APT29, IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune, UNC3524, Midnight Blizzard, Group G0016

Archived: 2026-04-02 12:00:55 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

APT29 has bypassed UAC.[30]

Enterprise T1087 .002 Account Discovery: Domain Account

During the SolarWinds Compromise, APT29 used PowerShell to discover domain accounts by exectuing `Get-ADUser` and `Get-ADGroupMember`.[24][15]

.004 Account Discovery: Cloud Account

APT29 has conducted enumeration of Azure AD accounts.[31]

Enterprise T1098 .001 Account Manipulation: Additional Cloud Credentials

During the SolarWinds Compromise, APT29 added credentials to OAuth Applications and Service Principals.[32][24]

.002 Account Manipulation: Additional Email Delegate Permissions

APT29 has used a compromised global administrator account in Azure AD to backdoor a service principal with `ApplicationImpersonation` rights to start collecting emails from targeted mailboxes; APT29 has also used compromised accounts holding `ApplicationImpersonation` rights in Exchange to collect emails.[33][27]

During the SolarWinds Compromise, APT29 added their own devices as allowed IDs for active sync using `Set-CASMailbox`, allowing it to obtain copies of victim mailboxes. It also added additional permissions (such as Mail.Read and Mail.ReadWrite) to compromised Application or Service Principals.[12][32][31]

.003 Account Manipulation: Additional Cloud Roles

During the SolarWinds Compromise, APT29 granted `company administrator` privileges to a newly created service principle.[24]

.005 Account Manipulation: Device Registration

APT29 has enrolled their own devices into compromised cloud tenants, including enrolling a device in MFA to an Azure AD environment following a successful password guessing attack against a dormant account.[33][34]

During the SolarWinds Compromise, APT29 registered devices in order to enable mailbox syncing via the `Set-CASMailbox` command.[12]

Enterprise T1583 .001 Acquire Infrastructure: Domains

For the SolarWinds Compromise, APT29 acquired C2 domains, sometimes through resellers.[10][35]

For Operation Ghost, APT29 registered domains for use in C2 including some crafted to appear as existing legitimate domains.[22]

.006 Acquire Infrastructure: Web Services

APT29 has registered algorithmically generated Twitter handles that are used for C2 by malware, such as HAMMERTOSS. APT29 has also used legitimate web services such as Dropbox and Constant Contact in their operations.[36][18]

Enterprise T1595 .002 Active Scanning: Vulnerability Scanning

APT29 has conducted widespread scanning of target environments to identify vulnerabilities for exploit.[13]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

During the SolarWinds Compromise, APT29 used HTTP for C2 and data exfiltration.[12]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

During the SolarWinds Compromise, APT29 used 7-Zip to compress stolen emails into password-protected archives prior to exfltration; APT29 also compressed text files into zipped archives.[12][37][24]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

APT29 added Registry Run keys to establish persistence.[30]

Enterprise T1037 Boot or Logon Initialization Scripts

APT29 has hijacked legitimate application-specific startup scripts to enable malware to execute on system startup.[27]

.004 RC Scripts

APT29 has installed a run command on a compromised system to enable malware execution on system startup.[27]

Enterprise T1110 .001 Brute Force: Password Guessing

APT29 has successfully conducted password guessing attacks against a list of mailboxes.[33]

.003 Brute Force: Password Spraying

APT29 has conducted brute force password spray attacks.[20][31][34]

Enterprise T1651 Cloud Administration Command

APT29 has used Azure Run Command and Azure Admin-on-Behalf-of (AOBO) to execute code on virtual machines.[31]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

APT29 has used encoded PowerShell scripts uploaded to CozyCar installations to download and install SeaDuke.[38][30][39][16]

During the SolarWinds Compromise, APT29 used PowerShell to create new tasks on remote machines, identify configuration settings, exfiltrate data, and execute other commands.[12][40][24]

.003 Command and Scripting Interpreter: Windows Command Shell

During the SolarWinds Compromise, APT29 used `cmd.exe` to execute commands on remote machines.[12][40]

.005 Command and Scripting Interpreter: Visual Basic

For the SolarWinds Compromise, APT29 wrote malware such as Sibot in Visual Basic.[13]

.006 Command and Scripting Interpreter: Python

APT29 has developed malware variants written in Python.[38]

.009 Command and Scripting Interpreter: Cloud API

APT29 has leveraged the Microsoft Graph API to perform various actions across Azure and M365 environments. They have also utilized AADInternals PowerShell Modules to access the API [19]

Enterprise T1586 .002 Compromise Accounts: Email Accounts

APT29 has compromised email accounts to further enable phishing campaigns and taken control of dormant accounts.[41][33]

