SUBJECT: **CYBER SECURITY-SIDEWINDERS RECENT CYBER ATTACK CAMPAIGN IMPERSONATING PAK NAVY (ADVISORY NO. 06/2025)**

Context. A recent phishing campaign targeting Pakistani officials has been observed. This cyber-attack allegedly associated with Indian Threat Actor (TA) SideWinder which has been active in Pakistan since past few years. Threat actor uses phishing emails seemingly originating from legitimate authorities to lure victims into downloading first stager malwares.

2. **Summary of Attack**

a. **Attack Vector**. Attacker sends spear phishing email to lure individuals into downloading fake audit plan named "CY SEC AUDIT PLAN.docx" (impersonating Cyber Security Directorate, Naval Headquarters).

b. Malicious document containing JPG image contacts malicious URL htttps[:]//paknavy.modpak[.]live/70137347_audit/Profile.rtf and downloads second stager payload to compromise the victim's computer.

c. **Malware Type/Exploit**. Trojan/Backdoor.

d. **File Behavior**. The downloaded file upon execution downloads second stage payload (Profile.rtf) which is a backdoor with embedded scripts to compromise the system. The backdoor has the capability to remotely control the victim's computer and steal data. It also checks local time during execution to identify the time zone, indicating that it is targeted malware. It also possesses stealth capability to remain hidden during execution.

Ser	File Hash (SHA-256)	Detection Ratio
1.	896ddb35cde29b51ec5cf0da0197605d5fd754c1f9f45e97d40cd287fb5a2d25	29/66

f. **Servers**. Following details/associated URLs have been revealed during investigation:

Ser	Domain	IP address	Detection Ratio
1.	htttps[:]//paknavy.modpak[.]live	151.236.12.150	12/94

4. **Recommendations**

a. Personal employed at various organizations be trained against falling victim to such phishing and social engineering attacks.

b. Keep all softwares, OS & browsers up to date to prevent exploitation of vulnerabilities.

c. Deploy email filtering solutions/(malware & spam check) to detect and block phishing emails

d. Disable macros in email attachments by default as these are commonly used in phishing attacks.

e. Inclusion/ updation of Malware hashes in Firewall and Threat Intelligence Database.

2. Kindly disseminate the above information to all concerned in your organization, attached/affiliated departments and ensure necessary protective measures.