**🎯 THREAT ACTOR PROFILE: APT33 (a.k.a. Elfin Group)**

**Overview:**

| **Attribute** | Details |
| --- | --- |
| **Name:** | APT33 (Elfin Group) |
| **Origin:** | Iran |
| **Active Since:** | ~2013 |
| **Motivation:** | Espionage, intellectual property theft, cyber sabotage |
| **Primary Targets:** | Education, Energy, Aerospace, Defence, Technology |
| **Region of Operation:** | Global (Middle East, US, Europe, UK) |

**Motivations:**

* Steal scientific research and intellectual property from educational institutions.
* Support Iran’s economic and military interests.
* Collect information on technological advancements and skills.

**Capabilities:**

* Sophisticated spear-phishing operations.
* Custom malware deployment.
* Exploits public-facing services (VPNs, RDP, outdated CMS).
* Uses open-source tools and scripts in addition to custom payloads.

**Known Malware / Toolsets:**

| **Malware** | Function |
| --- | --- |
| **Shamoon** | Disk-wiping malware for destructive attacks. |
| **DropShot** | Downloader used to deliver additional payloads. |
| **TURNEDUP** | Backdoor for persistent access and C2 communication. |
| **PowerShell & VBS scripts** | Reconnaissance and lateral movement. |

**Past Campaigns:**

* 2017: Targeted aviation and energy sector organizations in the US and Saudi Arabia.
* 2018–2022: Conducted espionage campaigns against universities and research institutions.
* Notable for attacking industries aligned with Iran’s strategic goals, including education.