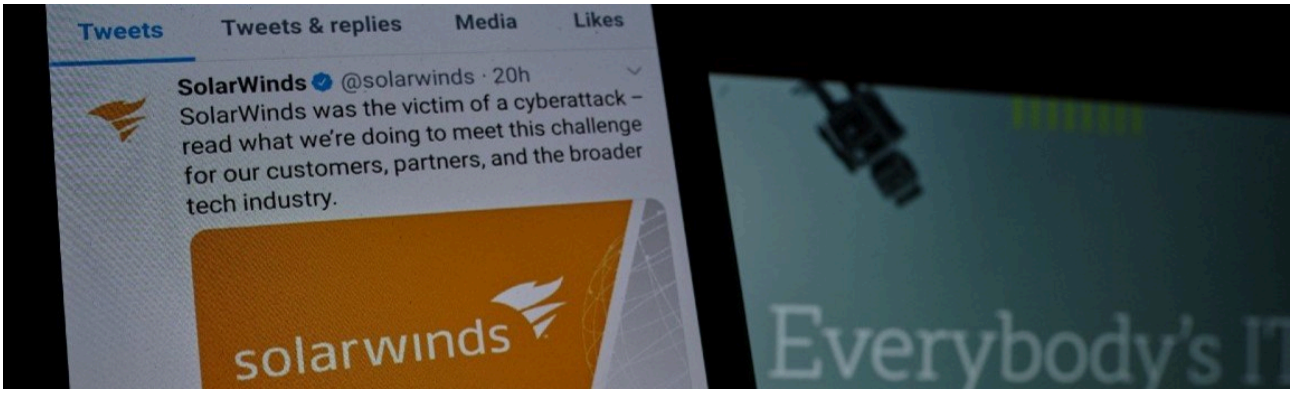
SOLARWINDS HACK - Sunburst, Supernova and more - CYFIRMA

By adminanna

Published: 2020-12-24 · Archived: 2026-04-05 20:28:09 UTC

Published On : 2020-12-24



Research on this cyberattack is ongoing. Its full magnitude and impact are still under investigation. This report will be updated by CYFIRMA researchers as new data comes to light.

Report covers the following:

OUTLINE

1. Summary
2. Introduction
3. Key Findings
4. Suspected Threat Actors
5. Insights
6. YARA Rules
7. Recommendations
8. Indicators of Compromise
9. Extract of List of Organizations affected by the campaign (As of 21 December 2020)

SUMMARY

Attack Vector: Vulnerabilities and Exploits, Steganography
Objective: Lateral Movement, Data Exfiltration, Credential Theft
Suspected Hacker Group: Unknown Russian Groups <Reach out to CYFIRMA for details>
Target Country: Global

Target Industry: Government agencies, Universities, Manufacturing, Hospitals, Telco and Technology, Semiconductor, Retail, Financial, and many more
Type of Attack: Supply Chain
Target Technology: SolarWinds – Orion Platform 2019.4 HF 5, 2020.2 with no hotfix, and 2020.2 HF 1
Detected Date: 13 December 2020
Attack Status: On-going
Risk Rate: High

INTRODUCTION

As per researchers, threat actors have gained access to numerous institutions and organizations around the world in a widespread campaign, known as UNC2452. This was executed by trojanizing SolarWinds Orion business software updates that inserted a vulnerability (SUNBURST) within their Orion Platform software builds for versions 2019.4 HF 5, 2020.2 with no hotfix, and 2020.2 HF 1, which, if present and activated, potentially allowed attackers to compromise the server on which the Orion products run.

Subsequent activity after this supply chain compromise has included lateral movement and data theft. The campaign is the work of a highly qualified set of possibly state-sponsored threat actors and the operation was carried out with significant operational efficacy and competency.

The cyberattack, which began to be exploited last spring, targeted numerous entities of the US administration, in addition to public and private organizations from around the world. Potentially attributed to Russia, it would be one of the most unsettling attacks identified in years.

In the subsequent analysis of the trojanized Orion artifacts, the .NET .dll app_web_logoimagehandler.ashx.b6031896.dll was dubbed SUPERNOVA, details of its operations are still being uncovered and progressively getting explored publicly.

After an initial period of inactivity of up to two weeks, the backdoors recover and run commands, called “Jobs,” which include the ability to transfer files, run files, profile the system, reboot the machine, and disable system services. The malware disguises its network traffic as the Orion Improvement Program (OIP) protocol and stores the recognition results within legitimate plug-in configuration files, allowing it to integrate with legitimate SolarWinds activity. The backdoors use multiple obfuscated block lists to identify forensic and antivirus tools running as processes, services, and drivers.

KEY FINDINGS

Post-compromise behavior following this supply chain compromise involved lateral movement and data theft. The campaign is the work of a highly-skilled threat actor and the operation was conducted with significant operational proficiency and persistence.

