Subject: **Advisory - Prevention Against , Cyber Espionage (Advisory No . 18)**

1. **Introduction.** The **spear phishing** emails with malicious documents having **geopolitical themes** are being spread by Iranian threat group. Attackers are leveraging the latest code execution and persistence techniques to distribute malicious macro-based documents to individuals in Asia and the Middle East.

2. **Summary of Malicious Emails**

   a. These documents are macro enabled that result in installing backdoor for further activity. Most emails are being propagated as **"National Assembly of Pakistan".**

   b. It is a staged spear phishing campaign targeting individuals in Asia and Middle East. The campaign followed following stages:-

      (1) In first part of the campaign they used a ,macro-based document that dropped a VBS file and an INI file.

      (2) The second part of the campaign, a new variant of the macro, that does not use VBS for Power Shell code execution. Instead, it uses one of the recently disclosed code execution techniques leveraging INF and SOT files.

3. **File Attachments.** Following file attachments can be encountered in phishing emails:-

   a. na.doc
   b. na.gov.pk.doc
   c. Connectel. pk. doc

4. **Indicators of Compromise.** The Malware makes following files on the infected system:-

   a. Drops payload named as **"WScriptexe".**
   b. Malware sets following key for persistence in registry/REGISTRY/USER/SI D/Software/Microsoft/Windows/Curre Version/Run/"Windows Defender Updater=cmstp.exe/scA program data\DefenderServices.inf.
   c. cmstp.exe runs on startup and executes script.
   d. Following files are created as a result:-
      (1) Defender.sct
      (2) Defender Services!.inf
      (3) vvinaowsDetender.ini

5. **Capabilities of Malware**

a. The malware is capable of getting system IP, user location, network configuration details, computer configurations, QS details and can wipe data.

b. Other capabilities include shutting down - System if security tools are discovered obtaining Screenshots and uploading information from system.

c. Drops payload of VBS or INI scripts which is then run by PowerShell.

6. **Recommendations**

a. Users can Protect themselves from such attacks by disabling macros in their MS word settings and are advised to remain vigilant when enabling macros.

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

c. In case if indicators Of ,compromise '(para .4) are found in the system: please disconnect the computer 'from intemet and reinstall windows.

d. Update all software including Windows OS, Microsoft Office and disable macros.

e. Prevent downloading attachments from emails from unknown, suspicious sources.