Threat Intelligence Project - Threat Actor Analysis APT29

Table of Contents

APT Selection

APT: APT29 (Cozy Bear/CozyDuke)

Nation-State Sponsor: Russia

Primary Targets: Government agencies, political organizations, and businesses (e.g., healthcare, energy, finance).

Known Campaigns:

- 2016 U.S. Presidential Election interference (often associated with the DNC hack).
- Attacks on COVID-19 vaccine research centers.
- SolarWinds supply chain attack (part of the broader 2020 attack on U.S. federal agencies).

Associated Groups: IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune, UNC3524, Midnight Blizzard

Summary:

APT29 is a highly sophisticated and well-documented threat group. They are linked to Russian Foreign Intelligence Service (SVR), and they are known for their stealthy and long-term cyber-espionage activities. APT29 has been involved in several high-profile campaigns and they have been operating since 2008, often targeting government networks in Europe and NATO countries. APT29 gained worldwide attention because of their involvement in major cyber-attack campaigns. Including 2016 attack on United States presidential election, 2020 COVID vaccine research attacks and SolarWinds attack, which was one of the largest supply chain attacks in the last decade.

APT29 is also known for using sophisticated malware such as Duke malware and its variants which they have used to conduct spear fishing campaigns to gain access. They specialize in keeping long term access on compromised networks which they go undetected for a long periods of time. Their tactics and techniques that they use have been mapped to MITRE frameworks, this makes them the most studied and dangerous APT groups. Their operations are mostly intelligence gathering instead of destructive cyber-attacks.

Campaign Analysis

Notable campaigns of APT29 include,

- **Operation Ghost (2013-2019)** – The APT29 started the campaign in 2013 and targeted the Ministries of foreign affairs in Europe and the Washington, D.C. embassy of a European Union country. They utilized unique malware families, steganography, and unique command and control (C2) infrastructures to conduct their espionage activities.
- **SolarWinds Compromise (2019-2021)** – The SolarWinds compromise was a supply chain attack conducted by APT29, discovered in mid-December 2020. The target of this attack includes government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. The APT29 used customized malware to inject malicious code into the SolarWinds Orion software build process, which was later distributed through a normal software update. They also used password spraying, token theft, API abuse, spear phishing, and other supply chain attacks to compromise user accounts and leverage their associated access.

APT29 used various Tactics, Techniques and Procedures (TTPs) to carry out their attacks against high-value targets. They gain initial access using spear-phishing emails with malicious attachments and links. They have used unique malware to execute operation using PowerShell. The group has remained persistence by creating new accounts and utilizing compromised credentials. To avoid detection, they used UPX and achieved credential access by preforming credential dumping. They perform network discovery extensively, laterally move around systems using remote services, and exfiltrate sensitive data across encrypted in-depth communication channels. They have also used web-based protocols for C2 communication.

The group is also known for its sophisticated malware, among them SUNBURST utilized in the attack against SolarWinds, MiniDuke, SoreFang, EnvyScout and RegDuke targeted at espionage with long-time access to the invaded networks. The main trait of their campaigns focuses on data theft and long-term infiltration.

Infrastructure Analysis

SolarWinds IOCs

File path

- C:\windows\syswow64\netsetupsvc.dll: TEARDROP memory module used to drop Cobalt Strike Beacon.

IPs

- 13.59.205.66
- 54.193.127.66
- 54.215.192.52
- 34.203.203.23
- 139.99.115.204
- 5.252.177.25
- 5.252.177.21
- 204.188.205.176
- 51.89.125.18
- 167.114.213.199

