SEQURETEK

SolarWinds SUNBURST Backdoor Supply Chain Attack

OVERVIEW

Two federal agencies and FireEye were breached through updates of widely-used IT infrastructure management software - the Orion network monitoring product from SolarWinds.

SolarWinds update spread a digitally-signed component of the Orion software framework that contains a backdoor Sunburst that communicates via HTTP to third party servers.

KNOWLEDGE BASE REGISTER

- Version Control

Issue Date	Version	Prepared by	Approved by
15th Dec 2020	v 1.0	Vidhi Patel/Sameer Prabhu	Cdr. Subhash Dutta

OVERVIEW

- Last week FireEye disclosed that attackers had compromised their systems and had accessed their Red Team assessment tools. FireEye and other security organisations then discovered a global campaign that attacked the networks of public and private organizations through **a compromised version of SolarWinds Orion business software update to distribute malware called SUNBURST.**
- Inserting malicious code into legitimate software updates for the Orion software **allows an attacker remote access into the victim's environment.**
- SolarWinds is a hugely popular piece of server software used by hundreds of thousands of organizations globally, including most Fortune 500 companies and multiple U.S. federal agencies.
- SolarWinds Orion is used for centralized monitoring and management, usually employed in large networks to keep track of all IT resources, such as servers, workstations, mobiles, and IoT devices. **Attackers have targeted versions 2019.4 through 2020.2.1 of the SolarWinds Orion** platform that was released between March and June 2020.
- Attackers gained access to victims via trojanized updates to SolarWind's Orion IT monitoring and management software. Post initial compromise activity following this supply chain compromise has included lateral movement and data theft.

TECHNICAL DETAILS

- Sunburst has been widespread across organizations in an attack. It uses multiple obfuscated blacklists to identify security and anti-virus tools running as processes, services, and drivers. It stores this information for later stages of an attack.
- ***SolarWinds.Orion.Core.BusinessLayer.dll*** **is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third party servers.**
- Authorized system administrators fetch and install updates to SolarWinds Orion via packages distributed by SolarWinds's website.
- The update package *CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp* (02af7cec58b9a5da1c542b5a32151ba1) contains the *SolarWinds.Orion.Core.BusinessLayer.dll* described in this report.
- After installation, the Orion software framework executes the .NET program *SolarWinds.BusinessLayerHost.exe* to load plugins, including

SolarWinds.Orion.Core.BusinessLayer.dll. The malware masquerades its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity.

- This plugin contains many legitimate namespaces, classes, and routines that implement functionality within the Orion framework. Hidden in plain sight, the class *SolarWinds.Orion.Core.BusinessLayer.OrionImprovementBusinessLayer* implements an HTTP-based backdoor. Code within the logically unrelated routine *SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager.RefreshInternal* invokes the backdoor code when the Inventory Manager plugin is loaded.
- *SolarWinds.Orion.Core.BusinessLayer.dll* is signed by SolarWinds, using the certificate with serial number 0f:e9:73:75:20:22:a6:06:ad:f2:a3:6e:34:5d:c0:ed. The file was signed on March 24, 2020.

