PTA CERT for Telecom Sector

Security Advisory-No: Ext:152-17

11, Sep 2018

Threat Classification: Malware

Overview: A malicious email with subject "PMAD Accts" is being sent to officers and staff of civil/ Government 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.

Summary of Malicious Email:

a. **Subject.** PMAD Accts.

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

1. **Antivirus Detection**
2. **Files extracted.** PMAD Accts.doc
3. **Detection Rate.** 18/59
4. **Percentage** %. 30.5

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

d. **C&C Servers**

S#	IP Addresses	URL Addresses	Hosting Country
(1)	54.37.205.242	pmacell.site	France
(2)	185.140.249.194	185.140.249.194/winh.exe	UAE Dubai

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

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

b. C:\ProgramData\Microsoft\RAC\Temp\sgIB3E4

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

d. C:\Users\Mudassar\AppData\Local\Microsoft\History\ History E5MSHist012018050920180510\index.dat

e. C:\UserslMudaasar\AppData\Local\Microsoft\Windows\WER\ReportQueue\AppCrash-EQ vEDT32. EXE_3f2e22ee8b8c291a1abf64ca54c77784fe5a085 cab_0bad1075\WERFCF5.tmp.appcompat

f. C:\Users\Mudassar\AppData\Roaming\Microsoft\Windows\Recent\ AutomaticDestinations\1 b4dd67f29cb1962.automaticDestinations-ms.

g. C:\Users\Mudassar\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\adecfb853d77462a.automaticDestinations-ms.

Malicious Information Extracted

a. The malware deletes 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 up 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".

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.

Recommendations:

a. Install and update licensed and well-reputed antivirus such as Kaspersky, Avira, Avast etc.
b. Block C&C Servers at pars 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.
f. In case of any incident, please report to this office.