**PTA CERT for Telecom Sector**

# Security Advisory-No: Ext:162-28

**07, Dec 2018**

**Threat Classification:** Vulnerability

**Overview:** A malicious email titled as "Visit AF&AD officers – 11/10/2018" is being sent to officers and staff of government departments. The email contains a malicious Winrar Compressed File. Downloading, extracting, and executing the compressed file executes malware in background that results in hacking of the computer.

**Summary of Malicious Email:**

- **a.** Subject. Visit AF&AD officers – 11/1 0/2018
- **b.** Name of Attachments. 11-10-2018 Fight details.zip
- **c.** Name of Compressed File. Depflight(details).doc (An Executable File masqueraded as word document file)
- **d.** Malware Type. Autoit compiled info stealing Trojan
- **e.** Originator of Email. Aviation_navi@yahoo.com
- **f.** Antivirus Detection rate. 09/55 (16.36%)
- **g.** C&C Servers

| Ser | IP address | Country |
|---|---|---|
| (1) | 185.203.118.198 | Bulgaria |
| (2) | 138.204.170.189 | Mexico |

**Indicators of Compromise:** The system is infected if following files are found in the system:

- **a.** C:\Users\<admin>\Local\Microsoft\Direct Input\Compatibility\mcrthost.exe
- **b.** C:\Users\<admin>WppData\Local\Temp\<rand. no>.jpeg
- **c.** HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Compatibility (Registry Key)

**Capabilities of Malware Document Identification:**

- **a.** The malware reads user information like IP address, MAC address, operating system details and Computer Name from the victim's computer.
- **b.** It uploads stored usernames and passwords present on victim's computer.
- **c.** The malware is also a key logger that records and steals usernames/ passwords of any account that victim logs in.
- **d.** The malware has the capability to gain persistence in victim's computer by setting the windows registry key on startup.

**Recommendations**

**a.** Install and update well reputed anti viruses such as Kaspersky, Avira, Avast etc.

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

**c.** In case if indicators of compromise are found in the system, please disconnect the computer from internet and reinstall Windows.

**d.** Update all software including Windows OS, Microsoft Office and all other software.

**e.** Always make sure that you have enabled two factor authentication on email accounts

**f.** Do not download attachments from emails unless you are about the source.

**g.** In case of any incident, please report to this office.