Subject: - **Advisory - Prevention against Cyber Espionage (Advisory No.40)**

1. Recently, phishing emails containing malware links have been received at official email accounts of top ranked Civil and Military officials including posted abroad. Clicking on such malicious links / URLs may result in data breach and sensitive data leakage. The attached files in emails look legitimate but contain embedded malicious links leading to malware execution in the background. Such malware may use **DLL hijacking technique** and executables such as "**software_reporter_tool.exe**".

2. **Summary of Malicious Email.** CVE-2017-11882

   a. **APT Group.** SideWinder APT

   b. **File Name.** Building Port Resilience against Pandemics.docs

   c. **Antivirus Detection Rate.** Low

   d. The malicious files are hosted on C&C Server as under: -

Ser	URL address	IP Address	Country
(1)	Pmaesa.bahariafoundation.org	5.252.195.27	Russia

3. **Capabilities of Malware**

   a. The Rich Text Format (RTF) based malware is specially designed for targeted attacks and can steal files / stored passwords from windows system and browsers.

   b. The attack involves windows certificates alterations to reside for persistence.

   c. The malware employs sleep function as defensive technique and checks for presence of debugger.

   d. The malware uses attack techniques **DLL hijacking** and attack based on **javascript.**

   e. The attacker can gain remote access of the system and can execute additional payload from it and run through certified file "**software_rempval_tool.exe**" to evade antivirus detection.

4. **Recommendations**

   a. IT setup within the, organization should **disable Microsoft Equation Editor in Office from registry** to avoid such attacks.

   b. Microsoft executables including **Verclsid, Rundll32, Regsvr32, Regsvcs / Regasm, Odbcconf, MSiexec, Mshta, InstallUtil, CMSTP, ControlPanel, Compiled HTML File** to be monitored as major malware executables and must be blacklisted.

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

d. Window Defender and Firewall of system to be kept on as recommended settings.

e. Be vigilant regarding redirected links and typing sensitive information online.

* * * * *