Subject:- **Prevention Against Cyber Espionage (Advisory No 12, September 2015)**

Email with specially crafted attached file containing highly sophisticated malware is targeting users of sensitive organizations. The malware is designed to steal information and take control of user's system.

2. **Modus Operandi**

a. **Attached File**. UN_4_21_2015.docx.

b. Opening the file executes malware in background and a decoy document is opened (Annex A).

c. Malware takes control of target computer and extracts files of interest to C & C server abroad.

d. Malware is very stealthy and most antivirus do not recognize it. However following hidden files and folders are created in computer which can be identified to see if system is infected or not:-

(1) "CVRAE9123.lgx" and "UN.doc" C:\Documents and Settings\%Name% \Application Data\Local Settings\Temp.

(2) "MicroScMgmt.exe","jli.dll"and"msvcr71.dll"in C:\Documents and Settings\ %Name%\Application Data\Microsoft.

(3) Cookies (administrator@<random host name>.txt) in C:\Documents and Settings\%Name%\Cookies.

e. **Effected Software.** Microsoft office 2003, 2007 and 2010.

f. **CVE Number** CVE -2013- 3906.

3. **Recommendations.** In order to prevent the user from attack, following is suggested:-

a. Change the following registry key HKEY_LOCAL_ MACHINE \ SOFTWARE\ Microsoft \ Gdiplus \Disable TIFFCodec =1,

b. Install EMET (the Enhanced Mitigation Experience Toolkit).

c. Use protected view and block ActiveX controls in Office documents downloaded.

d. Install well reputed antivirus / firewall software that block know malwares:-

(1) Bitdefender total security

(2) Kaspersky internet security

(3) Eset NOD32 internet security

e. Malicious /suspicious emails may be forwarded on following emails address for analysis:-

(1) **eagle 1978@mail.com**

(2) **shikra343@gmail.com**