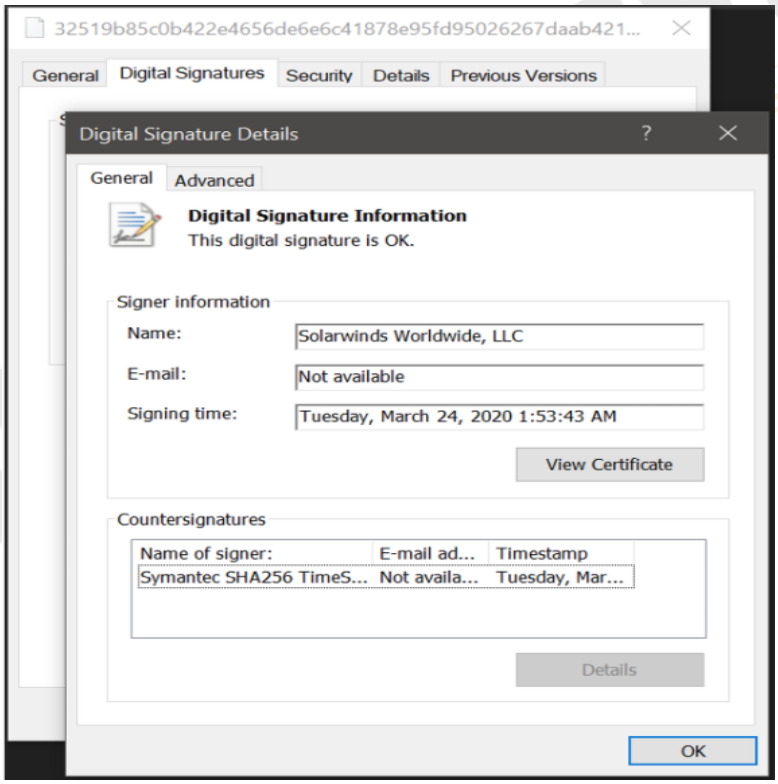

Figure 1: SolarWinds digital signature on software with backdoor

- On execution of the malicious *SolarWinds.Orion.Core.BusinessLayer.OrionImprovementBusinessLayer.Initialize* method the sample verifies that its lower-case process name hashes to the value which is matched with a process named "*solarwinds.businesslayerhost*".

- The malware only executes if the filesystem write time of the assembly is at least 12 to 14 days prior to the current time; the exact threshold is selected randomly from an interval. It continues to check by a legitimate recurring background task. Once the threshold is met, the sample creates the named pipe 583da945-62af-10e8-4902-a8f205c72b2e to act as a guard that only one instance is running before reading *SolarWinds.Orion.Core.BusinessLayer.dll.config* from disk and retrieving the XML field appSettings.
- The appSettings fields' keys are legitimate values that the malicious logic re-purposes as a persistent configuration.
- The malware checks that the machine is domain joined and retrieves the domain name before execution continues.
- A userID is generated by computing the MD5 of all network interface MAC addresses that are up is used to communicate with C2 servers.
- The backdoor determines its C2 server using a Domain Generation Algorithm (DGA) to construct and resolve a subdomain of *avsvmcloud[.]com*.
- If all blocklist and connectivity checks pass, the sample starts generating domains in a while loop via its DGA
- After an initial period off, it retrieves and execute commands **"Jobs"**, that transfer files, execute files, profiles the system, reboots the machine and disable system services.
- Backdoor's behaviour and network protocol blend in with legitimate SolarWinds activity, by masquerading as the OIP protocol and storing reconnaissance results within plugin configuration files.

INDICATORS OF COMPROMISE

IP ADDRESSES

13[.]59[.]205[.]66	34[.]203[.]203[.]23	204[.]188[.]205[.]176
54[.]193[.]127[.]66	139[.]99[.]115[.]204	51[.]89[.]125[.]18
54[.]215[.]192[.]52	5[.]252[.]177[.]21	167[.]114[.]213[.]199

URLs

6a57jk2ba1d9keg15cbg.appsync-api.eu-west-1.avsvmcloud[.]com

7sbvaemscs0mc925tb99.appsync-api.us-west-2.avsvmcloud[.]com

gq1h856599gqh538acqn.appsync-api.us-west-2.avsvmcloud[.]com

ihvpgv9psvq02ffo77et.appsync-api.us-east-2.avsvmcloud[.]com

k5kcubuassl3alrf7gm3.appsync-api.eu-west-1.avsvmcloud[.]com

mhdosoksaccf9sni9icp.appsync-api.eu-west-1.avsvmcloud[.]com

avsvmcloud[.]com	freescanonline[.]com	panhardware[.]com	virtualwebdata[.]com
databasegalore[.]com	globalnetworkissues[.]com	seobundlekit[.]com	websitetheme[.]com
deftsecurity[.]com	highdatabase[.]com	thedoccloud[.]com	zupertech[.]com
digitalcollege[.]org	incomeupdate[.]com	virtualdataserver[.]com	

FILE HASHES

MD5

FILE HASH	FILENAME
02AF7CEC58B9A5DA1C542B5A32151BA1	CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp
08E35543D6110ED11FDF558BB093D401	Solarwinds Worldwide, LLC
2C4A910A1299CDAE2A4E55988A2F102E	SolarWinds.Orion.Core.BusinessLayer.dll
846E27A652A5E1BFBD0DDD38A16DC865	SolarWinds.Orion.Core.BusinessLayer.dll
B91CE2FA41029F6955BFF20079468448	SolarWinds.Orion.Core.BusinessLayer.dll
4F2EB62FA529C0283B28D05DDD311FAE	OrionImprovementBusinessLayer.2.cs
56CEB6D0011D87B6E4D7023D7EF85676	app_web_logoimagehandler.ashx.b6031896.dll