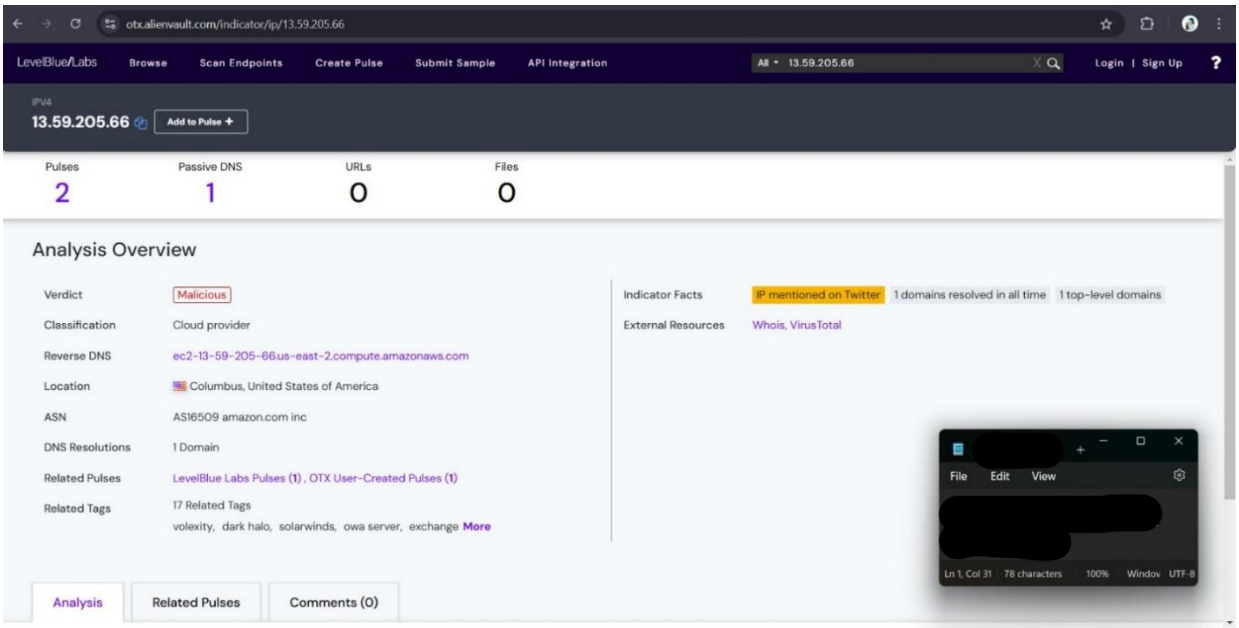

Figure 1 IP 13.59.205.66 in AlienVault OTX

Hashes

Sha256	Association
d0d626deb3f9484e649294a8dfa814c5568f846d5a a02d4cdad5d041a29d5600	Troj/SunBurst-A(Installer|CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp)
53f8dfc65169ccda021b72a62e0c22a4db7c4077f0 02fa742717d41b3c40f2c7	Mal/Generic-S(Solarwinds Worldwide LLC)
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e 1ded3c0b0aa8211fe858d6	Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll)
292327e5c94afa352cc5a02ca273df543f2020d0e7 6368ff96c84f4e90778712	Mal/Generic-S(OrionImprovementBusinessLayer.2.cs)
c15abaf51e78ca56c0376522d699c978217bf041a 3bd3c71d09193efa5717c71	Mal/Sunburst-B(app_web_logoimagehandler.ashx.b6031896.dll).SuperNova webshell backdoor
019085a76ba7126fff22770d71bd901c325fc68ac5 5aa743327984e89f4b0134	Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll)
b820e8a2057112d0ed73bd7995201dbed79a79e1 3c79d4bdad81a22f12387e07	Teardrop

