

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB)

No. 1-5/2003 (NTISB-II)

Islamabad June 2019

Subject: Advisory – Prevention Against InPage Urdu Exploit (Advisory No. 15)

10 JUN 2019

M(A)

M(I.T)

A.S(Rew. Div.)

1. Introduction. InPage Urdu software developed and produced by an India based company "Concept Software Private Limited" is largely used worldwide for Urdu page making and Pakistan is its top consumer. Recently a targeted malware campaign titled as "OFFICIUM Training Plan Dte NITB + POF" is being sent to officers and staff of civil, defense / government organizations from a spoofed email. The email contains an unknown InPage exploit. Downloading and opening the InPage file executes a malware in background that results in backing of the computer.

2. Summary of Malicious Email

- a. Subject. OFFICIUM Training Plan Dte NITB + POF
- b. Name of attachment. Staff training Dte.inp
- c. Malware Type. Zero Day Exploit of InPage Professional
- d. Spoofed Email. pslicense@nitb.gov.pk
- e. Antivirus Detection Rate. 0/55 (0%)
- f. Affected Softwares. All versions of 'InPage Urdu'
- g. Threat Level. Critical
- h. C & C Servers

Ser	C & C URL	C & C IP address	IP Location
(1)	-	209.177.158.26	USA
(2)	-	212.83.46.63	Germany

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

- a. C:\Users\- b. C:\Users\- c. C:\Users\

11 JUN 2019

C(A)

S(A&C)/JB

S.S. (Forward)

229
12/06/19

Bynet

75780

Received in Chairman's Sectt.
on 10 JUN 2019

- d. C:\Users\- e. C:\Users\

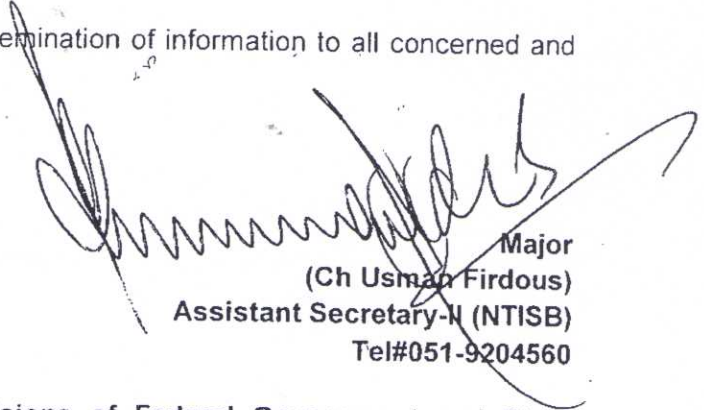
4. **Capabilities of Malware**

- a. Reads user's computer information like operating system details, directory files list, IP address, route interfaces details, Windows Services Information, System Information, Computer Name and processes information from the victim's computer.
- b. The malware has the ability to act as a key logger, file stealer and it can read information about user's open windows along with time stamps.
- c. It can steal stored usernames, passwords of victim's accounts and it can take remote access of system.
- d. The malware can automatically execute itself on windows startup and attacker can run additional commands on infected system.

5. **Recommendations.** In order to safeguard from threat presented by "InPage" software following are recommended: -

- a. **Instead of using InPage, following software be used: -**
 - (i) Microsoft Word with Urdu Language.
 - (ii) Urdu Word.Processor.
- b. **Download and execute the Inpage malware detection tool from <https://tiny.cc/h21P6y> to detect this particular malware.** If found infected, then please contact your system administrator or **backup your data and reinstall windows.**
- c. **Install and update well reputed antiviruses** such as Kaspersky, Avira, Avast etc.
- d. **In case if indicators of compromise (para 3) are found in the system, please disconnect the computer from internet and reinstall windows.**
- e. Don't download attachments from emails unless you are sure about the source.
- f. **Strict implementation of Software Restriction Policies (SRP) must be implemented to block binaries executing from %APPDATA% and %TEMP% locations as most malware runs from these paths.**
- g. **Monitor IP traffic within the network for malicious connections with IPs mentioned in para 2(h) for detection of infected endpoints.**

6. Forwarded for perusal and dissemination of information to all concerned and under command, please.



Major
(Ch Usman Firdous)
Assistant Secretary-II (NTISB)
Tel#051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Government.

1. SPS to Cabinet Secretary, Cabinet Division Islamabad
2. PS to AS-III, Cabinet Division Islamabad
3. APS to Secretary, NTISB, Cabinet Division Islamabad
4. APS to Deputy Secretary, NTISB, Cabinet Division Islamabad