**APT Group: Suckfly (MITRE ID: G0039)**

**Country: China**

**Overview:**  
Suckfly is a Chinese cyber-espionage group known for targeting organizations in the technology, telecommunications, and transportation sectors. Their operations focus on gathering intelligence and stealing sensitive data for national interests.

**TTPs:**

* **Initial Access:** Gains entry primarily through spear-phishing campaigns, often using malicious attachments or links that appear legitimate.
* **Execution:** Deploys malware such as *Maltose* and *Tianfu* to execute commands on infected systems.
* **Persistence:** Establishes persistence through backdoors and modifying system settings to maintain long-term access.
* **Credential Access:** Utilizes credential harvesting tools and keyloggers to collect sensitive login information.
* **Lateral Movement:** Moves laterally within networks by exploiting vulnerabilities and using stolen credentials.
* **Exfiltration:** Conducts data exfiltration using encrypted communications to evade detection.

**Notable Campaigns:**  
Suckfly has conducted numerous campaigns targeting high-profile organizations, particularly in the Asia-Pacific region, focusing on obtaining sensitive technological and operational information.

**Malware/Tools:**

* *Maltose* malware for remote access
* *Tianfu* exploit framework
* Keylogging and credential harvesting tools

**Defense:**

* Implement comprehensive email filtering solutions and employee training to reduce phishing risks.
* Employ advanced endpoint detection and response (EDR) systems to monitor for suspicious activities.
* Regularly patch and update systems to mitigate vulnerabilities that could be exploited.