**OSINT Threat Intelligence Brief  
Prepared by:** Adefolaji Fasanya **Organization:** NovaLink Aerospace Solutions **Date:** 05/26/2025 **Threat Actor:** APT29 (Cozy Bear)

**Overview**APT29, also known as Cozy Bear, is a sophisticated, Russian state-sponsored threat actor linked to cyber espionage campaigns targeting government agencies, defense contractors, think tanks, and private sector organizations. Their operations are known for stealth, persistence, and intelligence-gathering objectives.

In May 2025, NovaLink Aerospace Solutions identified a series of spear phishing attempts traced back to known APT29 infrastructure. The tactics aligned with historic campaigns attributed to the group, including credential harvesting and the use of living-off-the-land binaries (LOLBins).

**Indicators of Compromise (IOCs)**

* **IP Addresses:**
  + 185.86.149.12
  + 192.241.206.88
* **Domains:**
  + secure-update[.]com
  + netbackup-services[.]org
* **Malware Families Identified:**
  + WellMess
  + WellMail

**Tactics, Techniques, and Procedures (TTPs)**

* Spear phishing emails with malicious PDF attachments targeting engineers and HR staff
* Execution of LOLBins such as mshta.exe and powershell.exe for stealthy post-exploitation activity
* Use of stolen credentials to access internal systems and move laterally within segmented networks
* Command-and-control traffic observed over HTTPS and DNS tunneling

**Mitigation Recommendations**

* Enforce multi-factor authentication (MFA) across all VPNs, email portals, and administrative systems
* Deploy advanced email security gateways with sandboxing and attachment detonation
* Monitor for execution of known LOLBins and flag anomalous PowerShell usage
* Conduct recurring user training sessions on phishing awareness and suspicious link handling
* Ingest OSINT and commercial threat intelligence feeds to enrich alerting and blocklists

**Appendix**

* Redacted phishing email sample
* VirusTotal analysis of malicious attachment
* Timeline of attempted intrusion
* MITRE ATT&CK mapping for observed behaviors