Subject: **Prevention Against Cyber Espionage - Advisory No. 05 February, 2018**

1. **Introduction.** PlugX malware is one of the most growing cyber espionage threats in Pakistan. Reliable reports and reasonable intelligence has indicated that it is targeting high valued Government assets of Pakistan. PlugX is a **remote access Trojan** (RAT) first identified in 2012 allowing remote users to perform data theft and take control of the affected systems without permission or authorization. PlugX is distributed through email attachments in spear-phishing campaigns **using vulnerability in either Adobe Acrobat Reader or Microsoft Word.**

2. It has been confirmed through reliable sources that IP address **(110.93.210.35) of Action Aid Pakistan** has been compromised as part of this malware dissemination.

3. **Summary of malware**

   a. **Malware Name.** PlugX Malware.

   b. **Malware Type.** Remote Access Trojan.

   c. **Method of Infection.** Spear Phishing Emails.

   d. **Detection Ratio.** Unknown.

   e. **Exploit used:** CVE-2017-0199.

4. **Capabilities of Malware**

   a. The malware first establishes persistence into the victim's machine and establishes a network connection with its C&C server.

   b. The malware extracts information about victim's system like computer name, IP address, network information and processor information.

   c. Malware has the ability to log keystrokes, collect screenshots, delete data and steal files from victim's machine.

5. **Recommendations**

   a. To avoid further loss of data from systems at your institution; an immediate mitigation of your compromised servers/ systems is required to guard against this potential threat.

   b. Deploy **reputable firewalls on all network nodes** to thwart data exfiltration attempts.

   c. Install a **licensed and updated antivirus like Kaspersky, AVAST, Avira** etc on all the endpoints.

   d. Take appropriate **hardening measures** to ensure the operating system security.

   e. **Update windows along with all installed softwares** like Adobe Reader, Microsoft Word and Media Players etc.