Subject: **Advisory – Prevention Against Hostile Cyber Attack (Advisory No. 9)**

1. **Introduction.** Recently, a malware has been identified; spreading through spoofed e-mails, and is involved targeting defese / intelligence organizations as well as government departments on large scale. These e-mails portray a legitimate subject "**CSD package details**" which contains a malicious link that re-directs the user to download discount schemes. Extracting and clicking the fake excel file execute a malware in background, which compromises victim's machine.

2. **Summary of Malicious Emails**

   a. **Subjects. CSD 2019 Discount Schemes**.

   b. **Name of Attachments. CSD_Schemes_2019.xls.**

   c. **Antivirus Detection Rate.** 5 / 67 (7.46% very low detection rate).

   d. **Malware Type.** Macro based Malware.

   e. **File Size** 794.5 Kb.

   f. **File Hash.** a6270064f1630cdf5bcda858762db516.

   g. **File Extension.** Microsoft Excel File (.**xls**).

   h. **C & C Servers**

Ser	C & C Servers URL	IP Address	Hosting Location	Registrant Country
(1)	unique.fontsupdate.com **(C & C server)**	37.72.168.164	Netherlands	-
(2)	rightapps.net/sms/securimage/images/csd_schemes_2019.php **(Malware Download Link)**	151.106.12.34	France	Pakistan

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

   a. C:\Users\<admin>\AppData**juchek.ttp**

   b. C:\Users\<admin>\AppData**bat.bat**

   c. HKEY\SOFTWARE\Microsoft\Windows\CurrentVerson\Run**juchek.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 2(h)**.

b. The malware has the ability to upload files, get system information, list files and act as a **Key logger.**

c. The malware can copy itself into registry and it can **automatically execute itself on windows boot.**

5. **Recommendations**

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

b. Make sure that **host based firewall is enabled** and configured to block all inbound traffic except from **white listed applications.**

c. **Check list of white listed applications** to see whether any unidentified applicaton has been accessed through firewall.

d. **Block C & C Servers at para 2(h)** in **firewalls of own networks.**

e. In case, **indicators of compromise (para 3)** are found in the system, please disconnect the computer from internet and reinstall windows.

f. **Update all installed softwares** including Windows OS, Microsoft Office and PDF reader.

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

h. All PC's present in the domain network must have distinct passwords and Active Directory Network Administrator password must be 8 to 10 characters long and shouldn't be shared with anyone.

i. Utilization of **internet explorer** as the **default search engine** is **Strongly prohibited** and regularly updated Google Chrome or Mozilla FireFox with AdBlock plugin must be used for secure internet surfing.

j. To avoid unauthorized access of email accounts, 2 x factor authentication must be enabled on all email accounts.