A REPORT ON APT29 AND THE MITRE ATT&CK FRAMEWORK

- **Aliases:** Cozy Bear, The Dukes, Nobelium, UNC2452, stellarParticles
- **Nation-State Affiliation:** Russia foreign intelligence Service (SVR)
- **Primary Targets:** Government agencies, think tanks, healthcare, technology, energy sectors, NATO member countries and research institutes.
- **Tactics & Techniques:** Espionage, credential theft, supply chain attacks
- **Notable Campaigns:** SolarWinds supply chain attack, spear-phishing against Western governments, COVID-19 vaccine research targeting

Notable Attacks

- **SolarWinds Supply Chain Attack (2020)**
- **COVID-19 Vaccine Research Targeting (2020-2021)**
- **Exploitation of Zimbra and TeamCity Servers (2024)**
- **Use of Commercial Spyware Exploits (2024)**

Tactics, Techniques, and Procedures (TTPs)

APT29 has been operating since 2008 follows a structured attack approach mapped to the MITRE ATT&CK framework. Below is a categorized list of their **TTPs**:

1. Initial Access

- Phishing **(T1566)** – Spear-phishing emails containing malicious links or attachments and often crafted to appear legitimate and from a trusted source.
- Exploiting Public-Facing Applications **(T1190)** – targets vulnerabilities in exposed services in web apps and email gateways like Zimbra and TeamCity which are commonly zero-day exploits.
- Supply Chain Compromise **(T1195)** – Infecting trusted software providers (e.g., SolarWinds attack) .
- Compromising IT and managed service providers **(T1197)** - compromise IT service providers and gain access to multiple targets.

2. Execution

- Command and Scripting Interpreter **(T1059)** – Implementation is done via PowerShell, Windows Command Prompt or custom scripts.
- User Execution **(T1204)** – Social engineering users to execute malicious payloads through spear-phishing.
- Scheduled Task/Job **(T1053)** – Running malicious scripts at scheduled intervals
- Process injection **(T1055)** – Injecting malicious code to a legitimate process to gain persistence and avoid detection.

3. Persistence

- Registry Run Keys / Startup Folder **(T1547.001)** – Modifying registry settings for persistence
- Scheduled Tasks **(T1053.005)** – Create scheduled tasks or jobs to execute malicious code at specific intervals.

• Valid Accounts **(T1078)** – Using stolen credentials for persistent access and avoiding detection.
• Hijack Execution Flow:DLL Side-Loading **(T1574.002)–** Loading of malicious DLL within a trusted application making it harder to detect.
• Create Account: Local account **(T1136.001) –** Creating local account on the already compromised system to maintain access.

4. Privilege Escalation

• Abusing System Services **(T1543.003)** – Manipulating legitimate services to gain elevated privileges
• Exploitation for Privilege Escalation **(T1068)** – Exploiting vulnerabilities in unpatched systems to escalate privilege.
• Bypass User Account Control **(T1548.002) –** Using various techniques to bypass detection and execute malware with administrative privileges.
• Web shell **(T1505.001) –** Escalates privileges on compromised web servers.
• User Execution **(T1204)** – Executes malicious code on user-interface which leads to privilege escalation.
• Default Accounts **(T1078.003) –** Exploiting weak and easily guessable accounts for initial access and escalating privileges.
• Drive by compromise **(T1189)** – Using user-driven compromise to escalate privileges.

5. Defense Evasion

• Timestamping **(T1070.006)** – Altering timestamps on logs and files to evade detection
• Obfuscated Files or Information **(T1027)** – Encrypting or encoding payloads to bypass security tools
• Signed Binary Proxy Execution **(T1218)** – Using trusted applications like rundll32.exe for malicious execution.
• Masquerading **(T1038) –** Disguising malicious activities by making them appear legitimate.
• Indicator Removal on Host **(T1070)** - Modifying and deleting security logs to hide malicious activities. Hiding files and directories.
• Impair defense **(T1562.002) –** Disabling and modifying security services running on a compromised system.

6. Credential Access

• Credential Dumping **(T1003)** – Extracting stored credentials from memory or registries
• Brute Force **(T1110)** – Guessing or cracking credentials for unauthorized access
• Pass the Hash **(T1550.002)** – Reusing hashed credentials for authentication
• Input Capture **(T1056) –** Using keylogging and input capture techniques to steal credentials.
• Account manipulation **(T1555)** – Adding accounts to privilege users
• Credential in files **(T1081) –** Searching for credentials stored in files.
• Data in Registry (**T1082)** – Targeting credentials stored in windows registry.

7. Lateral Movement

- Remote Desktop Protocol **(T1021.001)** – Using compromised RDP sessions.
- Valid Accounts **(T1078) -** Using compromised credentials to access other systems.
- Windows Management Instrument **(T1047)** – Executing remote access for lateral movement.
- Remote Services **(T1021)** – Exploiting SSH and SMB for movement within networks.