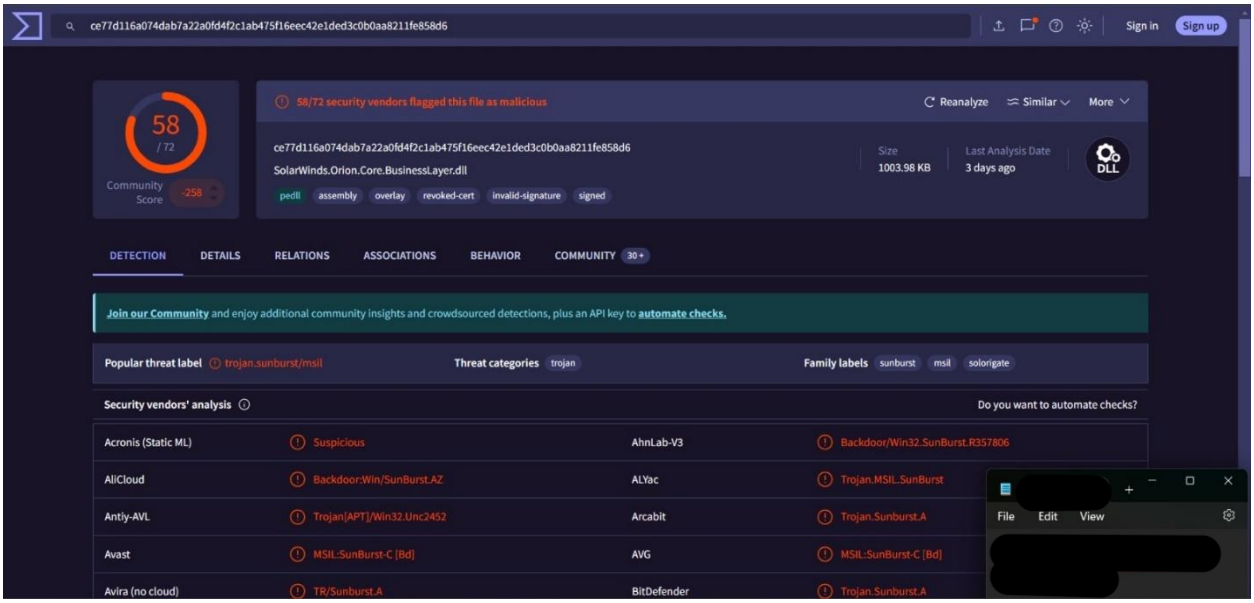

Figure 2 One hash in VirusTotal

Domain	Association
avsvmcloud.com	SUNBURST
databasegalore.com	SUNBURST/BEACON
deftsecurity.com	SUNBURST
ervsystem.com	TEARDROP
incomeupdate.com	BEACON
kubecloud.com	BEACON
lcomputers.com	BEACON
mobilnweb.com	Unknown Association
panhardware.com	SUNBURST/BEACON
seobundlekit.com	SUNBURST
solartrackingsystem.net	BEACON
thedoccloud.com	SUNBURST
virtualdataserver.com	SUNBURST
virtualwebdata.com	SUNBURST
webcodez.com	BEACON
websitetheme.com	SUNBURST
zupertech.com	SUNBURST/BEACON

Operation Ghost IOCs

Hashes

SHA-1	Association
4BA559C403FF3F5CC2571AE0961EAFF6CF0A50F6	PolyglotDuke - Win32/Agent.ZWH
CF14AC569A63DF214128F375C12D90E535770395	PolyglotDuke - Win32/Agent.AAPY
539D021CD17D901539A5E1132ECAAB7164ED5DB5	PolyglotDuke - Win32/Agent.ZWH
0E25EE58B119DD48B7C9931879294AC3FC433F50	PolyglotDuke - Win64/Agent.OL
0A5A7DD4AD0F2E50F3577F8D43A4C55DDC1D80CF	RegDuke Loader - MSIL/Tiny.BG
194D8E2AE4C723CE5FE11C4D9CFEFBBA32DCF766	RegDuke Loader - MSIL/Agent.TGC
64D6C11FFF2C2AADAACEE01B294AFCC751316176	RegDuke Loader - MSIL/Agent.SVP
6ACC0B1230303F8CF46152697D3036D69EA5A849	RegDuke Loader - MSIL/Agent.SXO
170BE45669026F3C1FC5BA2D48817DBF950DA3F6	RegDuke Loader - MSIL/Agent.SYC
5905C55189C683BC37258AEC28E916C41948CD1C	RegDuke Backdoor - MSIL/Agent.CAW
B05CABA461000C6EBD8B237F318577E9BCCD6047	MiniDuke - Win32/Agent.TSG
A88DA2DD033775F7ABC8D6FB3AD5DD48EFBEADE1	FatDuke - Win32/Agent.TSH
9E96B00E9F7EB94A944269108B9E02D97142EEDC	FatDuke Loader - Win32/Agent.AAPY
AF2B46D4371CE632E2669FEA1959EE8AF4EC39CE	LiteDuke - Win32/Agent.AART

