Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise

Updates:

- **May 14, 2021:** *The Cybersecurity and Infrastructure Security Agency (CISA) has updated this page based on public release of detailed eviction guidance for this activity: AR21-134A: Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise and Supplemental Direction Version 4 to Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise.*
- **May 7, 2021:** *CISA Fact Sheet: Russian SVR Activities Related to SolarWinds Compromise lists advisories on the SVR malicious activity.*
- **April 15, 2021:** *Statement from the White House provides U.S. Government attribution of this activity to the SVR.*

Since December 2020, CISA has been responding to a significant cybersecurity incident affecting networks of multiple U.S. government agencies, critical infrastructure entities, and private sector organizations, in which advanced persistent threat (APT) actors—identified on April 15, 2020, as the Russian Foreign Intelligence Service (SVR) actors—gained long-term access to organizations' enterprise networks and moved laterally to Microsoft cloud systems, i.e., Azure Active Directory (AD) and Microsoft 365 (M365) environments. The SVR actors used privileged access to collect and exfiltrate sensitive data and created backdoors to enable their return.

***Note:** although the guidance on this webpage is tailored to federal departments and agencies, CISA encourages critical infrastructure and private sector organizations to review and apply it, as appropriate. For more information on CISA's response to this activity, refer to cisa.gov/supply-chain-compromise.*

Russian SVR APT Actor Activity

Russian SVR APT Actor Activity

The SVR actors added malicious code to certain versions of the SolarWinds Orion platform and leveraged it for initial access to select enterprise networks. Through incident response, CISA determined that, in other instances, the SVR actors obtained initial access by password guessing, password spraying, and exploiting inappropriately secured administrative credentials via remote services.

In some instances, once inside the network, the SVR actors bypassed multi-factor authentication (MFA) and moved laterally to Microsoft cloud systems by compromising federated identity solutions. SVR actors:

- Stole the Active Directory Federation Service (ADFS) token-signing certificate to forge Security Assertion Markup Language (SAML) tokens. This technique—referred to as "Golden SAML"—enabled SVR actors to bypass the federated resource provider's MFA and password requirements and thereby move laterally to M365 environments.
- Modified or added trusted domains in Azure AD. This technique enabled SVR actors to add new federated identity providers (iDPs) and thereby move laterally to Azure AD environments. (See FireEye White Paper: Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452.)

After gaining access to cloud environments, the SVR actors established persistence mechanisms for Application Programming Interface (API)-based access and collected and exfiltrated data.

The SVR actors have demonstrated sophisticated defense evasion skills. They:

- Hid their command and control (C2) communications with extensive obfuscation,
- Hid their activity among legitimate user traffic, and
- Established difficult-to-detect persistence mechanisms (e.g., in API).

Note: for more information on this activity, including tactics, techniques, and procedures (TTPs), refer to CISA Alerts and joint publications:

- Joint NCSC-CISA-FBI-NSA CSA: Further TTPs associated with SVR cyber actors
- AA21-116A Joint FBI-DHS-CISA Cybersecurity Advisory: SVR Cyber Operations: Trends and Best Practices for Network Defenders
- Joint NSA-CISA-FBI Cybersecurity Advisory: Russian SVR Targets U.S. and Allied Networks
- AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments
- AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

Risk/Impact Assessment

Risk/Impact Assessment

Organizations that used affected versions of SolarWinds Orion should conduct a risk assessment, if they have not already done so, to determine if their network was compromised, and if applicable, the severity of compromise. As defined in CISA Activity Alert

AA20-352A:Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations, networks with SolarWinds Orion products will fall into one of three categories.

- **Category 1** includes agency networks that 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, use the affected versions of SolarWinds Orion products.
- **Category 2** includes agency networks where the presence of the malicious binary has been identified—with or without beaconing to `avsvmcloud[.]com`.
- **Category 3** includes agency 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` Canonical Name record [CNAME] responses).

Note: As described above, CISA is aware of other initial access vectors. Organizations should not assume they are not compromised by this actor solely because they have never used affected versions of SolarWinds Orion. Those organizations should investigate to confirm they have not observed related threat actor TTPs.

