Russia - APT29

Executive Summary

APT29, also known as Cozy Bear, Midnight Blizzard, The Dukes, Dark Halo, and NobleBaron, is a Russian state-sponsored cyber group linked to the Foreign Intelligence Service (SVR). APT29 has recently advanced its tradecraft by leveraging legitimate cloud services and Software-as-a-Service (SaaS) platforms to conduct covert, highly targeted cyber espionage campaigns. Their operations have primarily focused on Western governments, diplomatic entities, and critical infrastructure. This shift toward cloud-native techniques allows their activity to blend into normal network traffic, significantly reducing the effectiveness of traditional security tools.

This evolution is part of a broader trend among nation-state actors using “living off the land” techniques to evade detection and maintain long-term access to compromised environments.

As geopolitical tensions continue to rise, organizations in targeted sectors must reassess their cloud security posture and detection strategies to defend against increasingly stealthy and persistent threats like APT29.

Key Points

- APT29 is a Russian state-sponsored cyber-espionage group linked to the SVR, known for targeting Western governments, diplomatic missions, non-governmental organizations (NGO), and critical infrastructure.
- The group has expanded its operations with a focus on persistent, highly targeted intelligence-gathering campaigns.
- APT29 increasingly leverages legitimate cloud and SaaS platforms to conduct operations that blend into regular network activity, making detection more difficult.
- These evolving tactics weaken traditional security models and increase risk for organizations dependent on cloud infrastructure, requiring improved behavioral monitoring and detection capabilities.

Risk Assessment

The NJCCIC has assessed that APT29 poses a significant and growing threat to organizations that manage sensitive government, diplomatic, or infrastructure data. The group can maintain covert, long-term access while evading conventional detection tools by abusing legitimate cloud services and employing "living off the land" (LOTL) techniques.

This shift is especially concerning for cloud-dependent organizations with limited visibility into user behavior and identity activity. APT29 has previously targeted sectors such as government and critical infrastructure and has deployed malware linked to earlier detections in similar environments. These tactics align with common gaps in

cloud and identity security postures, increasing the likelihood of successful intrusions and reinforcing the need for immediate improvements in detection and response capabilities.

Threat Actor Summary

APT29, associated with the SVR, primarily targets government, diplomatic, non-governmental, and critical infrastructure sectors in countries such as the United States (US), the United Kingdom, NATO members, and other Western allies. Since 2008, the group has been actively tracked by the cybersecurity community and remains a key player in Russia's foreign intelligence operations.

Technical Analysis

Tactics, Techniques, & Procedures

APT29 is known for its covert and persistent cyber-espionage campaigns. The group typically gains access through spearphishing attacks and, more recently, by compromising cloud identity systems and using stolen credentials to infiltrate cloud environments, often without deploying malware.

Inside networks, the group relies on legitimate tools like PowerShell, Windows Management Instrumentation (WMI), and LOTL techniques to evade detection. While APT29 has used custom malware such as WellMess and GoldMax, it increasingly favors trusted services and non-malware methods to maintain access and exfiltrate data, making detection and attribution more difficult.

Infrastructure

APT29 employs a range of infrastructures to support its command-and-control (C2) operations, including virtual private servers (VPS), compromised third-party websites, and cloud-based services. In recent campaigns, APT29 has leveraged platforms like Microsoft 365, Dropbox, and Google Drive to manage C2 channels and exfiltrate data. The group also favors hijacked email accounts within compromised organizations to distribute phishing emails and maintain a low profile.

Victims

APT29's targeting closely aligns with Russia's foreign intelligence priorities, focusing on espionage rather than disruption. Victims typically include entities involved in diplomacy, foreign policy, international security, and sensitive research. The group's operations support Russian strategic objectives by exfiltrating classified or policy-relevant information from adversarial governments and institutions.

Target Sectors

- Government and Diplomatic Institutions
- Defense and Military Contractors
- Energy and Critical Infrastructure
- Healthcare and Global Health Organizations
- Think Tanks and Policy Organizations
- Technology and Research Institutions

Geographic Focus

- United States
- United Kingdom
- Canada
- NATO Member States
- EU Countries
- Ukraine
- Nordic and Baltic States
- United Nations (UN) and NGOs

Attribution

APT29 has been widely attributed to the SVR by both government agencies and private cybersecurity firms in the US and internationally. This attribution is supported by strong forensic evidence, including consistent use of operational infrastructure, malware development patterns, and targeting that aligns with SVR intelligence-gathering priorities. The group's activity patterns, including working hours aligned with Moscow's time zone, Russian language artifacts, and the strategic nature of its intrusions, further reinforce its linkage to Russian state interests.

Timeline of Activity

Start Date	End Date	Location	Sector	Activity
2008	Ongoing	Global	Government, Think Tanks, and Technology	A long-term cyber espionage campaign focused on intelligence collection targeting Western governments, NGOs, and research institutions.

