Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No. 19)**

1. **Introduction.** A malware has been found spreading **through emails and social engineering** that is specially designed to target Pakistan's army/ defense / intelligence organizations as well as DAs abroad in a well-planned targeted manner. These emails portray a legitimate looking document on **"Poland and Pakistan together for Security"**. Downloading and clicking on fake document executes a malware in background which will compromise victim's machine.

2. **Summary of Malicious Email**

   a. **Email Subject.** **Poland and Pakistan together for Security**

   b. **MD5 Hash.** 1cf37a0a8a5f5704a3df692d84a16a71

   c. **Vulnerability ID.** CVE-2017-11882

   d. **Malware APT Group.** SideWinder

   e. **Download File.** Protocol.doc

   f. **Antivirus Detection Rate.** Low

   g. **File Size.** 702 KB

   h. **File Extension.** .doc

   i. **C&C Servers**

Ser.	URL	IP Address	Country
(1)	fqn-cloud.net	185.99133.58	New Zealand

3. **Indicators of Compromise**

   a. Files downloaded or rewritten from another process: -

      (3) C:\ProgramData\SyncFiles**rekeywiz.exe**

      (4) C:\ProgramData\SyncFiles**Duser.dll**

   b. Changes auto run value in registry: -

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

4. **Capabilities of Malware**

   a. The RTF based malware is specially designed for targeted attacks and can steals files and keystrokes (along with stored usernames / passwords) from Windows system and browsers.

   b. The attacker can gain remote access of the system and can execute additional payload from it and run Microsoft certified files to evade antivirus detection.

   c. The adversary gets persistence through hooking by changing auto run value in the registry.

5. Recommendations

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

b. Update all software including Windows OS, Microsoft Office and all other on regular basis.

c. Uninstall all **not in use applications** and **software** from system and personal phone.

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