



SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity from Known Tactics, Techniques, and Procedures

March 17, 2021

Cybersecurity and Infrastructure Security Agency



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> and <https://www.cisa.gov/supply-chain-compromise>.

INTRODUCTION

The advanced persistent threat (APT) actor associated with the SolarWinds Orion supply chain compromise moved laterally to multiple systems—including Microsoft cloud environments—and established difficult-to-detect persistence mechanisms. The Cybersecurity and Infrastructure Security Agency (CISA) is providing this resource to assist network defenders in scoping the intrusion by detecting artifacts from known tactics, techniques, and procedures (TTPs) associated with this activity. Although this resource is tailored to organizations that were compromised via the SolarWinds Orion supply chain compromise, CISA is aware of other initial access vectors and organizations should not assume they are not compromised by this APT actor solely because they have never used affected versions of SolarWinds Orion. Additionally, this resource addresses follow-on activity observed in the Microsoft Azure Active Directory (AD), Office 365 (O365), and M365 environments. Organizations should confirm they have not observed related TTPs described in this resource, and, if they detect related activity, refer to CISA Alert [AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure](#), and Private Sector Organizations and contact CISA for further assistance.

For additional technical information on the SolarWinds Orion supply chain and Active Directory/M365 compromise, refer to us-cert.cisa.gov/remediating-apt-compromised-networks. For information on CISA's response to this activity, refer to [cisa.gov/supply-chain-compromise](https://www.cisa.gov/supply-chain-compromise).

Threat Actor Tactics and Techniques

Figure 1 and table 1 identify threat actor tactics and techniques observed by incident responders using the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 8. See the [ATT&CK for Enterprise framework](#) for all referenced threat actor tactics and techniques. **Note:** Neither figure 1 nor table 1 should be considered exhaustive—not all techniques have been used in every incident, and some techniques may not have been identified.

