**APT Group: PittyTiger (MITRE ID: G0011)**

**Country: China**

**Overview:**  
PittyTiger is a Chinese APT group known for cyber-espionage activities, targeting organizations in defense, government, and technology sectors. Active since at least 2011, the group focuses on stealing intellectual property and sensitive information.

**TTPs:**

* **Initial Access:** Spear-phishing emails with malicious attachments or links.
* **Execution:** Custom malware, including remote access Trojans (RATs), deployed to compromised systems.
* **Persistence:** Creation of new system services and scheduled tasks.
* **Credential Access:** Use of keyloggers and credential-stealing malware.
* **Lateral Movement:** Exploitation of network vulnerabilities for moving across systems.
* **Exfiltration:** Stolen data is encrypted and exfiltrated via HTTP/S channels.

**Notable Campaigns:**  
PittyTiger has targeted organizations in Southeast Asia, focusing on military and diplomatic entities, with several campaigns tied to geopolitical espionage.

**Malware/Tools:**

* Custom RATs
* Credential stealers
* Exploit tools for lateral movement

**Defense:**

* Implement advanced email filtering and user training.
* Monitor for unusual network activity, particularly in high-value systems.
* Use encryption for sensitive data and restrict access to critical assets.