**Subject:** **Prevention Against Cyber Espionage (Advisory No 10, 2016)**

**1.** **Introduction.** A malicious email titled as **"Social Calendar PMA Course May 2016"** is being sent to officers and staff of Government departments. The email is a' **malicious excel file** and ask users to enable macro to view the file. **Enabling the macro downloads and executes malware** in background which results in hacking of computer.

**2.** **Summary of Malicious Email**

**a.** **Subject.** Social Calendar PMA Course -May 2016.

**b.** **Name of Attachment.** PMA List Updated May 2016.xls **(Anx A)**

**c.** **Malware Type.** Macro based malware

**d.** **C&C Servers.** Following be blocked at NW Firewall:-

| Ser | URL | IP | Country |
|---|---|---|---|
| (1) | cluster3.convio.net | 69.48.252.146-147 | USA |
| (2) | ocsp. digicert.com | 93.184.220.29 | USA |
| (3) | www.harvard.edu | 104.16.153.6 | USA |
| (4) | www.unfoundation.org | 69.48.252.158 | USA |
| (5) | www.kaust.edu.sa | 109.171.129.32 | Saudia Arabia |
| (6) | - | 91.210.107.110 | Russia |
| (7) | - | 46.165.249.223 | Germany |

**3.** **Indicators of Compromise.** Following files can be found on the infected system:-

**a.** C:\Users\admin\AppData\Roaming\Microsoft\WdfuHost.exe (Fake Putty Suite).

**b.** C:\Users\admin\AppData\Roaming\Microsoft\Windows\ Cookies\ **PDONS9QH .txt**

**c.** C:\Users\admin\AppData\Roaming\Microsoft\Windows\ Cookies\ **admin@www.harvard .txt**

**4.** **Capabilities of Malware**

**a.** The malware downloads a file mentioned in para 3a, from its C&C server that gives attacker the **unrestricted remote access to victim's computer.**

b. The attacker can  manually execute commands remotely on the victim's system.

c. It also access **potentially sensitive information from local browsers** like stored usernames and passwords.

d. The malware automatically installs itself for auto run at Windows startup.

e. Investigation are underway to further identify the charactertics of malware.

5. **Recommendations**

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

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

c. Install and update well reputed antiviruses such as Kaspersky, Bit defender, 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 Zone alarm.

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

g. Never enable macros in Microsoft Word, Power Point and Excel files specially downloaded from Internet