Subject: **Prevention against Cyber Espionage (Advisory No 09 2016)**

1. **Introduction.** A new malware .is being sent to officers and staff of Government departments. The email attachment is a false report of "Red Cell" which presents a link to download the malware**.(Annex- A).**

2. **Summary of Malicious Email**

a. **Subject. Red Cell Special Memorandum.**

b. **File Name. Red Cell Special Memorandum.docx.**

c. **File Type. Microsoft Word Document with link to download malware**

3. **Indicators of Compromise.** In case if following files and folders are found in the computer, it means that computer is hacked:-

a. C:\AUsers\admin\AppDatalocal\Temp\RarSFX0\1176frg3fg.js.

b. C:\AUsers\admin\AppDatalocal\Temp\RarSFXO\ **Red Cell Special Mernorandum.pdf (Annex B).**

c. C:\PersfLogs\sys\chromee.exe.

4. **C&C (Command & Control) Servers**

a. 95.211.189.56 (Netherland).

b. http://pakinternetwork-mailinglist-userweebly.corn (USA).

5. **Capabilities of Malware.** The malware collects sensitive information like keystrokes username , passwords , power point , word and excel documents from internal and external hard-disks and uploads them to C&C server mentioned at Para 4a.

6. **Recommendations**

a. In case if indicators of compromise (Para 3) are found in the system, please disconnect the computer from intemet and reinstall Windows.

b. Block C&C Servers at Para 4 in firewalls of own networks.

c. Install and update well reputed antiviruses such as Kaspersky, Bitdefender, Nod 32, Avast etc.

d. Update all softwares including Windows OS, Microsoft Office and all other softwares.

e. Install and regularly update software firewall such as Comodo Firewall or Zonealarm.

f. Don't download attachments from emails unless you are sure about the source.