**Advanced Persistent Threats:**

APT Group 1: ShadowCrest

* **TTPs:** ShadowCrest employs social engineering tactics, phishing emails, and exploits known vulnerabilities in third-party applications. They occasionally utilize brute force attacks in their campaigns. Their targets span healthcare, educational institutions, and financial sectors.

APT Group 2: CyberSerpent

* **TTPs:** CyberSerpent focuses primarily on supply chain attacks, implanting backdoors in software distributed by legitimate vendors. They have been known to attempt SQL injection attacks, but their primary focus is not on web-based attacks. CyberSerpent targets technology companies and defense contractors.

APT Group 3: DarkNexus

* **TTPs:** DarkNexus is known for launching DDoS attacks and exploiting vulnerabilities in IoT devices. While not directly involved in web-based attacks, they have collaborated with other APT groups to exploit web application vulnerabilities in some cases. DarkNexus targets critical infrastructure and telecommunication networks.

APT Group 4: PhantomByte

* **TTPs:** PhantomByte specializes in sophisticated web-based attacks, including SQL injection, brute force, and directory traversal techniques. They are known for using custom obfuscation tools to evade detection. PhantomByte precisely targets financial institutions and government sectors.

APT Group 5: GhostRAT

* **TTPs:** PhantomRAT specializes in remote access Trojans (RATs) for network infiltration and data theft. While they have collaborated with other groups on web-based attacks, it's not their primary modus operandi. PhantomRAT often targets aerospace and energy sectors.