Traces of SUPERNOVA (Latest)

By analyzing artifacts from the SolarWinds Orion supply chain attack, security researchers uncovered another backdoor, likely coming from a different threat actor. Dubbed SUPERNOVA, the malware is a webshell planted in

the code of the Orion network and application monitoring platform and has allowed adversaries to execute arbitrary code on machines running the Trojan horse version of the software.

The webshell is a Trojan variant of a legitimate .NET library (app_web_logoimagehandler.ashx.b6031896.dll) present in the SolarWinds Orion software, modified to allow it to bypass automated defense mechanisms. Orion software uses the DLL to expose an HTTP API, allowing the host to respond to other subsystems when requesting a specific GIF image.

Researchers analysing the DLL concluded that malware could escape even manual analysis, as the code implemented in the legitimate DLL is harmless and of "relatively high quality". Threat actors have added four new parameters to the legitimate SolarWinds file to receive signals from the command and control infrastructure (C2).

The malicious code contains a unique method, DynamicRun, that compiles the parameters to an in-memory .NET assembly on the fly, leaving no artifacts on the disk of a compromised device. In this way, the attacker can send arbitrary code to the infected device and execute it in the context of the user, who most often has elevated privileges and visibility on the network.

Most webshells run their payloads in the context of the runtime environment or by calling a subshell or process such as CMD, PowerShell, or Bash.

Microsoft believes that SUPERNOVA is likely the work of an adversary different than the one who breached cybersecurity firm FireEye and more than half a dozen US government entities.

SUNBURST Backdoor (Earlier)

SolarWinds.Orion.Core.BusinessLayer.dll is a digitally signed Orion software system component that includes a backdoor that communicates to a third-party servers using HTTP. This SolarWinds Orion plugin is being monitored as a trojanised version.

It retrieves and runs commands, called "Jobs," after an initial sleeping time of up to two weeks, which includes file capability, executing scripts, profiling programs, rebooting the computer, and deactivating device services. The malware masks its network traffic as a protocol for the Orion Improvement Program (OIP) and stores recognition results from invalid plugin configuration files that allow it to integrate with legit SolarWinds operation. The backdoor is used to classify forensic and anti-virus methods as systems, utilities, and drivers using several fog lists.

Post-Compromise Operations

After gaining initial access, this group uses a variety of tactics to cover up their activities when advancing laterally. These threat actors tend to keep a light malware footprint, choosing to provide the legal certificate and remote access to the victim's environment.

TEARDROP is a memory-only dropper that operates as a service, spawns a thread, and reads "gracious truth.jpg" from a file that is likely to have a bogus JPG header. Then, verify that HKU\SOFTWARE\Microsoft\CTF exists, decode an embedded payload using a custom XOR rolling algorithm, and manually load an embedded payload

into memory using a custom PE-like file format. TEARDROP has no incompatible coding for any previously seen malware.

The threat actor sets hostnames on their command-and-control infrastructure to represent the legal hostname contained in the victim's setting. This helps the adversary to pass into the atmosphere, avoid suspicion, and avoid detection.

SolarWinds.Orion.Core.BusinessLayer.dll (b91ce2fa41029f6955bff20079468448) is a SolarWinds-signed plugin feature of the Orion software system that includes an obfuscated backdoor that communicates to third party servers through HTTP. After an initial inactive duration of up to two weeks, it retrieves and executes commands called "Jobs," which provide the ability to pass and execute data, device profile, and disable system services.

Backdoor's behavior and network protocol combine into legitimate SolarWinds operations, such as masking the Orion Improvement Program (OIP) protocol and storing identification data in plugin configuration files. Backdoor uses a range of blocklists to identify forensically and anti-virus approaches through networks, services, and drivers.

Researchers have claimed that FireEye, Microsoft, and Godaddy worked together to build a "kill switch," for the Sunburst malware.

SUSPECTED THREAT ACTORS

Unknown Russian Groups. Reach out to CYFIRMA for detailed insights on the attributions and correlations.

INSIGHTS

SolarWinds is a well-known managed services provider that provides a range of tools and services to organizations to manage their IT infrastructure. Adversaries have interfered with the SolarWinds' Orion platform, a software used to monitor and manage large networks. It is expected that the software update version between 2019.4 and 2020.2.1 has been exploited by the adversaries. The company has now released a fix to version 2020.2.1 HF 2.

Researchers warned that software updates for SolarWinds' Orion product had been subverted by backdoors dubbed SUPERNOVA and SUNBURST. Malicious software updates, which have been signed with valid digital signatures, could steal files, profile systems, and disable system services.

Threat actors are upgrading their arsenal with new and sophisticated malware tools to target organizations and exfiltrate sensitive information. Threat actors are observed pushing their malware/tools as part of updates of a legitimate application and using steganography to evade detection.

For more research data on Yara Rules, IoCs, and hashes, email CONTACT@CYFIRMA.COM

Source: https://www.cyfirma.com/solarwinds-hack-sunburst-supernova-and-more/