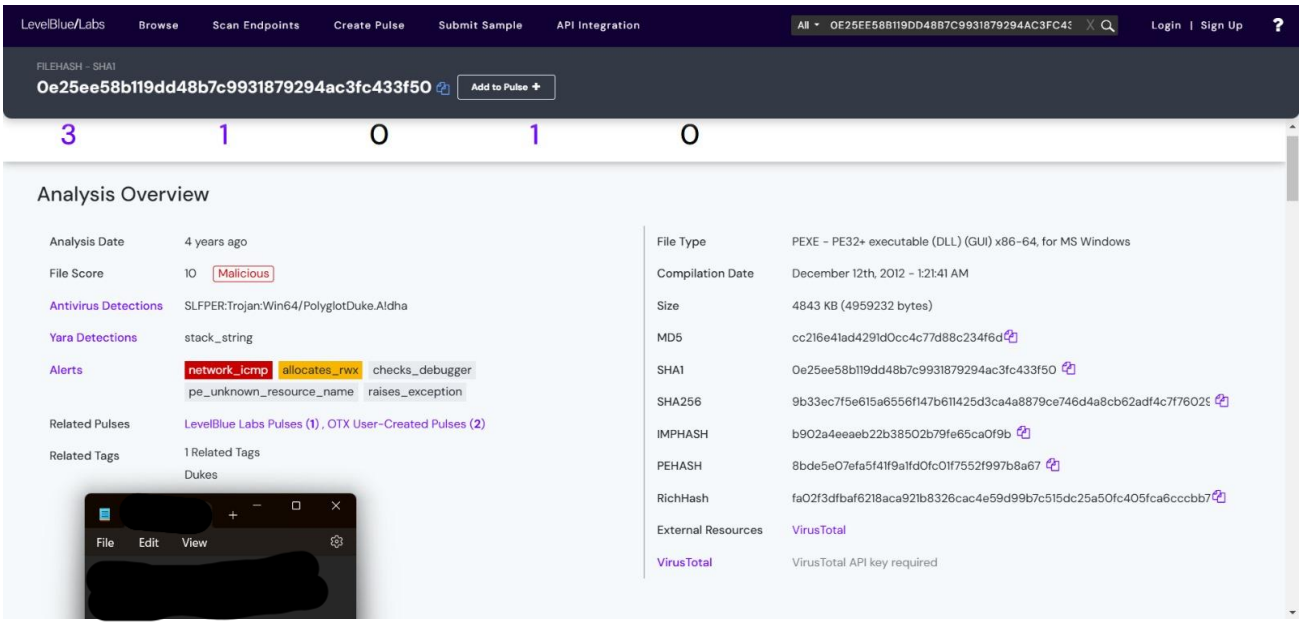

Figure 3 One of the hashes in AlienVaultOTX

Domains

Domain	Association
acciaio.com.br	PolyglotDuke
ceycarb.com	PolyglotDuke
coachandcook.at	PolyglotDuke
fisioterapiabb.it	PolyglotDuke
lorriratzlaff.com	PolyglotDuke
mavin21c.dothome.co.kr	PolyglotDuke
motherlodebulldogclub.com	PolyglotDuke
powerpolymerindustry.com	PolyglotDuke
publiccouncil.org	PolyglotDuke
rulourialuminiu.co.uk	PolyglotDuke
ecolesndmessines.org	MiniDuke
salesappliances.com	MiniDuke
busseylawoffice.com	FatDuke
fairfieldsch.org	FatDuke
ministernetwork.org	FatDuke
bandabonga.fr	LiteDuke