2014	2015	US	Government	Breach of unclassified US State Department and White House networks via phishing and malware.
2016	2016	US	Political (DNC)	Targeted the Democratic National Committee (DNC) using spearphishing. Believed APT 28 was also involved.
2020	2020	US, UK, and Canada	Healthcare and Research	Targeted organizations involved in COVID-19 vaccine development, exploiting vulnerabilities and conducting credential harvesting.

March 2020	December 2020	Global	IT, Government, and Private Sector	SolarWinds supply chain attack: Compromised Orion Software to infiltrate US federal agencies and private companies.
2021	2022	Europe and US	Government and Think Tanks	Phishing and malware campaigns using new backdoors. Targeted diplomatic and policy organizations.
2023	2024	NATO-aligned nations	Government and military	Continued phishing campaigns targeting government officials and diplomats, including abusing Microsoft Teams for initial access.

Key Intelligence Gaps

The NJCCIC has identified several critical intelligence gaps that limit a complete assessment of APT29. One major unknown is how deeply they've been able to compromise cloud identity services like Azure AD or Okta, which could give them wide access to sensitive systems. It's also unclear if APT29 is developing new malware designed

specifically for cloud environments, which would affect how to detect and defend against them. There is also limited knowledge about whether APT29's recent activity has shifted to target new regions or industries, especially in response to current geopolitical events.

Another challenge is the lack of clear indicators showing how they move laterally within cloud or hybrid networks, which limits our ability to spot their presence early. Since APT29 often uses public infrastructure and built-in tools, it's becoming harder to attribute certain attacks to them. Finally, there is no solid understanding of how long APT29 threat actors typically stay inside a compromised environment, especially in cloud systems, which makes it difficult to judge how much damage they may cause before detection.

MITRE ATT&CK Table (based on v12)

Tactics	Techniques	Sub Technique	Procedure	D3FEND	Deployed Control
Initial Access	Phishing	Spearphishing attachment	Sent targeted spearphishing emails with malicious attachments	D3-EMA, D3-FWM	Email filtering, malware sandboxing, and user awareness
Execution	Command and Scripting interpreter	PowerShell	Used PowerShel scripts to execute payloads and establish persistence	D3-PSA	PowerShell logging, script block loggings
Persistence	Boot or Logon AutoStart Execution	Registry Run Key	Set values in Windows Registry Run keys to maintain persistence across reboots	D3-RPI	Registry monitoring and endpoint detection

Privilege Escalation	Exploitation for privilege Escalation	N/A	Exploited privilege escalation vulnerabilities to gain system level access	N/A	Patch management, EDR, and least privilege enforcement
Defense Evasion	Obfuscated files or information	N/A	Used base64 and custom encryption to obfuscate payloads and command strings	D3-OBS	Endpoint protection and file integrity monitoring
Credential Access	OS Credential Dumping	LSASS Memory	Used tools to dump credentials from LSASS	D3-CDA	LSASS protection, credential guard, and memory analysis
Discovery	System Information Discovery	N/A	Queried hostnames, domain information, and system specs after gaining initial access	D3-HDI	Host-based intrusion detection
Lateral Movement	Remote Services	Remote desktop protocol	Leveraged RDP to move laterally between systems within compromised environments	D3-RDP and D3-RMA	Network Segmentation, RDP monitoring, and MFA

Command and control	Application Layer Protocol	Web Protocols	Used HTTPs to communicate with C2 infrastructure, often over ports 443 to blend with normal traffic	D3-WAF and D3-NTA	Web Proxy, TLS inspection, and anomaly detection
Exfiltration	Exfiltration over C2 channel	N/A	Data was exfiltrated over the same encrypted channel used for C2 to avoid detection	D3-DAL and D3-NTA	Data loss prevention and traffic monitoring
Impact	Data manipulation	N/A	Modified internal documents to confuse incident responders and hinder attribution	N/A	File integrity monitoring and version control

Victims

Name	Date Reported	Sector	City/State/Province/etc.	Country/Region
US Department of State	2014-2015	Government	Washington, D.C.	US
White House	2015	Government	Washington, D.C.	US
Democratic National Committee (DNC)	2016	Political Organization	Washington, D.C.	US

US Department of Treasury	2020	Government	Washington, D.C	US
US Department of Homeland Security	2020	Government	Washington, D.C.	US
SolarWinds	2020	IT	Austin, Texas	US
FireEye	2020	Cybersecurity	California	US
COVID-19 Vaccine Research Orgs.	2020	Healthcare	Various	US, UK, and Canada
Norwegian Parliament	2020	Government	Oslo	Norway
Microsoft (Email Breach)	2023	Technology	Redmond, Washington	US
US Federal Agencies	2024	Government	Various	US
NATO-Aligned Diplomatic Missions	2023-2024	Government/ Foreign Affairs	Various	Europe

Indicators of Compromise (IOC)

Malware

Malicious Tool Name	Hash Type	File Hash	Associated Files Hash	Brief Description	Malware Analysis Report (Hyperlink, or N/A)	First Reported	Last Reported

