Subject: **Prevention Against Cyber Espionage (Advisory No 11) October, 2017)**

1. **Introduction.** A malicious email titled as **"Frequent Violation of PPRA Rules 2004"** is being sent to officers and staff Government departments. The email contains a **word document** file. Downloading and executing the file executes malware in background that results in hacking of the computer.

2. **Summary of Malicious Email**

   a. **Subject.** Frequent Violation of PPRA Rules - 2004
   b. **Name of Attachments.** Supply Chain Management.docx
   c. **File Type.** Microsoft Word Document (.docx)
   d. **Originator's Email.** mdppra@mail.co.uk
   e. **Malware Type.** RTF based exploit.
   f. **Antivirus Detection Rate.** 14/57 (24.56%)
   g. **Affected Softwares.** Word 2007, 2010, 2013 (old version)

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

Ser	URL	IP	Hosting Country
a	mgamphs.edu.bd	192.185.185.173	USA
.	feed43.com	66.228.47.94	USA
c	-	185.203.116.58	Bulgaria

4. **Indicators of compromise.** The malware makes following files on the infected system:-

   a. C:\Users\<admin>\AppData\Roaming\Microsoft\MicroSeMgmt.exe
   b. CAUsers\<admin>\AppData\Roaming\Microsoft\msvcr71.d11
   c. CAUsers\<admin>\AppData\Roaming\Microsoft\jili.dll

5. **Capabilities of Malware**

   a. Reads user's computer information like operating system details, directory
      files list, network, IP, route and interfaces details, Windows Services Information, System Information, Computer Name, processes information from the victim's computer.

   b. The malware has the ability to act as a key logger, file stealer and it can read information about user's open windows along with time stamps.

   c. The malware can automatically execute itself on windows startup.

6. **Recommendations**

   a. **Install and update well reputed antiviruses** such as Kaspersky, Avira, Avast etc.

b. Block C&C Servers at para 2g in firewalls of own networks.

c. In case if indicators of compromise (para 3) are found in the system, please disconnect the computer from internet and reinstall Windows.

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

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