Subject: **Prevention against Cyber Espionage (Advisory No 11 , 2016)**

1. **Introduction.** A malicious email titled as **"Telecom Policy 2015 — Cyber Crime Bill"** is being sent to officers and staff of Government departments.

2. **Summary of Malicious Email**

- **a.** **Subject.** Telecom Policy 2015 — Cyber Crime Bill.
- **b.** **Name of Attachment.** Cyber_Crime_bill.doc.
- **c.** **Malware Type.** MS Word Exploit followed by malware based attack.
- **d.** **Originator of Email.** naweedzaman@transseksualov.com.
- **e.** **C&C Servers**
  - **(1)** www.sehalsolutions.com/bill/.
  - **(2)** www.insigniaadvertising.com.pk/bill/.
  - **(3)** www.mail.sendwithyou.co.uk/.

3. **Affected Software.** Microsoft Office 2003, 2007, 2010 and 2013 which are not updated after Jun 2015.

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

- **a.** C:\Users\admin\AppData\Roaming\Microsoft\MicrosScMgmt.exe
- **b.** C:\Users\admin\AppData\Roaming\Microsoft\jili.dll
- **c.** C:\Users\admin\AppData\Roaming\Microsoft\msvcrt71.dll

5. **Capabilities of Malware**

- **a.** Malware collects following sensitive information and uploads to foreign C&C Servers:-
  - **(1)** Key strokes i.e. usernames and passwords.
  - **(2)** MS Office documents including Word, Powerpoint etc.
- **b.** Adds itself to **system startup** to continue hacking after system reboot.
- **c.** Uses certificates from legitimate trusted publisher **SunMicrosystems)** which enables it to evade most antiviruses and firewalls.

6. **Recommendations**

- **a.** In case if indicators of compromise (para 4) are found in the system, please disconnect the computer from internet and reinstall Windows.
- **b.** Block C&C Servers at para 2e in firewalls of own networks.
- **c.** Install and update well reputed antiviruses such as Kaspersky, Bitdefender, Nod 32, Avast etc.
- **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.