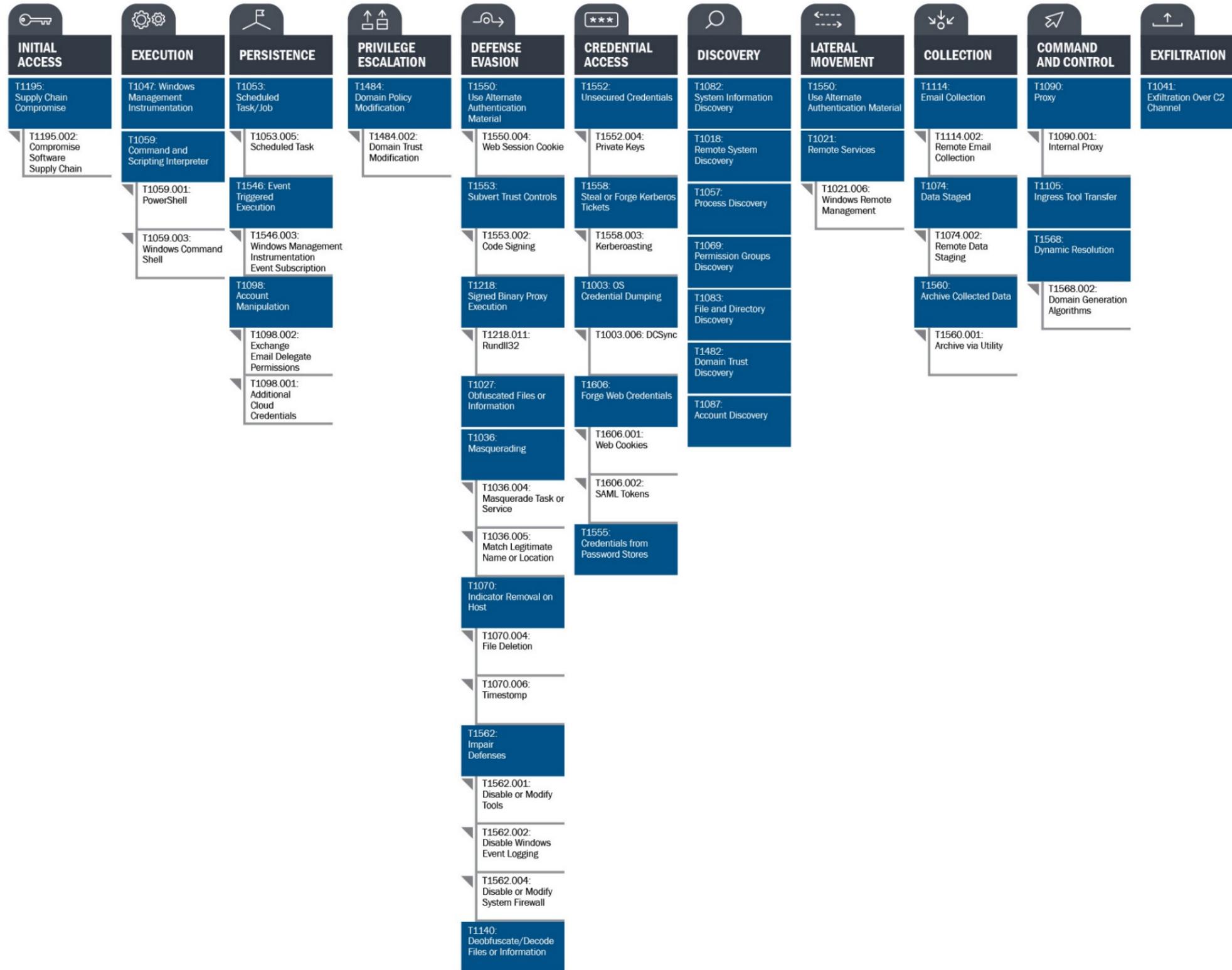


Figure 1: MITRE ATT&CK Techniques Observed

Table 1 identifies tactics and techniques observed by incident responders and provides associated detection recommendations.

Table 1: Threat Actor Techniques and Associated Detection Artifacts

Tactic	Technique	Threat Actor Activity	Detection Recommendations
Credential Access [TA0006] 	Forge Web Credentials: SAML Tokens [T1606.002]	The threat actor created tokens using compromised Security Assertion Markup Language (SAML) signing certificates. ¹	Monitor for anomalous logins from on-premises and cloud environments that trust the token signing certificate. Search for logins to service providers using SAML Single Sign On (SSO) that do not have corresponding events 4769, 1200, and 1202. ²
Defense Evasion [TA0005] 	Use Alternate Authentication Material [T1550]	The actor used forged SAML tokens to impersonate existing users in the environment with full authentication. ^{3,4}	The users being leveraged are valid users, so the artifacts are behavioral. Look for user accounts, especially privileged and service accounts, behaving abnormally. Cyber attackers prefer to use compromised credentials, so identifying accounts that use multiple login pathways, geolocations, or virtual private network (VPN) services might lead to discovery of compromised credentials, malicious autonomous systems numbers (ASNs), and suspicious activity. Internal IP management or scanning capability may show IP addresses switching between default (WIN-*) hostnames and victim's hostnames. ⁵
Lateral Movement [TA0008] 			
Execution [TA0002] 	Scheduled Task/Job: Scheduled Task [T1053.005]	The threat actor used <code>scheduler</code> and <code>schtasks</code> to create new tasks on remote hosts as part of lateral movement. The threat actor also manipulated Scheduled Tasks by updating an existing legitimate task to execute their tools and then returned the Scheduled Task to its original configuration. ^{6,7}	Audit existing scheduled tasks in the environment and review against known and expected scheduled tasks; MITRE ATT&CK recommends looking “for changes to tasks and services that do not correlate with known software, patch cycles etc.” ⁸ Verify the tasks do what they are intended to do, as this actor is known to alter existing legitimate tasks. MITRE ATT&CK also recommends monitoring “processes and command-line arguments for actions that could be taken to create tasks or services.” ⁹ In Windows 10, monitor process execution from the <code>svchost.exe</code> . In older

Tactic	Technique	Threat Actor Activity	Detection Recommendations
Persistence [TA0003] 	Scheduled Task/Job: Scheduled Task [T1053.005]	The threat actor created a Scheduled Task to maintain SUNSPOT persistence when the host booted. ¹²	versions of Windows, monitor the Windows Task Scheduler <code>taskeng.exe</code> . If you do not observe Scheduled Tasks used for persistence, then the adversary may have removed the task after it was no longer needed. ¹⁰ Monitor Windows Scheduled Tasks stored in <code>%systemroot%\System32\Tasks</code> . Look for changes related to Scheduled Tasks that do not correlate with known software updates etc. ¹¹
Defense Evasion [TA0005] 	Masquerading: Masquerade Task or Service [T1036.004]	The threat actor named tasks <code>\Microsoft\Windows\SoftwareProtectionPlatform\EventCacheManager</code> in order to appear legitimate. ¹³	
Execution [TA0002] 	Windows Management Instrumentation [T1047]	The threat actor used Windows Management Instrumentation (WMI) for the remote execution of files for lateral movement. ^{14,15,16}	Monitor network traffic for WMI connections. WMI connections in environments that do not usually use WMI may be an indicator of compromise. Capture command-line arguments of <code>wmic</code> via process monitoring and look for commands that are used for remote behavior. ¹⁷ According to Microsoft, the following was used for lateral movement via WMI: <code>wmic /node:[target] process call create "rundll32 c:\windows\[folder]\[beacon].dll [export]"</code> . ¹⁸ Note: detecting WMI connections for execution requires detecting it at the time it happens.
Lateral Movement [TA0008] 			
Persistence [TA0003] 	Event Triggered Execution: Windows Management Instrumentation Event Subscription [T1546.003]	The threat actor used WMI event subscriptions for persistence. ^{19,20}	