MITRE ATT&CK Mapping

SolarWinds Mapping

TACTIC	TECHNIQUE - ID	SUB TECHNIQUE - ID	USE
RECONNAISSANCE	Gather Victim Identity Information - T1589	Credentials T1589.001	For the SolarWinds Compromise, APT29 conducted credential theft operations to obtain credentials to be used for access to victim environments.
RESOURCE DEVELOPMENT	Acquire Infrastructure – T1583	Domains – T1583.001	For the SolarWinds Compromise, APT29 acquired C2 domains, sometimes through resellers.
	Compromise Infrastructure – T1584	Domains – T1584.001	For the SolarWinds Compromise, APT29 compromised domains to use for C2
	Develop Capabilities – T1587	Malware – T1587.001	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.
INITIAL ACCESS	Exploit Public-Facing Application – T1190		During the SolarWinds Compromise, APT29 exploited CVE-2020-0688 against the Microsoft Exchange Control Panel to regain access to a network.
	External Remote Services – T1133		For the SolarWinds Compromise, APT29 used compromised identities to access networks via SSH, VPNs,

			and other remote access tools.
	Supply Chain Compromise – T1195	Compromise Software Supply Chain – T1195.002	During the SolarWinds Compromise, APT29 gai ned initial network access to some victims via a trojanized update of SolarWinds Orion software.
	Trusted Relationship – T1199		During the SolarWinds Compromise, APT29 gai ned access through compromised accounts at cloud solution partners, and used compromised certificates issued by Mimecast to authenticate to Mimecast customer systems.
	Valid Accounts – T1078	Domain Accounts – T1078.002	During the SolarWinds Compromise, APT29 use d domain administrators' accounts to help facilitate lateral movement on compromised networks.
		Local Accounts – T1078.003	During the SolarWinds Compromise, APT29 use d compromised local accounts to access victims' networks.
		Cloud Accounts – T1078.004	During the SolarWinds Compromise, APT29 use d a compromised O365 administrator account to create a new Service Principal.
EXECUTION	Command and Scripting Interpreter – T1059	PowerShell – T1059.001	During the SolarWinds Compromise, APT29 use d PowerShell to create new tasks on remote machines, identify configuration settings, exfiltrate data, and

			execute other commands.
		Windows Command Shell – T1059.003	During the SolarWinds Compromise, APT29 used cmd.exe to execute commands on remote machines.
		Visual Basic – T1059.005	For the SolarWinds Compromise, APT29 wrote malware such as Sibot in Visual Basic.
	Scheduled Task/Job – T1053	Scheduled Task – T1053.005	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.
	Windows Management Instrumentation – T1047		During the SolarWinds Compromise, APT29 used WMI for the remote execution of files for lateral movement.
PERSISTENCE	Account Manipulation – T1098	Additional Cloud Credentials – T1098.001	During the SolarWinds Compromise, APT29 added credentials to OAuth Applications and Service Principals.

		Additional Email Delegate Permissions – T1098.002	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.
		Additional Cloud Roles – T1098.003	During the SolarWinds Compromise, APT29 granted company administrator privileges to a newly created service principle.
		Device Registration – T1098.005	During the SolarWinds Compromise, APT29 registered devices in order to enable mailbox syncing via the Set-CASMailbox command.
	Event Triggered Execution – T1546	Windows Management Instrumentation Event Subscription – T1546.003	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.
	External Remote Services – T1133		For the SolarWinds Compromise, APT29 used compromised identities to access networks via SSH, VPNs, and other remote access tools.
	Scheduled Task/Job – T1053	Scheduled Task – T1053.005	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.
	Valid Accounts – T1078	Domain Accounts – T1078.002	During the SolarWinds Compromise, APT29 used domain administrators' accounts to help facilitate lateral movement on compromised networks.
		Local Accounts – T1078.003	During the SolarWinds Compromise, APT29 used compromised local accounts to access victims' networks.
		Cloud Accounts – T1078.004	During the SolarWinds Compromise, APT29 used a compromised O365 administrator account to create a new Service Principal.
PRIVILEGE ESCALATION	Account Manipulation – T1098	Additional Cloud Credentials – T1098.001	During the SolarWinds Compromise, APT29 added credentials to OAuth Applications and Service Principals.
		Additional Email Delegate Permissions – T1098.002	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.
		Additional Cloud Roles – T1098.003	During the SolarWinds Compromise, APT29 granted company administrator privileges to a newly created service principle.
		Device Registration – T1098.005	During the SolarWinds Compromise, APT29 registered devices in order to enable mailbox syncing via the Set-CASMailbox command.
	Domain or Tenant Policy Modification – T1484	Trust Modification – T1484.002	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.
	Event Triggered Execution – T1546	Windows Management Instrumentation Event Subscription – T1546.003	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.