.003 Compromise Accounts: Cloud Accounts

APT29 has used residential proxies, including Azure Virtual Machines, to obfuscate their access to victim environments.[33]

Enterprise T1584 .001 Compromise Infrastructure: Domains

For the SolarWinds Compromise, APT29 compromised domains to use for C2.[10]

Enterprise T1136 .003 Create Account: Cloud Account

APT29 can create new users through Azure AD.[31]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

During the SolarWinds Compromise, APT29 stole users' saved passwords from Chrome.[24]

Enterprise T1213 Data from Information Repositories

During the SolarWinds Compromise, APT29 accessed victims' internal knowledge repositories (wikis) to view sensitive corporate information on products, services, and internal business operations.[24]

.003 Code Repositories

During the SolarWinds Compromise, APT29 downloaded source code from code repositories.[42]

Enterprise T1005 Data from Local System

APT29 has stolen data from compromised hosts.[27]

During the SolarWinds Compromise, APT29 extracted files from compromised networks.[12]

Enterprise T1001 .002 Data Obfuscation: Steganography

During Operation Ghost, APT29 used steganography to hide the communications between the implants and their C&C servers.[22]

Enterprise T1074 .002 Data Staged: Remote Data Staging

During the SolarWinds Compromise, APT29 staged data and files in password-protected archives on a victim's OWA server.[12]

Enterprise T1140 Deobfuscate/Decode Files or Information

During the SolarWinds Compromise, APT29 used 7-Zip to decode their Raindrop malware.[43]

Enterprise T1587 .001 Develop Capabilities: Malware

APT29 has used unique malware in many of their operations.[3][30][19][27]

For the SolarWinds Compromise, APT29 used numerous pieces of malware that were likely developed for or by the group, including SUNBURST, SUNSPOT, Raindrop, and TEARDROP.[9][11][37]

For Operation Ghost, APT29 used new strains of malware including FatDuke, MiniDuke, RegDuke, and PolyglotDuke.[22]

.003 Develop Capabilities: Digital Certificates

APT29 has created self-signed digital certificates to enable mutual TLS authentication for malware.[25][26]

Enterprise T1484 .002 Domain or Tenant Policy Modification: Trust Modification

During the SolarWinds Compromise, APT29 changed domain federation trust settings using Azure AD administrative permissions to configure the domain to accept authorization tokens signed by their own SAML signing certificate.[15][44]

Enterprise T1482 Domain Trust Discovery

During the SolarWinds Compromise, APT29 used the `Get-AcceptedDomain` PowerShell cmdlet to enumerate accepted domains through an Exchange Management Shell.[12] They also used AdFind to enumerate domains and to discover trust between federated domains.[24][37]

Enterprise T1568 Dynamic Resolution

APT29 has used Dynamic DNS providers for their malware C2 infrastructure.[27]

During the SolarWinds Compromise, APT29 used dynamic DNS resolution to construct and resolve to randomly-generated subdomains for C2.[12]

Enterprise T1114 .002 Email Collection: Remote Email Collection

APT29 has collected emails from targeted mailboxes within a compromised Azure AD tenant and compromised Exchange servers, including via Exchange Web Services (EWS) API requests.[33][27]

During the SolarWinds Compromise, APT29 collected emails from specific individuals, such as executives and IT staff, using `New-MailboxExportRequest` followed by `Get-MailboxExportRequest`.[12][13]

Enterprise T1573 Encrypted Channel

APT29 has used multiple layers of encryption within malware to protect C2 communication.[16]

Enterprise T1585 .001 Establish Accounts: Social Media Accounts

For Operation Ghost, APT29 registered Twitter accounts to host C2 nodes.[22]

Enterprise T1546 .003 Event Triggered Execution: Windows Management Instrumentation Event Subscription

APT29 has used WMI event subscriptions for persistence.[30]

During the SolarWinds Compromise, APT29 used a WMI event filter to invoke a command-line event consumer at system boot time to launch a backdoor with `rundll32.exe`.[37][44]

During Operation Ghost, APT29 used WMI event subscriptions to establish persistence for malware.[22]

.008 Event Triggered Execution: Accessibility Features

APT29 used sticky-keys to obtain unauthenticated, privileged console access.[30][45]

Enterprise T1048 .002 Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

During the SolarWinds Compromise, APT29 exfiltrated collected data over a simple HTTPS request to a password-protected archive staged on a victim's OWA servers.[12]