Tactic	Technique	Threat Actor Activity	Detection Recommendations
Exfiltration [TA0010] 	Exfiltration over C2 Channel [T1041]	The threat actor used HTTP for command and control (C2) and data exfiltration. ²¹ The threat actor’s malware used HTTP PUT or HTTP POST requests when collected data was being exfiltrated to their C2 server. ²²	Look for unusual outbound HTTP PUT or HTTP POST requests. If the payload is bigger than 10000 bytes, the POST method is used. If the payload is smaller than 10000 bytes, the PUT method is used. All HTTP POST and HTTP PUT requests will have a JavaScript Object Notation (JSON) containing the keys <code>userId</code> , <code>sessionId</code> , and <code>steps</code> . The steps field contains a list of objects with the following keys: <code>Timestamp</code> , <code>Index</code> , <code>EventType</code> , <code>EventName</code> , <code>DurationMs</code> , <code>Succeeded</code> , and <code>Message</code> . The JSON key <code>EventType</code> is hardcoded to the value <code>Orion</code> , and the <code>EventName</code> is hardcoded to <code>EventManager</code> . ²³
Defense Evasion [TA0005] 	Masquerading: Match Legitimate Name or Location [T1036.005]	The threat actor renamed a version of AdFind to <code>sqlceip.exe</code> or <code>csrss.exe</code> in an attempt to appear as the Structured Query Language (SQL) Server Telemetry Client or Client Service Runtime Process, respectively. ^{24,25}	Investigate executables with parameters that do not match their known behavior. Profile expected behavior of binaries, especially code that runs with admin permissions, to identify unusual behavior. Compare the hashes of running versions of executables with the hashes of known legitimate executables. The following resources provide examples of uses of Rundll32 seen. <ul style="list-style-type: none"> • Volatility: Dark Halo Leverages SolarWinds Compromise to Breach Organizations • Microsoft: Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers
Signed Binary Proxy Execution: Rundll32 [T1218.011]	The threat actor used Rundll32 to execute payloads. ^{26,27}		
Discovery [TA0007] 	Remote System Discovery [T1018]	The threat actor used AdFind to enumerate remote systems. ²⁸	Look for executables with the following parameters (they may be the AdFind utility renamed): <code>[renamed-adfind].exe -h [internal domain] -sc u:[user] > .\[machine]\[file].[log txt]</code> . ²⁹ Refer to Microsoft: Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop for other uses of this executable. Note: this executable may be renamed to evade detection; refer to MITRE T1036.005 for guidance on detecting renamed files.

Tactic	Technique	Threat Actor Activity	Detection Recommendations
Discovery [TA0007] 	System Information Discovery [T1082]	The threat actor used <code>fsutil</code> to determine if there was sufficient available free space before executing actions that might generate large files on disk. ³⁰	Look for the following <code>fsutil</code> command: <code>fsutil volume diskfree c:.</code> ³¹
Defense Evasion [TA0005] 	Indicator Removal on Host: Timestamp [T1070.006]	The threat actor modified timestamps of backdoors to match legitimate Windows files. ³²	Use forensic techniques to detect files that have had their timestamps modified. Detecting timestomping may be possible by using file modification monitoring that collects information on file handle opens and can compare timestamp values. ³³
Credential Access [TA0006] 	OS Credential Dumping: DCSync [T1003.006]	The actor leveraged privileged accounts to replicate directory service data with domain controllers. ^{34,35,36}	MITRE ATT&CK recommends the following: “Monitor domain controller logs for replication requests and other unscheduled activity possibly associated with DCSync. Also monitor for network protocols and other replication requests from IPs not associated with known domain controllers.” ³⁷
Defense Evasion [TA0005] 	Indicator Removal on Host: File Deletion [T1070.004]	Once remote access was achieved, the threat actor frequently removed their tools, including custom backdoors. ³⁸	Monitor command-line deletion functions and compare them with binaries or other files that the threat actor may have dropped and removed. Monitor for known deletion and secure deletion tools that the actor may have introduced to the network. ³⁹
Defense Evasion [TA0005] 	Indicator Removal on Host [T1070]	The threat actor removed evidence of email export requests using <code>Remove-MailboxExportRequest</code> . The threat actor temporarily replaced legitimate utilities with their own, executed their payload, and then restored the original file. ^{40,41}	Enable command-line parameter monitoring, and look for: <code>C:\Windows\system32\cmd.exe /C powershell.exe -PSConsoleFile exshell.psc1 -Command “Get-MailboxExportRequest -Mailbox user@organization.here Remove-MailboxExportRequest -Confirm:\$False”.</code> ⁴²

