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.**

M (IR-Ops)
M (IR-P)
M (Cus-Ops)
M (Cus-P)
M (Admn/HR)
M (IT)
M (I...
M (L...
M (H...
M (L... Cus)
... (IT)
... Rev. Div.)
...

FBR eDOX Dy.No. 154984
Received in Chairman's Sectt
on 20 JUL 2022

SS(IT-2) 21-7-22

PR/ PRAL

f. Windows defender and firewall be kept on recommended settings.

5. For any query or issues with regarding Cyber Security, report may please be forwarded to the following email addresses: -

a. **eagle1978@mail.com**
b. **falcon098@writeme.com**
c. **asntisb2@cabinet.gov.pk**

6. Kindly disseminate the same message to all concerned in your organizations, all attached/ affiliated departments and ensure necessary protective measures.

Appendix I

1. **File Description**

Ser	File Name	Malware Category	File Signature	
a.	Fresh Demand – Deputation.xlsx	Trojan:W97M/AutorunMacro.D [FSE]	MD5	dbd11c7f0074580015daa16b5900ac7b
			SHA1	A6c40baa4dc4773b56ae47adbc21f6b68629090b

2. **Files included**

Ser	Files	Virus Total Score	Suspicious Behavior Score
a.	Fresh Demand – Deputation.xls	9 / 59	86 / 100
b.	Sensrv.bin		
c.	Sensrv.dll		
d.	Sensrv.bat		
e.	Rundll32.exe		
f.	Schtasks.exe	Note: Remote Access Trojan uses these windows utilities for its execution and persistence	

3. **Dropped Files**: The Microsoft Excel file downloads Remote Access Trojan and different malicious files at stored on the following locations to gain persistence:-

   a. C:/Users/Public/Music/secsrv.dll

   b. C:/Users/Public/Music/secsrv.bat

Note: Computer Generated Documents Do Not Require Signature.