America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CYBERSECURITY ADVISORY

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

Last Revised: April 15, 2021 **Alert Code:** AA20-352A

Give Feedback

Summary

Updated April 15, 2021: The U.S. Government attributes this activity to the Russian Foreign Intelligence Service (SVR). Additional information may be found in a statement from the White House. For more information on SolarWinds-related activity, go to https://us-cert.cisa.gov/remediating-apt-compromised-networks <https://us-cert.cisa.gov/remediating-apt-compromised-networks> ***and https://www.cisa.gov/supply-chain-compromise*** <https://www.cisa.gov/supply-chain-compromise>***.***

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.

(*Updated January 6, 2021*): One of the initial access vectors for this activity is a supply chain compromise of a Dynamic Link Library (DLL) in the following SolarWinds Orion products (see Appendix A). **Note**: prior versions of this Alert included a single bullet that listed two platform versions for the same DLL. For clarity, the Alert now lists these platform versions that share the same DLL version number separately, as both are considered affected versions.

- 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, version 2020.2.5300.12432
- Orion Platform 2020.2 HF1, version 2020.2.5300.12432

Note (*updated January 6, 2021*): CISA has evidence that there are initial access vectors other than the SolarWinds Orion platform and has identified legitimate account abuse as one of these vectors (for details refer to Initial Access Vectors section). 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 continuing to work to confirm initial access vectors and identify any changes to the tactics, techniques, and procedures (TTPs). CISA will update this Alert as new information becomes available. Refer to CISA.gov/supply-chain-compromise <https://www.cisa.gov/supply-chain-compromise> for additional resources.

(*Updated January 6, 2021*): On December 13, 2020, CISA released Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise <https://cyber.dhs.gov/ed/21-01/>, ordering federal civilian executive branch departments and agencies to disconnect affected devices. CISA has subsequently issued supplemental guidance <https://cyber.dhs.gov/ed/21-01/#supplemental-guidance-v3> to Emergency Directive (ED) 21-01, most recently on January 6, 2021. **Note**: this Activity Alert does not supersede the requirements of ED 21-01 or any supplemental guidance 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.

Give Feedback

(*Updated January 8, 2021*) For a downloadable list of indicators of compromise (IOCs), see the STIX file </sites/default/files/publications/aa20-352a.stix.xml>.

(Updated April 15, 2021) See the following Malware Analysis Reports (MARs) for additional technical details and associated IOCs:

- AR21-039A: MAR-10318845-1.v1 - SUNBURST <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039a>
- AR21-039B: MAR-10320115-1.v1 - TEARDROP <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039b>
- AR21-105A: MAR-10327841-1.v1 – SUNSHUTTLE <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-105a>

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 TTPs that have not yet been discovered. CISA will continue to update this Alert and the corresponding IOCs as new information becomes available.

Initial Infection Vectors [TA0001 <https://attack.mitre.org/versions/v8/tactics/ta0001/

(*Updated January 6, 2021*): 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. CISA incident response investigations have identified that initial access in some cases was obtained by password guessing [T1101.001 <https://attack.mitre.org/versions/v8/techniques/t1110/001/>], password spraying [T1101.003 <https://attack.mitre.org/versions/v8/techniques/t1110/003/>], and inappropriately secured administrative credentials [T1078 <https://attack.mitre.org/versions/v8/techniques/t1078/>] accessible via external remote access services [T1133

<https://attack.mitre.org/versions/v8/techniques/t1133/>]. Initial access root cause analysis is still ongoing in a number of response activities and CISA will update this section as additional initial vectors are identified.

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 (MFA) protecting access to Outlook Web App (OWA).[1 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>] 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 [T1195.002 <https://attack.mitre.org/versions/v8/techniques/t1195/002/>]

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 <https://www.solarwinds.com/securityadvisory>] (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 backdoor 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 thes accounts are trusted.

