Subject:- **Prevention Against "Urgent Action Required- PDF and DAWN" - Advisory No 14 March, 2018**

1**.** **Introduction.** Malicious emails titled as **"Urgent Action Required-PDF"** and **"DAWN Reporter"** are being sent to officers and staff of defense/ intelligence organizations. These emails contain a malware hidden in a **Word** file. Downloading and running the file, executes malware in background that results in hacking of the computer.

2**.** **Summary of Malicious Emails**

a. **Subjects**

(1) Urgent Action Required-PDF.

(2) DAWN Reporter.

b. **Name of Attachments.** doc.rtf

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

d. **Antivirus Detection Rate.** 8/65 **(12.3% Very Low).**

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

f. **C&C Servers**

| Ser | URL | IP | Hosting Country |
|---|---|---|---|
| (1) | reset.defencepk.org | 37.48.81.10 | Netherland |
| (2) | Ip177.ip-217-182-38.eu | 217.182.38.177 | France |
| (3) | http:Weaks.dawn-mx.com | 89.47.163.211 | Lithuania |

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

a. CAUsers\<admin>\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\Win Memory Loader. lnk.

b. CAUsers\<admin>\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\cmd manager.lnk.

c. CAUsers\<admin>\AppData\Local\Temp\YYHWK6QCOGH0A0A.sct.

d. C:\Users\<admin>\AppData\Local\Temp\AS4Z4XHVV4VQWHG.sct

e. C:\Users\<admin>\AppData\Local\Temp\wininet.exe.

f. C:\Users\<admin>\AppData\Local\Temp\svctrls.exe.

4. **Capabilities of Malware .**

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

b. The malware has the ability to steal the usernames and passwords of infected systems.

c. The malware lean cy1l itself into windows startup location and it automatically execute itself on windows boot.

d. The malware has a **very low detection ratio (12.3% only).**

5. **Recommendations.**

a. **Install and Updatte Well reputed antiViruses** such as KesperSky, Avira, Avast 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 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.