Subject: - **Cyber Threat Advisory - Malware Analysis Report : PIM June Training Activity (Advisory No. 26)**

1. Analysis of suspicious email with the subject "**PIM June Training activity**" and a malicious attachment "**Details 2022.03.03_1501.xlsm**" revealed that document file "**Details 2022.03.03_1501.xlsm**"is a sophisticated and targeted attack by hostile Cyber actors and is spreading through email amongst defence organizations for information gathering and system control. Detail analysis is appended in ensuing paragraphs.

2. The summary of malicious email containing Microsoft Excel Spreadsheet integrated with exploit and malware is attached as (**Appendix-I**)

3. Analysis of malicious file reveals following behavior: -

   a. It can download different malicious payloads and files from **Command** and **Control Server.**

   b. The attacker can gain remote access of the system and can perform different malicious functions.

   c. It can execute a hazardous VBA script (Macro) with suspicious auto execution of **remote access Trojan.**

   d. It can schedule itself and other malicious processes for persistence.

   e. It can access and manipulate user directories and files.

   f. Data stored on infected computer can be fetched.

4. **Recommendations.** Above in view, following preventive measures must be ensured by all concerned: -

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

   b. Be vigilant regarding **redirected links** and typing sensitive information online.

   c. **Disable Macros** in all systems available in network and ensure user privileges are managed.

   d. Uninstall all not in use applications / software from system and personal phone.

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

   f. Window defender and firewall be kept on **recommended** settings.