	Scheduled Task/Job – T1053	Scheduled Task – T1053.005	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.
	Valid Accounts – T1078	Domain Accounts – T1078.002	During the SolarWinds Compromise, APT29 used domain administrators' accounts to help facilitate lateral movement on compromised networks.
		Local Accounts – T1078.003	During the SolarWinds Compromise, APT29 used compromised local accounts to access victims' networks.
		Cloud Accounts – T1078.004	During the SolarWinds Compromise, APT29 used a compromised O365 administrator account to create a new Service Principal.
DEFENSE EVASION	Deobfuscate/Decode Files or Information – T1140		During the SolarWinds Compromise, APT29 used 7-Zip to decode their Raindrop malware.
	Domain or Tenant Policy Modification – T1484	Trust Modification – T1484.002	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
	Impair Defenses – T1562	Disable or Modify Tools – T1562.001	During the SolarWinds Compromise, APT29 used the service control manager on a remote system to disable services associated with security monitoring products
		Disable Windows Event Logging – T1562.002	During the SolarWinds Compromise, APT29, used AUDITPOL to prevent the collection of audit logs.
		Disable or Modify System Firewall – T1562.004	During the SolarWinds Compromise, APT29 used netsh to configure firewall rules that limited certain UDP outbound packets.
	Indicator Removal – T1070		During the SolarWinds Compromise, APT29 temporarily replaced legitimate utilities with their own, executed their payload, and then restored the original file.
		File Deletion – T1070.004	During the SolarWinds Compromise, APT29 routinely removed their tools, including custom backdoors, once remote access was achieved.
		Timestomp – T1070.006	During the SolarWinds Compromise, APT29 modified timestamps of backdoors to match legitimate Windows files.
		Clear Mailbox Data – T1070.008	During the SolarWinds Compromise, APT29 removed evidence of email export requests

			using Remove-MailboxExportRequest.
	Masquerading – T1036	Masquerade Task or Service – T1036.004	During the SolarWinds Compromise, APT29 named tasks \Microsoft\Windows\SoftwareProtectionPlatform\EventCacheManager in order to appear legitimate.
		Match Legitimate Name or Location – T1036.005	During the SolarWinds Compromise, APT29 renamed software and DLLs with legitimate names to appear benign
	Subvert Trust Controls – T1553	Code Signing – T1553.002	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.
	System Binary Proxy Execution – T1218	Rundll32 – T1218.011	During the SolarWinds Compromise, APT29 used Rundll32.exe to execute payloads.
	Use Alternate Authentication Material – T1550		During the SolarWinds Compromise, APT29 used forged SAML tokens that allowed the actors to impersonate users and bypass MFA, enabling APT29 to access enterprise cloud applications and services.
		Application Access Token – T1550.001	During the SolarWinds Compromise, APT29 used compromised service principals to make changes to the Office 365 environment.
		Web Session Cookie – T1550.004	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.
	Valid Accounts – T1078	Domain Accounts – T1078.002	During the SolarWinds Compromise, APT29 used domain administrators' accounts to help facilitate lateral movement on compromised networks.
		Local Accounts – T1078.003	During the SolarWinds Compromise, APT29 used compromised local accounts to access victims' networks.
		Cloud Accounts – T1078.004	During the SolarWinds Compromise, APT29 used a compromised O365 administrator account to create a new Service Principal.
CREDENTIAL ACCESS	Credentials from Password Stores – T1555		During the SolarWinds Compromise, APT29 used account credentials they obtained to attempt access to Group Managed Service Account (gMSA) passwords.
		Credentials from Web Browsers – T1555.003	During the SolarWinds Compromise, APT29 stole users' saved passwords from Chrome.
	Forge Web Credentials – T1606	Web Cookies – T1606.001	During the SolarWinds Compromise, APT29 bypassed MFA set on OWA accounts by generating a cookie value from a previously stolen secret key.
		SAML Tokens – T1606.002	During the SolarWinds Compromise, APT29 created tokens using compromised SAML signing certificates.

