Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No.28)**

1. A malware is being spread through **spoofed email** targeting civil / military and intelligence organizations including DAs abroad in a well planned targeted manner. For this purpose, attackers have crafted a malicious MS-Word file that looks likes like a legitimate document having the subject" **Invitation-Pakistan Air Show Karachi 2021"** . This email was previously propagated with the subject "**SOP for Logging out Mail and PCs".** Downloading and clicking on the fake MS-Word document executes a malware in the background on the target system / computer, eventually, victim machine is compromised and becomes prone to data exfiltration. The crafted MS-Word document mimics as a verified Microsoft software thus rendering it undetectable through anit-virus.

2. **Summary of Malicious Email.**

a. **Subject.** Invitation -Pakistan Air Show Karachi 2021

b. **Spoofed Email address**. itc14@paf.gov.pk/notifiactions@mail-ntp.net

c. **Download File.** Air Show 2021-Karachi.chm

d. **MD5 Hash**. e2cbde3b921dc3f9d5786b0c9da5c578

e. **Antivirus Detection Rate.** Nil

f. **File Size**. 1 Kbs

g. **File Extension.** .chm

h. **CSC Servers.**

Ser	URL Address	IP address	Country
(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 \ **DefenderUpdater.**

4. **Capabilities of Malware.**

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

b. The attacker can gain remote access of 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.**

e. Window defender and Firewall of system to be on recommended settings.

6. **Reporting of Suspicious Files / Emails.** Any malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures:-

email:- **asntisb2@cabinet.gov.pk**