Threat Brief: SolarStorm and SUNBURST Customer Coverage

By Unit 42

Published: 2020-12-15 · Archived: 2026-04-05 13:27:54 UTC

Executive Summary

On Sunday, Dec. 13, FireEye released information related to a breach and data exfiltration originating from an unknown actor FireEye is calling UNC2452. Unit 42 tracks this and related activity as the group named SolarStorm, and has published an ATOM containing the observed techniques, IOCs and relevant courses of action in the Unit 42 ATOM Viewer. According to FireEye, SolarStorm has compromised organizations across the globe via a supply chain attack that consists of a trojanized update file for the SolarWinds Orion Platform.

FireEye's blog, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor," contains a wealth of useful information, all of which has been analyzed by Unit 42 researchers to help ensure Palo Alto Networks customers are protected.

Any organization utilizing SolarWinds Orion IT management software is potentially at risk from this threat. These organizations should immediately identify Orion systems in their network, determine if they are compromised with the SUNBURST backdoor and seek out further evidence of compromise. Instructions on how to perform these tasks using the Palo Alto Networks Next Generation Firewall, Cortex XDR and XSOAR are available in this report, as well as additional resources and indicators of compromise (IOCs). Palo Alto Networks has also launched SolarStorm Rapid Response Programs.

The details of this attack and its impact continue to evolve. We will update this report with new details as they become available.

What's Known About SolarStorm and SUNBURST

- SolarStorm specifically targeted supply chains during their attack on SolarWinds' Orion IT performance and statistics monitoring software.
- SolarStorm is a highly skilled threat actor, with a significant operational security mindset, as can be observed in its post-exploitation activity.
- SolarWinds recently filed an SEC report indicating that, while they have over 300,000 customers, fewer than 18,000 customers were running the trojanized version of the Orion software.
- SolarStorm threat actors created a legitimate digitally signed backdoor, SUNBURST, as a trojanized version of a SolarWinds Orion plug-in. The trojanized software acts as a powerful supply chain infiltration mechanism for delivery.
- SUNBURST has been observed delivering multiple payloads, mostly focused on memory-only droppers, such as the FireEye-dubbed TEARDROP and Cobalt Strike BEACON.
- SUNBURST's command and control (C2) traffic masquerades as legitimate Orion Improvement Program traffic.
- FireEye has released signatures and specific indicators to help identify SolarStorm's activity.

FireEye's research has been a cornerstone in providing not only useful signatures, but also indicators which help with tracking and hunting for SolarStorm activity. A synopsis of those indicators is included below.

SUNBURST

At the time of this publication, the Windows Installer Patch file including the trojanized version of the SolarWinds Orion product was still reachable:

Filename: SolarWinds-Core-v2019.4.5220-Hotfix5.msp
SHA256: d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600

This installer contains:

- Legitimate SolarWinds Orion update components.
- A digitally signed SUNBURST backdoor, and its legitimate configuration file:
    - SHA256: 32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
        - Filename: SolarWinds.Orion.Core.BusinessLayer.dll
        - Certificate SN: 0f:e9:73:75:20:22:a6:06:ad:f2:a3:6e:34:5d:c0:ed
    - SHA256: efbec6863f4330dbb702cc43a85a0a7c29d79fde0f7d66eac9a3be43493cab4f
        - Filename: SolarWinds.Orion.Core.BusinessLayer.dll.config

The infrastructure related to this series of attacks includes:

- Trojanized update file hosted at:
    - hxxps://downloads.solarwinds[.]com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.20574/SolarWinds-Core-v2019.4.5220-Hotfix5.msp
- DGA-generated C2s as subdomains of:
    - avsvmcloud[.]com
- C2 domains found during SUNBURST incidents, including CNAME records, or subsequent phases of the incident, such as BEACON components:
    - freescanonline[.]com
    - deftsecurity[.]com
    - thedoccloud[.]com
    - websitetheme[.]com
    - highdatabase[.]com
    - incomeupdate[.]com
    - databasegalore[.]com
    - panhardware[.]com
    - Zupertech[.]com
    - Virtualdataserver[.]com
    - digitalcollege[.]org
    - solartrackingsystem[.]net
    - webcodez[.]com
    - seobundlekit[.]com
    - virtualwebdata[.]com
    - lcomputers[.]com
    - avsvmcloud[.]com
    - Mobilnweb[.]com
    - kubecloud[.]com

TEARDROP

SUNBURST deployed several different payloads, and in at least one instance, a memory-only dropper FireEye dubbed TEARDROP to deploy a Cobalt Strike BEACON. During analysis of the information available, Unit 42 identified related activity involving TEARDROP malware that was used to execute a customized Cobalt Strike BEACON. This sample contains a beacon request to the *previously unreported domain* mobilnweb[.]com.

