Subject:- **Prevention Against Cyber Espionage - (Advisory No 15) March, 2018)**

1. **Introduction.** A malicious email named as "PMAD: IT Filling Guidelines" is being sent to officers and staff of defense/ intelligence organizations. Email contains a malware hidden in **Word** file. Downloading and clicking the file executes, malware in the background that results in hacking of the computer.

2. **Summary of Malicious Emails**

   a. **Subjects.** PMAD: IT Filling Guidelines.

   b. **Name of Attachments.** Doc.rtf.

   c. **Malware Type.** RTF based Exploit.

   d. **Antivirus Detection Rate.** 8/68 **(11.7% Very Low).**

   e. **CVE (Common Vulnerabilities and Exposures).** WE-2017-0199.

   f. **C&C Servers**

Ser	URL	IP	Hosting Country
(1)	http://pmadgovpk.org/ special/doc.rtf	89.47.163.211	Lithuania
(2)	Ip177.ip-217-182-38.eu	217.182.38.177	France

3. **Indicators of Compromise.** The malware makes following files on the infected system:-

   a. CAUsers1<admin>\AppData\Roaming\Microsoft\Windows1StartMenu\ Programs\Startup\Win Memory Loader. Ink.

   b. CAUsers\<admin>1AppDatalocal\Temp\YYHWK6QCOGHOA0A.sct.

   c. CAUsers\<admin>\AppData\Local\Temp\winsctrls.exe.

4. **Capabilities of Malware.**

   a. The malware is capable of getting system IP, user location, network configuration details, computer configurations and it can upload these details on its C&C server mentioned in para 2f.

   b. The malware has the ability to act as a keylogger and steal the username and passwords of infected systems.

   C. The malware can copy itself into windows startup location and it can automatically execute *itself on windows boot.*

5. **Recommendations**

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

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

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

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

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