Resources

- CISA Activity Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
- CISA Emergency Directive (ED) 21-01: Mitigate SolarWinds Orion Code Compromise

Remediating Malicious Activity: Category 1 and 2 Organizations

Remediating Malicious Activity: Category 1 and 2 Organizations

Although unaffected by this incident, **Category 1** organizations should work to maintain strong network posture and resilience. Refer to https://www.cisa.gov/cybersecurity and https://us-cert.cisa.gov/resources/federal for assistance. CISA recommends Category 1 organizations:

- Maintain up-to-date antivirus signatures and engines. See Protecting Against Malicious Code.
- Ensure systems have the latest security updates. See Understanding Patches and Software Updates.
- Enforce a strong password policy. See Choosing and Protecting Passwords.
- Exercise caution when opening email attachments, even if the attachment is expected and the sender appears to be known. See Using Caution with Email Attachments.
- Sign up to receive CISA’s alerts on security topics and threats.

- Sign up for CISA's free vulnerability scanning and testing services to help organizations secure internet-facing systems from weak configuration and known vulnerabilities.
- Email vulnerability@cisa.dhs.gov to sign up. See https://www.cisa.gov/cyber-resource-hub for more information about vulnerability scanning and other CISA cybersecurity assessment services.

Category 2 organizations should continue enhanced monitoring for any possible follow-on adversary activity. Refer to resources below for more information.

Resources:

- CISA Activity Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
- CISA Activity Alert AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments
- CISA Emergency Directive (ED) 21-01: Mitigate SolarWinds Orion Code Compromise

According to ED 21-01 and associated supplemental guidance, all federal agencies that ran affected versions of SolarWinds Orion must "conduct system memory, host storage, network, and cloud forensic analysis," "hunt for indicators of compromise (IOCs) or other evidence of threat actor activity, such as secondary actions on objectives (AOO)," and "[i]dentify and remove all threat actor-controlled accounts and identified persistence mechanisms."

Remediating Malicious Activity: Category 3 Organizations

Remediating Malicious Activity: Category 3 Organizations

Remediation plans for dealing with malicious compromises are necessarily unique to every organization, and success requires careful consideration. To assist affected organizations in crafting eviction plans, CISA has released AR21-134A: Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise, which provides in-depth steps and resources for eviction. The guidance has three phases:

- **Phase 1: Pre-Eviction.** Actions to detect and identify APT activity and prepare the network for eviction.
- **Phase 2: Eviction.** Actions to remove the APT actor from on-premises and cloud environments. This phase includes rebuilding devices and systems.
- **Phase 3: Post-Eviction.** Actions to ensure eviction was successful and the network has good cyber posture.

In accordance with ED-21-01: Supplemental Direction Version 4, agencies which had or have affected versions of SolarWinds Orion and have evidence of follow-on threat actor activity must execute and complete applicable eviction steps by July 16, 2021.

Completing all the steps provided in the eviction guidance is necessary to fully accomplish eviction.

The eviction will be resource-intensive and highly complex, requiring the enterprise network to be disconnected from the internet for 3–5 days; however, failure to perform a comprehensive and thorough remediation will expose enterprise networks and cloud environments to substantial risk of long-term undetected APT activity, including email monitoring, data collection, and exfiltration. CISA recommends organization leadership read the CISA Insights, Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise: Risk Decisions for Leaders, for more information.

Resources: CISA, Federal Government, and International Partner Publications

Resources: CISA, Federal Government, and International Partner Publications

Note: the following publications focus on the SolarWinds Orion Compromise and Related Activity

Table 1: CISA, Federal Government, SLTT, and International Partners Publications

Publication Date	Title
SolarWinds Orion Compromise and Related Activity	
5/14/2021	Analysis Report AR21-134A: Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise
5/14/2021	CISA Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise and Supplemental Direction ***Note:*** *initial publication of ED 21-01 was 12/13/2021; latest update to supplemental direction (version 4) was 5/14/2021.*
5/7/2021	Fact Sheet: Russian SVR Activities Related to SolarWinds Compromise
5/7/2021	Joint NCSC-CISA-FBI-NSA Cybersecurity Advisory: Further TTPs Associated with SVR Cyber Actors
5/7/2021	Current Activity: Joint NCSC-CISA-FBI-NSA Cybersecurity Advisory on Russian SVR Activity

