**APT Group: G0128 (MuddyWater/Seedworm)**

**Country:** Iran

**Overview:**

MuddyWater, also known as Seedworm, is an Iranian cyber-espionage group that focuses on governmental, telecommunications, oil, and critical infrastructure sectors in the Middle East and beyond. The group is involved in geopolitical espionage, targeting organizations in sectors of strategic interest to Iran.

**TTPs:**

* **Initial Access:** MuddyWater often gains access to networks using spear-phishing emails with malicious attachments, frequently leveraging Microsoft Office documents containing macros or remote template injections to drop malware.
* **Execution:** The group is known for using PowerShell-based scripts to execute malicious payloads on compromised systems. These scripts provide backdoor access and command execution capabilities.
* **Persistence:** MuddyWater employs registry modifications, scheduled tasks, and custom malware such as *POWERSTATS* to maintain long-term access. They are known for building custom malware that evolves throughout their campaigns.
* **Privilege Escalation:** They exploit known vulnerabilities in Windows systems for privilege escalation, allowing them to gain higher privileges within the victim’s network.
* **Credential Access:** The group utilizes tools such as *LaZagne* and keyloggers to steal credentials. They also use social engineering techniques to trick users into divulging their login information.
* **Lateral Movement:** MuddyWater moves laterally within networks by using stolen credentials and legitimate administrative tools, including PsExec, RDP, and WMI.
* **Command and Control (C2):** MuddyWater establishes C2 channels via HTTP and HTTPS communications. They often employ legitimate cloud services to mask their C2 traffic and avoid detection.
* **Exfiltration:** Data exfiltration occurs through encrypted channels, typically focusing on sensitive governmental and defense-related information. The group uses custom tools to siphon off data without triggering alarms.

**Notable Campaigns**

MuddyWater has conducted a number of high-profile campaigns, particularly against Middle Eastern governments, telecommunications providers, and oil companies. Their activities have aligned with broader Iranian geopolitical objectives, including gathering intelligence on regional adversaries.

**Malware/ools:**

* *POWERSTATS* – A PowerShell-based backdoor used for remote access and command execution.
* *LaZagne* – A credential recovery tool for extracting stored passwords.
* Custom PowerShell scripts for command execution and persistence.

**Defense Strategies**

* Use application whitelisting to block unauthorized scripts and PowerShell execution, which MuddyWater heavily relies on.
* Ensure robust email security, including phishing awareness training and implementing email sandboxing.
* Regularly update systems and patch vulnerabilities, particularly those exploited in PowerShell and Office macros.
* Deploy network monitoring solutions to detect unusual traffic patterns and suspicious C2 communications.