SHA1

FILE HASH	FILENAME
1B476F58CA366B54F34D714FFCE3FD73CC30DB1A	CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp
47D92D49E6F7F296260DA1AF355F941EB25360C4	SolarWinds Worldwide, LLC
2F1A5A7411D015D01AAEE4535835400191645023	SolarWinds.Orion.Core.BusinessLayer.dll
D130BD75645C2433F88AC03E73395FBA172EF676	SolarWinds.Orion.Core.BusinessLayer.dll
76640508B1E7759E548771A5359EAED353BF1EEC	SolarWinds.Orion.Core.BusinessLayer.dll
C2C30B3A287D82F88753C85CFB11EC9EB1466BAD	OrionImprovementBusinessLayer.2.cs
75AF292F34789A1C782EA36C7127BF6106F595E8	app_web_logoimagehandler.ashx.b6031896.dll

SHA256

SHA256	FILENAME
D0D626DEB3F9484E649294A8DFA814C5568F846D5AA02D4CDAD5D041A29D5600	CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp
53F8DFC65169CCDA021B72A62E0C22A4DB7C4077F002FA742717D41B3C40F2C7	Solarwinds Worldwide, LLC
019085A76BA7126FFF22770D71BD901C325FC68AC55AA743327984E89F4B0134	SolarWinds.Orion.Core.BusinessLayer.dll
CE77D116A074DAB7A22A0FD4F2C1AB475F16EEC42E1DED3C0B0AA8211FE858D6	SolarWinds.Orion.Core.BusinessLayer.dll
32519B85C0B422E4656DE6E6C41878E95FD95026267DAAB4215EE59C107D6C77	SolarWinds.Orion.Core.BusinessLayer.dll
292327E5C94AFA352CC5A02CA273DF543F2020D0E76368FF96C84F4E90778712	OrionImprovementBusinessLayer.2.cs
C15ABAF51E78CA56C0376522D699C978217BF041A3BD3C71D09193EFA5717C71	app_web_logoimagehandler.ashx.b6031896.dll

PREVENTIVE AND CORRECTIVE DEFENCE ACTIONS

- **Preventive Actions**
  - Upgrade SolarWinds Orion Platform to version 2020.2.1 HF 2.
  - Block the IoCs in the corresponding security devices.
  - All these IoCs are combined in our Threat Intelligence Feed that is integrated with our SOC to provide proactive threat protection to our clients.
  - Employ content scanning and filtering on the organization mail servers. Inbound e-mails should be scanned for known threats and should block any attachment types that could pose a threat.
  - Update your Operating system and software to latest version.
  - Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
  - Do not trust emails from untrusted source.
  - Do not open links and attachments from untrusted sources.
  - Back-up data, store it outside of network connection.
  - Use strong password and change it at regular interval. Use multi-factor authentication.
  - Implement strict access control and auditing in your environment at operating system and network layers. Limit access to the Orion servers to only those authorized persons who require access as part of their duties.
  - Ensure you have installed the latest versions of the SolarWinds Orion Platform, including hotfixes and service releases.
  - Be careful not to expose your Orion Platform website on the public internet.
  - Disable unnecessary ports, protocols, and services on your host operating system and on applications, like SQL Server.
  - If you deploy multiple Orion servers in your environment, dedicate these servers where possible and minimize the installation of any third-party software.
  - Do not create local Orion-based accounts. We recommend at minimum utilizing Windows Authentication, or implementing a SAML v2 based solution, if you cannot integrate Windows or SAML-based authentication.
  - Apply proper segmentation controls on the network where you have deployed the SolarWinds Orion Platform.

- Corrective Actions
  - If infected, disconnect the affected system from the Network. Reset all credentials used by or stored in SolarWinds Orion.
  - Change passwords for accounts that have access to SolarWinds servers/infrastructure.
  - Inform the Information Security Team.
  - Use antivirus or anti-malware software to clean the malware.