**APT Group: G0027 (Emissary Panda/Threat Group 3390)**

**Country:** China

**Overview:**

Emissary Panda, also known as TG-3390 or APT 27, is a Chinese cyber-espionage group known for targeting defense, aerospace, and governmental sectors. The group typically focuses on intellectual property theft and gaining access to sensitive data for political or commercial advantage.

**TTPs:**

* **Initial Access:** APT 27 uses spear-phishing emails with malicious attachments and exploits vulnerabilities in web applications to gain access to target networks.
* **Execution:** The group has been known to deploy backdoor malware such as *Zox* and *HyperBro* to execute commands on compromised systems and maintain long-term access.
* **Persistence:** APT 27 uses advanced persistence mechanisms, including web shells and backdoors, to ensure continuous access. They often employ custom malware tailored for specific victims.
* **Privilege Escalation:** The group exploits known vulnerabilities in Windows systems to escalate privileges, allowing them to perform a range of malicious activities with higher-level permissions.
* **Credential Access:** Tools such as *Mimikatz* are used to dump credentials from compromised systems, enabling the group to move laterally across the network.
* **Lateral Movement:** Once inside the network, APT 27 moves laterally using legitimate Windows services, such as Remote Desktop Protocol (RDP) and Windows Management Instrumentation (WMI).
* **Command and Control (C2):** The group typically establishes communication channels with compromised systems using custom-developed malware over HTTPS, making it harder to detect.
* **Exfiltration:** Sensitive information, including intellectual property, research data, and defense-related documents, is exfiltrated using encrypted channels.

**Notable Campaigns:**

APT 27 has been associated with numerous campaigns targeting high-value organizations, including military contractors and government entities. One well-known campaign involved infiltrating the networks of defense contractors in the U.S. and Europe to steal military blueprints and defense-related intellectual property.

**Malware/Tools:**

* *HyperBro* – A custom backdoor used to maintain access and execute commands remotely.
* *Zox* – Another backdoor primarily used for espionage operations.
* *Mimikatz* – A tool used for credential dumping.

**Defense Strategies:**

* Strengthen email security through advanced phishing detection systems and educate employees on recognizing spear-phishing attempts.
* Implement strong endpoint detection and response (EDR) systems to monitor for unusual behaviors and lateral movement within networks.
* Use multi-factor authentication (MFA) to prevent unauthorized access via stolen credentials.
* Regularly patch known vulnerabilities in both software and operating systems to minimize attack vectors.