Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No. 27)**

1. Recently, a malware has been reported through **spoofed email** that has targeted M/s **CyberNet,** Pakistan. MKalware is being propagated through a crafted word document / file that looks like a ligity file with subject "**Bank Slip**". Downloading / clicking on malicious document executes a malware in background that eventually compromises victim's machine.

2. **Summary of Malicious Email**

   a. **Email Subject.** Bank Transfer confirmation

   b. **Downloaded File.** Bank Slip.docx

   c. **MD5 Hash.** 7b471ef2a080580a5df21c864ce20391

   d. **Vulnerability ID.** CVE-2017-11882 / CVE-2017-0199

   e. **Antivirus Detection Rate.** Low

   f. **File Size.** 11.4 Kbs

   g. **File Extension.** .docx

   h. **C&C Servers**

Ser	URL address	IP Address	Country
(1)	-	192.227.129.19	India

3. **Indicators of Compromise**

   a. Files downloaded or rewritten from another process

      (1) C:\Users\<admin>\AppData\Roaming\Microsoft\Office\Recent\index.dat

4. **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 adversary resides in system by creating several copies and severe execution points of original sample.

   c. 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.

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

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.**

e. Window defender and Firewall of system to be on recommended settings.