Tactic	Technique	Threat Actor Activity	Detection Recommendations
Discovery [TA0007] 	Permission Groups Discovery [T1069]	The threat actor used the <code>Get-ManagementRoleAssignment PowerShell cmdlet</code> to enumerate Exchange management role assignments through an Exchange Management Shell. ⁴³	Enable command-line parameter monitoring, and look for: <code>C:\Windows\system32\cmd.exe /C powershell.exe -PSConsoleFile exshell.psc1 -Command "Get-ManagementRoleAssignment - GetEffectiveUsers select Name,Role,EffectiveUserName,AssignmentMethod,IsValid ConvertTo-Csv -NoTypeInformation % {\$ _ -replace ' `n','_'} Out-File C:\temp\1.xml".⁴⁴</code>
Discovery [TA0007] 	File and Directory Discovery [T1083]	The threat actor obtained information about the configured Exchange virtual directory using <code>Get-WebServicesVirtualDirectory</code> . ⁴⁵	Enable command-line parameter monitoring, and look for: <code>C:\Windows\system32\cmd.exe /C powershell.exe -PSConsoleFile exshell.psc1 -Command "Get-WebServicesVirtualDirectory Format-List".⁴⁶</code>
Execution [TA0002] 	Command and Scripting Interpreter: Windows Command Shell [T1059.003]	The threat actor used <code>cmd.exe</code> to execute commands on remote machines. ⁴⁷	Microsoft Windows <code>cmd.exe</code> was used to run <code>powershell.exe</code> , <code>AdFind</code> (often renamed to a number of other names), and other commands. ⁴⁸ Use process tracking, event logging, and PowerShell monitoring functions to identify use of these command-line tools.
Execution [TA0002] 	Command and Scripting Interpreter: PowerShell [T1059.001]	The threat actor used PowerShell to create new tasks on remote machines, identify configuration settings, exfiltrate data, and to execute other commands. ⁴⁹	Review PowerShell <code>cmdlets</code> that involve adding or changing permissions or roles to existing accounts, applications, and service principals or that use <code>Out-File</code> filenames and unusual locations (such as <code>C:\TEMP</code>). ⁵⁰ Organizations should review these sources and determine if the changes they make are expected and authorized.
	Account Discovery [T1087]	The threat actor obtained a list of users and their roles from an Exchange server using <code>Get-ManagementRoleAssignment</code> . ^{54,55}	Look for PowerShell being used to create Scheduled Tasks on remote machines with command parameters that look like this: <code>\$scheduler = New-Object -ComObject ("Schedule.Service");\$scheduler.Connect(\$env:COMPUTERNAME);\$</code>

Tactic	Technique	Threat Actor Activity	Detection Recommendations
Discovery [TA0007] 	Domain Trust Discovery [T1482]	The threat actor used the <code>Get-AcceptedDomain</code> PowerShell cmdlet to enumerate accepted domains through an Exchange Management Shell. They also used <code>AdFind</code> to enumerate domains and to discover trust between federated domains. ⁵⁶	<pre>folder = \$scheduler.GetFolder("\Microsoft\Windows\SoftwareProtectionPlatform");\$task = \$folder.GetTask("EventCacheManager");\$definition = \$task.Definition;\$definition.Settings.ExecutionTimeLimit = "PT0S";\$folder.RegisterTaskDefinition(\$task.Name,\$definition ,6,"System",\$null,5);echo "Done".⁵¹</pre>
Persistence [TA0003] 	Account Manipulation: Exchange Email Delegate Permissions [T1098.002]	The threat actor added their own devices as allowed identifications (IDs) for active sync using <code>Set-CASMailbox</code> , allowing their devices to obtain copies of victim mailboxes. The actor also added additional permissions (such as <code>Mail.Read</code> and <code>Mail.ReadWrite</code>) to compromised application or service principals. ⁵⁷	<p>Look for events related to Beacon commands <code>jump psexec</code> and <code>jump psexec_psh</code>—these commands will generate an EventID 7045 (Service Installation) from <code>System.evtx</code>. The additional commands will generate an EventID 400 event log (PowerShell Engine Startup) from <code>Windows PowerShell.evtx</code>.</p> <p>Since this attacker is adept at PowerShell, CISA recommends enabling PowerShell logging and monitoring use of the tool. Look cmdlets in PowerShell logs, including the following:⁵²</p> <ul style="list-style-type: none"> • <code>Get-ManagementRoleAssignment</code> • <code>Get-AcceptedDomain</code> • <code>Get-CASMailbox</code> • <code>Get-Mailbox</code> • <code>Get-OrganizationConfig</code> • <code>Get-OwaVirtualDirectory</code> • <code>Get-Process</code> • <code>Get-WebServicesVirtualDirectory</code> • <code>New-MailboxExportRequest</code> • <code>Remove-MailboxExportRequest</code> • <code>Set-CASMailbox</code> • <code>Export-pfxcertificate</code> • <code>Export-Certificate</code> • <code>Add-AdfsCertificate</code> • <code>Get-AdfsCertificate</code> • <code>Get-AdfsSslCertificate</code> • <code>New-AdfsAzureMfaTenantCertificate</code> • <code>SEt-AdfsCertificate</code>

