APT29 (Cozy Bear) Threat Analysis Report

THREAT INTELLIGENCE REPORT
APT29 - Advanced Persistent Threat

Executive Summary:
APT29, also known as Cozy Bear, is a sophisticated threat actor associated with Russian intelligence services. This report analyzes recent campaigns.

Initial Access (MITRE ATT&CK):
- T1566.001: Spearphishing Attachment
  Attackers send targeted emails with malicious Office documents
- T1190: Exploit Public-Facing Application
  Exploitation of web servers and VPN gateways

Execution Techniques:
- T1059.001: PowerShell
  Heavy use of PowerShell for payload execution
- T1059.003: Windows Command Shell
  Batch scripts for lateral movement

Persistence:
- T1053.005: Scheduled Task/Job
  Created scheduled tasks for persistence
- T1543.003: Windows Service
  Malicious service installation

Indicators of Compromise (IOCs):
File Hashes:
  MD5: a1b2c3d4e5f67890123456789012345678901234ab
  SHA256: 7a8b9c0d1e2f3456789abcdef0123456789abcdef0123456789abcdef012345

Network Indicators:
  IP: 192.0.2.45
  Domain: malicious-update.example
  URL: http://c2-server.example/beacon.php

Recommendations:
- Implement email filtering for suspicious attachments
- Monitor PowerShell execution logs
- Regular security updates for public-facing applications