Threat Report: APT28 Campaign

APT28 targeted U.S.-based organizations using spear phishing emails. Techniques included:

- T1566.001: Spearphishing Attachment

- T1059: Command and Scripting Interpreter

Indicators of compromise included malicious domains, hashes, and IPs.

Recommendations:

- Educate users on phishing detection

- Enable attachment sandboxing

- Monitor PowerShell usage patterns

Report by Nicholas Magner