Subject: **Advisory – Prevention against Cyber Espionage (Advisory No.4)**

1. **Introduction.** Recently, a malware found spreading through spoofed email targeting defense / intelligence organizations. These emails portray a legitimate looking **"Hajj and Umra package"** details and contain and it a contains a malicious link that redirects the user to download a zip attachment. Extracting and clicking the fake pdf file executes a malware in background compromise victim's machine.

2. **Summary of Malicious Email**

   a. **Email Subject.** Applications Invited – Hajj and Umra Contingent – 2019.

   b. **Spoofed Email address.** Info13@mail-fwd.net.

   c. **Download Package.** Hajj.zip.

   d. **Antivirus Detection Rate.** Nil/55 (0%)

   e. **File Size.** 915 bytes.

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

   g. **Download address.** https://hajj-umra.cdn-io.net/images/F856ECCB/6782/1266/61a2b417/Hajj.zip.

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

   i. **C&C Servers**

Ser	URL address	IP Address	Country
(1)	https://hajj-umra.cdn-io.net	185.243.115.39	Netherlands

3. **Indicators of Compromise.** The system is infected, if the 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)

   d. C:\Users\<admin>\AppData\Local\Temp**Hajj.pdf**(368KB)

4. **Capabilities of Malware**

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

b. The malware is specially designed for targeted attacks and can **steal files** and other sensitive data from windows system.

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

5. **Recommendations**

c. **Don't rely on Windows defender, always install and update well reputed antiviruses** such as Kaspersky, Avira, Avast etc.

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

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

f. Uninstall all unwanted softwares form your system and android phone.

g. **Don't download attachments form emails unless you are sure about the source.**

h. 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.**

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

j. Blacklist C&C server mentioned in para 2(i) in firewalls of own network.