The TEARDROP DLL has a SHA256 of: 118189f90da3788362fe85eafa555298423e21ec37f147f3bf88c61d4cd46c51

and contains a beacon request for the URI /2019/Person-With-Parnters-Brands-Our/ with the User-Agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36. Within that same configuration, we also observed an additional URI setting containing the string /2019/This-Person-Two-Join-With/.

Protecting Our Customers

As of the time of writing, based on signatures and observables that have been released, Palo Alto Networks customers are protected across our product ecosystem, with specific protections deployed or being deployed in the following products and subscriptions for the Next-Generation Firewall (NGFW). It is imperative for customers to employ the best practices for Palo Alto Networks products in order to ensure your appliances are configured in a manner best suited for your protection.

Due to the nature of these attacks, we recommend our customers perform the following searches immediately. If you are unable, Palo Alto Networks will help you locate SolarWinds Orion servers owned by your organization and assess whether you've been compromised free of charge. After we've completed our analysis, we'll provide you with a SolarStorm Assessment Report brought to you by Expanse and Crypsis.

Cortex XDR

Cortex XDR customers are protected using the product's WildFire integration, as well as through Local Analysis, the Password Theft Protection module and the Behavioral Threat Protection (BTP) engine. Protections are continually being evaluated, developed and deployed for Cortex XDR.

Cortex XDR Managed Threat Hunting

Our Cortex XDR Managed Threat Hunting Team (MTH) has proactively searched all Cortex XDR Pro customer logs to identify potentially impacted organizations and provide them an assessment of their risk. Leverage the power of automation with Cortex XSOAR to speed up the discovery of SolarWind installations within your network, uncover signs of potential SolarStorm activity and automate response actions such as the quarantining of compromised endpoints.

WildFire (NGFW security subscription)

Customers using WildFire are protected from downloading known SUNBURST backdoor files and Cobalt Strike BEACON files associated with SolarStorm.

Gap analysis and threat hunting leveraging the FireEye-provided Yara signatures and observables has enabled Unit 42 researchers to identify potential malware samples. We continue to seek out new malware associated with SolarStorm, build and deploy protections for them within WildFire.

AutoFocus

AutoFocus customers can track SolarStorm's activity in the tags SolarStorm, SUPERNOVA, TEARDROP and SUNBURST.

IoT Security (NGFW security subscriptions)

The IoT Security subscription has the capability of identifying SolarWinds servers. These devices are being added to the IoT Security user portal UI, and the Device-ID attribute will be pushed to PAN-OS. These devices will be displayed to users as "SolarWinds Network Management Device" within the IoT Security user portal UI. In PAN-OS, users will see the Device-ID attribute "Profile" = "SolarWinds Network Management Device". This feature will be enabled for all IoT Security customers this week.

Threat Prevention DNS Security (NGFW security subscriptions)

Threat Prevention and DNS Security provide protection against C2 beacons and associated traffic. Protections are continually being evaluated, developed and deployed for Threat Prevention subscription.

The following threat prevention signatures have been added with Content version 8354:

Snort Rule	PANW UTID
Backdoor.BEACON_5.snort	86237
Backdoor.BEACON_6.snort	86238
Backdoor.SUNBURST_11.snort	86239
Backdoor.SUNBURST_14.snort	86240
Backdoor.BEACON_7.snort	86242
Backdoor.SUNBURST_12.snort	86243
Backdoor.BEACON_8.snort	86244
Backdoor.SUNBURST_13.snort	86245
Backdoor.SUNBURST_1.snort	86246
Backdoor.SUNBURST_10.snort	86247
Backdoor.BEACON_2.snort	86248
Backdoor.BEACON.snort	86249
Backdoor.BEACON_0.snort	86250
Backdoor.BEACON_1.snort	86251

Table 1: Snort to PANW UTID

URL Filtering (NGFW security subscription)

As of the time of writing, associated infrastructure described in this blog have accurate verdicts of malware.

Continue Reading: ***SolarStorm Response With Next-Generation Firewall***

Back to Top

Source: https://unit42.paloaltonetworks.com/fireeye-solarstorm-sunburst/