Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No.3)**

1. **Introduction.** Recently a malware has been identified, spreading through spoofed emails and targeting defence / intelligence organizations. These emails portray a legitimate looking news and contains a malicious link that redirects the user to download a zip attachment. Extracting and clicking the file executes a malware in background which can compromise victim's machine.

2. **Summary of Malicious Email.**

a. **Email Subject.** United Nations to include Government Servants and Para Military Forces

b. **Spoofed Email address.** info6@ispr.mail-do.net

c. **Download Package.** un-distribution.zip

d. **Antivirus Detection Rate.** 02 /55 ((3.63%)

e. **File Size.** 932 bytes

f. **File Extension.** zip (archival file format)

g. **Download Address.** https://www.s3-cdn.net/images/50E7C0B2/
6782/1196/6b473c8b/un-distribution.zip

h. **Exploit Technique.** DLL Injection into legitimate file

i. **C&C Servers.**

Ser	URD Address	IP Address
(1)	https://www.s3-cdn.net	185.243.114.116

3. **Indicators of Compromise.** The system will be infected if following files are found in the system:-

a. C:\ProgramData\dsk\dat2\credwiz.exe (Digital Signature Protected File)

b. C:\ProgramData\dsk\dat2\duser.dll (Malicious DLL)

c. C:\Users\<admin>\AppData\Local\Temp\bd.hta(83KB)

4. **Capabilities of Malware.**

a. The malware has valid digital signatures and hence it has a very low detection rate.

b. The malware is specially designed for targeted attacks and can steal files and keystrokes from windows system.

c. The attacker can gain remote access of the system and can execute additional payload from it.

5. **Recommendations.**

a. **Install and update will reputed antiviruses** such as Kaspersky, Avira, Avast etc.

b. In case indicators of compromise (para 3) are found in the system, please disconnect the computer from internet and reinstall Windows.

c. Update all softwares including Windows OS, Microsoft Office and all other softwares on regular basis.

d. Uninstall all unwanted softwares from your system and android phone.

e. Don't download attachments from emails, unless you are sure about the source.

f. It is **mandatory** to **enable 2 factor authentication on all your email accounts (Gmail,Yahoo, Hotmail etc), social media accounts (Facebook, Whatsapp etc) especially internet banking to prevent any sort of unauthorized access** and financial loss.

g. **Never forward your OTP (One Time Password) to anyone as it can easily hack your accounts.**