Subject:- **Prevention Against Cyber Espionage (Advisory No 02 May 2017)**

1. **Introduction.** A malicious email titled as **"Newly Posted Invoices"** is being sent to officers and staff of Government departments. The email contains an **executable jar** file. Downloading and executing the file executes malware in background that results in hacking of the computer.

2. **Summary of Malicious Email**

a. **Subject.** Newly posted Invoices.

b. **Name of Attachments.** 0.6970770 1490718243.jar.

c. **Malware Type.** Remote access Trojan.

d. **Originator of Email.** Reservation @kohkoodsunshine.com

e. .**Antivirus Detection Rate.** 23/57 (40.35%).

f. **C&C (Command & Control) Servers**:-

Ser	URL	IP	Hosting Country	Registrant Country
(1)	Bishbish.duckdns. org	(Dynamic DNS that changes frequently)	USA	France

3. **Indicators of compromise.** The malwares makes following files on the infected system:-

a. C:\Users\<admin>\llmPwVNLELY**WPkXbkCOTPq**

b. C:\Users\<admin>**ID.txt**

c. C:\Users\<admin>**RoYUArVmKPV.oJJKiJ**

d. C:\Users\<admin>\AppData\Local\Temp**<rand. no>.class**

4. **Capabilities of Malware**

a. Malware scans the computer for security utilities like antivirus, firewalls, task- managers etc and disables them permanently.

b. The malware gains the complete control of the system and disables the user's admin privileges..

c. The malware gives the remote access to the hacker to perform further operations.

5. **Recommendations**

a. **Install and update well reputed antiviruses** Such as Kaspersky,Avira, Avast etc.

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

c. In case of indicators of compromise (para 3) are found in the system, please disconnect of compromise 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 attachments from emails unless you are sure about the source.