What We Have Learned So Far about the “Sunburst”/SolarWinds Hack | FortiGuard labs

By Udi Yavo

Published: 2020-12-21 · Archived: 2026-04-06 00:04:05 UTC

Introduction

Recently, it was reported that a nation-state threat-actor managed to infiltrate a large number of organizations—including multiple US government agencies. They did this by distributing backdoor software, dubbed SunBurst, by compromising SolarWind’s Orion IT monitoring and management software update system. Based on SolarWind’s data, 33,000 organizations use Orion’s software, and 18,000 were directly impacted by this malicious update. As more and more details have become available, it has become clear that this is one of the most evasive and significant cyberattacks to date.

Over the past week, the FortiGuard Labs research teams have worked tirelessly to uncover more details on the attack to ensure our customers are protected, details of which can be found in our Threat Signal Blog. In this blog, we share more detail on what we have learned, the protections currently provided by products in our portfolio, as well as the proactive steps we have taken leveraging our FortiEDR platform to ensure the security of our customers.

SunBurst Campaign Overview

To help readers better understand this campaign, I will describe at a high-level the steps taken by the SunBurst malware and the threat actor after the initial infiltration.

After a successful infiltration of the supply-chain, the SunBurst backdoor— a file named SolarWinds.Orion.Core.BusinessLayer.dll—was inserted into the software distribution system and installed as part of an update package from the vendor. Once downloaded, it then lies dormant for 12 to 14 days before taking any action. Once the waiting period is over, the Backdoor takes steps to ensure it is running in one of the environments targeted by the attacker, as opposed to a lower value organization, or in a sandbox or other malware analysis environment. The attacker appears to have wanted to stay as far below the industry’s radar as possible while carrying out its specific mission.

Here is a high-level overview of the steps it takes to do so:

- Machine domain name validation. It checks the domain name of the compromised machine to ensure:
  - It doesn’t contain certain strings.
  - It is not a SolarWinds domain.
  - It doesn’t contain the string ‘test’.
- It validates that no analysis tools, such as WireShark, are running.

- It also checks to ensure that unwanted security software is not running.

Once all of the validations are completed, it calls home to the threat actor and sends information to identify the breached organization. ***Note***: Since most of the organizations breached by this malware were NOT a target of the threat actor, this is where the attack appears to have ended for many organizations.

The C2 domain name is composed from a prefix that is generated based on data from the machine. An example domain can be seen in Figure 1:

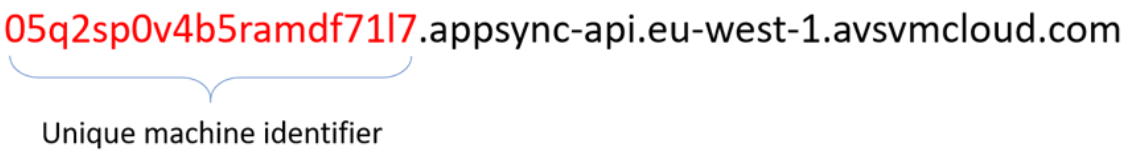

Figure 1: Example of SunBurst-generated domain

As a next step, the threat actor leverages a memory-only payload called TEARDROP to deliver a CobaltStrike BEACON, among other payloads. CobaltStrike is a commercially available, full-featured penetration testing toolkit that advertises itself as "adversary simulation software." However, it is also commonly used by attackers. To date, FortiEDR has actively detected and blocked many attacks leveraging CobaltStrike in real-time, including this one.

Proactive SunBurst Campaign Mitigations

As soon as the IOCs were disclosed, or otherwise uncovered though investigation, the FortiGuard Labs and other teams analyzed all of the data on “Sunburst” and then devised a proactive strategy to mitigate the attack as well as to help organizations understand its impact.

As mentioned, most organizations were not targeted, and therefore the existence of the malicious DLL file does not necessarily mean that actual damage was done.

Steps Fortinet is Taking to Ensure the Security of our Customers:

1. All published and subsequent IOCs were immediately added to our Cloud intelligence and signatures databases to ensure detection of the malicious files by Fortinet’s security solutions, including FortiGate, FortiSIEM, FortiSandbox, FortiEDR, FortiAnalyzer, and FortiClient. As new IOCs are uncovered, they will also be immediately added to our databases.

