Cyber Threat Intelligence Brief – APT29 (Cozy Bear / Midnight Blizzard)

Date: 2025-10-02

Author: Tafadzwa Victor Chipere

Classification: Public (Portfolio Sample)

Executive Summary

APT29, attributed to the Russian Foreign Intelligence Service (SVR), continues to target UK and allied organisations. Recent activity focuses on cloud identity abuse, credential theft, and phishing. This brief summarises high-priority TTPs, recent campaigns, and actionable recommendations for UK enterprises.

Key Points:

• APT29 has targeted UK government, critical national infrastructure, political organisations, and research.

• Current campaigns exploit cloud services using token theft and dormant/unused accounts.

• Techniques include spearphishing attachments (T1566.002) and PowerShell execution/obfuscation (T1059.001).

• Defenders should focus on Azure AD/Entra logs, anomaly detection, and phishing-resistant MFA.

Threat Actor Profile

Aliases: APT29, Cozy Bear, The Dukes, Midnight Blizzard

Sponsor: Russian SVR (state-sponsored)

Motivation: Strategic espionage against government, defence, research and policy organisations.

Targeting (UK relevance): Public advisories note activity against UK/European government and research bodies.

Recent Campaigns (Highlights)

• HTML Smuggling Phishing (2023–2024): delivery of WINELOADER via malicious attachments targeting European political organisations.

• Cloud Infrastructure Abuse (2023–2025): password spraying (T1110.003), Graph API misuse (T1106), abuse of dormant accounts to bypass MFA.

• Historic reference: SolarWinds supply-chain compromise (2020).

Key TTPs (MITRE ATT&CK Mapping)

Tactic	Technique & ID	Example Use by APT29
Initial Access	T1566.002 – Spearphishing Attachment	Malicious HTML/ISO attachments to deliver WINELOADER
Execution	T1059.001 – PowerShell	Obfuscated commands for payload execution
Credential Access	T1110.003 – Password Spraying	Cloud account attacks to gain initial foothold
Persistence	T1136 – Create Accounts / Dormant Accounts	Registering devices & re-activating unused accounts
Defence Evasion	T1553 – Subvert Trust Controls	Token theft & Graph API abuse
C2 / Exfiltration	T1071 – Application Layer Protocol	HTTPS C2 to compromised infrastructure

Detection & Recommendations (Summary)

• Enable and review: Entra ID/Azure AD sign-in logs, Graph API usage, device registration events.

• Hunt for: PowerShell with encoded commands; unusual sign-in patterns (time/location anomalies).

• Mitigations:

– Enforce conditional access and phishing-resistant MFA.

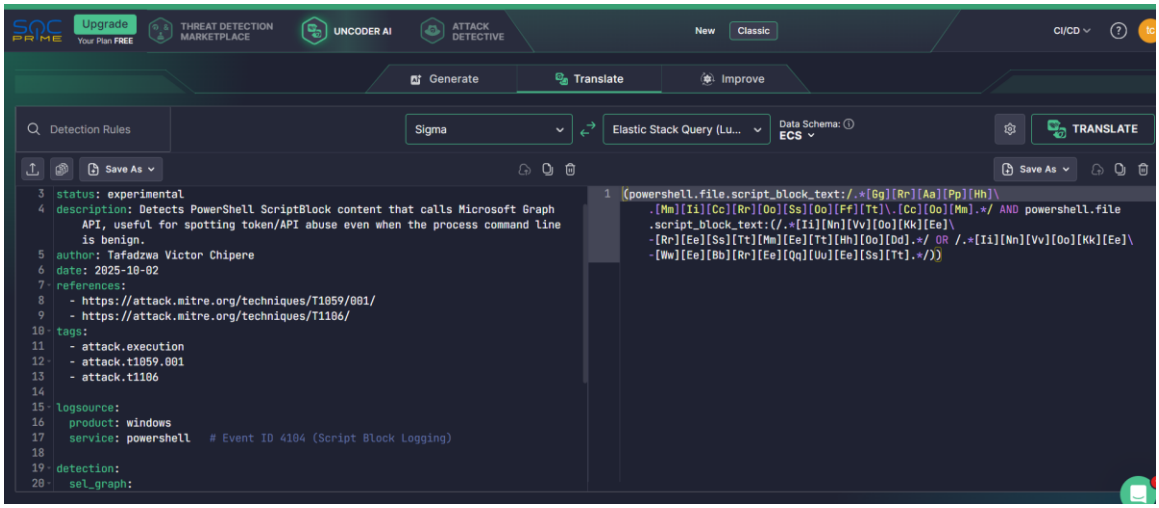
– Disable legacy authentication.

– Review and purge dormant accounts; monitor device registration.

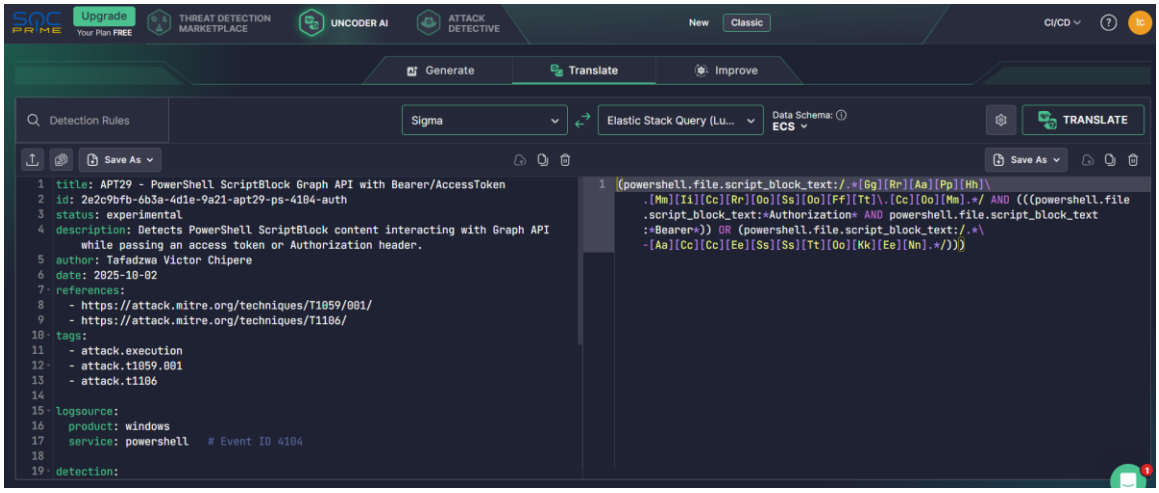
– Apply anomaly detection to Graph API requests.

– Validate coverage using Atomic Red Team / MITRE CALDERA emulation.

Screenshots



• Figure 1: Uncoder.io – Sigma rule (process_creation) and Elastic query translation (PNG).



• Figure 2: Uncoder.io – Sigma rule (PowerShell ScriptBlock EID 4104) and KQL/Splunk translation (PNG).