THREAT BULLETINS

UPDATE: Active Exploitation of SolarWinds Breach

TLP:WHITE

Dec 17, 2020

*This updated alert provides details of an **active exploitation** highlighting nation state threat actor activity detected in the recent*

*compromise of the technology solutions company **SolarWinds**. In addition to the update, you may access the original Health-ISAC Threat Bulletin here.*

*On December 17, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) distributed a cyber activity alert (AA20-352A) to provide additional insight (found below under **MITRE ATT&CK**) highlighting the attack techniques leveraged against U.S. government agencies, critical infrastructure entities, and private sector organizations as it pertains to the MITRE ATT&CK framework.*

*CISA has **evidence of additional initial access vectors**, other than the SolarWinds Orion platform, however, these are still being investigated. Health-ISAC will update this alert as new information becomes available.*

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.

On December 13, 2020, information technology solutions company SolarWinds previously 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.

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. SolarWinds believes the 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:

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.

MITRE ATT&CK:

Initial Infection Vectors [*TA0001*]

CISA is investigating incidents that exhibit adversary TTPs consistent with this activity, including some where victims either do not leverage SolarWinds Orion or where SolarWinds Orion was present but where there was no SolarWinds exploitation activity observed. Volexity has also reported publicly that they observed an intrusion into a think tank using, as an initial intrusion vector, a Duo multi-factor authentication bypass in Outlook Web App (OWA) to steal the secret key. Volexity attributes this intrusion to the same activity as the SolarWinds Orion supply chain compromise, and the TTPs are consistent between the two. This observation indicates that there are other initial access vectors beyond SolarWinds Orion, and there may still be others that are not yet known.

SolarWinds Orion Supply Chain Compromise

SolarWinds Orion is an enterprise network management software suite that includes performance and application monitoring and network configuration management along with several different types of analyzing tools. SolarWinds Orion is used to monitor and manage on premise and hosted infrastructures. To provide SolarWinds Orion with the necessary visibility into this diverse set of technologies, it is common for network administrators to configure SolarWinds Orion with pervasive privileges, making it a valuable target for adversary activity.

The threat actor has been observed leveraging a software supply chain compromise of SolarWinds Orion products. The adversary added a malicious version of the binary solarwinds.orion.core.businesslayer.dll into the SolarWinds software lifecycle, which was then signed by the legitimate SolarWinds code signing certificate. This binary, once installed, calls out to a victim-specific avsvmcloud[.]com domain using a protocol designed to mimic legitimate SolarWinds protocol traffic. After the initial check-in, the adversary can use the Domain Name System (DNS) response to selectively send back new domains or IP addresses for interactive command and control (C2) traffic. Consequently, entities that observe traffic from their SolarWinds Orion devices to avsvmcloud[.]com should not immediately conclude that the adversary leveraged the SolarWinds Orion backdoor. Instead, additional investigation is needed into whether the SolarWinds Orion device engaged in further unexplained communications. If additional Canonical Name record (CNAME) resolutions associated with the avsvmcloud[.]com domain are observed, possible additional adversary action leveraging the back door has occurred.

Based on coordinated actions by multiple private sector partners, as of December 15, 2020, avsvmcloud[.]com resolves to 20.140.0[.]1, which is an IP address on the Microsoft blocklist. This negates any future use of the implants and would have caused communications with this domain to cease. In the case of infections where the attacker has already moved C2 past the initial beacon, infection will likely continue notwithstanding this action.

SolarWinds Orion typically leverages a significant number of highly privileged accounts and access to perform normal business functions. Successful compromise of one of these systems can therefore enable further action and privileges in any environment where these accounts are trusted.

Anti-Forensic Techniques

The adversary is making extensive use of obfuscation to hide their C2 communications. The adversary is using virtual private servers (VPSs), often with IP addresses in the home country of the victim, for most communications to hide their activity among legitimate user traffic. The attackers also frequently rotate their “last mile” IP addresses to different endpoints to obscure their activity and avoid detection.