2. In order to reconstruct the attack and gain more insights and indicators, FortiGuard Labs research and intelligence teams started to hunt for more indicators based on the initially disclosed data. As part of this effort, we have discovered and analyzed a new variant of TEARDROP. In Figure 2, you can see this TEARDROP variant read the fake jpeg header and its main unpacking routine:

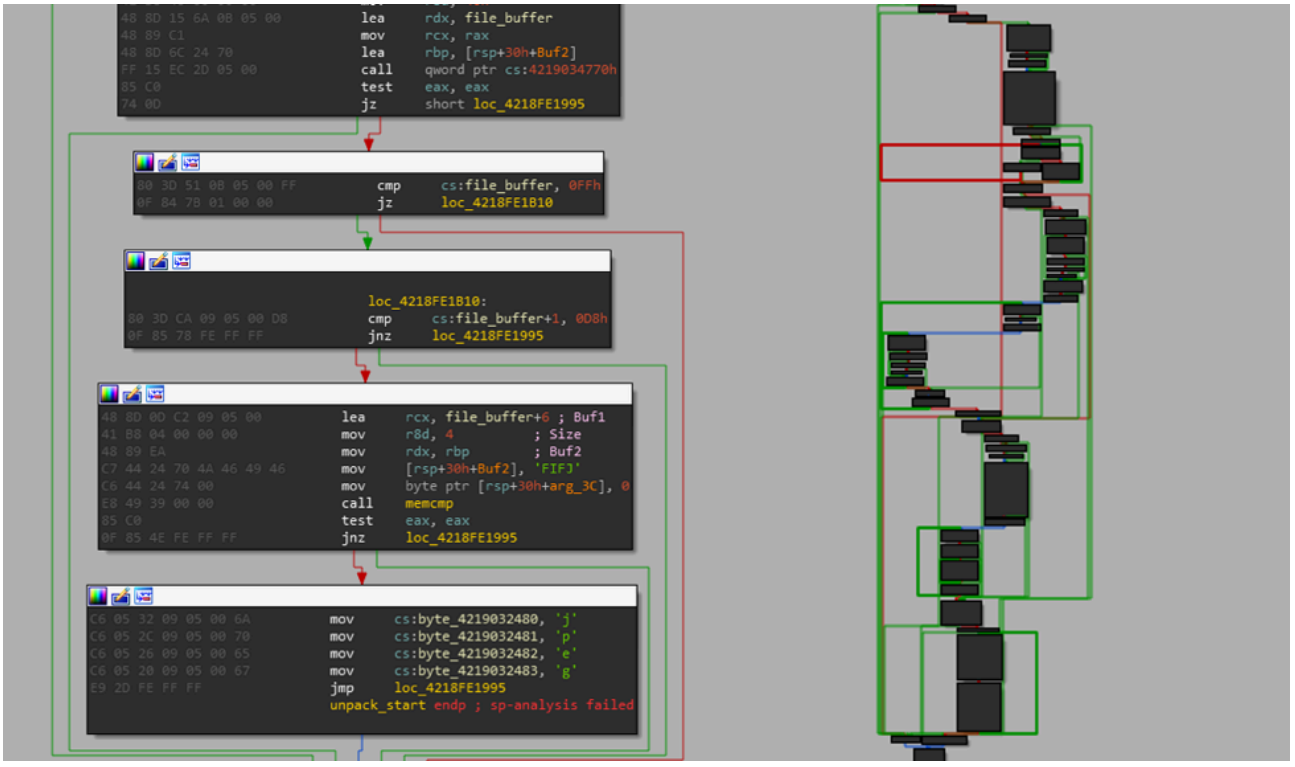

Figure 2: TEARDROP under the microscope

3. We also proactively scanned our FortiEDR Cloud data lake for indicators to determine if customers may have been breached. Customers that were potentially impacted are being contacted.

4. Our MDR and FortiEDR research teams have also devised tools that can help organizations understand the scope of a breach in case they have been impacted by this supply-chain attack. These tools are being shared with customers upon request. As mentioned, most organizations were not targeted, and understanding the scope of the breach is critical for determining follow-up steps.