Give Feedback

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 <https://attack.mitre.org/versions/v8/techniques/t1027/003/>]) to obscure C2 communications.[3

<https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>] 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 <https://attack.mitre.org/versions/v8/tactics/ta0004>, TA0003 <https://attack.mitre.org/versions/v8/tactics/ta0003/>]

(*Updated January 6, 2021*): The adversary has been observed using multiple persistence mechanisms across a variety of intrusions. CISA has observed the threat actor adding authentication credentials, in the form of assigning tokens and certificates, to existing

Azure/Microsoft 365 (M365) application service principals. These additional credentials provide persistence and escalation mechanisms and a programmatic method of interacting with the Microsoft Cloud tenants (often with Microsoft Graph Application Programming Interface [API]) to access hosted resources without significant evidence or telemetry being generated.

(*Updated January 6, 2021*): Microsoft reported that the actor has added new federation trusts to existing on-premises 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, as well as a Sentinel detection for identifying changes to the identity federation from a user or application.[4]

User Impersonation

(*Updated January 6, 2021*): The adversary's initial objectives, as understood today, appear to be to collect information from victim environments. One method 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 APIs. During the persistence phase, the additional credentials being attached to service principals obfuscates the activity of user objects, because they appear to be accessed by the individual, and such individual access is normal and not logged in all M365 licensing levels.

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 and OneDrive)

(*New January 6, 2021*): Detection: Identifying Compromised Azure/M365 Resources

CISA created Sparrow.ps1[5 <https://github.com/cisagov/sparrow>] to help detect possible compromised accounts and applications in the Azure/M365 environment. Sparrow is intended for use by incident responders and focuses on the narrow scope of user and application activity endemic to identity- and authentication-based attacks seen recently in multiple sectors. It is neither comprehensive nor exhaustive of available data and is intended to narrow a larger set of available investigation modules and telemetry to those specific to recent intrusions on federated identity sources and applications. Sparrow can be found on CISA's GitHub page at https://github.com/cisagov/Sparrow <https://github.com/cisagov/sparrow>.

Give Feedback

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.

- (*Updated January 6, 2021*): Most organizations have SAML tokens with 1-hour validity periods. Long SAML token validity durations, such as 24 hours, could be unusual. Exact values (measured in precise seconds) is also considered 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 January 6, 2021*): Tokens with missing or unusual MFA details, when MFA is enforced, is considered an anomaly and should be investigated. This requires correlation of identity provider (iDP) logs with cloud access; differences in claims indicate manipulated values. All claims should have a corresponding iDP entry.

(*New December 21, 2020*): see the National Security Agency (NSA) Cybersecurity Advisory: Detecting Abuse of Authentication Mechanisms <https://media.defense.gov/2020/dec/17/2002554125/-1/-1/0/authentication_mechanisms_csa_u_oo_198854_20.pdf> 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.

Give Feedback

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 <https://attack.mitre.org/versions/v8/techniques/t1012/>]
- *Obfuscated Files or Information* [T1027 <https://attack.mitre.org/versions/v8/techniques/t1027/>]
- *Obfuscated Files or Information: Steganography* [T1027.003 <https://attack.mitre.org/versions/v8/techniques/t1027/003>]
- *Process Discovery* [T1057 <https://attack.mitre.org/versions/v8/techniques/t1057/>]
- *Indicator Removal on Host: File Deletio*n [T1070.004 <https://attack.mitre.org/versions/v8/techniques/t1070/004>]
- *Application Layer Protocol: Web Protocols* [T1071.001 <https://attack.mitre.org/versions/v8/techniques/t1071/001>]
- *Application Layer Protocol: DNS* [T1071.004 <https://attack.mitre.org/versions/v8/techniques/t1071/004>]
- *File and Directory Discovery* [T1083 <https://attack.mitre.org/versions/v8/techniques/t1083/>]
- *Ingress Tool Transfer* [T1105 <https://attack.mitre.org/versions/v8/techniques/t1105/>]
- *Data Encoding: Standard Encoding* [T1132.001 <https://attack.mitre.org/versions/v8/techniques/t1132/001>]
- *Supply Chain Compromise: Compromise Software Dependencies and Development Tools* [T1195.001 <https://attack.mitre.org/versions/v8/techniques/t1195/001>]
- *Supply Chain Compromise: Compromise Software Supply Chain* [T1195.002 <https://attack.mitre.org/versions/v8/techniques/t1195/002>]
- *Software Discovery* [T1518 <https://attack.mitre.org/versions/v8/techniques/t1518/>]
- *Software Discovery: Security Software* [T1518.001 <https://attack.mitre.org/versions/v8/techniques/t1518/001>]