FireEye has reported that the adversary is using steganography (Obfuscated Files or Information: Steganography [T1027.003]) to obscure C2 communications.3 This technique negates many common defensive capabilities in detecting the activity. **Note**: CISA has not yet been able to independently confirm the adversary’s use of this technique.

According to FireEye, the malware also checks for a list of hard-coded IPv4 and IPv6 addresses—including RFC-reserved IPv4 and IPv6 IP—in an attempt to detect if the malware is executed in an analysis environment (e.g., a malware analysis sandbox); if so, the malware will stop further execution. Additionally, FireEye analysis identified that the backdoor implemented time threshold checks to ensure that there are unpredictable delays between C2 communication attempts, further frustrating traditional network-based analysis.

While not a full anti-forensic technique, the adversary is heavily leveraging compromised or spoofed tokens for accounts for lateral movement. This will frustrate commonly used detection techniques in many environments. Since valid, but unauthorized, security tokens and accounts are utilized, detecting this activity will require the maturity to identify actions that are outside of a user’s normal duties. For example, it is unlikely that an account associated with the HR department would need to access the cyber threat intelligence database.

Taken together, these observed techniques indicate an adversary who is skilled, stealthy with operational security, and is willing to expend significant resources to maintain covert presence.

Privilege Escalation and Persistence [TA0004, TA0003]

The adversary has been observed using multiple persistence mechanisms across a variety of intrusions. CISA has observed the threat actor adding authentication tokens and credentials to highly privileged Active Directory domain accounts as a persistence and escalation mechanism. In many instances, the tokens enable access to both on-premise and hosted resources. Microsoft has released a query that can help detect this activity.

Microsoft reported that the actor has added new federation trusts to existing infrastructure, a technique that CISA believes was utilized by a threat actor in an incident to which CISA has responded. Where this technique is used, it is possible that authentication can occur outside of an organization's known infrastructure and may not be visible to the legitimate system owner. Microsoft has released a query to help identify this activity.

User Impersonation

The adversary's initial objectives, as understood today, appear to be to collect information from victim environments. One of the principal ways the adversary is accomplishing this objective is by compromising the Security Assertion Markup Language (SAML) signing certificate using their escalated Active Directory privileges. Once this is accomplished, the adversary creates unauthorized but valid tokens and presents them to services that trust SAML tokens from the environment. These tokens can then be used to access resources in hosted environments, such as email, for data exfiltration via authorized application programming interfaces (APIs).

CISA has observed in its incident response work adversaries targeting email accounts belonging to key personnel, including IT and incident response personnel.

These are some key functions and systems that commonly use SAML.

1. Hosted email services
2. Hosted business intelligence applications
3. Travel systems
4. Timecard systems
5. File storage services (such as SharePoint)

Detection: Impossible Logins

The adversary is using a complex network of IP addresses to obscure their activity, which can result in a detection opportunity referred to as “impossible travel.” Impossible travel occurs when a user logs in from multiple IP addresses that are a significant geographic distance apart (i.e., a person could not realistically travel between the geographic locations of the two IP addresses during the time period between the logins). **Note**: implementing this detection opportunity can result in false positives if legitimate users apply virtual private network (VPN) solutions before connecting into networks.

Detection: Impossible Tokens

1. The following conditions may indicate adversary activity.
2. Most organizations have SAML tokens with 1-hour validity periods. Long SAML token validity durations, such as 24 hours, could be unusual.
3. The SAML token contains different timestamps, including the time it was issued and the last time it was used. A token having the same timestamp for when it was issued and when it was used is not indicative of normal user behavior as users tend to use the token within a few seconds but not at the exact same time of issuance.

4. A token that does not have an associated login with its user account within an hour of the token being generated also warrants investigation.

