Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No. 20)**

1. **Introduction.** Recently, a malware is spreading **through social engineering** that is targeting army / defense / intelligence organizations as well as DAs abroad in a well-planned targeted manner. These emails portray a legitimate looking **MOUs document regarding Pakistan-Philippines Agreement.** Downloading and clicking on fake document executes a malware in background that will compromise victim's machine.

2. **Summary of Malicious Email**

a. **Subjects.** Pakistan-Philippines Agreement! MoU's.doc

b. **MD5 Hash.** 2ba61596f9ec352eebe6e410a25867f6

c. **Download File.** MoU's.doc

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

e. **Malware APT Group.** SideWinder

f. **Antivirus Detection Rate.** Low

g. **File Size.** 806 Kbs

h. **File Extension.** .doc

i. **C&C Servers**

Ser.	URL	IP Address	Country
(2)	cdn-sop.net	172.93.188.161	Hong Kong

3. **Indicators of Compromise**

a. Files downloaded or rewritten from another process: -

(1) C:\ProgramData\SyncFiles\rekeywiz.exe

(2) 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**

c. Creates Task scheduler for dual persistence: -

(1) Key UpdateService with value C:\ProgramData\SyncFiles\ rekeywiz.exe

4. **Capabilities of Malware**

a. The Rich Text Form (RTF) based malware is specially designed for targeted attacks and can steal 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.**