Give Feedback

- *Create or Modify System Process: Windows Service* [T1543.003 <https://attack.mitre.org/versions/v8/techniques/t1543/003>]
- *Subvert Trust Controls: Code Signing* [T1553.002 <https://attack.mitre.org/versions/v8/techniques/t1553/002>]
- *Dynamic Resolution: Domain Generation Algorithms* [T1568.002 <https://attack.mitre.org/versions/v8/techniques/t1568/002>]
- *System Services: Service Execution* [T1569.002 <https://attack.mitre.org/versions/v8/techniques/t1569/002>]
- *Compromise Infrastructure* [T1584 <https://attack.mitre.org/versions/v8/techniques/t1584/>]

Mitigations

(*Updated January 6, 2021*) SolarWinds Orion Owners

Networks with SolarWinds Orion products will generally fall into one of three categories. (**Note**: for the purposes of mitigation analysis, a network is defined as any computer network with hosts that share either a logical trust or any account credentials with SolarWinds Orion.)

- **Category 1** includes those who do not have the identified malicious binary code on their network and can forensically confirm that the binary was never present on their systems. This includes networks that do not, and never did, utilize the affected versions of SolarWinds Orion products (see Appendix A).

Give Feedback

- **Category 2** includes networks where the presence of the malicious binary has been identified—with or without beaconing to `avsvmcloud[.]com`. This includes networks that previously utilized affected versions of SolarWinds Orion but where the organization has forensically verified (through comprehensive network monitoring and analysis) that platforms running the affected software either:

  a. Had no beaconing, or

  b. Only beaconed to `avsvmcloud[.]com` and have not had any secondary C2 activity to a separate domain or IP address or other adversary activity or secondary actions on objectives (AOOs),[6 <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/seven_ways_to_apply_the_cyber_kill_chain_with_a_threat_intelligence_platform.pdf>] such as SAML token abuse.

Give Feedback

- Category 2 organizations, after conducting appropriate forensic analysis to ensure they only have Category 2 activity, can rebuild the platform, harden the configuration based on SolarWinds secure configuration guidelines, and resume use as determined by and consistent with their thorough risk evaluation. For entities not subject to ED 21-01, this can be accomplished by following the steps below. Federal agencies subject to ED 21-01 must follow the appropriate steps as outlined in the effective ED 21-01 supplemental guidance.

  a. Denying all incoming and outgoing (`any:any`) communications outside of the organization's device network management enclave, with additional assurance that communications to the public internet to and from hosts running SolarWinds Orion products has been blocked.

  b. Cloud instances of Orion should only monitor cloud resources in that cloud infrastructure.

  c. On-premises instances of Orion should not be permissioned with any cloud/hosted identity accounts.

  d. Restoration of SolarWinds may be done from the legacy database following the SolarWinds restore guidance (http://solarwinds.com/upgrading-your-environment <http://solarwinds.com/upgrading-your-environment>). Restoration for affected versions wil differ from restoration for unaffected versions—agencies must ensure that they are following the correct restoration guidance.

Give Feedback

e. Before building SolarWinds:

   a. All account credentials, or other shared secrets (e.g., Simple Network Management Protocol [SNMP] strings) that are or had been utilized by the affected SolarWinds Orion device being rebuilt should be changed.

   b. Enable MFA for these credentials, whenever possible.

   c. Provide service accounts with the minimum privilege necessary for the role performed, whenever possible.

   d. For accounts where MFA is not possible (e.g., service accounts), use randomly generated long and complex passwords (greater than 25 characters) and implement a maximum 90-day rotation policy for these passwords.

   e. Remove all inbound trust relationships to the SolarWinds Orion device being rebuilt.

f. Re-building a SolarWinds Orion Platform to at least version 2020.2.1 HF2 and updating the host to the latest supported build, at least Windows 2016.

g. Following the SolarWinds secure configuration (hardening) guidelines provided by the vendor, which can be found at: https://documentation.solarwinds.com/en/Success_Center/orionplatform/conten
core-secure-configuration.htm <https://documentation.solarwinds.com/en/success_center/orionplatform/content/core-secure-configuration.htm>. CISA does not recommend configuring the SolarWinds software to implement SAML-based authentication that relies on Microsoft's Active Directory Federated Services if it has not already been configured to leverage SAML. This configuration is currently being exploited by the threat actor with this activity.

h. Configuring logging to ensure that all logs on the host operating system and SolarWinds platform are being captured and stored for at least 180 days.

i. Configure logging to ensure that all logs from the host OS, SolarWinds platform, and associated network logs are being captured and stored for at least 180 days in a separate, centralized log aggregation capability.

