FireEye, Microsoft create kill switch for SolarWinds backdoor

bleepingcomputer.com/news/security/fireeye-microsoft-create-kill-switch-for-solarwinds-backdoor/

Lawrence Abrams

By
Lawrence Abrams

- December 16, 2020
- 04:21 PM
- 1

Microsoft, FireEye, and GoDaddy have collaborated to create a kill switch for the SolarWinds Sunburst backdoor that forces the malware to terminate itself.

This past weekend it was revealed that Russian state-sponsored hackers breached SolarWinds and added malicious code to a Windows DLL file used by their Orion IT monitoring platform.

This malicious DLL is a backdoor tracked as Solarigate (Microsoft) or Sunburst (FireEye) and was distributed via SolarWinds' auto-update mechanism to approximately 18,000 customers, including the U.S. Treasury, US NTIA, and the U.S. Department of Homeland Security.

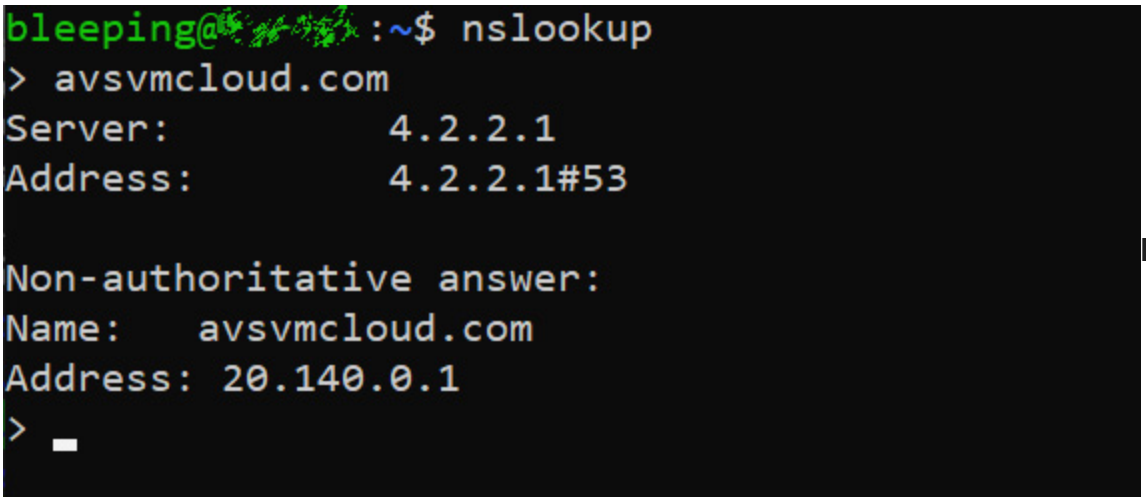
As part of a coordinated disclosure with Microsoft and SolarWinds, FireEye released a report on Sunday with an analysis of the supply chain attack and how the Sunburst backdoor operates. This research revealed that the Sunburst backdoor would connect to a

command and control (C2) server at a subdomain of avsvmcloud[.]com to receive 'jobs', or commands to execute.

The FireEye report also revealed that if the C2 server resolved to an IP address in one of the following ranges, the malware would terminate and update a setting, so the malware never executes again.

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- 224.0.0.0/3
- fc00:: - fe00::
- fec0:: - ffc0::
- ff00:: - ff00::
- 20.140.0.0/15
- 96.31.172.0/24
- 131.228.12.0/22
- 144.86.226.0/24

Yesterday, the command and control server domain, avsvmcloud[.]com, was seized and now resolves to the IP address 20.140.0.1, which belongs to Microsoft. This domain takeover allows Microsoft and its partners to sinkhole the malicious traffic and analyze it to identify further victims.



DNS lookup of C2

FireEye and Microsoft create a Sunburst kill switch

Today, Brian Krebs was the first to reveal that FireEye, Microsoft, and Godaddy collaborated to create a kill switch for the Sunburst malware.

In a statement also sent to BleepingComputer, FireEye explains that they used the avsvmcloud[.]com takeover to create a kill switch that unloads the Sunburst malware on infected machines.

