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

No. 1-5/2003 (NTISB-II) **Islamabad 15 August, 2018**

Subject: **Advisory - Prevention Against Cyber. Espionage Malicious Email Titled "PMAD Accts" (Advisory No 152)**

M(A)

M(I.T) ✓

A.S(RevDiv)

1. **Introduction.** A **malicious email** with subject **"PMAD Accts"** is being sent to **officers** and staff of **civil/ Govt departments, defense/ intelligence** organizations as well as DAs abroad. Downloading and opening the file from email **executes the malware in background** and **opens a fake document in foreground,** that results in **hacking of the system.**

2. **Summary of Malicious Email**

a. **Subject.** PMAD Accts.

b. **Name of Attachment.** PMAD Accts.doc.

c. **Antivirus Detection**

(1) **Files extracted.** PMAD Accts.doc

(2) **Detection Rate.** 18/59

(3) **Percentage %.** 30.5

d. **Malware Type.** Trojan based Key logger.

e. **C&C Servers**

Ser	IP Addresses	URL Addresses	Hosting Country
(1)	54.37.205.242	pmacell.site	France
(2)	185.140.249.194	185.140.249.194/winh.ex	UAE Dubai

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

a. C:\ProgramData\Microsoft\RAC\Temp **\sglB701.**

b. CAProgramData\Microsoft\RAC\Temp\sq1B3E4

c. Numerous temporary files are found in folder C:\User\Mudassar\Local\Temp

d. C:\User\Mudassar\Local\Microsoft\Windo\History\History. IE5\MSHist 012018050920180510\index.dat

e. C:\Users\Mudassar\App Data\Local\Microsoft\Windows\WER\ReportQueue\AppCrash-EQNEDT32.exe-3f2e22ee8b8c291abf64ca54c7 7784fe5a5a085-cab-obad1075\WERFCF5.temp.appcompat

f. CAUsers\Mudassar\AppData\Roaming\Microsoft\Windows\Recent AutomaticDestination'sA **b4dd67f29cb1962.automaticDestinations-ms.**

C(IT)
6/8/2018

g. CAUsers\MudassappData\Roaming\MicrosoftWindows\Recent\
AutomaticDestination,s\adecfb853d77462a.autoMaticDestinations-ms

4. **Malicious Information Extracted**

a. The malware **delete i** keys from registry far **Microsoft** Office.

b. The malware is **evasive** where it **reads the** keyboard layout followed by a **significant ^ode** branch **decision.**

c. The **Trojan** looks Op many **procedures** within the same **disassembly**
Stream which is often used to hide **usage.**

d. The malware **spawns** the **Microsoft Equation** Editor process **"EQNEDT32.EXE"** with command line "-Embeddin".

5. **Capabilities of Malware**

a. The rnalware is caPable of **getting system IP, user location, network configuration details,** computer configurations and upload these details on its **C&C server** mentioned at **para 2e.**

b. The malware has the ability to act as a **key logger** and **steal** the **usernames** and **passwords** of **infected systems.**

6. **Recommendations**

a. **Install** and **update licensed** and well reputed **antiviruses** such as Kasper'sky, Avira, Avast etc.

b. Block **C&C Servers** at **para 2e** in **firewalls** of own **networks.**

c. In case, if indicators of **compromise** (para 3) are found in the system. **disconnect** the computer from internet and reinstall windows.

d. Update all **softwares** including **Windows OS, Microsoft Office.**

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

7. Forwarded for perusal and dissemination of information to all concerned, please.

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

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

Copy to :-

SPS to Cabinet Secretary, Cabinet Division , Islamabad

PS to AS-III, Cabinet Division, Islamabad

APS Secretary, NTISB

APS Deputy Secretary, NTISB