Publication Date	Title
4/26/2021	FBI-DHS-CISA Joint Cybersecurity Advisory AA21-116A: Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders
4/26/2021	CISA Current Activity: FBI-DHS-CISA Joint Advisory on Russian Foreign Intelligence Service Cyber Operations
4/15/2021	CISA Malware Analysis Report: MAR-10327841-1.v1 – SUNSHUTTLE
4/15/2021	CISA Current Activity: CISA and CNMF Analysis of SolarWinds-related Malware
4/15/2021	NSA-CISA-FBI Joint Cybersecurity Advisory: Russian SVR Targets U.S. and Allied Networks
4/15/2021	CISA Current Activity: NSA-CISA-FBI Joint Advisory on Russian SVR Targeting U.S. and Allied Networks
4/8/2021	CISA Current Activity: Using Aviary to Analyze Post-Compromise Threat Activity in M365 Environments
3/18/2021	CISA Alert AA21-077A: Detecting Post-Compromise Threat Activity Using the CHIRP IOC Detection Tool
3/18/2021	CISA Current Activity: Using CHIRP to Detect Post-Compromise Threat Activity in On-Premises Environments
3/9/2021	CISA Insights: SolarWinds and Active Directory/M365 Compromise: Risk Decisions for Leaders
3/9/2021	CISA Current Activity: Guidance on Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise
2/8/2021	CISA Malware Analysis Report: MAR-10318845-1.v1 - SUNBURST
2/8/2021	CISA Malware Analysis Report: MAR-10320115-1.v1 - TEARDROP
2/8/2021	CISA Activity Alert AA20-352A: APT Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations ***Note:*** *initial publication of Alert was 12/17/2020; latest update was 4/15/2021.*
1/8/2021	CISA Alert AA21-008A: Detecting Post- Compromise Threat Activity in Microsoft Cloud Environments

Publication Date	Title
1/8/2021	CISA Current Activity: CISA Releases New Alert on Post-Compromise Threat Activity in Microsoft Cloud Environments and Tools to Help Detect This Activity
1/6/2021	CISA Current Activity: CISA Updates Emergency Directive 21-01 Supplemental Guidance and Activity Alert on SolarWinds Orion Compromise
1/5/2021	CISA/FBI/NSA/ODNI Joint Statement
12/30/2020	Canadian Centre for Cyber Security Alert: Recommendations for SolarWinds Supply-Chain Compromise - Update 1
12/29/2020	Australian Cyber Security Centre Alert: Potential SolarWinds Orion compromise
12/26/2020	CERT/CC: Vulnerability Note VU#843464: SolarWinds Orion API authentication bypass allows remote command execution
12/24/2020	CISA Current Activity: CISA Releases Free Detection Tool for Azure/M365 Environment
12/24/2020	Canadian Centre for Cyber Security Alert: Recommendations for SolarWinds Supply-Chain Compromise
12/23/2020	CISA: Supply Chain Compromise webpage
12/23/2020	CISA Current Activity: CISA Releases CISA Insights and Creates Webpage on Ongoing APT Cyber Activity
12/23/2020	CISA Insight: What Every Leader Needs to Know About the Ongoing APT Cyber Activity
12/22/2020	MS-ISAC: The SolarWinds Cyber-Attack: What SLTTs Need to Know ***Note:*** *latest update was 12/22/2020.*
12/21/2020	UK NCSC statement on the SolarWinds compromise
12/19/2020	CISA Current Activity: CISA Updates Alert and Releases Supplemental Guidance on Emergency Directive for SolarWinds Orion Compromise
12/17/2020	CISA Current Activity: NSA Releases Cybersecurity Advisory on Detecting Abuse of Authentication Mechanisms
12/17/2020	NSA Cybersecurity Advisory: Detecting Abuse of Authentication Mechanisms

Publication Date	Title
12/17/2020	Canadian Centre for Cyber Security Alert: Advanced Persistent Threat Compromises (CISA)
12/16/2020	CISA/FBI/ODNI Joint Statement
12/15/2020	UK National Cyber Security Centre: Dealing with the SolarWinds Orion compromise
12/14/2020	Australian Cyber Security Centre Alert: Potential SolarWinds Orion compromise
12/13/2020	CISA Current Activity: Active Exploitation of SolarWinds Software
General Cybersecurity Information	
5/19/2019	NCSC: Security Architecture Anti-Patterns

