EVAL PLAN

TRUEFORT

SolarWinds IoC

TRUEFORT

Table of Contents

Overview

A supply chain attack beginning in Spring 2020 of SolarWinds Orion platform has led to attackers compromising SolarWinds users' networks. *SolarWinds.Orion.Core.BusinessLayer.dll* is digitally signed by SolarWinds as part of the Orion software framework and contains a backdoor that communicates via HTTP to third-party servers.

Trojanized updates were digitally signed on SolarWinds site (*hxxps://downloads.solarwinds[.]com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.20574/SolarWinds-Core-v2019.4.5220-Hotfix5.msp*).

Once the update is installed, the malicious DLL is loaded into the legitimate *SolarWinds.BusinessLayerHost.exe* or *SolarWinds.BusinessLayerHostx64.exe*.

About two weeks later DNS queries are made for *avsvmcloud[.]com*. CNAME responses will point to the command-and-control domain.

Subdomains are generated by concatenating a victim User ID with a reversible encoding of the victim's local machine domain name. The attacker likely utilizes the DGA subdomain to vary the DNS response to victims as a means to control the targeting of the malware. These subdomains are concatenated with one of the following to create the hostname to resolve:

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

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

.appsync-api.us-east-1[.]avsvmcloud[.]com

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

Once loaded, the backdoor goes through an extensive list of checks to make sure it is running in an actual enterprise network and not on an analyst's machines. It then contacts and connects to the command-and-control (C2) server.

Indicators of Compromise

DNS Lookups

Any DNS queries containing the following FQDN's are an indication of compromise.

Associated Malware	DNS Record Type	FQDN	IP	Target
SUNBURST	CNAME	6a57jk2ba1d9keg15cbg.appsync-api.eu-west-1.avsvmcloud[.]com		freescanonline[.]com
SUNBURST	CNAME	7sbvaemscs0mc925tb99.appsync-api.us-west-2.avsvmcloud[.]com		deftsecurity[.]com
SUNBURST	CNAME	gq1h856599gqh538acqn.appsync-api.us-west-2.avsvmcloud[.]com		freescanonline[.]com
SUNBURST	CNAME	ihvpgv9psvq02ffo77et.appsync-api.us-east-2.avsvmcloud[.]com		thedoccloud[.]com
SUNBURST	CNAME	k5kcubuassl3alrf7gm3.appsync-api.eu-west-1.avsvmcloud[.]com		thedoccloud[.]com
SUNBURST	CNAME	mhdosoksaccf9sni9icp.appsync-api.eu-west-1.avsvmcloud[.]com		thedoccloud[.]com
SUNBURST	A	deftsecurity[.]com	13.59.205.66	
SUNBURST	A	freescanonline[.]com	54.193.127.66	
SUNBURST	A	thedoccloud[.]com	54.215.192.52	
SUNBURST	A	websitetheme[.]com	34.203.203.23	
SUNBURST	A	highdatabase[.]com	139.99.115.204	
BEACON	A	incomeupdate[.]com	5.252.177.25	
	A	databasegalore[.]com	5.252.177.21	
	A	panhardware[.]com	204.188.205.176	
	A	zupertech[.]com	51.89.125.18	
	A	zupertech[.]com	167.114.213.199	

Foreign IP Addresses

[See excel workbook]

Any connections made to these IP's are an indication of compromise. Most traffic will appear over port 80 but it is possible other protocols may be used. Any traffic to these addresses should be considered malicious.

File Hashes

[See excel workbook]

Files specified have been identified as malicious by researchers and indicate compromise even though they may have valid signatures from SolarWinds. File hashes have also been provided to confirm a file is known as being malicious.

SUPPLY CHAIN ATTACK
Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE
When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

DEFENSE EVASION
The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

RECON
The backdoor gathers system info

INITIAL C2
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

EXFILTRATION
The backdoor sends gathered information to the attacker.

HANDS-ON-KEYBOARD ATTACK
The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.

