SolarWinds Attacks: Stealthy Attackers Attempted To Evade Detection

By About the Author

Archived: 2026-04-05 20:22:58 UTC

As we continue our analysis on the tools used in the SolarWinds attacks, one of the most striking aspects we've noticed is how careful the attackers were to avoid drawing attention to themselves. Software supply chain attacks are relatively stealthy to begin with, since signed software from a trusted source is less likely to raise red flags. However, the attackers weren't content to rely on the cover this provided and also took several other steps to avoid detection.

To begin with, the Sunburst backdoor (Backdoor.Sunburst), which was delivered using a Trojanized update to SolarWinds Orion, sets a delay time of up to 14 days before execution. In other words, no malicious activity will begin until this period has elapsed.

The length of time selected is most likely to increase the likelihood that the log entries of the initial malicious activity have been deleted before any subsequent post-breach activity is initiated, thereby making it difficult to correlate the two sets of malicious events. Many organizations, including even managed security services providers (MSSPs), will often purge their security logs after seven days to minimize storage costs and make searching them easier.

Sunburst will also check the current Windows domain the machine belongs to. If the domain contains the string 'test' or one of 13 additional specific domains that appear related to lab systems such as "swdev.local" and "apac.lab", the threat will cease to execute. A full list is in Appendix A.

Avoiding Security Software and Researchers

Attacks begin with a Trojanized version of SolarWinds' Orion software. The attackers modified Orion in order to deliver the Sunburst backdoor to the computer. Sunburst is first stage malware, designed to perform reconnaissance on the infected computer, perform checks for security tools, and deliver a second stage payload, if required.

The main Sunburst code is contained in a class named SolarWindows.Orion.Core.BusinessLayer that, when first instantiated, calls a member function called Update. The function name is a ruse, as the code does not perform any update, but instead is designed to disable security software, avoid security researcher systems, and possibly avoid running on systems not of interest to the attackers. The function contains three lists – a list of process names, a list of driver filenames, and a list of processes and service name pairs. These names are all obfuscated in the code by hashing them using the FNV1A algorithm and using variable names that masquerade as timestamps.

The function will:

- Get a list of running processes.
- Check if the process names match items on the process list
- Get a list of all installed drivers
- Check if the driver names match items on the drivers list
- If a match is found, the malicious code does not perform further actions and returns

This process and driver list contains tools that commonly run on security researcher systems and thus, this functionality appears to be designed not to run on such systems in order to avoid discovery. The full list of security tools can be found in Appendix A. Furthermore, the lists also contained names related to a variety of security software programs including:

- Security software process names
    - AVG/AVAST
    - Panda
    - Kaspersky
    - Tanium
- Driver names
    - CyberArk - cybkerneltracker.sys
    - Altiris Symantec - atrsdfw.sys (Ghost Pre-installation boot environment driver)
    - Raytheon Cyber Solutions - eaw.sys
    - CJSC Returnil Software - rvsavd.sys
    - Verasys Digital Guardian - dgdmk.sys
    - Sentinel One – sentinelmonitor.sys
    - Hexis Cyber Solutions - hexisfsmonitor.sys
    - Dell SecureWorks - groundling32.sys, groundling64.sys
    - SAFE-Cyberdefense - safe-agent.sys
    - Cybereason – crexecprev.sys
    - Absolute - psepfilter.sys, cve.sys
    - Bromium - brfilter.sys, brcow_x_x_x_x.sys
    - LogRhythm - lragentmf.sys
    - OESIS OPSwat - libwamf.sys

The security vendors on this list have most likely been chosen as the attacker has determined that their products are unlikely be installed at organizations of interest to the attackers. Given the indiscriminate nature of supply chain as a vector, with an estimated 18,000 SolarWinds customers affected, the attackers probably wanted to avoid any risk of detection in organizations that weren't of interest to them.

Interestingly, the process solarwindsdiagnostics is also blacklisted. Presumably this is included to avoid detection during any SolarWinds testing or troubleshooting.

Disabling security software

Sunburst also attempts to specifically disable some software security services via the registry. This allows Sunburst to perform its malicious actions completely undetected. If the attackers worked quickly and restored the

services afterwards, a security administrator would potentially have no record of the activity, nor have even noticed the temporary lack of protection.

Figure 1. Example of how Sunburst disables security software. In this case it checks if the CrowdStrike processes csfalconservice or csfalconcontainer are running, and if so, it sets the csagent, csfalconservice, and csdevicecontrol services to be disabled.

This function will:

- Get a list of running processes
- Check if the process names match items on the process/services name pair list
- Disable the security software by modifying its service registry entry
- After the software has been confirmed to be disabled, usually after a reboot, the malicious code will then contact the command and control (C&C) server and potentially perform further malicious actions

To disable the security software, Sunburst will simply set the products' service start setting to Disabled. In Windows, this is done by setting the registry keys:

- HKLM\ SYSTEM\CurrentControlSet\services\<service name>\Start = 4

This will cause the security software not to load at the next reboot.

It should be noted that the attackers do not attempt to disable any Symantec products. Presumably this is because of an anti-tampering feature in Symantec software, which prevents its own service from being disabled.

The process and services pair list include software from the following vendors:

- CrowdStrike
- Carbon Black
- FireEye
- ESET
- F-Secure

Interestingly, the list also included Microsoft Defender, but only the service key permissions are changed. Currently, this has an unknown effect. In addition, some other unknown products are also included, but were effectively commented out. The attackers may have discovered this technique was ineffective for these products.

Finally, Sunburst will check if api.solarwinds.com resolves to a valid address before continuing.

Low profile threat

The SolarWinds attacks are among the best-planned and adept attacks we have seen in recent years. The attackers have gone to great lengths to both find an effective path into their targeted organizations and, once inside their networks, maintain a low profile. Our analysis of these tools is ongoing and we plan to publish further blogs in the coming weeks.

Protection/Mitigation

Tools associated with these attacks will be detected and blocked on machines running Symantec Endpoint products.

File-based protection:

- Backdoor.Sunburst
- Backdoor.Sunburst!gen1
- Backdoor.SuperNova
- Backdoor.Teardrop

Network-based protection:

- System Infected: Sunburst Malware Activity

Appendix A

Drivers Avoided

Security Software Avoided
