Alert (AA20-352A)

Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

Original release date: December 17, 2020 | Last revised: December 23, 2020

Summary

> *This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 8 framework. See the ATT&CK for Enterprise version 8 for all referenced threat actor tactics and techniques.*

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of compromises of U.S. government agencies, critical infrastructure entities, and private sector organizations by an advanced persistent threat (APT) actor beginning in at least March 2020. This APT actor has demonstrated patience, operational security, and complex tradecraft in these intrusions. CISA expects that removing this threat actor from compromised environments will be highly complex and challenging for organizations.

One of the initial access vectors for this activity is a supply chain compromise of the following SolarWinds Orion products (see Appendix A).

- Orion Platform 2019.4 HF5, version 2019.4.5200.9083
- Orion Platform 2020.2 RC1, version 2020.2.100.12219
- Orion Platform 2020.2 RC2, version 2020.2.5200.12394
- Orion Platform 2020.2, 2020.2 HF1, version 2020.2.5300.12432

Note (*updated December 23, 2020*): CISA has evidence that there are initial access vectors other than the SolarWinds Orion platform. Specifically, we are investigating incidents in which activity indicating abuse of Security Assertion Markup Language (SAML) tokens consistent with this adversary's behavior is present, yet where impacted SolarWinds instances have not been identified. CISA is working to confirm initial access vectors and identify any changes to the TTPs. CISA will update this Alert as new information becomes available. Refer to CISA.gov/supply-chain-compromise for additional resources.

On December 13, 2020, CISA released Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise, ordering federal civilian executive branch departments and agencies to disconnect affected devices. **Note:** this Activity Alert does not supersede the requirements of Emergency Directive 21-01 (ED-21-01) and does not represent formal guidance to federal agencies under ED 21-01.

CISA has determined that this threat poses a grave risk to the Federal Government and state, local, tribal, and territorial governments as well as critical infrastructure entities and other private sector organizations. CISA advises stakeholders to read this Alert and review the enclosed indicators (see Appendix B).

Key Takeaways (*updated December 18, 2020*)

- This is a patient, well-resourced, and focused adversary that has sustained long duration activity on victim networks.
- CISA is investigating other initial access vectors in addition to the SolarWinds Orion supply chain compromise.
- Not all organizations that have the backdoor delivered through SolarWinds Orion have been targeted by the adversary with follow-on actions.
- Organizations with suspected compromises need to be highly conscious of operational security, including when engaging in incident response activities and planning and implementing remediation plans.

(*Updated December 19, 2020*) For a downloadable list of IOCs, see the STIX file.

Technical Details

Overview

CISA is aware of compromises, which began at least as early as March 2020, at U.S. government agencies, critical infrastructure entities, and private sector organizations by an APT actor. This threat actor has demonstrated sophistication and complex tradecraft in these intrusions. CISA expects that removing the threat actor from compromised environments will be highly complex and challenging. This adversary has demonstrated an ability to exploit software supply chains and shown significant knowledge of Windows networks. It is likely that the adversary has additional initial access vectors and tactics, techniques, and procedures (TTPs) that have not yet been discovered. CISA will continue to update this Alert and the corresponding indicators of compromise (IOCs) as new information becomes available.

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 the APT using a secret key that the APT previously stole in order to generate a cookie to bypass the Duo multi-factor authentication protecting access to Outlook Web App (OWA).[1] 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[2] (see Appendix A). 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.[4]

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.[5]

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 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.

- Hosted email services
- Hosted business intelligence applications
- Travel systems
- Timecard systems
- 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

The following conditions may indicate adversary activity.

- Most organizations have SAML tokens with 1-hour validity periods. Long SAML token validity durations, such as 24 hours, could be unusual.
- 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.
- A token that does not have an associated login with its user account within an hour of the token being generated also warrants investigation.

(*New December 21, 2020*): see the National Security Agency (NSA) Cybersecurity Advisory: Detecting Abuse of Authentication Mechanisms for additional detection methods as well as mitigation recommendations.

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:

- Out-of-band communications guidance for staff and leadership;
- An outline of what “normal business” is acceptable to be conducted on the suspect network;
- A call tree for critical contacts and decision making; and
- 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.

- *Query Registry* [T1012]
- *Obfuscated Files or Information* [T1027]
- *Obfuscated Files or Information: Steganography* [T1027.003]
- *Process Discovery* [T1057]
- *Indicator Removal on Host: File Deletio*n [T1070.004]
- *Application Layer Protocol: Web Protocols* [T1071.001]
- *Application Layer Protocol: DNS* [T1071.004]
- *File and Directory Discovery* [T1083]
- *Ingress Tool Transfer* [T1105]
- *Data Encoding: Standard Encoding* [T1132.001]
- *Supply Chain Compromise: Compromise Software Dependencies and Development Tools* [T1195.001]
- *Supply Chain Compromise: Compromise Software Supply Chain* [T1195.002]
- *Software Discovery* [T1518]
- *Software Discovery: Security Software* [T1518.001]
- *Create or Modify System Process: Windows Service* [T1543.003]
- *Subvert Trust Controls: Code Signing* [T1553.002]
- *Dynamic Resolution: Domain Generation Algorithms* [T1568.002]
- *System Services: Service Execution* [T1569.002]
- *Compromise Infrastructure* [T1584]

Mitigations

SolarWinds Orion Owners

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

- Category 1 (*updated December 19, 2020*) includes those who do not have the identified malicious binary. These owners (except federal agencies subject to ED 21-01) can patch their systems and resume use as determined by and consistent with their internal risk evaluations.
- 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.
- 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.