Give Feedback

j. Implementing subsequent SolarWinds Orion Platform updates. CISA recommends installing all updates within 48 hours of release.

- **Category 3** includes those networks that used affected versions of SolarWinds Orion and have evidence of follow-on threat actor activity, such as binary beaconing to `avsvmcloud[.]com` and secondary C2 activity to a separate domain or IP address (typically but not exclusively returned in `avsvmcloud[.]com` CNAME responses). Additionally, organizations that have observed communications with `avsvmcloud[.]com` that appear to suddenly cease prior to December 14, 2020—not due to an action taken by their network defenders—fall into this category. Assume the environment has been compromised, and initiate incident response procedures immediately. Recovery and remediation of Category 3 activity requires a complex reconstitution and mitigation plan, which may include comprehensively rebuilding the environment. This should be coordinated with an organization’s leadership and incident response team.

Compromise Mitigations

(*Updated January 6, 2021*): 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 n 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. A Microsoft blog post, Advice for incident responders on recovery from systemic identity compromises outlines processes and procedures needed to remediate this type of activity and retain administrative control of an environment. In addition to the recommendations in this blog post, CISA recommends the following actions:

1. Take actions to remediate kerberoasting, including, as necessary or appropriate, engaging with a 3rd party with experience eradicating APTs from enterprise networks. For Windows environments, refer to the following:
    a. See Microsoft's documentation on kerberoasting: https://techcommunity.microsoft.com/t5/microsoft-security-and/detecting-ldap-based-kerberoasting-with-azure-atp/ba-p/462448 <https://techcommunity.microsoft.com/t5/microsoft-security-and/detecting-ldap-based-kerberoasting-with-azure-atp/ba-p/462448>.

    b. Change all account credentials, or other shared secrets (e.g., SNMP strings) that were potentially exposed:

        i. Enable MFA for these credentials, whenever possible;

        ii. Provide service accounts with the minimum level of privilege necessary for the role performed, whenever possible; and

        iii. For accounts where MFA is not possible, require use of randomly generated long and complex passwords (greater than 25 characters) and implement a maximum 90-day rotation policy for these passwords.

    c. Replace the user accounts with a Group Managed Service Account (gMSA). See https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview <https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview>, and Implement Group Managed Service Accounts: https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview <https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview>.

    d. Set account options for service accounts to support AES256_CTS_HMAC_SHA1_96 and not support DES, RC4, or AES128 bit encryption

e. 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 <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos>

f. 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 <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password>.

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 <https://cyber.dhs.gov/ed/21-01/#what-does-the-directive-mean-by-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 <https://cyber.dhs.gov/ed/21-01/> (and forthcoming associated guidance) for mitigation steps.

Give Feedback

- **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 <https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software>, 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.

Give Feedback

- (*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.
- 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 <https://us-cert.cisa.gov/ncas/alerts/aa20-245a> 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

- 1-844-Say-CISA (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/ <http://www.us-cert.cisa.gov/>.

Appendix A: Affected SolarWinds Orion Products

Give Feedback

Table 1 identifies recent versions of SolarWinds Orion Platforms and indicates whether they have been identified as having the Sunburst backdoor present. (*Updated January 6, 2021*: added SHA-1 and MD5 hashes to table 1; updated SHA-256 hash for version 2019.4 HF6).