Enterprise T1190 Exploit Public-Facing Application

APT29 has exploited CVE-2019-19781 for Citrix, CVE-2019-11510 for Pulse Secure VPNs, CVE-2018-13379 for FortiGate VPNs, and CVE-2019-9670 in Zimbra software to gain access.[13][23]

During the SolarWinds Compromise, APT29 exploited CVE-2020-0688 against the Microsoft Exchange Control Panel to regain access to a network.[12][13]

Enterprise T1203 Exploitation for Client Execution

APT29 has used multiple software exploits for common client software, like Microsoft Word, Exchange, and Adobe Reader, to gain code execution.[3][13][18]

Enterprise T1068 Exploitation for Privilege Escalation

APT29 has exploited CVE-2021-36934 to escalate privileges on a compromised host.[39]

Enterprise T1133 External Remote Services

APT29 has used compromised identities to access networks via VPNs and Citrix.[23][33]

For the SolarWinds Compromise, APT29 used compromised identities to access networks via SSH, VPNs, and other remote access tools.[10][24]

Enterprise T1083 File and Directory Discovery

During the SolarWinds Compromise, APT29 obtained information about the configured Exchange virtual directory using `Get-WebServicesVirtualDirectory`.[12]

Enterprise T1606 .001 Forge Web Credentials: Web Cookies

During the SolarWinds Compromise, APT29 bypassed MFA set on OWA accounts by generating a cookie value from a previously stolen secret key.[12]

.002 Forge Web Credentials: SAML Tokens

During the SolarWinds Compromise, APT29 created tokens using compromised SAML signing certificates.[32] [15]

Enterprise T1589 .001 Gather Victim Identity Information: Credentials

For the SolarWinds Compromise, APT29 conducted credential theft operations to obtain credentials to be used for access to victim environments.[24]

Enterprise T1665 Hide Infrastructure

APT29 uses compromised residential endpoints, typically within the same ISP IP address range, as proxies to hide the true source of C2 traffic.[34]

During the SolarWinds Compromise, APT29 set the hostnames of their C2 infrastructure to match legitimate hostnames in the victim environment. They also used IP addresses originating from the same country as the victim for their VPN infrastructure.[9]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

During the SolarWinds Compromise, APT29 used the service control manager on a remote system to disable services associated with security monitoring products.[37]

.002 Impair Defenses: Disable Windows Event Logging

During the SolarWinds Compromise, APT29, used `AUDITPOL` to prevent the collection of audit logs.[37]

.004 Impair Defenses: Disable or Modify System Firewall

During the SolarWinds Compromise, APT29 used `netsh` to configure firewall rules that limited certain UDP outbound packets.[37]

.008 Impair Defenses: Disable or Modify Cloud Logs

APT29 has disabled Purview Audit on targeted accounts prior to stealing emails from Microsoft 365 tenants.[33]

Enterprise T1070 .004 Indicator Removal: File Deletion

APT29 has used SDelete to remove artifacts from victim networks.[30]

During the SolarWinds Compromise, APT29 routinely removed their tools, including custom backdoors, once remote access was achieved.[9]

.006 Indicator Removal: Timestomp

APT29 has used timestomping to alter the Standard Information timestamps on their web shells to match other files in the same directory.[27]

During the SolarWinds Compromise, APT29 modified timestamps of backdoors to match legitimate Windows files.[37]

.008 Indicator Removal: Clear Mailbox Data

During the SolarWinds Compromise, APT29 removed evidence of email export requests using `Remove-MailboxExportRequest`.[12]

Enterprise T1105 Ingress Tool Transfer

APT29 has downloaded additional tools and malware onto compromised networks.[30][25][3][27]

During the SolarWinds Compromise, APT29 downloaded additional malware, such as TEARDROP and Cobalt Strike, onto a compromised host following initial access.[9]

Enterprise T1680 Local Storage Discovery

During the SolarWinds Compromise, APT29 used `fsutil` to check available free space before executing actions that might create large files on disk.[37]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

During the SolarWinds Compromise, APT29 named tasks `\Microsoft\Windows\SoftwareProtectionPlatform\EventCacheManager` in order to appear legitimate.[12]

.005 Masquerading: Match Legitimate Resource Name or Location

APT29 has renamed malicious DLLs with legitimate names to appear benign; they have also created an Azure AD certificate with a Common Name that matched the display name of the compromised service principal.[17][33]

During the SolarWinds Compromise, APT29 renamed software and DLLs with legitimate names to appear benign.[12][40]

Enterprise T1556 .007 Modify Authentication Process: Hybrid Identity

APT29 has edited the `Microsoft.IdentityServer.Servicehost.exe.config` file to load a malicious DLL into the AD FS process, thereby enabling persistent access to any service federated with AD FS for a user with a specified User Principal Name.[46]

