Subject: - **Cyber Threat Advisory - Malware Analysis Report - Fresh Demand Deputation (Advisory No. 27)**

1. A phishing email with the subject "**Fresh Demand - Deputation**" containing a malicious attachment "**Fresh Demand - Deputation.xlsx**" is currently circulating. Analysis divulges that the attached file "**Fresh Demand _ Deputation.xlsx**" is a sophisticated and targeted attack by hostile Cyber actors and is spreading through email amongst defence organizations for information gathering and gaining system control. Detail analysis is appended in following paragraphs.

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

3. Analysis of malicious file reveals following behaviour: -

   a. Attacker can gain remote access of the system and can perform different malicious functions.

   b. Creates, deletes, alters and executes different files in user directories / folders.

   c. Executes a lethal VBA script (**Macro**) with suspicious auto execution of **Remote Access Trojan**.

   d. Schedules itself and other malicious processes for persistence.

   e. Captures the screenshots of infected computer.

   f. Fetches data stored on the infected computer / system

   g. Executes and terminates different processes on infected computer.

   h. Turns on microphone of infected machine.

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 that user privileges are being properly 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. Windows defender and firewall be kept on **recommended** settings.