**APT Group: Scarlet Mimic (MITRE ID: G0029)**

**Country: China**

**Overview:**  
Scarlet Mimic is a Chinese APT group known for its cyber-espionage activities targeting various sectors, including government, telecommunications, and media. Their operations primarily focus on gathering intelligence and stealing sensitive data for geopolitical purposes.

**TTPs:**

* **Initial Access:** Gains entry through spear-phishing emails that include malicious attachments or links, often tailored to specific targets.
* **Execution:** Utilizes malware such as *PowerShell* scripts and *Cobalt Strike* to execute commands on compromised systems.
* **Persistence:** Establishes persistent access using scheduled tasks and registry modifications.
* **Credential Access:** Employs credential dumping tools to harvest usernames and passwords.
* **Lateral Movement:** Uses tools like *PsExec* and legitimate remote access methods to navigate through networks.
* **Exfiltration:** Data exfiltration occurs via encrypted protocols to avoid detection.

**Notable Campaigns:**  
Scarlet Mimic has been involved in campaigns against telecommunications companies and government agencies, often focusing on regions relevant to China's strategic interests.

**Malware/Tools:**

* *Cobalt Strike* for command and control
* PowerShell scripts for execution
* Credential dumping tools

**Defense:**

* Implement comprehensive email security measures and user awareness training to mitigate phishing attacks.
* Use endpoint detection and response (EDR) systems to identify malicious behavior and lateral movement.
* Regularly audit and patch software to reduce vulnerabilities that could be exploited by attackers.