Severity

High

Analysis Summary

Sidewinder is a suspected Indian threat actor group that has been active since 2012. They have been observed attacking political, military, and corporate organizations throughout Asia, with Pakistan, China, Nepal, and Afghanistan being the most common targets. RAZOR TIGER, Rattlesnake, APT-C-17, and T-APT-04 are the aliases for Sidewinder APT. This APT has been targeting Pakistani government officials with a decoy file related to FOCUSED TALK ON RUSSIAN UKRAINE CONFLICT IMPACT ON PAKISTAN in its most recent effort. They employ custom implementations to attack existing vulnerabilities and then deploy a Powershell payload in the final stages to distribute the malware. Sidewinder was also detected employing credential phishing sites that were copied from their victims' webmail login pages.

Impact

- Information Theft and Espionage

Indicators of Compromise

MD5

- e9aaacfec5ac9c9e3b2cac127322faf5

SHA-256

- 5dfe303f04e3432101b676fa0f230667eb6c9bc1715d5b4042f99d9522aa00fe

SHA-1

- a3c6a7f8634776af20725b6dd7ce36911f077167

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.