Table 2: Industry Publications

Publication Date	Title
SolarWinds Orion Compromise and Related Activity	
3/4/2021	MITRE's Center for Threat-Informed Defense Public Resources (GitHub): Solorigate ***Note:*** *latest update was 3/4/2021.*
1/12/2021	Cisco Event Response: SolarWinds Orion Platform Software Attack ***Note:*** *latest update was 1/12/2021.*
12/31/2020	Microsoft: Internal Solorigate Investigation Update
12/21/2020	Microsoft: Solorigate Research Center
12/21/2020	Microsoft: Understanding “Solorigate”’s Identity IOCs - for Identity Vendors and their customers
12/18/2020	MITRE (Medium): Identifying UNC2452-Related Techniques for ATT&CK
12/17/2020	Microsoft: Latest Threat Intelligence (15 December 2020) - FireEye and SolarWinds Events

Publication Date	Title
12/15/2020	CrowdStrike: The Imperative to Secure Identities: Key Takeaways from Recent High- Profile Breaches
12/14/2020	Volexity: Dark Halo Leverages SolarWinds Compromise to Breach Organizations
12/14/2020	Symantec: Sunburst: Supply Chain Attack Targets SolarWinds Users
12/14/2020	Cisco Talos: FireEye Breach Detection Guidance
12/14/2020	Cisco Talos Threat Advisory: SolarWinds supply chain attack
12/14/2020	Cisco Talos: SolarWinds Orion Platform Supply Chain Attack
12/13/2020	FireEye: Global Intrusion Campaign Leverages Software Supply Chain Compromise
12/13/2020	FireEye: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor
12/13/2020	Microsoft: Important steps for customers to protect themselves from recent nation- state cyberattacks
12/13/2020	Microsoft: Customer Guidance on Recent Nation-State Cyber Attacks
12/8/2020	FireEye: Unauthorized Access of FireEye Red Team Tools
Malware Analysis	
1/20/2021	Microsoft: Deep dive into the Solorigate second- stage activation: From SUNBURST to TEARDROP and Raindrop
1/18/2021	Symantec: Raindrop: New Malware Discovered in SolarWinds Investigation
1/11/2021	CrowdStrike: SUNSPOT: An Implant in the Build Process
12/24/2020	FireEye: SUNBURST Additional Technical Details
12/22/2020	CheckPoint Research: SUNBURST, TEARDROP and the NetSec New Normal
12/18/2020	Microsoft: Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers

Publication Date	Title
12/17/2020	McAfee: Additional Analysis into the SUNBURST Backdoor
12/17/2020	Palo Alto Networks: SUPERNOVA: A Novel .NET Webshell
Incident Response, Remediation, and Hardening	
1/19/2021	FireEye: Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452
12/28/2020	Microsoft: Using Microsoft 365 Defender to protect against Solorigate
12/22/2020	Microsoft: Protecting Microsoft 365 from on-premises attacks
12/22/2020	Microsoft: Azure Active Directory Workbook to Assess Solorigate Risk
12/21/2020	Microsoft: Advice for incident responders on recovery from systemic identity compromises
12/21/2020	FireEye (GitHub): FireEye Mandiant SunBurst Countermeasures
12/16/2020	Microsoft: SolarWinds Post-Compromise Hunting with Azure Sentinel
10/28/2020	Trimarc: Securing Microsoft Azure AD Connect
8/9/2018	Microsoft: AD Forest Recovery - Resetting the krbtgt Password
2/18/2016	CrowdStrike: Investigating PowerShell: Command and Script Logging
4/8/2015	FireEye: Windows Management Instrumentation (WMI) Offense, Defense, and Forensics
Technical and Investigation Information from SolarWinds	
2/24/2021	FAQ: Security Advisory ***Note:*** *latest update was 2/24/2021.*
1/19/2021	CISA/CERT Upgrading Your Environment ***Note:*** *latest update was 1/19/2021.*

Publication Date	Title
1/11/2021	New Findings from Our Investigation of SUNBURST
12/17/2020	SolarWinds Security Advisory
N/A	Secure Configuration for the Orion Platform
Detection Tools	
N/A	CISA: CHIRP
N/A	CISA: Sparrow
N/A	CrowdStrike: • CrowdStrike Reporting Tool for Azure (CRT) • CrowdStrike CRT Github page
N/A	FireEye Mandiant: Azure AD Investigator
N/A	Microsoft: • Microsoft open sources CodeQL queries used to hunt for Solorigate activity • Solorigate CodeQL queries

Note: *The information you have accessed or received is being provided "as is" for informational purposes only. DHS and CISA do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS or CISA.*