Subject: **Prevention Against Cyber Espionage (Advisory No 15) October, 2017**

1. **Introduction.** A malicious email titled as **"FBR -Taxpayer Verification"** is being sent to officers and staff of Government departments. The email contains a malicious link which contains a download link to a malware. Downloading and executing the file from email executes malware in background and displays a fake FBR document.

2. **Summary of Malicious Email**

   a. **Subject.FBR —** Taxpayer Verification

   b. **File Name.** FBR-Guidelines.hta

   c. **File Type.hta** (HTML based executable file)

   d. **Anti Virus Detection Rate.** 09/54 **(16.67% Very low detection ratio)**

   e. **Malware Type.** Power shell based trojan

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

Ser	C&C URL	IP address	Hosting Country
	14.142.243.78.static-Delhi.vsnl.net.in	14.142.243.78	India
		103.199.17.90	Vietnam

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

   a. HKCU\Software\Microsoft\Windows\Current version\Run /f **chromium**

   b. C:\Users\<admin>\Downloads\FBR-Guidelines.hta

   c. C:\Users\<admin>\Downloads\FBR **guidelines.pdf**

5. **Capabilities of Malware**

   a. Reads user's computer information like operating system details, directory files list, network, IP from the victim's computer.

   b. The malware has the capability to steal usernames and passwords stored in the browsers like chrome , firefox and internet explorer etc and uploads them to its C&C server mentioned in para3.

   c. The malware can install itself in windows startup location and can automatically execute itself on windows reboot.

6. **Recommendations**

   a. **Install and UPDATE well reputed antiviruses** such as Kaspersky, Bitdefender, Nod32, Avast etc.

   b. Block C&C Servers at para 3 in firewalls of own networks.

   c. In case if indicators of compromise (para 4) are found in the system, please disconnect the computer from intemet and reinstall Windows.

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

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

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