	OS Credential Dumping – T1003	DCSync – T1003.006	During the SolarWinds Compromise, APT29 used privileged accounts to replicate directory service data with domain controllers
	Steal or Forge Kerberos Tickets – T1558	Kerberoasting – T1558.003	During the SolarWinds Compromise, APT29 obtained Ticket Granting Service (TGS) tickets for Active Directory Service Principle Names to crack offline.
	Steal Web Session Cookie – T1539		During the SolarWinds Compromise, APT29 stole Chrome browser cookies by copying the Chrome profile directories of targeted users.
	Unsecured Credentials – T1552	Private Keys – T1552.004	During the SolarWinds Compromise, APT29 obtained PKI keys, certificate files, and the private encryption key from an Active Directory Federation Services (ADFS) container to decrypt corresponding SAML signing certificates.
DISCOVERY	Account discovery – T1087		During the SolarWinds Compromise, APT29 obtained a list of users and their roles from an Exchange server using Get-ManagementRoleAssignment
		Domain Account – T1087.002	During the SolarWinds Compromise, APT29 used PowerShell to discover domain accounts by exectuing Get-ADUser and Get-ADGroupMember.
	Domain Trust Discovery – T1482		During the SolarWinds Compromise, APT29 used the Get-

			AcceptedDomain Power Shell cmdlet to enumerate accepted domains through an Exchange Management Shell.[5] They also used AdFind to enumerate domains and to discover trust between federated domains.
	File and Directory Discovery – T1083		During the SolarWinds Compromise, APT29 obtained information about the configured Exchange virtual directory using Get-WebServicesVirtualDirectory.
	Permission Groups Discovery – T1069		During the SolarWinds Compromise, APT29 used the Get-ManagementRoleAssignment PowerShell cmdlet to enumerate Exchange management role assignments through an Exchange Management Shell.
		Domain Groups – T1069.002	During the SolarWinds Compromise, APT29 used AdFind to enumerate domain groups.
	Process Discovery – T1057		During the SolarWinds Compromise, APT29 used multiple command-line utilities to enumerate running processes.
	Remote System Discovery – T1018		During the SolarWinds Compromise, APT29 used AdFind to enumerate remote systems
	System Information Discovery – T1082		During the SolarWinds Compromise, APT29 used fsutil to check available free space before executing actions