- **Step 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.
  - 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.
- **Step 2**
  - Affected organizations should immediately **disconnect or power down affected all instances of affected versions of SolarWinds Orion from their network**.
  - Additionally:
    - **Block all traffic** to and from hosts, external to the enterprise, where any version of SolarWinds Orion software has been installed.
    - **Identify and remove** all threat actor-controlled accounts and identified persistence mechanisms.
- **Step 3**
  - **Only after all known threat actor-controlled accounts and persistence mechanisms have been removed:**
    - 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.
    - Rebuild hosts monitored by the SolarWinds Orion monitoring software using trusted sources.
    - Reset all credentials used by or stored in SolarWinds software. Such credentials should be considered compromised.
    - 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.
    - 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.
    - 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.
    - Set account options for service accounts to support `AES256_CTS_HMAC_SHA1_96` and not support `DES`, `RC4`, or `AES128` bit encryption.
    - 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.
    - 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.
- (*New December 19, 2020*) For all network devices (routers, switches, firewalls, etc.) managed by affected SolarWinds servers that also have indications of additional adversary activity, CISA recommends the following steps:
  - Device configurations
    - Audit all network device configurations, stored or managed on the SolarWinds monitoring server, for signs of unauthorized or malicious configuration changes.
    - Audit the configurations found on network devices for signs of unauthorized or malicious configuration changes. Organizations should ensure they audit the current network device running configuration and any local configurations that could be loaded at boot time.
  - Credential and security information reset
    - Change all credentials being used to manage network devices, to include keys and strings used to secure network device functions (SNMP strings/user credentials, IPsec/IKE preshared keys, routing secrets, TACACS/RADIUS secrets, RSA keys/certificates, etc.).
  - Firmware and software validation
    - Validate all network device firmware/software which was stored or managed on the SolarWinds monitoring server. Cryptographic hash verification should be performed on such firmware/software and matched against known good hash values from the network vendor. CISA recommends that, if possible, organizations download known good versions of firmware.
- (*New December 19, 2020*) For network devices managed by the SolarWinds monitoring server, the running firmware/software should be checked against known good hash values from the network vendor. CISA recommends

that, if possible, organizations re-upload known good firmware/software to managed network devices and perform a reboot.

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.

Contact Information

CISA encourages recipients of this report to contribute any additional information that they may have related to this threat. For any questions related to this report, please contact CISA at

- 1-888-282-0870 (From outside the United States: +1-703-235-8832)
- central@cisa.dhs.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on the CISA/US-CERT homepage at http://www.us-cert.cisa.gov/.

Appendix A: Affected SolarWinds Orion Products

Table 1 identifies recent versions of SolarWinds Orion Platforms and indicates whether they have been identified as having the Sunburst backdoor present.

Table 1: Affected SolarWinds Orion Products

Orion Platform Version	Sunburst Backdoor Code Present	File Version	SHA-256
2019.4	Tampered but not backdoored	2019.4.5200.8890	a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc
2019.4 HF1	No	2019.4.5200.8950	9bee4af53a8cdd7ecabe5d0c77b6011abe887ac516a5a22ad51a058830403690
2019.4 HF2	No	2019.4.5200.8996	bb86f66d11592e3312cd03423b754f7337aeebba9204f54b745ed3821de6252d
2019.4 HF3	No	2019.4.5200.9001	ae6694fd12679891d95b427444466f186bcdcc79bc0627b590e0cb40de1928ad
2019.4 HF4	No	2019.4.5200.9045	9d6285db647e7eeabdb85b409fad61467de1655098fec2e25aeb7770299e9fee
2020.2 RC1	Yes	2020.2.100.12219	dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
2019.4 HF5	Yes	2019.4.5200.9083	32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
2020.2 RC2	Yes	2020.2.5200.12394	019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
2020.2 2020.2 HF1	Yes	2020.2.5300.12432	ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
2019.4 HF6	No	2019.4.5200.9106	8dfe613b00d495fb8905bdf6e1317d3e3ac1f63a626032fa2bdad4750887ee8a
2020.2.1 2020.2.1 HF1	No	2020.2.15300.12766	143632672dcb6ef324343739636b984f5c52ece0e078cfee7c6cac4a3545403a
2020.2.1 HF2	No	2020.2.15300.12901	cc870c07eeb672ab33b6c2be51b173ad5564af5d98bfc02da02367a9e349a76f