Operational Security

Due to the nature of this pattern of adversary activity—and the targeting of key personnel, incident response staff, and IT email accounts—discussion of findings and mitigations should be considered very sensitive, and should be protected by operational security measures. An operational security plan needs to be developed and socialized, via out-of-band communications, to ensure all staff are aware of the applicable handling caveats.

Operational security plans should include:

1. Out-of-band communications guidance for staff and leadership.
2. An outline of what “normal business” is acceptable to be conducted on the suspect network.
3. A call tree for critical contacts and decision making.
4. Considerations for external communications to stakeholders and media.

MITRE ATT&CK® Techniques

CISA assesses that the threat actor engaged in the activities described in this Alert uses the below-listed

ATT&CK techniques.

1. *Query Registry* [T1012]
2. *Obfuscated Files or Information* [T1027]
3. *Obfuscated Files or Information: Steganography* [T1027.003]
4. *Process Discovery* [T1057]

5. *Indicator Removal on Host: File Deletion* [T1070.004]
6. *Application Layer Protocol: Web Protocols* [T1071.001]
7. *Application Layer Protocol: DNS* [T1071.004]
8. *File and Directory Discovery* [T1083]
9. *Ingress Tool Transfer* [T1105]
10. *Data Encoding: Standard Encoding* [T1132.001]
11. *Supply Chain Compromise: Compromise Software Dependencies and Development Tools* [T1195.001]
12. *Supply Chain Compromise: Compromise Software Supply Chain* [T1195.002]
13. *Software Discovery* [T1518]
14. *Software Discovery: Security Software* [T1518.001]
15. *Create or Modify System Process: Windows Service* [T1543.003]
16. *Subvert Trust Controls: Code Signing* [T1553.002]
17. *Dynamic Resolution: Domain Generation Algorithms* [T1568.002]
18. *System Services: Service Execution* [T1569.002]
19. *Compromise Infrastructure* [T1584]

Affected SolarWinds Orion Products

Please see Appendix A within CISA Alert (AA20-352A) which identifies recent versions of SolarWinds Orion Platforms and indicates whether they have been identified as having the Sunburst backdoor present.

Indicators of Compromise:

Due to the operational security posture of the adversary, most observable IOCs are of limited utility; however, they can be useful for quick triage. Please see CISA Alert (AA20-352A) for a compilation of IOCs from a variety of public sources provided for convenience. CISA will be updating this list with CISA developed IOCs as our investigations evolve.

Currently known IOCs 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.

Updated Recommendations:

SolarWinds Orion Owners

Owners of vulnerable SolarWinds Orion products will generally fall into one of three categories.

1. Category 1 includes those who do not have the identified malicious binary. These owners can patch their systems and resume use as determined by and consistent with their internal risk evaluations.
2. Category 2 includes those who have identified the presence of the malicious binary—with or without beaconing to avsvmcloud[.]com. Owners with malicious binary whose vulnerable appliances only unexplained external communications are with avsvmcloud[.]com—a fact that can be verified by comprehensive network monitoring for the device—can harden the device, re-install the updated software from a verified software supply chain, and resume use as determined by and consistent with a thorough risk evaluation.
3. Category 3 includes those with the binary beaconing to avsvmcloud[.]com and secondary C2 activity to a separate domain or IP address. If you observed communications with avsvmcloud[.]com that appear to suddenly cease prior to December 14, 2020— not due to an action taken by your network defenders—you fall into this category. Assume the environment has been compromised, and initiate incident response procedures immediately.

Compromise Mitigations

If the adversary has compromised administrative level credentials in an environment—or if organizations identify SAML abuse in the environment, simply mitigating individual issues, systems, servers, or specific user accounts will likely not lead to the adversary's removal from the network. In such cases, organizations should consider the entire identity trust store as compromised. In the event of a total identity compromise, a full reconstitution of identity and trust services is required to successfully remediate. In this reconstitution, it bears repeating that this threat actor is among the most capable, and in many cases, a full rebuild of the environment is the safest action.

