Sunburst: Supply Chain Attack Targets SolarWinds Users

By About the Author

Archived: 2026-04-05 13:31:59 UTC

UPDATE December 16 2020: *Our blog has been updated with analysis of the Teardrop second-stage malware and an example of the post-compromise attack chain. We have also provided clarification on the use of Symantec's name in a certificate used to sign the SolarWinds software.*

Thousands of organizations have been affected by a supply chain attack that compromised the update mechanism for SolarWinds Orion software in order to deliver a backdoor Trojan known as Sunburst (Backdoor.Sunburst) (aka Solorigate).

Details on the attacks were disclosed yesterday (December 13) by the security firm FireEye. SolarWinds has also published a security advisory for its customers.

The campaign has been underway since at least March 2020. Any Orion user who downloaded an update in this period is likely to have been infected with Sunburst. According to FireEye, the attackers conducted further malicious activity on a subset of victim organizations that were of interest to them.

By their nature, supply chain attacks are indiscriminate and will infect any user of the compromised software. They are carried out in order to provide the attacker with access to a large number of organizations, a subset of which will be identified as targets of interest for further compromise.

The Trojanized software was signed by a certificate marked as being issued by Symantec. Symantec sold its certificate authority business to Digicert in 2018. The certificate in question was a legacy certificate still using the Symantec brand name. Symantec has contacted Digicert, which has confirmed that it is investigating the issue.

Symantec has identified more than 2,000 computers at over 100 customers that received Trojanized software updates. We have found a small number of organizations where a second stage payload (Backdoor.Teardrop) was used.

Sunburst analysis

An existing SolarWinds DLL called SolarWinds.Orion.Core.BusinessLayer.dll was modified by the attackers to include an added class.

The malware is designed to remain inactive for a period after installation. It will then attempt to resolve a subdomain of avsvmcloud[.]com. The DNS response will deliver a CNAME record that directs to a command and control (C&C) domain.

In SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager.RefreshInterval() code is added to call OrionImprovementBusinessLayer.Initialize().

OrionImprovementBusinessLayer is a malicious class added by the attacker. It has the following functionality:

- Terminates the backdoor thread
- Set delay time before execution
- Collect and upload system information including:
    - Domain
    - SID of administrator account
    - Hostname
    - Username
    - Operating system version
    - Path of system directory
    - Days elapsed since the system started
    - Information on network adapters, including:
        - Description
        - MACAddress
        - DHCPEnabled
        - DHCPServer
        - DNSHostName
        - DNSDomainSuffixSearchOrder
        - DNSServerSearchOrder
        - IPAddress
        - IPSubnet
        - DefaultIPGateway
- Download and run code
- Iterate the file system
- Create and delete files
- Calculate file hashes
- Read, write, and delete registry entries
- Reboot the system

Second-stage payload: Teardrop

A second stage payload, a backdoor called Teardrop, is deployed against a targets of interest to the attackers. Symantec has observed two variants of Teardrop, both of which behave similarly and are used to deliver a further payload – the Cobalt Strike commodity malware.

The first variant (SHA256: b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07) is a DLL. The malicious code is contained in the export Tk_CreateImageType, ordinal 209. When executed, that malicious code reads a file named upbeat_anxiety.jpg from the current directory and ensures it has a jpg header. It will also check that the registry key HKCU\Software\Microsoft\CTF exists. An embedded copy of Cobalt Strike is then extracted and executed. That CobaltStrike sample connects to infinitysoftwares[.]com for command and control.

The second variant (SHA256:1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c) is similar, except that the file it loads is called festive_computer.jpg. The embedded CobaltStrike payload connects to ervsystem[.]com for command and control.

Post-compromise attack chain

The post-compromise attack chain for one computer investigated saw the initial Sunburst malware, a modified solarwinds.orion.core.businesslayer.dll, installed through the Orion update process on the victim computer on the 7th of the month.

On the 28th of the month, 21 days later, the legitimate executable solarwinds.businesslayerhost.exe, which loads the malicious DLL, created a copy of Teardrop in a file called cbsys.dll, in the c:\windows\panther folder. This filename and path appear to be unusual since most instances of Teardrop were created in a file called netsetupsvc.dll in the c:\windows\syswow64 folder, as documented by FireEye.

The Backdoor.Teardrop sample is a DLL with malicious code contained in the export Tk_CreateImageType. When executed, that export reads a file named upbeat_anxiety.jpg from the current directory and ensures it has a jpg header. It will also check that the registry key HKCU\Software\Microsoft\CTF exists. An embedded copy of Cobalt Strike is then extracted. That CobaltStrike samples connects a C&C server - infinitysoftwares[.]com.

At this point, the attackers launch WMI to execute rundll32.exe to load another malicious DLL called resources.dll in the path csidl_windows\desktoptileresources\. Resources.dll attempts to obtain credentials by accessing lsass.exe using similar techniques to Mimikatz, a widely used credential dumping tool.

Adfind, a tool that is able to query Active Directory, is then introduced to the system as searchindex.exe and then executed (cmd.exe /c SearchIndex.exe -sc u:<removed> > .\h.txt). Results are saved in the file h.txt. Using this information, the attackers are attempting to gain elevated privileges (e.g. domain administrator) to access the domain or laterally traverse the environment.

Recommended actions

Orion users should update to Orion Platform version 2020.2.1 HF 2.

Orion users should check their networks for indications of post-compromise activity, including:

- Use of Teardrop in-memory malware to drop Cobalt Strike Beacon.
- Command and control (C&C) infrastructure leaks the configured hostname in RDP SSL certificates. Scanning for your organization’s hostnames can uncover malicious IP addresses used by the attackers, indicating post-compromise activity.
- Geolocation of IP addresses used for remote access may reveal if a compromised account is being simultaneously used by a legitimate user and the attackers.
- The attackers use multiple IP addresses per VPS provider. If a malicious login from an unusual ASN is identified, other logins from that ASN may also be malicious.
- Logs for SMB sessions may show access to legitimate directories and follow a delete-create-execute-delete-create pattern in a short period of time.

It should be borne in mind that although there may be some commonalities in post-compromise activity, each victim is likely to see different patterns in activity. That activity is likely to involve heavy use of living-off-the-land techniques to minimize the likelihood of being detected, something the attackers seem to be prioritizing based on how they conducted the first stages of the attack.

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

Indicators of Compromise