8. Collection and Exfiltration

- Data Staging **(T1074)** – Aggregating sensitive files before exfiltration.

- Exfiltration Over Web Services **(T1567)** – Sending stolen data via cloud platforms or encrypted channels.
- Data Transfer Size Limits **(T1022)** – Breaking down large data sets into smaller chunks to avoid detection.
- Application layer protocol **(T1071)** – Using protocols such as HTTPS and DNS to exfiltrate data.

Solarwinds supply chain attack

The SolarWinds supply chain attack, credited to APT29 (Cozy Bear), was one of the most urgent cyber-espionage operations in recent history. The attack leveraged compromised software updates process in Orion network monitoring platform to infiltrate thousands of organizations, including U.S. government agencies and Fortune 500 companies. The compromised system allowed them to inject malicious code to legitimate Orion software updates. SolarWinds distributed the malicious updates to customers in over 18,000 organizations who downloaded and installed the updates.

1. Attack Breakdown & MITRE ATT&CK Mapping

Phase 1: Initial Access

APT29 compromised SolarWinds Orion software updates, embedding SUNBURST malware which was a trojan software. This granted access to any organization that installed the malicious update.

- T1195.002 (Supply Chain Compromise): This compromise Orion software updates.
    - Attackers modified the Orion software build system to insert a malicious DLL.
- T1072 - Software Deployment Tools
    - Used SolarWinds Orion as a legitimate software tool for malware distribution.

Phase 2: Execution

Once inside target networks, the malware executed commands, collected system information, and established persistence.

- T1059.001 - Command and Scripting Interpreter: PowerShell
    - Executed malicious PowerShell scripts that modified registry keys and scheduled tasks that remained active even after rebooting.
- T1204.002 - User Execution: Malicious File
    - Executed the malware in every user who had installed the updates.

Phase 3: Persistence

APT29 used multiple techniques to maintain long-term access.

- T1547.001 - Boot or Logon Autostart Execution: Modified registries in the users PCs
    - Modified registry keys to ensure persistence after reboots.
- T1053.005 - Scheduled Task/Job: Scheduled Task
    - Created scheduled tasks to re-establish backdoors.

Phase 4: Privilege Escalation

To gain higher privileges, APT29 exploited system vulnerabilities and misconfigurations and used stolen credentials to gain privilege access.

- T1068 - Exploitation for Privilege Escalation
    - Exploited unpatched Windows services.
- T1078 - Valid Accounts
    - Used stolen admin credentials to gain elevated access.

Phase 5: Defense Evasion

APT29 used obfuscation and stealth tactics to bypass security solutions.

- T1027.002 - Obfuscated Files or Information: Software Packing
    - Encrypted and packed payloads to evade detection.
- T1070.004 - Indicator Removal: File Deletion
    - Deleted logs and evidence of presence.

- T1562.001 – Impaired Defences: Disable and modify Tools
    - Disabled security monitoring tools to avoid security alerts and detection.

Phase 6: Credential Access

Credential harvesting by APT29 to move laterally within networks.

- T1003.001 - Credential Dumping: LSASS Memory
    - Extracted credentials from Local Security Authority Subsystem Service (LSASS).
- T1550.002 - Use of Valid Accounts: Pass the Hash
    - Used NTLM hashes to authenticate without passwords.

Phase 7: Lateral Movement

Once inside, APT29 moved across the network to enlarge access.

- T1021.001 - Remote Services: Remote Desktop Protocol (RDP)
  - Used RDP to move between compromised machines while evading detection.
- T1570 - Lateral Tool Transfer
  - Transferred additional tools across the network.

Phase 8: Collection and Exfiltration

APT29 staged stolen data before exfiltrating it.

- T1074.001 - Data Staging: Local Data Staging
  - Aggregated sensitive documents on internal servers.
- T1567.002 - Exfiltration Over Web Services: Cloud Storage
  - Sent stolen data to Microsoft Azure and Dropbox.

Phase 9: Command and Control

APT29 staged stolen malware to communicate with C2 servers using HTTPs requests and DNS tunneling.

- T1071.001 – Application Layer Protocol: Web protocols
  - Communication with C2 servers using HTTPS and DNS to mimic legitimate communication.

