**APT Group: Silent Librarian (MITRE ID: G0122)**

**Country: Iran**

**Overview:**  
Silent Librarian, also known as Cobalt Dickens, is an Iranian APT group primarily focused on cyber-espionage targeting academic institutions, research organizations, and libraries. The group is linked to Iran’s efforts to obtain research and intellectual property, particularly in higher education sectors worldwide.

**TTPs:**

* **Initial Access:** Conducts spear-phishing attacks using fake login pages that mimic university portals and library websites to steal credentials.
* **Execution:** Once access is gained, Silent Librarian uses stolen credentials to infiltrate academic databases and systems to exfiltrate sensitive research data.
* **Persistence:** They maintain access by using compromised credentials and establishing web shells.
* **Credential Access:** Silent Librarian primarily focuses on phishing to steal login credentials, particularly those related to academic portals.
* **Lateral Movement:** Uses compromised accounts to move within networks and access restricted academic and research information.
* **Exfiltration:** Exfiltrates sensitive academic and proprietary research data, often focusing on scientific and technological research.

**Notable Campaigns:**  
Silent Librarian has targeted numerous universities worldwide, particularly those in the U.S., Europe, and Australia. The group has been involved in campaigns aimed at stealing academic research for Iran’s state-sponsored objectives.

**Malware/Tools:**

* Phishing kits mimicking university login pages
* Web shells for persistence

**Defense:**

* Implement multi-factor authentication (MFA) for university portals and research systems.
* Train staff and students on phishing risks and how to identify fake login pages.
* Use advanced threat detection systems to monitor and prevent unauthorized access to academic networks.