

Subject: **Advisory - Prevention Against Cyber. Espionage Malicious Email Titled "PMAD Accts" (Advisory No 49)**

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/win.h.ex	UAE Dubai

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

- a. C:\ProgramData\Microsoft\RAC\Temp \sgl**B701**.
- b. C:\ProgramData\Microsoft\RAC\Temp\sq1B3E4
- c. Numerous temporary files are found in folder
C:\User\Mudassar\Local\Temp
- d. C:\User\Mudassar\Local\Microsoft\Windows\History\History.
IE5\MSHist 012018050920180510\index.dat
- e. C:\Users\Mudassar\AppData\Local\Microsoft\Windows\WER\ReportQueue\AppCrash-EQNEDT32.exe-3f2e22ee8b8c291abf64ca54c7 7784fe5a5a085-cab-obad1075\WERFCF5.temp.appcompat
- f. C:\Users\Mudassar\AppData\Roaming\Microsoft\Windows\Recent AutomaticDestinations\A **b4dd67f29cb1962.automaticDestinations-ms**.
- g. C:\Users\Mudassar\AppData\Roaming\Microsoft\Windows\Recent AutomaticDestinations\adecfb853d77462a.autoMaticDestinations-ms

4. **Malicious Information Extracted**

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

- b. The malware is **evasive** where it **reads the** keyboard layout followed by a **significant code** 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 malware 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.