Subject: **Prevention Against Cyber Espionage (Advisory No.09) August, 2017)**

1. **Introduction.** A Malicious email titled as **"Indian Army kidnaps Pakistan Army officer LT. Col(rtd.) M. Habib from Nepal for spy swap"** is being sent to officers and staff of Government departments from a spoofed email. The email contains an **InPage exploit.** Downloading and opening the In Page file executes a malware in background that results in hacking of the computer.

2. **Summary of Malicious Email**

   a. **Subject.** Indian Army kidnaps Pakistan Army officer LT. Col (Retd.) M. Habib from Nepal for spy swap

   b. **Name of Attachments.** KulbhushanYadhav_Vs_MdHabib_SpySwap.inp

   c. **Malware Type.** Zero Day Exploit of **InPage** Professional till 2012.

   d. **Spoofed Email.** editor.farida@dawn.com

   e. **Antivirus Detection Rate.** 0/55 (0%)

   f. **Affected Softwares.** All versions of **`InPage Urdu'** till 2012.

   g. **C&C Servers**

Ser	URL	IP	Hosted Country
(1)	police.portal.pk	195.22.126.74	Poland
(2)	http://176.123.26.59/windowsmgr/javasUpdates.exe	176.123.26.59	Moldova

3. **Indicators of Compromise.** The malware makes following files on the infected system:-

   a. C:\Users\<admin>\AppData\Roaming\network.exe

   b. C:\Users\<admin>\AppData\Roaming\shortcut.vbs

   c. CAUsers\<admin>\AppData\Local\PerfsLog\Sys\InstntAccel.exe

   d. CAUsers\<admin>V\ppData\Local\PerfsL0g\Sys\LangEngUTF8.exe

   e. CAUsers\<admin>\AppData\Local\Perf5Log\5ysILangEngUTF^{16}.ex

   f. C:\Users\<admin>\APPData\Local\PerfsLog\Sys\OpenOffce.exe

   g. C:\Users\<admin>\AppData\Local\PerfsLog\Sys\OptimisedDisply.e

   h. C:\Users\<admin>\AppData\Local\PerfsLog\Sys\RuntimeLibsUpdte.

   j. C:\Users \ <admi n>lAppData \ Roarning \Microsoft\VVindows\StartMenu \ Programs \Startup**desktop.ini.url**

4. **Capabilities of Mailman** Reads user's computer information like operating system details, directory files list, network, IP, route and interfaces details, Windows Services Information, System Information, Computer Name, processes information from the victim's computer

   a. The malware has the ability to act as a keylogger, filestealer and it can read information about user's open windows along with time stamps.

b. It can steal stored user names and passwords of victim's accounts and can take remote control of the system.

c. The malware can automatically execute itself on windows startup.

5. **Recommendations**

a. Instead of using In Page, following software be used:-

(1) Microsoft Word with Urdu Language.

(2) Urdu Ward Processor 1.1.

b. **Install and update well reputed antiviruses** such as Kaspersky, Avira, Avast etc.

c. Block C&C Servers at para 2g in firewalls of own networks.

d. In case if indicators of compromise (para 3) are found in the system, please disconnect the computer from Internet and reinstall Windows.

e. Update all softwares including Windows OS, Microsoft Office, In Page Professional etc.

f. Don't download attachments from emails unless you are sure about the source.