Subject: **Prevention Against Cyber Espionage (Advisory No 05) May, 2017**

1. **Introduction.** A malicious email titled as **"Order No.:6734373"** is being sent to officers and staff of Government departments. The email contains a compressed **Winrar** file. Downloading and extracting the file executes malware in background that results in hacking of the computer.

2. **Summary of Malicious Email**

   a. **Subject.** Order No. :6734374

   b. **Name of Attachments.** Order No.6734374_pdf.ace

   c. **Malware Type.** Trojan based malware

   d. **Originator of Email.** sasima@actcom2000.com

   e. **Antivirus Detection Rate.** 23/55(41.81%)

   f. **C&C Servers**

Ser	URL	IP	Hosting Country	Registrant Country
(1)	smtp.zoho.com	204.141.32.118	USA	India

3. **Indicators of Compromise.** The malware makes following files on the infected system:-

   a. C:\Users\<admin>\AppData\Roaming\pid.txt

   b. C:\Users\<admin>\AppData\Roaming\pidloc.txt c..
   C:\Users\<admin>\AppData\Roaming\WindowsUpd
   ate.exe

   d. CAUsers\<admin>\AppData\Local\Temp\Screens\screenshotjpg

4. **Capabilities of Malware**

   a. Reads user information like operating system details, and Computer Name from the victim's computer.

   b. The malware steals stored usernames and passwords information of victim's personal accounts.

   c. The malware also takes screenshots of infected system and uploads them to its own mailing account.

5. **Recommendations**

   a. **Install and update well reputed antiviruses** such as Kaspersky, Avira, Avast etcc.

   b. Block C&C Servers at para 2f in firewalls of own networks.

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

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

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

f. Don't download atta6hments from emails unless you are sure about the source.