Appendix B: 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. Below is 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. ***Note:*** *removed two IOCs (12.227.230[.]4, 65.153.203[.]68) and corrected typo, updated December 19, 2020.*

Table 2: Indicators of Compromise

IOC	Type	Notes	References	Source
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77	hash	Backdoor.Sunburst	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/	

IOC	Type	Notes	References	Source
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc	hash	Backdoor.Sunburst	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber- attacks/	
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af	hash	Backdoor.Sunburst	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber- attacks/	
13.59.205[.]66	IPv4	DEFTSECURITY[.]com	https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
deftsecurity[.]com	domain	Domain malicious on VT, registered with Amazon, hosted on US IP address 13.59.205.66, malware repository, spyware and malware	https://www.virustotal.com/gui/domain/deftsecurity.com/details https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
54.193.127[.]66	IPv4	FREESCANONLINE[.]com	https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c	hash	No info available	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/	
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77	hash	No info available	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/	
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b	hash	No info available	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/	
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed	hash	No info available	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/	

IOC	Type	Notes	References	Source
avsvmcloud[.]com	domain	Reported by FireEye/ The malicious DLL calls out to a remote network infrastructure using the domains avsvmcloud.com. to prepare possible second-stage payloads, move laterally in the organization, and compromise or exfiltrate data. Malicious on VT. Hosted on IP address 20.140.0.1, which is registered with Microsoft. malware callhome, command and control	https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/ FireEye Report Talos Volexity
3.87.182[.]149	IPv4	Resolves to KUBECLOUD[.]com, IP registered to Amazon. Tracked by Insikt/RF as tied to SUNBURST intrusion activity.	https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity

IOC	Type	Notes	References	Source
3.16.81[.]254	IPv4	Resolves to SEOBUNDLEKIT[.]com, registered to Amazon. Tracked by Insikt/RF as tied SUNBURST intrusion activity.	https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
54.215.192[.]52	IPv4	THEDOCCLOUD[.]com	https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134	hash	Trojan.MSIL.SunBurst	ttps://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber- attacks/	
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6	hash	Trojan.MSIL.SunBurst	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber- attacks/	
8.18.144[.]11	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]12	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]9	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]20	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]40	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]44	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]62	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]130	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]135	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity

IOC	Type	Notes	References	Source
8.18.144[.]136	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]149	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]156	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]158	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]165	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]170	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]180	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.144[.]188	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.145[.]3	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.145[.]21	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.145[.]33	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.145[.]36	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.145[.]131	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.145[.]134	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.145[.]136	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity

IOC	Type	Notes	References	Source
8.18.145[.]139	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.145[.]150	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.145[.]157	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
8.18.145[.]181	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
13.57.184[.]217	IPv4	*(corrected typo in this IOC December 18, 2020)*	https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
18.217.225[.]111	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
18.220.219[.]143	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
20.141.48[.]154	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
34.219.234[.]134	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
184.72.1[.]3	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
184.72.21[.]54	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
184.72.48[.]22	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
184.72.101[.]22	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
184.72.113[.]55	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
184.72.145[.]34	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity

IOC	Type	Notes	References	Source
184.72.209[.]33	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
184.72.212[.]52	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
184.72.224[.]3	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
184.72.229[.]1	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
184.72.240[.]3	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
184.72.245[.]1	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
196.203.11[.]89	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
digitalcollege[.]org	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
freescanonline[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
globalnetworkissues[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
kubecloud[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
lcomputers[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
seobundlekit[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
solartrackingsystem[.]net	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
thedoccloud[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity

IOC	Type	Notes	References	Source
virtualwebdata[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
webcodez[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/	Volexity
d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600	hash		https://blog.malwarebytes.com/threat-analysis/2020/12/advanced-cyber-attack-hits-private-and-public	
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71	hash		https://blog.malwarebytes.com/threat-analysis/2020/12/advanced-cyber-attack-hits-private-and-public	

References

[1] Volexity: Dark Halo Leverages SolarWinds Compromise to Breach Organizations
[2] SolarWinds Security Advisory
[3] FireEye: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compr…
[4] GitHub: Azure / Azure-Sentinel - AzureAADPowerShellAnomaly.yaml
[5] GitHub: Azure / Azure-Sentinel - ADFSDomainTrustMods.yaml

Revisions

Initial version: December 17, 2020
December 18, 2020: Updated note regarding initial vectors and key takeaways.
December 19, 2020: Updated mitigation guidance, indicators of compromise table, and provided a downloadable STIX file of the IOCs.
December 21, 2020: Added reference to NSA Cybersecurity Advisory: Detecting Abuse of Authentication Methods
December 23, 2020: Added link to CISA.gov/supply-chain-compromise

This product is provided subject to this Notification and this Privacy & Use policy.