SUNBURST	SHA256	32519c7f1ed0d7c46b4d7c85cf1a9be7c224e0555029f51bc23314890033ad17	N/A	Backdoor embedded in SolarWinds Orion software. Part of the SolarWind supply chain attack.	FireEye Analysis	March 2020	December 2020
WELLMAIL	SHA256	1d8871c4eb64f98210c01c2ab7a2e675396b1a69c21d158a7dbd3a3e1467f9b2	N/A	Custom malware used in COVID-19 vaccine-related espionage. Used for exfiltrating files.	NCSC Report	2020	2020
WELLMESS	SHA256	79c41e1f7f07ec4a4fd60f661ce3b11d09ce47a28e1ed6a9e6f6fa2f03fbc3a6	N/A	Remote access trojan (RAT) supporting HTTP, HTTPS, and command execution. Used in targeted attacks on COVID-19 research organization.	NCSC Report	2018	2020

GoldMax	SHA256	ef90581e8a914f4ecf87eb960b1752fd6f409c9e6e6d195be8c2676e6b347e7d	N/A	Persistent malware used for C2 operations over HTTPS with evasive capabilities. Linked to post SolarWinds activity.	CISA Alert	May 2020	January 2021
Cobalt Strike (Beacon)	SHA256	Varies	N/A	Commercial penetration testing tools used post-compromised to establish persistence and lateral movement.	CISA Alert	2019	Ongoing
Kazuar	SHA256	a5adf2c6dd9d0bce750be28d09b80c14843a1e496dcfa98ecac8dc5535b7c6a8	N/A	.NET backdoor with strong obfuscation, used for espionage.	Palo Alto	2017	2021

Network

Network Artifact	Details	Intrusion Phase	First Reported	Last Reported
avsvmcloud[.]com	SUBBURST backdoor C2 domain	C&C	December 2020	April 2021
databasegalore[.]com	BEACON C2 domain for Cobalt Strike	C&C	December 2020	April 2021

deftsecurity[.]com	Malware hosting	C&C and payload delivery	December 2020	April 2021
13.59.205.66	Cobalt Strike C2 IP	C&C	2020	2021
54.193.127.66	Malware distribution server IP	C7C and initial payload	2020	2021
204.188.205.66	Phishing infrastructure/ credential capture IP	Initial Access	2020	2021
hxxps://matclick[.]com/wp-query[.]php	GraphicalProton HTTPS C2 URL	C&C	December 2023	December 2023
65.20.97.203	Tunnel endpoint for GraphicalProton backdoor	C&C/ lateral movement	December 2023	December 2023
65.21.51.58	Tunnel endpoint	C&C/ lateral movement	December 2023	December 2023
103.76.128.34	Exploitation server linked to JetBrains TeamCity CVE abuse	Initial access	September 2023	December 2023

System Artifacts

Host Artifact	Type	Details	Tactic	First Reported	Last Reported

netsetupsvc.dll	DLL	SUNBURST loader DLL planted via SolarWinds Orion compromise	Execution/ Persistence	December 2020	2021
GoldMax backdoor executable	Binary/ Process	Hides in hidden directories. Persistence via cron job on Linux.	Persistence	May 2020	2021
TrailBlazer implant	Binary/ Process	Hides as legitimate filenames. Persistence via WMI event subscription.	Persistence/ Command & Control	2019	2021
Registry key at HKLM:\Software\Classes\CLSID\{...}\ProgID\{...}	Registry	PowerShell script loader payload embedded in CLSID key, executed via rund1132.exe	Execution/ Defense Evasion	2021	2021
wine.exe + side-loaded malicious .dll (GRAPELOADER)	Process/ DLL	Zip contains genuine PowerPoint launcher (wine.exe) that side loads DLL implementing Grapeloader.	Execution/ Persistence	April 2025	April 2025

Custom Cobalt Strike loader mapped over ntdll.dll shellcode	DLL mapping/ In-memory loader	BEATDROP downloader maps its own version for ntdll.dll, spawns suspended thread, injects shellcode to evade detection.	Execution	January 2022	January 2022

Common Vulnerabilities and Exposures (CVEs)

CVE Number	CVSS Score	Patch Available (Y/N)	Other Remediation	Date Reported	Patch Applied (Y/N/UNK/NA)
CVE-2020-10148	7.8	Y	Update SolarWinds Orion platform	December 2020	Y
CVE-2021-34473	9.8	Y	Apply Microsoft Exchange Server patches	March 2021	Y
CVE-2021-26855	9.1	Y	Exchange Server patch, disable external access	March 2021	Y
CVE-2023-42793	8.6	Y	Update JetBrains TeamCity server	September 2023	Unknown

CVE-2019-19781	9.8	Y	Apply Citrix ADC and Gateway patches	December 2019	Y
CVE-2020-0688	7.5	Y	Microsoft Exchange Server patch	February 2020	Y