Subject: - **Cyber Security Advisory – Spear Phishing Cases on Rise – Golden Jackal (Advisory No. 51)**

Context. Cyber threats actors are continuously targeting strategic entities to gain access to sensitive information for exploitation. A spear-phishing campaign has been observed operating via a crafted letter of MoFA with subject "Gallery of Officers Who Have Received National and Foreign Awards". The email asks recipients to forward their personal details on the email "ad.o&m@gov.pk".

2. **Malware Details**

   a. **APT Group Involved**. GoldenJackal aka JackalControl /JackalSteal.

   b. **Initial Infection Vector**. A skype installer is used to install a NET executable named as skype32.exe.

   c. **Affected Areas**. Diplomatic Missions in Afghanistan and Pakistan.

   d. **Persistence**. For persistence, Windows service "WEvMngs" is created on the infected systems.

3. **Recommendations**

   a. Admins must check theme files of their WordPress sites as it is the most common infectious point in this campaign.

   b. Web Admins must employ file integrity monitoring systems to catch JS injections and prevent your site from being a RAT distribution point.

   c. Internet users can protect themselves from such threats by enabling script blocking settings on their browser.

   d. Place 2FA on all important accounts (such as bank, social media IDs).

   e. It is advised to install Firewall/Antivirus.

   f. Upgrade WordPress to latest version on all websites.