			that might create large files on disk.
	System Network Configuration Discovery – T1016	Internet Connection Discovery – T1016.001	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.[I]
LATERAL MOVEMENT	Remote Services – T1021	Remote Desktop Protocol – T1021.001	During the SolarWinds Compromise, APT29 used RDP sessions from public-facing systems to internal servers.
		SMB/Windows Admin Shares – T1021.002	During the SolarWinds Compromise, APT29 used administrative accounts to connect over SMB to targeted users.
		Windows Remote Management – T1021.006	During the SolarWinds Compromise, APT29 used WinRM via PowerShell to execute commands and payloads on remote hosts.
	Use Alternate Authentication Material – T1550		During the SolarWinds Compromise, APT29 used forged SAML tokens that allowed the actors to impersonate users and bypass MFA, enabling APT29 to access enterprise cloud applications and services.
		Application Access Token – T1550.001	During the SolarWinds Compromise, APT29 used compromised service principals to make changes to the Office 365 environment.
		Web Session Cookie – T1550.004	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.
COLLECTION	Archive Collected Data – T1560	Archive via Utility – T1560.001	During the SolarWinds Compromise, APT29 used 7-Zip to compress stolen emails into password-protected archives prior to exfiltration; APT29 also compressed text files into zipped archives.
	Data from Information Repositories – T1213		During the SolarWinds Compromise, APT29 accessed victims' internal knowledge repositories (wikis) to view sensitive corporate information on products, services, and internal business operations.
		Code Repositories – T1213.003	During the SolarWinds Compromise, APT29 downloaded source code from code repositories.
	Data from Local System – T1005		During the SolarWinds Compromise, APT29 extracted files from compromised networks.
	Data Staged – T1074	Remote Data Staging – T1074.002	During the SolarWinds Compromise, APT29 staged data and files in password-protected archives on a victim's OWA server.
	Email Collection – T1114	Remote Email Collection – T1114.002	During the SolarWinds Compromise, APT29 collected emails from specific individuals, such as executives and IT staff, using New-MailboxExportRequest followed by Get-MailboxExportRequest.
COMMAND AND CONTROL	Application Layer Protocol – T1071	Web Protocols – T1071.001	During the SolarWinds Compromise, APT29 use

			d HTTP for C2 and data exfiltration.
	Dynamic Resolution – T1568		During the SolarWinds Compromise, APT29 used dynamic DNS resolution to construct and resolve to randomly-generated subdomains for C2.
	Hide Infrastructure – T1665		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.
	Ingress Tool Transfer – T1150		During the SolarWinds Compromise, APT29 downloaded additional malware, such as TEARDROP and Cobalt Strike, onto a compromised host following initial access.
	Proxy – T1090	Internal Proxy – T1090.001	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.
EXFILTRATION	Exfiltration Over Alternative Protocol – T1048	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol – T1048.002	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.

Operation Ghost Mapping

TACTIC	TECHNIQUE - ID	SUB TECHNIQUE - ID	USE
RESOURCE DEVELOPMENT	Acquire Infrastructure – T1583	Domains – T1583.001	For Operation Ghost, APT29, registered domains for use in C2 including some crafted to appear as existing legitimate domains.
	Develop Capabilities – T1587	Malware – T1587.001	APT29 used steganography to hide the communications between the implants and their C&C servers.
	Establish Accounts – T1585	Social Media Accounts – T1585.001	For Operation Ghost, APT29 registered Twitter accounts to host C2 nodes.
INITIAL ACCESS	Valid Accounts – T1078	Domain Accounts – T1078.002	For Operation Ghost, APT29 used stolen administrator credentials for lateral movement on compromised networks.
PERSISTENCE	Event Triggered Execution – T1546	Windows Management Instrumentation event Subscription – T1546.003	During Operation Ghost, APT29 used WMI event subscriptions to establish persistence for malware.
PRIVILEGE ESCALATION	Event Triggered Execution – T1546	Windows Management Instrumentation event Subscription – T1546.003	During Operation Ghost, APT29 used WMI event subscriptions to establish persistence for malware.

	Valid Accounts – T1078	Domain Accounts – T1078.002	For Operation Ghost, APT29 used stolen administrator credentials for lateral movement on compromised networks.
DEFENSE EVASION	Obfuscated Files or Information – T1027	Steganography – T1027.003	During Operation Ghost, APT29 used steganography to hide payloads inside valid images.
	Valid Accounts – T1078	Domain Accounts – T1078.002	For Operation Ghost, APT29 used stolen administrator credentials for lateral movement on compromised networks.
COMMAND AND CONTROL	Data Obfuscation – T1001	Steganography – T1001.002	During Operation Ghost, APT29 used steganography to hide the communications between the implants and their C&C servers.
	Web Service – T1102	Bidirectional communication – T1102.002	For Operation Ghost, APT29 used social media platforms to hide communications to C2 servers.