

Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No 56) Nov 18**

**Introduction.** A malicious email titled as "**Visit AF&AD Officers-11/10/2018**" is being sent to officers and staff of government department. 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.

2. **Summary of Malicious Email**

- a. **Subject.** Visit AF&AD officers - 11/10/2018
- b. **Name of Attachments.** 11-10-2018 Flight Details. zip
- c. **Name of Compressed File.** Depflight (details).doc (An Executable File masqueraded as word documents file).
- d. **Malware Type.** Autoit Complied Info Stealing Trojan
- e. **Originator of Email.** aviation\_navi@yahoo.com
- f. **Antivirus Detection Rate.** 09/55 (16.36%)
- g. **C&C Servers.**

3.

<b>Ser</b>	<b>IP Address</b>	<b>Country</b>
(1)	185.203.118.198	Bulgaria
(2)	138.204.170.189	Mexico

**Indication of Compromise.** The system is infected if following files are found in the system.

- a. C:\Users\mcrthost.exe
- b. C:\Users\- c. HKCU\Software\Microsoft \ Windows \ Current Version\Run\Microsoft **Compatibility** (Registry Key)

4. **Capabilities of Malware**

- 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.

5. **Recommendations.**

- a. **Install and update well reputed antiviruses** such as Kaspersky, Avira, Avast etc.

**SECRET**

- b. Block C&C Servers at para 2g in firewalls of own networks.
- c. In case if indicators of compromise (para 3) 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 to factor authentication on all email accounts.**
- f. Don't download attachments from emails unless you are sure about the source.