Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No. 18-A)**

1. **Introduction.** A malware is spreading through email targeting army / defense / intelligence organizations as well as DAs abroad in a well-planned targeted manner. The email portrays as a legitimate file offering to **provide information regarding Audit Observation in Federal Board of Revenue.** Downloading and clicking the counterfeit document result in executing of a malware in the background which can compromise victim's machine / system.

2. **Summary of Malicious Email**

a. **Email Subject.** FBR Audit Observation

b. **MD5 Hash.** ea0b79cd48fe50cec850e8b9733d11b2

c. **Download File.** Audit_Observation2019.zip

d. **Antivirus Detection Rate.** Low

e. **File Size.** 1.22 KB

f. **File Extension.** .zip

g. **C&C Servers**

Ser	URL address	IP Address	Country
(3)	fbr-gov.aws-pk.net	5.181.156.251	Moldova
(4)	cdn-aws-s2.net	185.141.25.212	Romania

3. **Indicators of Compromise**

a. Files downloaded or rewritten from another process: -

(3) C:\Users\admin\AppData\Local\Temp**[random].hta**

(4) C:\ProgramData\tvFiles\rekeywiz.exe

(5) C:\ProgramData\tvFiles\Duser.dll

b. Changes auto run value in registry: -

(1) HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Run with key **tv** and value **C:\ProgramData\tvFiles\rekeywiz.exe**

4. **Capabilities of Malware**

a. The malware is specially designed for targeted attacks and steals files and keystrokes (along with auto saved usernames / passwords) from Windows system and browser.

b. The attacker can gain remote access of the system and can execute additional payload on the compromised system.

c. The malware is designed to run through certified Microsoft file **mshta.exe** and tampered Microsoft **Duser.dll** for low detection and extended persistence.

d. The malware is also capable to read internet cache settings and executes through WMI.

5. **Recommendations**

e. **Regularly update well reputed antiviruses** such as Kaspersky, Avira, Avast etc. and scan system regularly.

f. Update all software including Windows OS, Microsoft Office etc on regular basis.

g. Uninstall all applications not in use and software from system and personal mobile / smart phone.

h. **Do not download attachments from Sails unless you are sure about the source.**