Tactic	Technique	Threat Actor Activity	Detection Recommendations
			<ul style="list-style-type: none"> • Set-AdfsSslCertificate • Update-AdfsCertificate • Set-mppreference • Compress-Archive • Invoke-Command • Invoke-WMIMethod <p>For more information on PowerShell logging, refer to FireEye: Greater Visibility Through PowerShell Logging.</p> <p>Modification of mail delegation rules and changes to the behavior or frequency of mail traffic being sent may be a sign that a compromised account is being leveraged by threat actors.⁵³</p>
<p>Defense Evasion [TA0005]</p> 	<p>Obfuscated Files or Information [T1027]</p>	<p>The threat actor used encoded PowerShell commands.⁵⁸</p>	<p>The attacker is known to use PowerShell's built-in ability to take Base64 encoded parameters (the <code>-EncodedCommand</code> parameter).⁵⁹ There are many ways this can be called, so defenders should familiarize themselves with what this can look like in PowerShell logs using the following resources:</p> <ul style="list-style-type: none"> • Palo Alto Networks Unit 42: Pulling Back the Curtains on Encoded Command PowerShell Attacks • Microsoft: Customer Guidance on Recent Nation State Cyber Attacks
<p>Persistence [TA0003]</p> 	<p>Account Manipulation: Additional Cloud Credentials [T1098.001]</p>	<p>The threat actor added credentials to Azure service principals/applications after gaining access to the Microsoft 365 (M365) environment.^{60,61}</p>	<p>Look for behavioral artifacts, such as accounts behaving abnormally, and verify information such as IP and/or user agent strings are normal. Identify if credentials have been added to service principals/applications (such as SharePoint and Microsoft Teams) that previously did not have them. Check</p>

Tactic	Technique	Threat Actor Activity	Detection Recommendations
Collection [TA0009] 	Email Collection: Remote Email Collection [T1114.002]	Collected emails from accounts of specific individuals, such as executives and IT staff, using <code>New-MailboxExportRequest</code> followed by <code>Get-MailboxExportRequest</code> . The actor used Azure service principals/applications with added credentials to exfiltrate emails from specific users. ⁶³	with administrators to ensure applications are supposed to have credentials (and the type of credential) associated with them. Monitor for use of Application Programming Interfaces (APIs) that create or import Secure Shell (SSH) keys, especially by unexpected users or accounts such as root accounts. ⁶²
Initial Access [TA0001] 	Supply Chain Compromise: Compromise Software Supply Chain [T1195.002]	The threat actor gained initial network access via a Trojanized update of SolarWinds Orion software. ^{64,65}	Refer to the SolarWinds Security Advisory for details on versions affected. Refer to CISA Alert: AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations for immediate mitigation recommendations.
Execution [TA0002] 	Command and Scripting Interpreter: Windows Command Shell [T1059.003]	The threat actor “lived off the land” by using native commands in Windows. The actor used multiple command-line utilities to enumerate running processes. ^{66,67}	Review the following Windows commands and investigate if each use was legitimate. (Note: this list of commands not exhaustive.) ^{68,69,70} <ul style="list-style-type: none"> • <code>cmd.exe</code> • <code>7z.exe</code> • <code>Powershell.exe</code> • <code>schtasks</code> • <code>certutil</code> • <code>whoami</code> • <code>rundll32.exe</code> • <code>wmic</code> • <code>auditpol</code> • <code>sc</code> • <code>net</code> • <code>netsc</code> • <code>fsutil</code>
Discovery [TA0007] 	Process Discovery [T1057]		

Tactic	Technique	Threat Actor Activity	Detection Recommendations
			<ul style="list-style-type: none"> reg nslookup
Privilege Escalation [TA0004] 	Domain Policy Modification: Domain Trust Modification [T1484.002]	The threat actor changed domain federation trust settings using Azure Active Directory (AD) administrative permissions to configure the domain to accept authorization tokens signed by their own SAML signing certificate. ⁷¹	Monitor for Event ID 307, which can be correlated to relevant Event ID 510 with the same Instance ID for change details. ⁷² Monitor for PowerShell commands such as: ⁷³ <ul style="list-style-type: none"> Update-MSOLFederatedDomain -DomainName: "Federated Domain Name" Update-MSOLFederatedDomain -DomainName: "Federated Domain Name" -supportmultipledomain
Defense Evasion [TA0005] 	Use Alternate Authentication Material [T1550]	The threat actor used SAML tokens to impersonate existing cloud users in the cloud environment with full authentication and was able to bypass multi-factor authentication (MFA). ^{74,75}	Look for behavioral artifacts in UnifiedAuditLogs (PowerShell - Exchange Online) to help detect potential SAML abuse. Note: prior to October 31, 2020 the UnifiedAuditLogs (PowerShell - Exchange Online) showed the UserAuthenticationMethod of 16457 to help detect potential SAML abuse (in conjunction with other indicators such as user behavior, whether the user is part of the domain (guest accounts produce 16457 somewhat frequently depending on how the environment is set up). However, since 16457 was removed, the artifacts will be behavioral.
Credential Access [TA0006] 	Forge Web Credentials: SAML Tokens [T1606.002]	The threat actor created tokens using compromised SAML signing certificates. ⁷⁶	
Lateral Movement [TA0008] 	Use Alternate Authentication Material [T1550]	The threat actor used forged SAML tokens that allowed them to impersonate users and bypass MFA, enabling them to access enterprise cloud applications and services. ⁷⁷	

