# COZY BEAR

*[ / 'kou.zi ber / ]*

APT29 (Cozy Bear) is a Russian SVR-linked threat actor active since 2008. Known for espionage against governments, think tanks, tech providers, and critical infrastructure, it recently (2024–2025) conducted supply chain attacks, cloud identity abuse, and a Microsoft email breach. APT29 is high-risk, using stealth and advanced techniques for long-term persistence.

## IDENTITY

| | |
|---|---|
| Attribution | : Russian Federation, assessed with high confidence as part of the SVR (Foreign Intelligence Service). |
| Active Since | : At least 2008. |
| Aliases | : ATK7, SeaDuke, BlueBravo, TA421, Cloaked Ursa, Group 100, Minidionis, Blue Kitsune, Nobelium, YTTRIUM, ITG11, The Dukes, Cozy Bear, IRON HEMLOCK, Grizzly Steppe, UAC-0029, G0016, SPIKEDWINE. |
| Motivation | : Espionage — focused on long-term intelligence collection in support of Russian state interests (diplomatic, defense, and geopolitical). |

## TTPs

| | |
|---|---|
| Initial Access | : Spearphishing, credential harvesting, password spraying, supply chain intrusions (e.g., SolarWinds Orion), exploitation of VPN and cloud identity services. |
| Persistence | : Use of OAuth consent phishing, Golden SAML abuse, cloud token hijacking, DLL sideloading, and long-term footholds in networks. |
| C2 Infrastructure | : Custom malware families with encrypted communications, often over HTTPS; abuse of legitimate cloud services (e.g., Microsoft 365, Azure, Google Drive) for covert C2. |
| Malware & Tools | : **SeaDuke, MiniDuke, CosmicDuke, CozyDuke** (custom backdoors), **SUNBURST / Solorigate** malware from SolarWinds campaign, **GoldMax, TrailBlazer, EnvyScout, BoomBox** post-SolarWinds toolset, Credential theft tools and living-off-the-land binaries (PowerShell, WMI). |
| Techniques | : Living-off-the-land (LotL), stealthy lateral movement, selective data exfiltration, cloud exploitation, evasion through multi-hop infrastructures |

## TARGET PROFILE

| | |
|---|---|
| Target Sectors | : Government ministries (foreign affairs, defense, intelligence), Research institutes, NGOs, and policy think tanks, Technology, IT/cloud service providers, Energy and critical infrastructure. |
| Geographies Targeted | : **United States** (government, contractors), **European Union / NATO members**, **Eastern Europe** (Ukraine, neighbors), Global diplomatic missions and NGOs. |

## THREAT ASSESSMENT

| | |
|---|---|
| Risk Level | : High (Strategic, Persistent) |
| Most Recent Activity | : 2024–2025 campaigns exploiting **cloud identity abuse** (Microsoft email breach via password spray, December 2024). Expanded **supply chain compromises** and targeting of Western diplomatic and defense institutions. |
| Evolution | : Demonstrates **discipline and patience**, often maintaining access for months or years. Early campaigns focused on traditional malware; more recent focus is on **cloud services, stealth persistence, and identity compromise.** |

## NOTABLE OPERATIONS

- **2008–2014 – The Dukes Campaigns:** Widespread espionage against European and U.S. government bodies using custom backdoors (MiniDuke, CosmicDuke).
- **2014 – State Department / White House Intrusions:** Major breaches of U.S. federal email systems.
- **2015–2016 – Democratic National Committee (DNC) Intrusion:** Espionage against U.S. political organizations.
- **2020 – SolarWinds Supply Chain Attack (SUNBURST):** Compromised thousands of organizations globally, including U.S. government agencies and Fortune 500 firms.
- **2021 – Microsoft 365 & Cloud Exploitation:** OAuth phishing and persistent intrusions against diplomatic missions.
- **2023–2024 – BlueBravo Activity:** Targeting of EU ministries and NATO-aligned organizations.
- **2024 – Microsoft Corporate Email Breach:** Password spraying enabled access to senior leadership email accounts.
- **2025 – Ongoing Campaigns:** Supply chain intrusions, continued targeting of Western governments, NGOs, and cloud infrastructure.