TEARDROP and CobaltStrike Detection

In addition to detection based on specific IOCs, analysis by our research teams has determined that the FortiEDR platform is and was capable of protecting devices against CobaltStrike and TEARDROP—out-of-the-box and without any prior knowledge of the threat—using its memory code tracing technology. FortiEDR has proven countless times that it is capable of blocking CobaltStrike in real-time during live incidents. An example of such a detection can be seen in Figure 3:

Figure 3: Real-World Detection of Cobalt-Strike by FortiEDR

Summary and Recommendations

1. Endpoint protection - Fortinet and SolarWinds Orion 2019.4 through 2020.2.1 HF1 customers

a. FortiClient, FortiEDR, and FortiGate all detect and block the execution of these malicious files.

b. By design, any supported version of FortiEDR will detect and protect against the weaponized, post-execution consequences of this attack out of the box. No change or upgrade to the platform is required.

i. Make sure to set post-execution policies to blocking mode. This will allow you to block malicious behavior even if the system is already compromised through a trusted source, such as this supply chain attack.

ii. Apply contextual pre-canned policies that can enable proactive actions in case of malicious or inconclusive activities. In this case, these actions would have removed the associated DLL file.

c. If you subscribe to the MDR service or were not in protection mode at the time of the attack, please work with the MDR team to assist you with proactive threat hunting.

2. Endpoint protection - Non-Fortinet and SolarWinds Orion 2019.4 through 2020.2.1 HF1 customers

a. Run forensics to validate the existence of the known malicious files based on published IOCs (SHA-1 hashes):

d130bd75645c2433f88ac03e73395fba172ef676
76640508b1e7759e548771a5359eaed353bf1eec
2f1a5a7411d015d01aaee4535835400191645023
395da6d4f3c890295f7584132ea73d759bd9d094
1acf3108bf1e376c8848fbb25dc87424f2c2a39c
e257236206e99f5a5c62035c9c59c57206728b28
6fdd82b7ca1c1f0ec67c05b36d14c9517065353b
bcb5a4dcbc60d26a5f619518f2cfc1b4bb4e4387
16505d0b929d80ad1680f993c02954cfd3772207
d8938528d68aabe1e31df485eb3f75c8a925b5d9
c8b7f28230ea8fbf441c64fdd3feeba88607069e
2841391dfbffa02341333dd34f5298071730366a
2546b0e82aecfe987c318c7ad1d00f9fa11cd305
e2152737bed988c0939c900037890d1244d9a30e

b. Threat hunt your memory for IOCs looking for TEARDROP or COBALT STRIKE. The relevant YARA signatures are listed here.

c. Hunt for suspicious dropped files based on the timeline of initial infections in your organization. One potential IOC is the existence of the following malicious DLL file:

c:\Windows\SysWOW64\netsetupsvc.dll file.

d. If any of these IOCs are detected, consider all affected machines—along with all user accounts on these machines—as compromised. Revoke all account credentials and isolate the devices for further investigation.

Best Practices

This event reemphasizes the need for best practices when it comes to maintaining software and systems. Here are three essential security best practices every organization should adopt:

- All new updates and patches should be run through a sandbox or similar analysis tool before being deployed to identify malware and supply-chain attacks. In this case, FortiSandbox would have identified the offending DLL file as malicious and removed it before it could impact the network.
- Advanced Endpoint Detection and Response technology is now an essential component of any security strategy. Deploying FortiEDR on endpoints and servers would have prevented malware such as CobaltStrike and TEARDROP from executing.
- Network segmentation is another critical security strategy required to protect today's advanced networks. Deploying a segmentation firewall as part of a Zero-Trust Network strategy, such as the FortiGate platform, would prevent malware from spreading across the network.

Additional Help

Enterprises seeking assistance in understanding their organizations exposure to this cyber campaign and/or who are leveraging the FortiEDR solution for prevention or detection of similar attacks can contact us (at no charge for a limited time) through the FortiGuard Incident Response services webpage.

Learn more about FortiGuard Labs threat research and the FortiGuard Security Subscriptions and Services portfolio.

Learn more about Fortinet's free cybersecurity training initiative or about the Fortinet NSE Training program, Security Academy program, and Veterans program.
