Subject:- **Prevention Against Cyber Espionage (Advisory No 13 dated Jun 2016)**

1. **Introduction.** A malicious email titled as **"Advisory — Prevention Against Cyber Espionage (Advisory No 63 Dated 11 June 2016)"** from a fake email address **"eagle.1978@mail.com"** is being sent to officers and staff of Government Staff. The email is a **fake advisory** which ask user to download a power point presentation that is actually a malware. The fake advisory was prepared by hostile quarters by using own advisory no 65, issued on 27 May 2016.

2. **Summary of Malicious Email**

a. **Subject.** Advisory — Prevention Against Cyber Espionage (Advisory No 63 Dated 11 June 2016).

b. **Method of Infection.** Fake links in the document of modified advisory (Anx A).

c. **File Name.** How to Remove Malware Traces. pps

d. **File Type.** PowerPoint slide show (.pps)

e. **Hacker's Email.** eagle.1978@mail.com

f. **Malware Type.** Exploit based Trojan.

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

Ser	URL	IP	Country
a.	212-129-13-110.rev.poneytelcom.eu	212.129.13.110	France
b.	-	45.43.192.172	USA
c.	http://t.ymlp52.com/umeakaejeyqafawsqadaueehqe/ click.php		Belgium

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

a. C:\Users\admin \AppData \Local\Temp\sysvolinfo.exe

b. C:\Users\admin\AppData\Local\Tem\driver.inf

c. C:\Users\admin\AppData\Local\Microsoft\NetCache\Content.MSO\ **msoF7C.tmp**

d. **C:recoveryx\protected.ie**

5. **Capabilities of Malware**

a. Upon opening the .pps slide, a user malware accepts some onscreen dialogues.

b. The malware uploads computer names, MAC address , IF address and operating system details to its C&C.

c. The malware also uploads documents and files including word, PowerPoint, excel, text files and stored usernames and passwords to its C&C servers.

d. Lastly, the malware launches a payload to take control of victim's computer and installs itself in windows startup location.

6. **Recommendations**

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

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

c. Install and update well reputed antiviruses such as Kaspersky, Bitdefender, Nod 32, Avast etc.

d. Update all browsers and 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.