🕵️ APT28 Case Study – Threat Actor Analysis
Author: Shraddha Mishra
Date: 22 July 2025
Internship: Cybersecurity Internship – Digisuraksha Parhari Foundation

---

🎯 Overview
APT28 (Fancy Bear) is a Russian state-sponsored threat group linked to the GRU. Known for cyber espionage, election interference, and targeting NATO, EU, and defense sectors.

🧩 MITRE ATT&CK Mapping

Tactic	Technique ID	Technique Name	Description
Initial Access	T1566.001	Spear Phishing Attachment	Malicious documents sent via email
Execution	T1059.001	PowerShell	Used for script execution
Credential Access	T1003	OS Credential Dumping	Mimikatz used to extract credentials
Persistence	T1547.001	Registry Run Keys	Malware set to auto-start
Defense Evasion	T1070.004	File Deletion	Logs and artifacts removed
Command & Control	T1071.001	Web Protocols	HTTP/S used for C2 communication

---

💉 Malware Used by APT28

- **X-Agent**: Modular backdoor for Windows, Android, iOS
- **Zebrocy**: Downloader and credential stealer
- **XTunnel**: Network tunneling tool for lateral movement
- **CHOPSTICK**: Advanced surveillance implant

📚 Case Studies

1. **2016 U.S. Election Interference**
APT28 breached the DNC and leaked emails via Guccifer 2.0 to influence public opinion.

2. **German Bundestag Hack (2015)**
Used spear-phishing to infiltrate German Parliament and exfiltrate sensitive data.

3. **TV5Monde Attack (France, 2015)**

Disrupted French TV channels and defaced websites, initially posing as ISIS.