Enterprise T1621 Multi-Factor Authentication Request Generation

APT29 has used repeated MFA requests to gain access to victim accounts.[47][34]

Enterprise T1027 .001 Obfuscated Files or Information: Binary Padding

APT29 used large size files to avoid detection by security solutions with hardcoded size limits.[17]

.002 Obfuscated Files or Information: Software Packing

APT29 used UPX to pack files.[30]

.003 Obfuscated Files or Information: Steganography

During Operation Ghost, APT29 used steganography to hide payloads inside valid images.[22]

.006 Obfuscated Files or Information: HTML Smuggling

APT29 has embedded an ISO file within an HTML attachment that contained JavaScript code to initiate malware execution.[39]

Enterprise T1588 .002 Obtain Capabilities: Tool

APT29 has obtained and used a variety of tools including Mimikatz, SDelete, Tor, meek, and Cobalt Strike.[30][3][27]

Enterprise T1003 .002 OS Credential Dumping: Security Account Manager

APT29 has used the `reg save` command to save registry hives.[27]

.004 OS Credential Dumping: LSA Secrets

APT29 has used the `reg save` command to extract LSA secrets offline.[27]

.006 OS Credential Dumping: DCSync

During the SolarWinds Compromise, APT29 used privileged accounts to replicate directory service data with domain controllers.[44][37][24]

Enterprise T1069 .002 Permission Groups Discovery: Domain Groups

During the SolarWinds Compromise, APT29 used AdFind to enumerate domain groups.[24]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

APT29 has used spearphishing emails with an attachment to deliver files with exploits to initial victims.[3][18][39][16]

.002 Phishing: Spearphishing Link

APT29 has used spearphishing with a link to trick victims into clicking on a link to a zip file containing malicious files.[30][18][48]

.003 Phishing: Spearphishing via Service

APT29 has used the legitimate mailing service Constant Contact to send phishing e-mails.[18]

Enterprise T1057 Process Discovery

During the SolarWinds Compromise, APT29 used multiple command-line utilities to enumerate running processes.[12][37][24]

Enterprise T1090 .001 Proxy: Internal Proxy

During the SolarWinds Compromise, APT29 used SSH port forwarding capabilities on public-facing systems, and configured at least one instance of Cobalt Strike to use a network pipe over SMB.[24][43]

.002 Proxy: External Proxy

APT29 uses compromised residential endpoints as proxies for defense evasion and network access.[34]

.003 Proxy: Multi-hop Proxy

A backdoor used by APT29 created a Tor hidden service to forward traffic from the Tor client to local ports 3389 (RDP), 139 (Netbios), and 445 (SMB) enabling full remote access from outside the network and has also used TOR.[30][31]

.004 Proxy: Domain Fronting

APT29 has used the meek domain fronting plugin for Tor to hide the destination of C2 traffic.[30]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

During the SolarWinds Compromise, APT29 used RDP sessions from public-facing systems to internal servers.[24]

.002 Remote Services: SMB/Windows Admin Shares

During the SolarWinds Compromise, APT29 used administrative accounts to connect over SMB to targeted users.[24]

.006 Remote Services: Windows Remote Management

During the SolarWinds Compromise, APT29 used WinRM via PowerShell to execute commands and payloads on remote hosts.[43]

.007 Remote Services: Cloud Services

APT29 has leveraged compromised high-privileged on-premises accounts synced to Office 365 to move laterally into a cloud environment, including through the use of Azure AD PowerShell.[49]

Enterprise T1018 Remote System Discovery

During the SolarWinds Compromise, APT29 used AdFind to enumerate remote systems.[37]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

APT29 has used named and hijacked scheduled tasks to establish persistence.[30]

During the SolarWinds Compromise, APT29 used `scheduler` and `schtasks` to create new tasks on remote host as part of their lateral movement. They manipulated scheduled tasks by updating an existing legitimate task to

execute their tools and then returned the scheduled task to its original configuration. APT29 also created a scheduled task to maintain SUNSPOT persistence when the host booted.[12][9][11]

Enterprise T1505 .003 Server Software Component: Web Shell

APT29 has installed web shells on exploited Microsoft Exchange servers.[13][27]

Enterprise T1528 Steal Application Access Token

APT29 uses stolen tokens to access victim accounts, without needing a password.[34]

Enterprise T1649 Steal or Forge Authentication Certificates

APT29 has abused misconfigured AD CS certificate templates to impersonate admin users and create additional authentication certificates.[50]

