Subject: **Prevention Against Cyber Espionage (Advisory No 03 May 2017)**

1. Introduction. A malicious email titled as **"Income Tax Calculato (Mr Rashid Mahmood)"** is being sent to officers and staff of Government departments. The email contains a malicious **excel** file. Downloading and enabling the macros executes malware in background that results in hacking of the computer.

2. Summary of Malicious Email

a. Subject. Income Tax Calculator (Mr Rashid Mahmood)

b. Name of Attachments. Tax Calculator.xls

c. Malware Type. Macro based Malware

d. Originator of Email. onlineservice@mail.com

e. Antivirus Detection Rate. 4/55 (7.27%)

f. C&C Servers

Ser	URL	IP	Hosted Country	Regi Coun
(1)	live.systemupdates.space	89.33.246.99	Romania	Switz erlan

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

a. C :\Prefeth\Apps\Service\wininet.exe

b. C:\Time\<rand. word.exe>

4. Capabilities of Malware

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

b. The malware executes a command named **"systeminfo.exe"** to know about detailed OS and network configuration information and uploads the result to its C&C server.

5. Recommendations

a. Permanently disable macros by following this path in Microsoft Office:- Click on File > Options > Trust Center > Trust Center Settings > Disable all macros with notification.

b. **Install and update well reputed antiviruses** such as Kaspersky, Avira, Avast etc.

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

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.

f. Install and regularly update software firewall such as Comodo Firewall

or Zonealarm.

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