THREAT BULLETINS

SolarWinds Breach Attributed to Latest US Agency Attacks

TLP:WHITE

Dec 14, 2020

On December 13, 2020, information technology solutions company SolarWinds reported they were breached by Nation State threat actors from Russia. The breach was used to leverage further attacks against several US federal agencies. SolarWinds released a statement that their systems experienced a highly sophisticated, manual supply chain attack on SolarWinds® Orion® Platform software builds for versions 2019.4 HF 5 through 2020.2.1, released between March 2020 and June 2020. The US Cybersecurity and Infrastructure Security Agency (CISA) released Emergency Directive 21-01, stating that potential exploitation poses an unacceptable risk and affected agencies shall immediately disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from their network.

SolarWinds is used by more than 300,000 organizations across the world. Including all five branches of the U.S. military, the Pentagon, State Department, Justice Department, NASA, the Executive Office of the President and the National Security Agency, the world's top electronic spy agency, according to the firm's website.

Health-ISAC's Threat Operations Center (TOC) will continue to gather information about this incident as it becomes available. We encourage Health-ISAC members to continue sharing on WeeSecrets and the AMBER mailing list or contact the TOC directly. The TOC will provide updates as more information becomes available.

The attached PowerPoint presentation is also provided to assist with high-level communications of key points related to this event within your own organization. Health-ISAC members are encouraged to use the PowerPoint file, put it in your own templates, if necessary, and share any updates (at your option) with the TOC, so we can make further improvements.

Analysis:

SolarWinds has released a statement that their systems experienced a highly sophisticated, manual supply chain attack on SolarWinds® Orion® Platform software builds for versions 2019.4 HF 5 through 2020.2.1, released between March 2020 and June 2020. We have been advised this attack was likely conducted by an outside nation state and intended to be a narrow, extremely

targeted, and manually executed attack, as opposed to a broad, system-wide attack.

SolarWinds.Orion.Core.BusinessLayer.dll is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third party servers. We are tracking the trojanized version of this SolarWinds Orion plug-in as SUNBURST.

After an initial dormant period of up to two weeks, it retrieves and executes commands, called “Jobs”, that include the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services. The malware masquerades its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers.

Multiple trojanized updates were digitally signed from March - May 2020 and posted to the SolarWinds updates website, including:

1. hxxps://downloads.solarwinds[.]com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.20574/SolarWinds-Core-v2019.4.5220-Hotfix5.msp

The trojanized update file is a standard Windows Installer Patch file that includes compressed resources associated with the update, including the trojanized SolarWinds.Orion.Core.BusinessLayer.dll component. Once the update is installed, the malicious DLL will be loaded by the legitimate SolarWinds.BusinessLayerHost.exe or SolarWinds.BusinessLayerHostx64.exe (depending on system configuration). After a dormant period of up to two weeks, the malware will attempt to resolve a subdomain of avsvmcloud[.]com. The DNS response will return a CNAME record that points to a Command and Control (C2) domain. The C2 traffic to the malicious domains is designed to mimic normal SolarWinds API communications. The list of known malicious infrastructure is available on FireEye’s GitHub page.

Indicators of Compromise:

Currently known Indicators of Compromise (IOC) have been entered into Health-ISAC's automated sharing platform for those members ingesting automated threat indicators. Health-ISAC's Threat Operation Center will continue to monitor the incident, while aggregating and ingesting IOCs made available.

Reference(s)	DHS, cisa, SolarWinds, Microsoft, SolarWinds, FireEye, FireEye, FireEye, cisa, Washington Post, GitHub
Cyber Threat Type	APT

Recommendations
We recommend taking the following steps related to your use of the SolarWinds Orion Platform:

1. Upgrade to Orion Platform version 2020.2.1 HF 1 as soon as possible to ensure the security of your environment. The latest version is available in the SolarWinds Customer Portal.
2. If you are not sure which version of the Orion Platform you are using, see directions on how to check that here. To check which hotfixes you have applied, please go here.
3. If you cannot upgrade immediately, please follow the guidelines available here for securing your Orion Platform instance. The primary mitigation steps include having your Orion Platform installed behind firewalls, disabling internet access for the Orion Platform, and limiting the ports and connections to only what is necessary.
4. An additional hotfix release, 2020.2.1 HF 2 is anticipated to be made available Tuesday, December 15, 2020. We recommend that all customers update to release 2020.2.1 HF 2 once it is available, as

the 2020.2.1 HF 2 release both replaces the compromised component and provides several additional security enhancements.

Health-ISAC is also recommending navigating to the countermeasures and rules that FireEye has released, which includes a trove of signatures along with other countermeasures that customers can use to detect and repel the attacks if the tools are used. Some researchers who reviewed the countermeasures said they appeared to show that the tools were not sensitive in nature.

In the event you are unable to follow SolarWinds' recommendations, the following are immediate mitigation techniques that could be deployed as first steps to address the risk of trojanized SolarWinds software in an environment. If attacker activity is discovered in an environment, we recommend conducting a comprehensive investigation and designing and executing a remediation strategy driven by the investigative findings and details of the impacted environment.

1. Ensure that SolarWinds servers are isolated / contained until a further review and investigation is conducted. This should include blocking all Internet egress from SolarWinds servers.
2. If SolarWinds infrastructure is not isolated, consider taking the following steps:
3. Restrict scope of connectivity to endpoints from SolarWinds servers, especially those that would be considered Tier 0 / crown jewel assets
4. Restrict the scope of accounts that have local administrator privileged on SolarWinds servers.
5. Block Internet egress from servers or other endpoints with SolarWinds software.
6. Consider (at a minimum) changing passwords for accounts that have access to SolarWinds servers / infrastructure. Based upon further review / investigation, additional remediation measures may be required.
7. If SolarWinds is used to managed networking infrastructure, consider conducting a review of network device configurations for unexpected / unauthorized modifications. Note, this is a proactive measure due to the scope of SolarWinds functionality, not based on investigative findings.

Sources
Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor | FireEye Inc

Russian government spies are behind a broad hacking campaign that has breached U.S. agencies and a top cyber firm

SolarWinds has just been made aware our systems experienced a highly sophisticated, manual supply chain attack on SolarWinds® Orion® Platform software builds for versions 2019.4 through 2020.2.1, released between March 2020 and June 2020.

Global Intrusion Campaign Leverages Software Supply Chain Compromise

FireEye Mandiant SunBurst Countermeasures

CISA: Active Exploitation of SolarWinds Software

CISA ISSUES EMERGENCY DIRECTIVE TO MITIGATE THE COMPROMISE OF SOLARWINDS ORION NETWORK MANAGEMENT PRODUCTS

DHS Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise

Customer Guidance on Recent Nation-State Cyber Attacks

Alert ID 7ab267cb

View Alert

Access the New Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, new notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org