GOVERNMENT OF PAKISTAN
REVENUE DIVISION
FEDERAL BOARD OF REVENUE
(IT WING)
*****

No.1 (7)S(IT)/2017//03267-R **Islamabad the 18th July, 2017**

All Chief Commissioners/
Chief Collectors/Director Generals

Subject: **ADVISORY – PREVENTION AGAINST CYBER ESPIONAGE (ADVISORY NO. 87 2017).**

Please refer to the subject.

2. National Telecom & Information Technology Security Board, Cabinet Division has instructed to all Ministries/Divisions to take necessary measures to safeguard against leakage of sensitive information, therefore, you are requested to ensure the following steps:-

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

Summary of Malicious Email

a. Subject. Indian Army kidnaps Pakistan Army officer LT. Col (Rrtd). M. Habib from Nepal of spy swap.
b. **Name of Attachments**. Kulbhushan Yadhav_Vs_ MdHabib_ SpySwap.inp
c. **Malware Type**. Zero Day Exploit of InPage Professional till 2012.
d. **Spoofed Email.** Editor.farida&down.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	Ploand
(2)	http://176.123.26.59/windo w smgr/javasUpdates.exe	176.12.26.59	Moldova

Indicators of Compromise. The malware makes followings 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\InstntAccel.exe
d. CAUsers\<admin>\V\Data\Local\PerfsLog\Sys\LangEngUTF8.exe
e. CAUsers\<admin>\AppDATA/Local\Perfs5Log\5Sys\LangEnUF16.exe
f. C:\Users\<admin>AppData/Local\PerfsLog\Sys\OpenOffce.exe
g. C:\Users\>admin>\App/Data\Local\PerfsLog\Sys\OptimisedDisply.e
h. C:/Users\<admin>APPData/Local/\PerfsLog\Sys\RuntimeLibsUpdte.

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.

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 firewals 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 software including Windows OS, Microsoft Office, In Page Professional etc.

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

Reporting of Suspicious Files/Emails. Any malicious cyber activity may be suggesting mitigation measures:-

a. Eagle 1978@mail.com

b. Falcon098@writeme.com

3. It is requested that above mentioned information may be ensured by all concerned in order to safeguard against leakage of sensitive information.

21/08/17

(Khawaja Adnan Zaheer)
Member (IT))

Copy to:-

1. S.A to Chairman For information

2. Member (FATE) for placement on FBR's Website.