Subject: **Advisory – Prevention Against Cyber Espionage (Advisory No.6)**

1. **Introduction.** Recently, a malware found spreading through spoofed email (ID: **dd.cbckp@fia.gov.pk**); targeting defense / intelligence organizations. These emails portray a legitimate looking **"Hajj and Umra package"** details and contain 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.** Update Required in CT Case Enq No 5856 / 2017

   b. **Spoofed Email address.** dd.cbckp@fia.gov.pk

   c. **Email Attachment.** Update Required Case Enq No 192 – 2018.docx

   d. **Antivirus Detection Rate.** 09 / 55 (16.36%)

   e. **File Extension.** Com (executable file presented as document file)

   f. **C&C Servers**

Ser	URL address	IP Address
(1)	frameworksupport.net	162.222.215.90
(2)	Khurram.com.pk/js/Update Requirement Case Enq No 192 – 2018	203.124.43.229

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

   a. C:\intel**msdtcv.exe** (31 KB)

   b. HKCU\Software\Microsoft\Windows\CurrentVersion\Run**msdtcv**

   c. C:\Users\<admin>\Downloads**Update Required Case Enq No 192 - 2018.docx.com** (31 KB)

4. **Capabilities of Malware**

   a. The malware reads user's system information and uploads it on its C&C server.

   b. It uploads stored information like usernames and passwords present on victim's computer and automatically programs the victim machine to run from auto start location.

   c. The attacker can gain remote access of the system with the help of this malware and can download additional payload from it.