Tactic	Technique	Threat Actor Activity	Detection Recommendations
Defense Evasion [TA0005] 	Deobfuscate/Decode Files or Information [T1140]	The threat actor used 7-Zip to decode their RAINDROP malware. ⁷⁸	Look for the use of compression utilities such as run from or in unusual locations such as <code>C:\Windows\system32</code> and others (these utilities may have previously existed on the system or have been installed by the threat actor). <code>7z.exe</code> creates compressed files (ending in <code>.7z</code>) that may then be securely deleted by the threat actor.
Collection [TA0009] 	Archive Collected Data: Archive via Utility [T1560.001]	The threat actor used 7-Zip to archive collected data of interest for removal from the environment. ⁷⁹	
Defense Evasion [TA0005] 	Impair Defenses: Disable Windows Event Logging [T1562.002]	The threat actor used <code>AUDITPOL</code> to prevent the collection of audit logs. ⁸⁰	Look for the built-in command <code>auditpol</code> used in the following ways ⁸¹ <ul style="list-style-type: none"> <code>auditpol /GET /category:"Detailed Tracking"</code> <code>auditpol /set /category:"Detailed Tracking" /success:disable /failure:disable</code>[execution of several commands and actions] <code>auditpol /set /category:"Detailed Tracking" /success:enable /failure:enable</code>
Defense Evasion [TA0005] 	Impair Defenses: Disable or Modify System Firewall [T1562.004]	The threat actor used <code>netsh</code> to configure firewall rules that limited certain User Datagram Protocol (UDP) outbound packets. ^{82,83}	Refer to the following resources for guidance on detecting this. <ul style="list-style-type: none"> CISA Activity Alert: AA21-008A Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments Microsoft: Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop

Tactic	Technique	Threat Actor Activity	Detection Recommendations
Defense Evasion [TA0005] 	Impair Defenses: Disable or Modify Tools [T1562.001]	The threat actor disabled services associated with security monitoring products by using the service control manager on a remote system. ⁸⁴	Look for the built-in command <code>sc</code> used the following ways: <ul style="list-style-type: none"> On the source machine: <code>sc \\[dest_machine] stop [service name][perform lateral move Source->Dest]</code> On the destination machine: <code>sc \\[source_machine] start [service name]</code>
Defense Evasion [TA0005] 	Masquerading [T1036]	The threat actor matched hostnames of its command and control (C2) infrastructure with legitimate hostnames in the victim environment. The actor primarily used IP addresses originating from the same country as the victim for their VPN infrastructure. ⁸⁵	Geolocate IP addresses and look for “impossible travel.” ⁸⁶ 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 VPN solutions before connecting into networks.
Defense Evasion [TA0005] 	Subvert Trust Controls: Code Signing [T1553.002]	The threat actor ensured Orion code containing SUNBURST was signed by SolarWinds code signing certificates by injecting the malware into the SolarWinds Orion software lifecycle. ⁸⁷	N/A
Defense Evasion [TA0005] 	Use Alternate Authentication Material: Web Session Cookie [T1550.004]	The threat actor used a forged duo-sid cookie to bypass MFA set on an email account. ⁸⁸	MITRE ATT&CK recommends the following: “Monitor for anomalous access of websites and cloud-based applications by the same user in different locations or by different systems that do not match expected configurations.” ⁸⁹
Credential Access [TA0006] 	Forge Web Credentials: Web Cookies [T1606.001]	The threat actor bypassed the MFA set on Outlook on the Web (OWA) accounts by generating a cookie value from a previously stolen secret key. ⁹⁰	MITRE ATT&CK recommends the following: “Monitor for anomalous authentication activity, such as logons or other user session activity associated with unknown accounts. Monitor for unexpected and abnormal access to resources, including access of websites and cloud-based applications by the same user in different locations or by different systems that do not match expected configurations.” ⁹¹

Tactic	Technique	Threat Actor Activity	Detection Recommendations
Credential Access [TA0006] ***	Steal or Forge Kerberos Tickets: Kerberoasting [T1558.003]	The threat actor obtained Ticket Granting Service (TGS) tickets for Active Directory Service Principal Names for offline cracking. ⁹²	Log Kerberos TGS service ticket requests by enabling Audit Kerberos Service Ticket Operations to log. Investigate irregular activity (e.g., accounts making numerous requests, accounts making requests within a short period, accounts triggering Event ID 4769). ⁹³ For more information on detecting kerberoasting, refer to TrustedSec: The Art of Detecting Kerberoast Attacks .
Credential Access [TA0006] ***	Credentials from Password Stores [T1555]	The threat actor used compromised account credentials to attempt access to Group Managed Service Account (gMSA) passwords. ⁹⁴	Monitor processes, system calls, and file read events and look for activity related to password searches (e.g., keyword searches for password, pwd, login, secure, credentials) in the process memory for credentials. Monitor file read events around known password storage applications. ⁹⁵
Credential Access [TA0006] ***	Unsecured Credentials: Private Keys [T1552.004]	The threat actor obtained the private encryption key from an Active Directory Federation Services (ADFS) container to decrypt corresponding SAML signing certificates. ⁹⁶	MITRE ATT&CK recommends the following: “Monitor access to files and directories related to cryptographic keys and certificates patterns that may indicate collection and exfiltration activity. Collect authentication logs and look for potentially abnormal activity that may indicate improper use of keys or certificates for remote authentication.” ⁹⁷
Lateral Movement [TA0008] 	Remote Services: Windows Remote Management [T1021.006]	The threat actor used WinRM via PowerShell to execute command and payloads on remote hosts. ⁹⁸	Monitor WinRM use by tracking service execution. Abnormal WinRM activity (e.g., if WinRM is normally not used or is normally disabled) observed, this may indicate suspicious behavior. Monitor WinRM processes, actions, and invoked script to correlate the activity with other related events. ⁹⁹
Collection [TA0009] 	Data Staged: Remote Data Staging [T1074.002]	The threat actor staged data and files in password-protected archives on a victim's OWA server. ¹⁰⁰	Monitor publicly writeable directories and central locations as well as recycle bins, temp folders, etc., that are commonly used for staging. Look for encrypted or compressed data, which may be a sign of staging. Indicators of data being staged include processes that appear to be reading files from disparate locations and writing them to the same directory or file, especially if they are suspected of performing encryption or compression (such as 7zip, RAR, ZIP, or zlib) on the files. ¹⁰¹ Monitor processes and command-line arguments and look for actions to collect and combine files. Data may be acquired and staged through remote