SolarWinds Orion Specific Mitigations

The following mitigations apply to networks using the SolarWinds Orion product. This includes any information system that is used by an entity or operated on its behalf.

Organizations that have the expertise to take the actions in Step 1 immediately should do so before proceeding to Step 2. Organizations without this capability should proceed to Step 2. Federal civilian executive branch agencies should ignore the below and refer instead to Emergency Directive 21-01 (and forthcoming associated guidance) for mitigation steps.

1. **Step 1**
    1. **Forensically image system memory and/or host operating systems hosting all instances of affected versions of SolarWinds Orion.** Analyze for new user or service accounts, privileged or otherwise.
    2. Analyze stored network traffic for indications of compromise, including new external DNS domains to which a small number of agency hosts (e.g., SolarWinds systems) have had connections.
2. **Step 2**
    1. Affected organizations should immediately **disconnect or power down affected all instances of affected versions of SolarWinds Orion from their network**.
    2. Additionally:
        1. **Block all traffic** to and from hosts, external to the enterprise, where any version of SolarWinds Orion software has been installed.
        2. **Identify and remove** all threat actor-controlled accounts and identified persistence mechanisms.
3. **Step 3**
    1. **Only after all known threat actor-controlled accounts and persistence mechanisms have been removed:**
        1. Treat all hosts monitored by the SolarWinds Orion monitoring software as compromised by threat actors and assume that the threat actor has deployed further persistence mechanisms.
        2. Rebuild hosts monitored by the SolarWinds Orion monitoring software using trusted sources.

3. Reset all credentials used by or stored in SolarWinds software. Such credentials should be considered compromised.
4. Take actions to remediate kerberoasting, including—as necessary or appropriate—engaging with a third party with experience eradicating APTs from enterprise networks. For Windows environments, refer to the following Microsoft's documentation on kerberoasting: https://techcommunity.microsoft.com/t5/microsoft-security-and/detecting-ldap-based-kerberoasting-with-azure-atp/ba-p/462448.
5. Require use of multi-factor authentication. If not possible, use long and complex passwords (greater than 25 characters) for service principal accounts, and implement a good rotation policy for these passwords.
6. Replace the user account by group Managed Service Account (gMSA), and implement Group Managed Service Accounts: https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview.
7. Set account options for service accounts to support AES256_CTS_HMAC_SHA1_96 and not support DES, RC4, or AES128 bit encryption.
8. Define the Security Policy setting for Network Security: Configure Encryption types allowed for Kerberos. Set the allowable encryption types to AES256_HMAC_SHA1 and Future encryption types: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos.
9. See Microsoft's documentation on how to reset the Kerberos Ticket Granting Ticket password twice: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password.

See Joint Alert on Technical Approaches to Uncovering and Remediating Malicious Activity for more information on incident investigation and mitigation steps based on best practices.

CISA will update this Alert, as information becomes available and will continue to provide technical assistance, upon request, to affected entities as they work to identify and mitigate potential compromises.

SolarWinds recommends 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.

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:

    1. Restrict scope of connectivity to endpoints from SolarWinds servers, especially those that would be considered Tier 0 / crown jewel assets
    2. Restrict the scope of accounts that have local administrator privileged on SolarWinds servers.
    3. Block Internet egress from servers or other endpoints with SolarWinds software.
3. 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.
4. 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.

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.

RiskIQ has provided additional tools and techniques organizations can use to detect vulnerable systems in their internet-facing environment. More information can be found at RiskIQ's blog post, SolarWinds Orion Hack: Know if You're Affected and Defend Your Attack Surface, found here:

https://www.riskiq.com/blog/external-threat-management/solarwinds-orion-hack/

Reference(s)	cisa, FireEye, Washington Post, SolarWinds, FireEye, GitHub, cisa, cisa, DHS, Microsoft

Report Source(s)	Government Agency

Alert ID 43759b6f

View Alert

Tags SolarWInds

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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