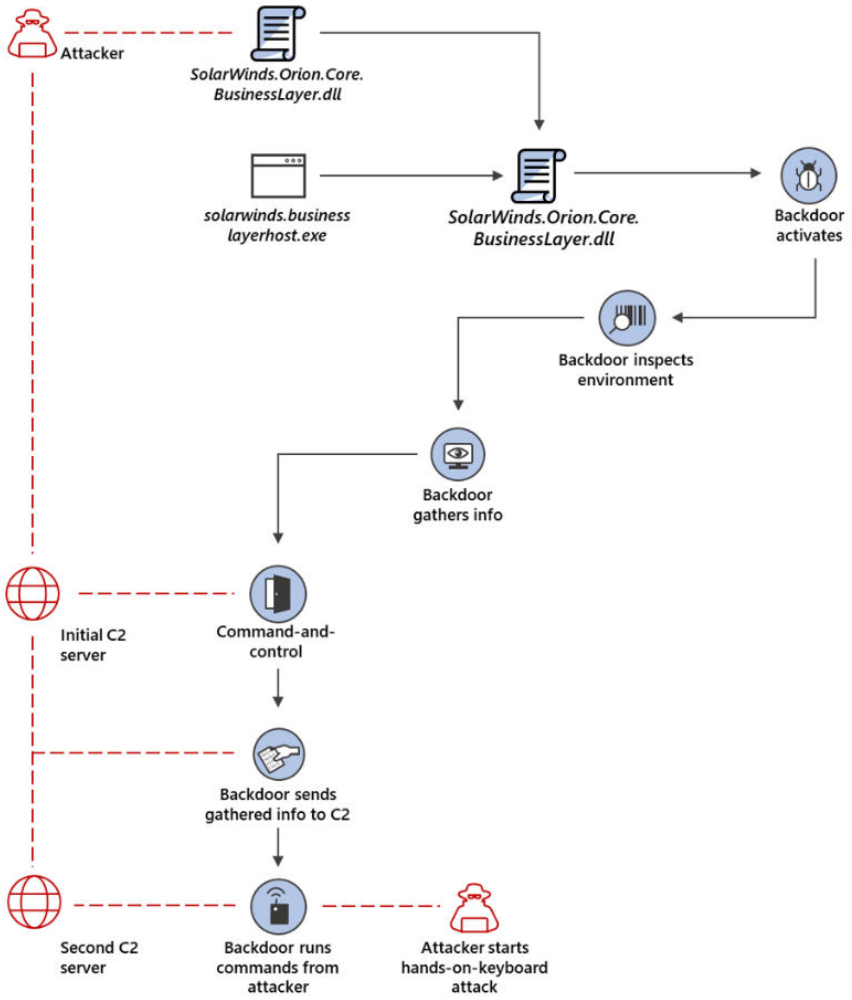

Figure 1. Infection Chain | Credit Microsoft

Reporter Queries

Historical Network Metric Dashboard

Foreign Addresses historically determined to resolve avsvmcloud.com

foreignAddress:50.63.202* OR foreignAddress:107.161.23.204 OR foreignAddress:184.168.221* OR foreignAddress:192.161.187.200 OR foreignAddress:209.141.38.71

Foreign addresses specified by FireEye

foreignAddress:13.59.205.66 OR foreignAddress:54.193.127.66 OR foreignAddress:54.215.192.52 OR foreignAddress:34.203.203.23 OR foreignAddress:139.99.115.204 OR foreignAddress:5.252.177.25 OR foreignAddress:5.252.177.21 OR foreignAddress:204.188.205.176 OR foreignAddress:51.89.125.18 OR foreignAddress:167.114.213.199

Incoming BusinessLayer command from local net

command:*BusinessLayer* AND foreignAddress:10.*

Compromised exe that is communicating outside the network

command:*BusinessLayer* AND foreignPort:80 AND NOT foreignAddress:10.* AND NOT foreignAddress:fe80*

Lateral movement

foreignPort:3389 OR foreignPort:22 OR foreignPort:5900

Top Users Dashboard

Users running BusinessLayerHost

Command: *BusinessLayer*

Resources

FireEye Blog Post

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

FireEye GitHub

https://github.com/fireeye/sunburst_countermeasures

Microsoft Blog Post

https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

SecurityTrails Historical DNS Records

https://securitytrails.com/domain/avsvmcloud.com/history/a

VirusTotal Graph

https://www.virustotal.com/graph/embed/g8c1baece7cab4e1aae553271df8772f8ca1dcaa7b1d84c508982f294f3ea45c8