Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No 22) Apr 18**

1. **Introduction.** Recently reports have indicated that attackers from Iran are using latest malware techniques **to distribute macro-based documents to individuals in Asia and Middle East.** These attackers are **focusing Pakistan Defense Institutions** and **utilize crafted spear-phishing emails** with **attached malicious word documents.** Downloading and opening the file from email **executes the malware in background** and **opens a fake document in foreground,** that results in **hacking of the system.**

2. **Summary of Malicious Email**

   a. **Subjects of Reported Emails**

      (1) National Assembly of Pakistan

      (2) Turkish Armed Forces

      (3) State Bank of Pakistan

   b. **Name of Attachments**

      (1) Important Notice: National Assembly.doc

      (2) Turkish vs Pakistan Armed Forces.doc

      (3) na.gov.pk.doc

      (4) Invest in Turkey.doc

   c. **Malware Type.** Macro based Malware with Remote Access Trojan capability.

   d. **Infection Vector.** Spear Phishing Emails.

   e. **Targeted Countries.** Turkey, Pakistan, Tajikistan.

3. **Indicators of Compromise.** The malware creates following files in hardcoded paths into the infected system:-

   a. C:\ProgramData\Defender.sct (A malicious JavaScript file).

   b. C:\ProgramData\DefenderService.inf (To execute JavaScript file).

   c. C:\ProgramData **MindowsDefender.ini** (Malicious PowerShell script).

   d. **\REGISTRY\USEMSID1Software1Microsoft\Windows\CurrentVersion \Run\"WindowsDefenderUpdater"** =cmstp.exe /s c:\programdat \ **DefenderService.inf** (Registry Key for Persistence).

4. **Capabilities of Malware**

a. The malware has ability to get IP address, OS details, Computer Name from the infected system.

b. Uploads screenshots and Keystrokes to its numerous C&C (Command and Control) server with a unique identifier.

c. Ability to execute commands like reboot, shutdown, clean, Screenshot, upload as instructed by the C&C server

5. **Recommendations**

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

b. Keep windows and android OS up to date,

c. Don't enable macros in Microsoft Word documents.

d. In case if indicators of Compromise (para 3) are found in the system, please

disconnect the computer from intemet and reinstall windows.

e. Don't download attachment from emails unless you are Sure about the source.