**APT Group: Putter Panda (MITRE ID: G0024)**

**Country: China**

**Overview:**  
Putter Panda is a Chinese cyber-espionage group linked to Unit 61486 of the People’s Liberation Army (PLA). They focus on stealing intellectual property from defense, aerospace, and satellite industries.

**TTPs:**

* **Initial Access:** Spear-phishing emails with malicious attachments or links.
* **Execution:** Deploys *PlugX* malware for system control.
* **Persistence:** Establishes backdoors and modifies system services.
* **Credential Access:** Uses *Mimikatz* to steal credentials.
* **Lateral Movement:** Exploits network vulnerabilities to move across systems.
* **Exfiltration:** Uses encrypted channels to steal sensitive data.

**Notable Campaigns:**  
Putter Panda has targeted Western defense contractors, focusing on aerospace and satellite technologies, stealing technical and military-related data.

**Malware/Tools:**

* *PlugX* RAT
* *Mimikatz*
* Network exploit tools

**Defense:**

* Train employees on phishing risks and use email security tools.
* Implement strong endpoint detection systems.
* Regularly patch and update software to avoid exploitation.