Subject: **Advisory - Prevention Against Cyber Espionage (NDC Course-60 Participants) (Advisory No. 26)**

1. Recently, a malware is being spread through **social engineering** tactics targeting personal of civil / military / intelligence organizations and Defence Attaches abroad in a well-planned targeted manner. The email mimics as a legitimate correspondence with the subject **"List of NDC course participants".** Downloading and clicking on fake document executes a malware in the background that eventually compromise victim's machine.

a. **Subject.** NDC Course-60 Participants

b. **Sponsor Country / State.** India (likely)

c. **Malware Types / Target OS.** Windows

d. **MD5 Hash.** df020e81b7ca7ca32868a8ac1f5eddd086f

e. **Download File.** NDC Participants.docx

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

g. **Malware APT Group.** SideWinder

h. **Antivirus Detection Rate.** Low

i. **File Size.** 675 Kbs

j. **File Extension.** .doc

k. **C&C Servers**

Ser	URL address	IP Address	Country
(1)	cdn-sop.net	172.93.188.161	Hong Kong
(2)	http://google.gov-pok.net/images/C&CFABDA/1/13897/0ac61c6e/main.file.rtf	172.93.189.220	Australia

2. **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\SyncFiles\rekeywiz.exe**

3. **Capabilities of Malware**

a. The 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.

d. The attacker can ran malware through Equation Editor that read other registry keys for execution and transferred information through temporary files.

4. Recommendations

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

b. Regularly scan systems for **software upgrades and security patches** for Windows OS, Microsoft Office and all other on applications.

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

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