

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

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

Islamabad 2 Nov 2020

03 NOV 2020

Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No. 21)**

M(A)
M(IT)

1. Introduction. Recently, a malware is found spreading through spoofed emails that is targeting army / defense / intelligence organizations as well as DAs abroad in a well-planned targeted manner. These emails portray a legitimate looking SOPs document regarding Mails and PC or government letter with subject "PMO Meeting Notice". Downloading and clicking on fake document executes a malware in background that will compromise victim's machine.

A.S (Rev. Div.)
4/4
Chief (IT)
CIO

2. Summary of Malicious Email

- a. **Email Subjects.** PMO, No. 5(1)2020-Admin, dt. 29-09-2020, Meeting Notice / SOP for Logging out Mail and PCs.
- b. **Spoofed Email address.** chairman@kpt.gov.pk / minister @ narcon.gov.pk
- c. **Download File.** PMO, No.5(1)2020-Admin, dt. 29-09-2020, Meetin Notice.chm/SOP for Logging out Mail and PCs.chm
- d. **MD5 Hash.** e2cbde3b921dc3f9d5786b0c9da5c578
- e. **Antivirus Detection Rate.** Nil
- f. **File Size.** 11 Kbs
- g. **File Extension.** .chm
- h. **C&C Servers**

Ser	URL address	IP	Cou
(1)	myprivatehostsvc.com/xuisy/css.php	162.0.229.47	US

3. Indicators of Compromise

- a. Files downloaded in temporary folder named as **MsAulis.msi**.
- b. New trigger added in task scheduler with key **1DefenderUpdater**.

4. Capabilities of Malware

- a. The malware is specially designed for targeted attacks and can steals files and keystrokes (along with stored usernames / passwords) from Windows system.
- b. The attacker can gain remote access of the system and can execute additional payload from it.
- c. The malware has capability to execute through Microsoft certified programs to remain undetected and gain persistence through scheduler.

FBR eDOX No. 196656-R
Received in Member (IT)
4/4/2020

49559961
196656-R

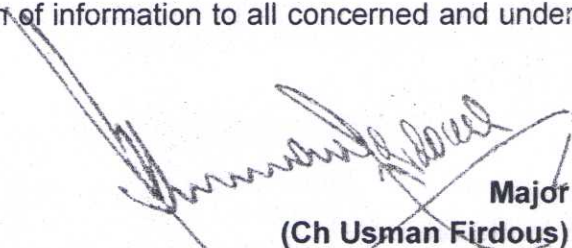
4/11/20

SS (IT)

5. **Recommendations**

- a. **Regularly update well reputed antiviruses** such as Kaspersky, Avira, Avast etc. and scan system regularly.
- b. Update all software including Windows OS, Microsoft Office and all other on regular basis.
- c. Uninstall all not in use **applications** and **software** from system and personal phone.
- d. **Do not download attachments from emails unless you are sure about the source.**

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


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

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

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-II, Cabinet Division, Islamabad
5. Secretary, NTISB, Cabinet Division, Islamabad
6. Deputy Secretary, NTISB, Cabinet Division, Islamabad
7. Director (IT), Cabinet Division, Islamabad