Enterprise T1558 .003 Steal or Forge Kerberos Tickets: Kerberoasting

During the SolarWinds Compromise, APT29 obtained Ticket Granting Service (TGS) tickets for Active Directory Service Principle Names to crack offline.[37]

Enterprise T1539 Steal Web Session Cookie

During the SolarWinds Compromise, APT29 stole Chrome browser cookies by copying the Chrome profile directories of targeted users.[24]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

During the SolarWinds Compromise, APT29 was able to get SUNBURST signed by SolarWinds code signing certificates by injecting the malware into the SolarWinds Orion software lifecycle.[9]

.005 Subvert Trust Controls: Mark-of-the-Web Bypass

APT29 has embedded ISO images and VHDX files in HTML to evade Mark-of-the-Web.[39]

Enterprise T1195 .002 Supply Chain Compromise: Compromise Software Supply Chain

During the SolarWinds Compromise, APT29 gained initial network access to some victims via a trojanized update of SolarWinds Orion software.[51][9][13][37]

Enterprise T1218 .005 System Binary Proxy Execution: Mshta

APT29 has use `mshta` to execute malicious scripts on a compromised host.[39]

.011 System Binary Proxy Execution: Rundll32

During the SolarWinds Compromise, APT29 used `Rundll32.exe` to execute payloads.[32][37]

Enterprise T1016 .001 System Network Configuration Discovery: Internet Connection Discovery

APT29 has ensured web servers in a victim environment are Internet accessible before copying tools or malware to it.[27]

During the SolarWinds Compromise, APT29 used GoldFinder to perform HTTP GET requests to check internet connectivity and identify HTTP proxy servers and other redirectors that an HTTP request travels through.[10]

Enterprise T1199 Trusted Relationship

APT29 has compromised IT, cloud services, and managed services providers to gain broad access to multiple customers for subsequent operations.[31]

During the SolarWinds Compromise, APT29 gained access through compromised accounts at cloud solution partners, and used compromised certificates issued by Mimecast to authenticate to Mimecast customer systems.[13][24]

Enterprise T1552 .004 Unsecured Credentials: Private Keys

During the SolarWinds Compromise, APT29 obtained PKI keys, certificate files, and the private encryption key from an Active Directory Federation Services (AD FS) container to decrypt corresponding SAML signing certificates.[44][13]

Enterprise T1550 .001 Use Alternate Authentication Material: Application Access Token

During the SolarWinds Compromise, APT29 used compromised service principals to make changes to the Office 365 environment.[24]

.003 Use Alternate Authentication Material: Pass the Ticket

APT29 used Kerberos ticket attacks for lateral movement.[30]

.004 Use Alternate Authentication Material: Web Session Cookie

During the SolarWinds Compromise, APT29 used stolen cookies to access cloud resources and a forged `duo-sid` cookie to bypass MFA set on an email account.[12][24]

Enterprise T1204 .001 User Execution: Malicious Link

APT29 has used various forms of spearphishing attempting to get a user to click on a malicious link.[18][48]

.002 User Execution: Malicious File

APT29 has used various forms of spearphishing attempting to get a user to open attachments, including, but not limited to, malicious Microsoft Word documents, .pdf, and .lnk files. [3][39][16]

Enterprise T1078 Valid Accounts

APT29 has used a compromised account to access an organization's VPN infrastructure.[33]

During the SolarWinds Compromise, APT29 used different compromised credentials for remote access and to move laterally.[9][10][13]

.002 Domain Accounts

During the SolarWinds Compromise, APT29 used domain administrators' accounts to help facilitate lateral movement on compromised networks.[24]

For Operation Ghost, APT29 used stolen administrator credentials for lateral movement on compromised networks.[22]

.003 Local Accounts

APT29 targets dormant or inactive user accounts, accounts belonging to individuals no longer at the organization but whose accounts remain on the system, for access and persistence.[34]

During the SolarWinds Compromise, APT29 used compromised local accounts to access victims' networks.[24]

.004 Cloud Accounts

APT29 has gained access to a global administrator account in Azure AD and has used `Service Principal` credentials in Exchange.[33][27]

During the SolarWinds Compromise, APT29 used a compromised O365 administrator account to create a new Service Principal.[24]

Enterprise T1102 .002 Web Service: Bidirectional Communication

For Operation Ghost, APT29 used social media platforms to hide communications to C2 servers.[22]

Enterprise T1047 Windows Management Instrumentation

APT29 used WMI to steal credentials and execute backdoors at a future time.[30]

During the SolarWinds Compromise, APT29 used WMI for the remote execution of files for lateral movement.[44][37]
