or Service

Adversaries masquerade the name of a task/service with the name of a legitimate task/service to make it appear benign and evade detection [12]. Adversaries commonly use identical or similar names of legitimate tasks/services executed by the Windows Task Scheduler, at (Linux and Windows), Windows services, and Linux systemd services.

6.5. T1497.003 Virtualization/Sandbox Evasion: Time Based Evasion

Adversaries employ various time-based evasion methods, such as delaying malware functionality upon initial execution, to avoid virtualization and analysis environments [13]. In the Solarwinds case, attackers delay Command and Control communication two weeks after the installation.

6.6. T1027.003 Obfuscated Files or Information: Steganography

In this MITRE ATT&CK technique, adversaries hide data in digital media such as images, audio, video, and text to prevent the detection of hidden information [14]. The TEARDROP malware used in the breach reads from the file gracious_truth.jpg that includes a malicious payload.

6.7. T1070.004 Indicator Removal on Host: File Deletion

Adversaries delete their malicious files to clear traces and minimize the adversary's footprint to avoid detection and inspection [15]. The threat actor removes their malicious files, including backdoors, after the remote access [1].

7. Discovery

7.1. T1057 Process Discovery

Adversaries obtain information about running processes on a system to understand common software and applications running on systems within the network [16]. The threat actor gets a list of processes to shape follow-on behaviors [1].

7.2 T1012 Query Registry

Adversaries query the Windows Registry to get information about the system, configuration, and installed software [17]. The threat actor obtains Cryptographic Machine GUID by querying the value of MachineGuid in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography key to generate a unique userID for each victim.

8. Lateral Movement

8.1. T1021 Remote Services

In this MITRE ATT&CK technique, adversaries use valid accounts to log into a remote service, such as remote desktop protocol (RDP), SSH, and VNC. The threat actor uses valid accounts and legitimate remote access to move laterally in the target network.

9. Command and Control

9.1. T1071.001 Application Layer Protocol: Web Protocols

According to this technique, adversaries communicate using application layer (L7) protocols and blend Command and Control traffic with existing web traffic to avoid detection and network filtering [18]. The malware used in this breach utilizes:

- HTTP GET or HEAD requests when data is requested
- HTTP PUT or HTTP POST requests when data is sent [1].

The malicious DLL avsvmcloud.com domain to call out a remote network infrastructure [7]. Block this domain and check network connection logs.

9.2. T1568.002 Dynamic Resolution: Domain Generation Algorithms

Adversaries use Domain Generation Algorithms (DGAs) to dynamically generate a C2 domain rather than relying on a list of static IP addresses or domains [19]. The backdoor used in this attack campaign uses a DGA to determine its C2 server [1].

10. Exfiltration

T1041 Exfiltration Over C2 Channel

In this MITRE ATT&CK technique, adversaries steal data by exfiltrating it over an existing C2 channel [20]. The threat actor uses HTTP PUT or HTTP POST requests when the collected data is being exfiltrated to the C2 server [1]. If the payload is bigger than 10000 bytes; the POST method is used. Otherwise, the PUT method is used.

References

[1] FireEye, “Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor.” https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. [Accessed: 15-Dec-2020]
[2] “Develop Capabilities: Malware.” https://attack.mitre.org/techniques/T1587/001/. [Accessed: 15-Dec-2020]
[3] “Acquire Infrastructure: Virtual Private Server.” https://attack.mitre.org/techniques/T1583/003/. [Accessed: 15-Dec-2020]
[4] fireeye, “fireeye/sunburst_countermeasures.” https://github.com/fireeye/sunburst_countermeasures. [Accessed: 15-Dec-2020]
[5] “Supply Chain Compromise: Compromise Software Supply Chain.” https://attack.mitre.org/techniques/T1195/002/.
[6] “System Services: Service Execution.” https://attack.mitre.org/techniques/T1569/002/.
[7] msrc, “Customer Guidance on Recent Nation-State Cyber Attacks – Microsoft Security Response Center.” https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks.
[8] “[No title].” https://twitter.com/vinodsparrow/status/1338431183588188160?s=20.
[9] “Create or Modify System Process: Windows Service.” https://attack.mitre.org/techniques/T1543/003/.
[10] “Valid Accounts.” https://attack.mitre.org/techniques/T1078/.
[11] “Subvert Trust Controls: Code Signing.” https://attack.mitre.org/techniques/T1553/002/.
[12] “MITRE ATT&CK T1036 Masquerading.” https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1036-masquerading.
[13] “Virtualization/Sandbox Evasion: Time Based Evasion.” https://attack.mitre.org/techniques/T1497/003/.
[14] “Obfuscated Files or Information: Steganography.” https://attack.mitre.org/techniques/T1027/003/.
[15] “Indicator Removal on Host: File Deletion.” https://attack.mitre.org/techniques/T1070/004/.
[16] “Process Discovery.” https://attack.mitre.org/techniques/T1057/.
[17] “Query Registry.” https://attack.mitre.org/techniques/T1012/.
[18] “Application Layer Protocol: Web Protocols.” https://attack.mitre.org/techniques/T1071/001/.
[19] “Dynamic Resolution: Domain Generation Algorithms.” https://attack.mitre.org/techniques/T1568/002/.
[20] “Exfiltration Over C2 Channel.” https://attack.mitre.org/techniques/T1041/.