Table 1: Affected SolarWinds Orion Products

Orion Platform Version	Sunburst Backdoor Code Present	File Version	SHA-256	SHA-1	MD5
2019.4	Tampered but not backdoored	2019.4.5200.8890	a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc	5e643654179e8b4cfe1d3c1906a90a4c8d611cea	e18a6a21eb44e77ca8d739a72209c370
2019.4 HF1	No	2019.4.5200.8950	9bee4af53a8cdd7ecabe5d0c77b6011abe887ac516a5a22ad51a058830403690	48e84a1ed30d36f6750bce8748fe0edbfa9fb3dc	b3f7ac8215b73e73e1e184933c788759

Orion Platform Version	Sunburst Backdoor Code Present	File Version	SHA-256	SHA-1	MD5
2019.4 HF2	No	2019.4.5200.8996	bb86f66d11592e3312cd03423b754f7337aeebba9204f54b745ed3821de6252d	162bb92a18bb39ac7e9a9997369a6efe0dd74094	563d4d55eae72710f9419975d087fd11
2019.4 HF3	No	2019.4.5200.9001	ae6694fd12679891d95b427444466f186bcdcc79bc0627b590e0cb40de1928ad	98bb0c5d1a711472225dc1194133f37c80159664	d22e80d03fe69389cbf3299f6f800f80

Orion Platform Version	Sunburst Backdoor Code Present	File Version	SHA-256	SHA-1	MD5
2019.4 HF4	No	2019.4.5200.9045	9d6285db647e7eeabdb85b409fad61467de1655098fec2e25aeb7770299e9fee	2a255070160b1c6fcad4f0586b64691fe8b6d0f8	6b5f205d79a647b275500597975314a5
2020.2 RC1	Yes	2020.2.100.12219	dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b	1acf3108bf1e376c8848fbb25dc87424f2c2a39c	731d724e8859ef063c03a8b1ab7f81ec

Orion Platform Version	Sunburst Backdoor Code Present	File Version	SHA-256	SHA-1	MD5
2019.4 HF5	Yes	2019.4.5200.9083	32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77	76640508b1e7759e548771a5359eaed353bf1eec	b91ce2fa41029f6955bff20079468448
2020.2 RC2	Yes	2020.2.5200.12394	019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134	2f1a5a7411d015d01aaee4535835400191645023	2c4a910a1299cdae2a4e55988a2f102e

Orion Platform Version	Sunburst Backdoor Code Present	File Version	SHA-256	SHA-1	MD5
2020.2 2020.2 HF1	Yes	2020.2.5300.12432	ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6	d130bd75645c2433f88ac03e73395fba172ef676	846e27a652a5e1bfbd0ddd38a16dc865
2019.4 HF6	No	2019.4.5200.9106	8dfe613b00d495fb8905bdf6e1317d3e3ac1f63a626032fa2bdad4750887ee8a	00f66fc1f74b9ecabf1aafc123f2ef0f94edc258	1412c74537fc769b5dd34b4c1da0bf48

Orion Platform Version	Sunburst Backdoor Code Present	File Version	SHA-256	SHA-1	MD5
2020.2.1 2020.2.1 HF1	No	2020.2.15300.12766	143632672dcb6ef324343739636b984f5c52ece0e078cfee7c6cac4a3545403a	8acbcc116baa80262d09635bd312018372fefca6	2d9b1245d42bb9f928da2528bb057de2
2020.2.1 HF2	No	2020.2.15300.12901	cc870c07eeb672ab33b6c2be51b173ad5564af5d98bfc02da02367a9e349a76f	babf9af689033fa2a825528715ae6dc625619e65	610ec1ab7701b410df1e309240343cdf

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; added multiple new IOCs on January 6, 2021 (new IOCs added are at the bottom of the table); corrected typos, added new IOC, and deleted duplicate hash on January 7, 2021.*

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/ <//msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/%20>	

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/ <https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/>	

IOC	Type	Notes	References	Source
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af	hash	Backdoor.Sunburst	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/ <//msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/%20>	

IOC	Type	Notes	References	Source
13.59.205[.]66	IPv4	DEFTSECURITY[.]com	https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
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.virustotal.com/gui/domain/deftsecurity.com/details> https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://w	Volexity

IOC	Type	Notes	References	Source
			ww.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	

IOC	Type	Notes	References	Source
54.193.127[.]66	IPv4	FREESCANONLINE[.]com	https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	

IOC	Type	Notes	References	Source
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c	hash	No info available	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/ <//msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/%20>	

IOC	Type	Notes	References	Source
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77	hash	No info available	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/ </msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/%20>	