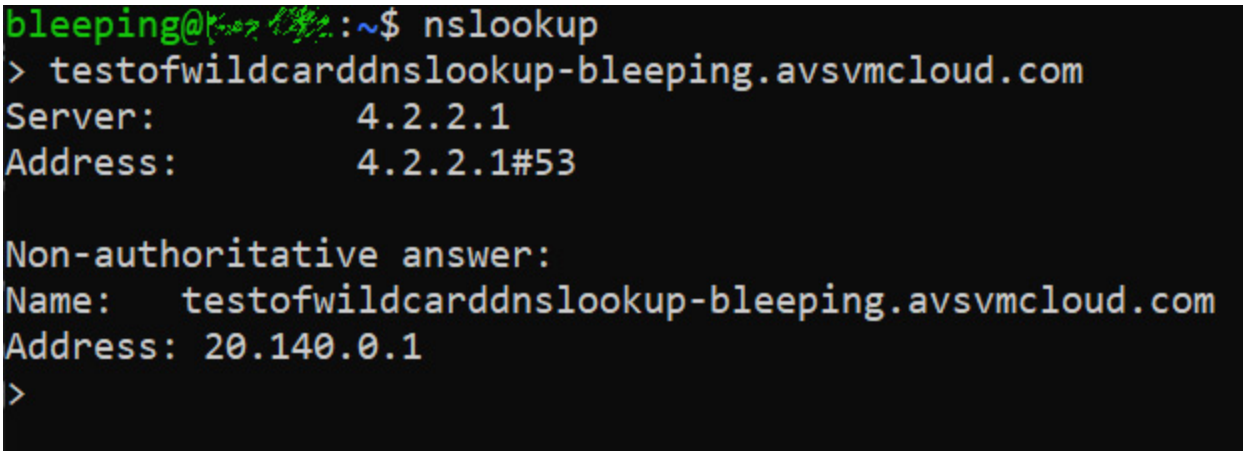
"SUNBURST is the malware that was distributed through SolarWinds software. As part of FireEye's analysis of SUNBURST, we identified a killswitch that would prevent SUNBURST from continuing to operate."

"Depending on the IP address returned when the malware resolves avsvmcloud[.]com, under certain conditions, the malware would terminate itself and prevent further execution. FireEye collaborated with GoDaddy and Microsoft to deactivate SUNBURST infections."

"This killswitch will affect new and previous SUNBURST infections by disabling SUNBURST deployments that are still beaconing to avsvmcloud[.]com," FireEye told BleepingComputer in a statement.

While FireEye does not provide specific details regarding the kill switch, we can see how the kill switch works from their previous analysis.

As part of this collaboration, GoDaddy has created a wildcard DNS resolution so that any subdomain of avsvmcloud[.]com resolves to 20.140.0.1. This is illustrated by a DNS lookup for a made-up subdomain, as shown below.



Wildcard DNS resolution for avsvmcloud[.]com

Due to this wildcard DNS resolution, when an infected machine tries to connect to its command and control server under the avsvmcloud[.]com domain, the subdomain will always resolve to the 20.140.0.1 IP address. As this IP address is part of the 20.140.0.0/15 range that is on the malware block list, it will cause the malware to terminate and prevent itself from executing again.

Microsoft IP address ranges were likely added to the block list to prevent their security operations from detecting the malicious activity.

FireEye warned that this kill switch would only terminate the original Sunburst infection. Organizations that were already breached by the threat actors likely have different methods to access the victim's network.

"However, in the intrusions FireEye has seen, this actor moved quickly to establish additional persistent mechanisms to access to victim networks beyond the SUNBURST backdoor. This killswitch will not remove the actor from victim networks where they have established other backdoors. However, it will make it more difficult to for the actor to leverage the previously distributed versions of SUNBURST," FireEye warned about the kill switch.

If is not known if the victims identified via the sinkhole/kill switch are being notified that they are compromised.

BleepingComputer has contacted Microsoft with questions related to the kill switch but was told they had nothing to share at this time.

Related Articles:

Microsoft: Windows 11 22H2 has reached RTM with build 22621

DuckDuckGo browser allows Microsoft trackers due to search agreement

Microsoft tests new Windows 11 Desktop search that only works with Edge

Get more from Microsoft Office with this training suite deal

Microsoft releases first ISO image for new Windows 11 Dev builds

- Command and Control
- Kill Switch
- Microsoft
- SolarWinds
- Solorigate
- Sunburst

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

Some-Other-Guy - 1 year ago

-
-

Organizations that were already breached by the threat actors likely have different methods to access the victim's network. "However, in the intrusions FireEye has seen, this actor moved quickly to establish additional persistent mechanisms to access to victim networks beyond the SUNBURST backdoor. This killswitch will not remove the actor from victim networks where they have established other backdoors.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: