Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No. 21)**

1. **Introduction.** Recently, a malware is found spreading **through spoofed emails** that is targeting army / defense / intelligence organizations as well as DAs abroad in a well-planned targeted manner. These emails portray a legitimate looking **SOPs document regarding Mails and PC or government letter with subject "PMO Meeting Notice".** Downloading and clicking on fake document executes a malware in background that will compromise victim's machine.

2. **Summary of Malicious Email**

   a. **Email Subjects.** PMO, No. 5(1)2020-Admin, dt. 29-09-2020, Meeting Notice / SOP for Logging out Mail and PCs.

   b. **Spoofed Email address.** chairman@kpt.gov.pk / minister @ narcon.gov.pk

   c. **Download File.** PMO, No.5(1)2020-Admin, dt. 29-09-2020, Meetin Notice.chm/SOP for Logging out Mail and PCs.chm

   d. **MD5 Hash.** e2cbde3b921dc3f9d5786b0c9da5c578

   e. **Antivirus Detection Rate.** Nil

   f. **File Size.** 11 Kbs

   g. **File Extension.** .chm

   h. **C&C Servers**

Ser	URL address	IP	Cou
(1)	myprivatehostsvc.com/xuisy/css.php	162.0.229.47	US

3. **Indicators of Compromise**

   a. Files downloaded in temporary folder named as **MsAulis.msi.**

   b. New trigger added in task scheduler with key **1DefenderUpdater.**

4. **Capabilities of Malware**

   a. The malware is specially designed for targeted attacks and can steals files and keystrokes (along with stored usernames / passwords) from Windows system.

   b. The attacker can gain remote access of the system and can execute additional payload from it.

   c. The malware has capability to execute through Microsoft certified programs to remain undetected and gain persistence through scheduler.

5. **Recommendations**

   a. **Regularly update well reputed antiviruses** such as Kaspersky, Avira, Avast etc. and scan system regularly.

b. Update all software including Windows OS, Microsoft Office and all other on regular basis.

c. Uninstall all not in use **applications** and **software** from system and personal phone.

d. **Do not download attachments from emails unless you are sure about the source.**