IOC	Type	Notes	References	Source
dab758bf98d9b36fa05766cd0284737abf89857b73ca89280267ee7caf62f3b	hash	No info available	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/ <//msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/%20>	

IOC	Type	Notes	References	Source
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed	hash	No info available	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/ </msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/%20>	

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.	https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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/ <//msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/%20> FireEye Report Talos Volexity

IOC	Type	Notes	References	Source
		1, which is registered with Microsoft. malware callhome, command and control		

IOC	Type	Notes	References	Source
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/ <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/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
54.215.192[.]52	IPv4	THEDOCCLOUD[.]com	https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
019085a76ba7126fff22770d71bd901c325fc68ac55aa7433279844e89f4b0134	hash	Trojan.MSIL.SunBurst	ttps://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/ <//msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/%20>	

IOC	Type	Notes	References	Source
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6	hash	Trojan.MSIL.SunBurst	https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/ <//msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/%20>	

IOC	Type	Notes	References	Source
8.18.144[.]11	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]12	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]9	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]20	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]40	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]44	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]62	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]130	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

Give Feedback

IOC	Type	Notes	References	Source
8.18.144[.]135	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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/ <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[.]149	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]156	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]158	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]165	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]170	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]180	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]188	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]3	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]21	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]33	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]36	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]131	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]134	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]136	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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/ <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[.]150	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]157	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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[.]181	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
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/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
18.217.225[.]111	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
18.220.219[.]143	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
20.141.48[.]154	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
34.219.234[.]134	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
184.72.1[.]3	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
184.72.21[.]54	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
184.72.48[.]22	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
184.72.101[.]22	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
184.72.113[.]55	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
184.72.145[.]34	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
184.72.212[.]52	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
184.72.224[.]3	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
184.72.229[.]1	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
184.72.240[.]3	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
184.72.245[.]1	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
196.203.11[.]89	IPv4		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
digitalcollege[.]org	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
freescanonline[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
globalnetworkissues[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
kubecloud[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
lcomputers[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
seobundlekit[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
solartrackingsystem[.]net	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
thedoccloud[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <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/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
webcodez[.]com	domain		https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity

IOC	Type	Notes	References	Source
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	

IOC	Type	Notes	References	Source
ervsystem[.]com	domain	*New January 6, 2021* Resolves to 198.12.75[.]112	https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds>	Symantec

IOC	Type	Notes	References	Source
infinitysoftwares[.]com	domain	*New January 6, 2021* *Updated January 7, 2021: corrected typo in this IOC; updated source*	https://otx.alienvault.com/pulse/5fdce61ef056eff2ce0a90de <https://otx.alienvault.com/pulse/5fdce61ef056eff2ce0a90de>	
mobilnweb[.]com	domain	*New January 6, 2021* *Updated January 7, 2021: updated source*		CISA

IOC	Type	Notes	References	Source
02AF7CEC58B9A5DA1C542B5A32151BA1	Hash	*New January 6, 2021* Sunburst Installer File Name(s): CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp		Symantec Sunburst: Supply Chain Attack Targets SolarWinds Users

IOC	Type	Notes	References	Source
0548eedb3d1f45f1f9549e09d00683f3a1292ec5	Hash	*New January 6, 2021* SSL hash for 198.12.75[.]112		
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589	Hash	*New January 6, 2021*		CISA

IOC	Type	Notes	References	Source
1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c	Hash	*New January 6, 2021* Sunburst Backdoor	https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds>	Symantec

IOC	Type	Notes	References	Source
1b476f58ca366b54f34d714ffce3fd73cc30db1a	Hash	*New January 6, 2021* Sunburst Installer File Name(s): CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp		Symantec Sunburst: Supply Chain Attack Targets Solar Winds Users
20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9	Hash	*New January 6, 2021*		CISA

IOC	Type	Notes	References	Source
2b3445e42d64c85a5475bdbc88a50ba8c013febb53ea97119a11604b7595e53d	Hash	*New January 6, 2021*	https://otx.alienvault.com/pulse/5fd6df943558e0b56eaf3da8 <https://otx.alienvault.com/pulse/5fd6df943558e0b56eaf3da8>	CISA
2dafddbfb0981c5aa31f27a298b9c804e553c7bc	Hash	*New January 6, 2021*		
6e4050c6a2d2e5e49606d96dd2922da480f2e0c70082cc7e54449a7dc0d20f8d	Hash	*New January 6, 2021*		CrowdStrike