Tactic	Technique	Threat Actor Activity	Detection Recommendations
			access tools with built-in features that interact directly with the Windows API or through Windows system management tools such as WMI and PowerShell. ¹⁰²
Command and Control [TA0011] 	Ingress Transfer Tool [T1105]	The threat actor downloaded additional tools, such as TEARDROP malware and Cobalt Strike, to the compromised host following the initial compromise. ^{103,104}	Refer to the following Malware Analysis Reports for IOCs associated with the APT actor's malware. If any IOCs are detected, remove the implant. <ul style="list-style-type: none"> • MAR-10318845-1.v1 - SUNBURST • MAR-10320115-1.v1 - TEARDROP
Command and Control [TA0011] 	Dynamic Resolution: Domain Generation Algorithms [T1568.002]	The threat actor used dynamic Domain Name System (DNS) resolution to construct and resolve to randomly generated subdomains for C2. ¹⁰⁵	This is challenging to detect. Look for domain generation algorithms (DGAs) by looking for domains in DNS logging that exhibit a high degree of entropy. For more information, refer to: <ul style="list-style-type: none"> • Red Canary: Using Entropy in Threat Hunting: a Mathematical Search for the Unknown • Active Countermeasures: Real Intelligence Threat Analytics
Command and Control [TA0011] 	Proxy: Internal Proxy [T1090.001]	The threat actor configured at least one instance of Cobalt Strike to use a network pipe over Server Message Block (SMB). ¹⁰⁶	Refer to the following Malware Analysis Reports for IOCs associated with the APT actor's malware. If any IOCs are detected, remove the implant. <ul style="list-style-type: none"> • MAR-10318845-1.v1 - SUNBURST • MAR-10320115-1.v1 - TEARDROP

Data Sources

The below recommendations serves as a starting point for network defenders as they look for the TTPs and use the detection methods described above. While this list is not inclusive of all threat actor activity, it provides visibility to detect behavior known—up to this point—to be associated with this activity. Defenders should be prepared to investigate unusual behavior in their environment in the course of this guidance.

- Review:
 - Azure Sign-in Logs, and
 - `UnifiedAuditLogs` (PowerShell - ExchangeOnline).
- Run Hawk and CrowdStrike Report Tool (CRT) to identify added devices and delegated mailbox permissions during the period of suspected compromise. Refer to CISA Alert: [AA21-008A Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments](#) for guidance on using these tools.
- Per MITRE, “Configure event logging for scheduled task creation and changes by enabling the ‘Microsoft-Windows-TaskScheduler/Operational’ setting within the event logging service. Several events will then be logged on scheduled task activity, including:
 - Event ID `106` on Windows 7, Server 2008 R2 - Scheduled task registered
 - Event ID `140` on Windows 7, Server 2008 R2 / 4702 on Windows 10, Server 2016 - Scheduled task updated
 - Event ID `141` on Windows 7, Server 2008 R2 / 4699 on Windows 10, Server 2016 - Scheduled task deleted
 - Event ID `4698` on Windows 10, Server 2016 - Scheduled task created
 - Event ID `4700` on Windows 10, Server 2016 - Scheduled task enabled
 - Event ID `4701` on Windows 10, Server 2016 - Scheduled task disabled.”¹⁰⁷
- Enable via GPO the audit process creation policy located at Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Configuration > Detailed Tracking, Policy name Audit Process Creation. (Logging of command line processes is disabled by default.) Additionally, enable the "Include command line in process creation events" setting.
 - Monitor Event ID `4688` for suspicious Process Command Lines. Be sure to enable logging of the Parent Process for detailed information.
 - Refer to Microsoft: [Command Line Process Auditing](#) for more information.

