**APT Group: Rocke (MITRE ID: G0106)**

**Country: China**

**Overview:**  
Rocke is a Chinese APT group known for targeting cloud service providers and cryptocurrency-related organizations. The group is primarily focused on stealing sensitive data and exploiting cloud infrastructure for financial gain.

**TTPs:**

* **Initial Access:** Compromises systems through vulnerabilities in cloud services and using phishing techniques.
* **Execution:** Deploys malware like *Rocke* to mine cryptocurrencies and maintain control over compromised systems.
* **Persistence:** Uses web shells and other backdoor techniques to maintain long-term access.
* **Credential Access:** Harvests credentials through phishing and exploits.
* **Lateral Movement:** Moves laterally within networks using compromised credentials and exploit techniques.
* **Exfiltration:** Exfiltrates stolen data through encrypted channels and often uses command-and-control (C2) servers to manage operations.

**Notable Campaigns:**  
Rocke has targeted multiple cloud service providers and cryptocurrency exchanges, aiming to exploit their infrastructure for mining operations and data theft.

**Malware/Tools:**

* *Rocke* malware (for cryptocurrency mining)
* Web shells and backdoor tools

**Defense:**

* Implement strong security measures for cloud services, including regular patching and vulnerability management.
* Employ multi-factor authentication (MFA) to secure access to sensitive systems.
* Monitor network activity for signs of unauthorized access or abnormal behavior.