IOC	Type	Notes	References	Source
92bd1c3d2a11fc4aba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690	Hash	*New January 6, 2021*		CISA
a3efbc07068606ba1c19a7ef21f4de15d15b41ef680832d7bcba485143668f2d	Hash	*New January 6, 2021*		CISA
a58d02465e26bdd3a839fd90e4b317eece431d28cab203bbdde569e11247d9e2	Hash	*New January 6, 2021*		CISA

IOC	Type	Notes	References	Source
b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07	Hash	*New January 6, 2021* Sunburst Backdoor	https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds>	Symantec

IOC	Type	Notes	References	Source
b8a05cc492f70ffa4adcd446b693d5aa2b71dc4fa2bf5022bf60d7b13884f666	Hash	*New January 6, 2021*	https://otx.alienvault.com/pulse/5fd6df943558e0b56eaf3da8 <https://otx.alienvault.com/pulse/5fd6df943558e0b56eaf3da8>	
cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70e01dc69048e6	Hash	*New January 6, 2021*		CISA
e0b9eda35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d	Hash	*New January 6, 2021*		CISA

IOC	Type	Notes	References	Source
e70b6be294082188cbe0089dd44dbb86e365f6a2	Hash	*New January 6, 2021* SSL hash for 107.152.35[.]77		
fd15760abfc0b2537b89adc65b1ff3f072e7e31c	Hash	*New January 6, 2021*	https://otx.alienvault.com/pulse/5fd6df943558e0b56eaf3da8 <https://otx.alienvault.com/pulse/5fd6df943558e0b56eaf3da8>	

IOC	Type	Notes	References	Source
ffdbdd460420972fd2926a7f460c198523480bc6279dd6cca177230db18748e8	Hash	*New January 6, 2021*	https://otx.alienvault.com/pulse/5fd6df943558e0b56eaf3da8 <https://otx.alienvault.com/pulse/5fd6df943558e0b56eaf3da8>	
107.152.35[.]77	IPv4	*New January 6, 2021* Resolves to infinitysoftwares[.]com		

IOC	Type	Notes	References	Source
13.59.205[.]66	IPv4	*New January 6, 2021*	https://otx.alienvault.com/pulse/5fd825b7fa4eb2223a0cf812 <https://otx.alienvault.com/pulse/5fd825b7fa4eb2223a0cf812>	
173.237.190[.]2	IPv4	*New January 6, 2021*		CISA

IOC	Type	Notes	References	Source
198.12.75[.]112	IPv4	New January 6, 2021 Resolves to ervsystem[.]com *Updated January 7, 2021: Corrected typo in resolves to domain*		Symantec Sunburst: Supply Chain Attack Targets SolarWinds Users

IOC	Type	Notes	References	Source
20.141.48[.]154	IPv4	*New January 6, 2021* *Updated January 7, 2021: updated reference and source*	https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>	Volexity
34.203.203[.]23	IPv4	*New January 7, 2021*		CISA

References

[1] Volexity: Dark Halo Leverages SolarWinds Compromise to Breach Organizations <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>

[2] SolarWinds Security Advisory <https://www.solarwinds.com/securityadvisory>

[3] FireEye: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>

[4] GitHub: Azure / Azure-Sentinel - ADFSDomainTrustMods.yaml <https://github.com/azure/azure-sentinel/blob/master/detections/auditlogs/adfsdomaintrustmods.yaml>

[5] GitHub: CISA: Sparrow <https://github.com/cisagov/sparrow>

[6] Lockheed Martin: Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platfor <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/seven_ways_to_apply_the_cyber_kill_chain_with_a_threat_intelligence_platform.pdf>

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|January 0 2021: Updated Initial Access Vectors, Mitigations, and IOCs|January 07, 2021: Updated IOCs|Febraury 08, 2021: Updated IOCs|April 13, 2021: Fixed Spelling Error|April 15, 2021: Updated with Attribution Statement and SUNSHUTTLE MAR

Give Feedback

Tags

Nation-State Actor: Russia

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

CISA.gov

An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>

Give Feedback