Subject: **Prevention Against Cyber Espionage (Advisory No, 14) October, 2017**

1. **Introduction.** A malicious email titled as "Uqab **UAV System"** is being sent to officers and staff of Government departments. The email contains a winrar compressed file which contains two attachments. Downloading and extracting the files from email executes malware in background and displays fake documents in the foreground that can hack the users' system.

2. **Summary of Malicious Email**

   a. **Subject.** Uqab UAV System

   b. **File Name.** UAV System.rar

   c. **Compressed Word Files**

      (1) Advisory41.doc

      (2) GIDS-UAV SYSTEM.doc

   d. **File Type.** Word Documents compressed in winrar files

   Anti Virus Detection Rate. 10/54 **(17.24% Very low detection ratio)**

   f. **Malware Type.** Exploit Based Trojan.

3. **C&C (Command & Control) Servers**

Ser	C&C URL	IP address	Hosting Country
a.	185.161.209.86.deltahost-ptr	185.161.209.86	Netherlands
b	176.107.179.182.deltahost-ptr	176.107.179.182	Ukraine

4. **Indicators of compromise.** In case if following files and folders are found in the computer, it means that computer is hacked:-

   a. CAUsers\<admin>\AppData\Locai\Hiberriate\Sys\Clock.exe

   b. CAUsers\<admin>\AppData\Local\Hibernate\Sys\NetLogOn.exe

   c. CAUsers\<admin>\AppData\Local\Hibernate\Sys\WorkspaceShare.exe

5. Capabilities of Malware

   a. Reads 'user's computer information like 'operating system details, directory files list, network, .IP, route and interfaces details, Windows Services Information, System Information, Computer Name, procps_se information from the victim's computer.

   b. The malware then 'starts to upload user's documents and files including Word, PowerPoint, Excel, text files and stored usernames and passwords to its C&C servers.

   c. The Malware can installs itself in windows startup location and can automatically execute itself on windows reboot.

6. **Recommendations**

a. **Install and UPDATE well reputed antiviruses** such as Kaspers,ky, Bitdefender, Nod32, Avast etc.

b. Block C&C SeNers at para 3 in firewalls of own networks.

c. In case if indicators of compromise (para 4) are found in the system, please disconnect the computer from intemet and reinstall Windows.

d. Update all softwares including VVindows OS, Microsoft Office and all other softwares.

e. Install and regularly update software firewall such as Comodo Firewall or Zonealarm.

f. Don't download attachments from emails unless sure about the source.