Timeline of Events

Date	Event
September 2019	Attackers gained access to SolarWinds' build system.
March 2020	Compromised **Orion** software updates were deployed
June 2020	**APT29** used the backdoor to infiltrate us agencies.
December 2020	FireEye discovered the breach and disclosed it publicly.
January 2021	**U.S.** government attributed the attack **to** APT29 (SVR)**.**

3. How the Attack Could Have Been Detected Using MITRE ATT&CK

- **Initial Access Detection**
    - Monitoring email logs for suspicious attachments or links.
    - Intrusion detection system (IDS) rules for known exploit signatures.
    - Web application firewall (WAF) alerts for anomalies in HTTP requests.
- **Execution Detection**
    - Logging and analyzing command execution (e.g., PowerShell, Bash).
    - Monitoring for unusual script execution behavior.
    - Behavioral anomaly detection using endpoint detection and response (EDR).
- **Persistence Detection**
    - Checking for new or modified scheduled tasks.
    - Monitoring changes to registry run keys or startup folders.
    - File integrity monitoring (FIM) on key system directories.
- **Privilege Escalation Detection**
    - Kernel log analysis for suspicious privilege elevation attempts.
    - Monitoring for sudden administrative privilege assignments.
    - Endpoint detection tools alerting on exploit behavior.

5. Defense Evasion Detection

- SIEM alerts on antivirus or logging services being disabled.
- Behavioral analysis of system calls and process injection.
- Checking integrity of security tool configurations.

6. Credential Access Detection

- Monitoring LSASS memory access for Mimikatz-like behavior.
- Detecting unexpected account logins or token manipulations.
- Watching for anomalous LDAP queries against Active Directory.

7. Lateral Movement Detection

- Anomalous RDP session monitoring.
- Logging and alerting on NTLM authentication anomalies.
- Unusual SMB session tracking.

8. Exfiltration Detection

- Network data loss prevention (DLP) alerts on unauthorized file transfers.
- Monitoring for large outbound data transfers.
- Detecting encryption of large amounts of data before transfer.

9. Impact Detection

- SIEM correlation of mass file modifications.
- Identifying unusual encryption process behavior.
- Backup system anomalies and sudden deletions. **Task 3: APT29 Threat Actor Report**

Threat Actor: APT29 (Cozy Bear)

Overview

APT29, also known as Cozy Bear**,** is a Russia-sponsored cyber-espionage group linked to the SVR**.** They target government agencies, defense contractors, think tanks, and healthcare organizations to steal sensitive data.

Key TTPs Used by APT29

Tactic	Technique
Initial Access	Supply Chain Compromise (T1195.002)
Execution	PowerShell (T1059.001)
Persistence	Registry Run Keys (T1547.001)
Privilege Escalation	Exploitation for Privilege Escalation (T1068)
Defense Evasion	Obfuscated Files (T1027.002)
Credential Access	Credential Dumping (T1003.001)
Lateral Movement	Remote Services (T1021.001)
Exfiltration	Exfiltration Over Cloud (T1567.002)

Indicators of Compromise (IoCs)

Malicious Domains:

- avsvmcloud.com
- solartrackingsystem.com
- windows-updater.com
- cdnserverservice.com
- cloudsyncpanel.com

IPs Used for C2:

- 45.124.132.106
- 193.36.119.162
- 45.124.132.10
- 190.97.165.171
- 193.36.116.119
- 185.99.133.226
- 185.140.55.35
- 31.13.195.210
- 103.193.4.101
- 141.255.164.36
- 141.255.164.11
- 141.255.164.40
- 111.90.151.120
- 111.90.147.248
- 91.132.139.195
- 86.106.131.155
- 152.89.160.81
- 178.157.13.168
- 141.98.214.14
- 116.202.251.5
- 116.202.251.49
- 220.158.216.139
- 193.34.167.162
- 185.207.205.174
- 152.44.45.10
- 37.120.247.163
- 51.89.115.119
- 190.97.165.204
- 51.89.115.117
- 193.36.119.184
- 164.132.135.102
- 169.239.128.132
- 169.239.129.121
- 89.33.246.82
- 213.227.154.58

Malware Hashes:

- **SUNBURST DLL**: (b91ce2fa41029f6955bff20079468448)
- **TEARDROP Loader:** (7c1a5de3db0e5ffbe19594b693d2c40e)
- **SNOWYAMBER**:(381a3c6c7e119f58dfde6f03a9890353a20badfa1bfa7c38ed e62c6b0692103c)
- **GraphicalProton**:(a66d76d86448965e57d7be96a57529c497e4b99d)

IMPORTANCE OF THREAT ACTOR PROFILING

- **Enhance Threat Intelligence** – Helps one understand the enemies how and why in every attack while anticipating future attacks.
- **Improve Incident Response** – Aids in resource allocation hence faster and more effective response
- **Strengthen Defense Strategies** – Security controls can be tailored to specific

threat groups.
- **Prioritize Security Investments** – Resources are allocated based on real world threats.

MITRE ATT&CK framework is very crucial in cybersecurity as it aids in aligning defenses to known TTPs hence improving threat hunting. It improves the readiness of the incident response as it provides threat intelligence that can be shared widely based on real world attacks.