- Monitor for modifications to domain trust settings, such as when a user or application modifies the federation settings on the domain or updates domain authentication from Managed to Federated via ActionTypes `Set_federation_settings_on_domain` and `Set_domain_authentication`. Run the CISA [Sparrow](#) tool and monitor the `Domain_Operations_Export.csv` and `Domain_List.csv` for any modifications to the domain trust settings.
- Review records of which accounts login where and command line logging help define a baseline where abnormal behavior can stand out. Enable command line logging (see that guidance above).
- Maintain awareness of which IPs belong to domain controllers. Add DCs to Replication Allow List, and then configure monitoring systems to alert on `DsGetNCChange` request originating from any IP not on the “Replication Allow List” (See AdSecurity reference for details.)
- Review output from tools that monitor and alert on file and directory integrity. These will provide useful data for many TTPs. The logging for this monitoring can be very verbose, so targeted use on important system directories may be a good compromise in large environments.
- Use `Sysinternals Autoruns` and Powershell module `Kansa` to detect and remove persistence.
 - Unfortunately, if the attacker is using WMI in more ephemeral ways, they will use and then clean up their tracks, forcing defenders to detect this activity in real time. Refer to FireEye’s whitepaper [Windows Management Instrumentation \(WMI\) Offense, Defense, and Forensics](#) for guidance on detection and mitigations.
- Employ vulnerability scanners against all externally-facing systems and internal systems. Use a scanner that scans by IP range. **Note:** before using the scanner, network defenders should have current knowledge of the organization’s internet-facing presence by IP ranges.

REFERENCES

- 1 <https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/>
- 2 <https://attack.mitre.org/versions/v8/techniques/T1606/002/>
- 3 <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- 4 <https://us-cert.cisa.gov/ncas/alerts/aa21-008a>
- 5 <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- 6 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 7 <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- 8 <https://attack.mitre.org/techniques/T1036/004/>
- 9 <https://attack.mitre.org/techniques/T1036/004/>
- 10 <https://attack.mitre.org/techniques/T1053/005/>
- 11 <https://attack.mitre.org/techniques/T1053/005/>
- 12 <https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/>
- 13 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 14 <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf>
- 15 <https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/>
- 16 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
- 17 <https://attack.mitre.org/techniques/T1047/>
- 18 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>

-
- 19 <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf>
 - 20 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
 - 21 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
 - 22 <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
 - 23 <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
 - 24 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
 - 25 <https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/>
 - 26 <https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/>
 - 27 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
 - 28 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
 - 29 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
 - 30 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
 - 31 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
 - 32 <https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/>
 - 33 <https://attack.mitre.org/versions/v8/techniques/T1070/006/>
 - 34 <https://adsecurity.org/?p=1729>

-
- 35 <https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/>
- 36 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
- 37 <https://attack.mitre.org/versions/v8/techniques/T1003/006/>
- 38 <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- 39 <https://attack.mitre.org/versions/v8/techniques/T1070/004/>
- 40 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 41 <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- 42 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 43 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 44 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 45 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 46 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 47 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 48 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 49 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 50 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 51 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 52 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 53 <https://attack.mitre.org/techniques/T1098/002/>
- 54 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 55 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
- 56 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>

-
- 57 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 58 <https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/>
- 59 <https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/>
- 60 <https://www.microsoft.com/security/blog/2020/12/21/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/>
- 61 <https://www.fireeye.com/content/dam/collateral/en/wp-m-unc2452.pdf>
- 62 <https://attack.mitre.org/techniques/T1098/001/>
- 63 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 64 <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- 65 <https://www.solarwinds.com/securityadvisory>
- 66 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 67 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
- 68 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 69 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
- 70 <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- 71 <https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/>
- 72 <https://attack.mitre.org/versions/v8/T1484/002/>
- 73 <https://attack.mitre.org/versions/v8/T1484/002/>
- 74 <https://www.microsoft.com/security/blog/2020/12/21/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/>
- 75 <https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/>

-
- 76 <https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/>
- 77 <https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/>
- 78 <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware>
- 79 <https://www.volexity.com/wblog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 80 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
- 81 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
- 82 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
- 83 <https://us-cert.cisa.gov/ncas/alerts/aa21-008a>
- 84 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
- 85 <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- 86 <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- 87 <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- 88 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 89 <https://attack.mitre.org/versions/v8/techniques/T1550/004/>
- 90 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 91 <https://attack.mitre.org/versions/v8/techniques/T1606/001/>
- 92 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
- 93 <https://attack.mitre.org/versions/v8/techniques/T1558/003/>

-
- 94 <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
- 95 <https://attack.mitre.org/versions/v8/techniques/T1555/>
- 96 <https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/>
- 97 <https://attack.mitre.org/versions/v8/techniques/T1552/004/>
- 98 <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware>
- 99 <https://attack.mitre.org/versions/v8/techniques/T1021/006/>
- 100 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 101 <https://attack.mitre.org/versions/v8/techniques/T1074/002/>
- 102 <https://attack.mitre.org/versions/v8/techniques/T1074/002/>
- 103 <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- 104 <https://attack.mitre.org/software/S0560/>
- 105 <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
- 106 <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware>
- 107 <https://attack.mitre.org/techniques/T1053/005/>

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.