Subject: **Advisory — Prevention Against Cyber Espionage (Advisory No 12 2016)**

1. **Introduction.** A malicious email titled as **"Military and Security Developments Involving the People's Republic of China 2016: ANNUAL REPORT TO CONGRESS."** is being sent to officers and staff of Government departments. The email presents a link to download a **detailed PowerPoint slide about China's Military capabilities.** Downloading and opening the slide, executes malware in the background which results in hacking of the computer.

2. **Summary of Malicious Email**

   a. **Subject.** Military and Security Developments Involving the People's Republic of China 2016 :ANNUAL REPORT TO CONGRESS.

   b. **Name of Attachment.** 2016 _China_ Military_PowerReport.pps

   c. **Malware Type.** Trojan.

   d. **C&C Servers.** Following IPs and URLs be blocked at Network Firewalls:-

Ser	URL	IP	Country
(1)	www.epg-cn.com	212.83.146.3	France
(2)	212-129-13-110. rev. poneytelcom.eu	212.129.13.11	France
(3)	212-83-191-15. rev. poneytelcom.eu	212.83.191.15	France
(4)	http://www.newsnstat.com/index.php?f=2016 _China_Military _Power Report.pps	212.83.146.3	France

3. **Indicators of Compromise.** Following files can be found on the infected system:-

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

   b. C:\Users\admin\AppData\Local\Microsoft\INetCache\ContentMSO \ **msoF7C.tmp**

   c. C:\Users\admin\AppDatalocal\Temp\driver.inf

4. **Capabilities of Malware**

   a. Upon opening the **.pps (power point slide show),** a malware is executed automatically.

b. The malware uploads user's location , username , MAC address , IP address and operating system details to its C&C.

c. The malware then starts to upload users documents and files including word ,powerpoint, excel , text files and stored usernames and passwords etc.

d. The malware only executes in 64 bit windows environment.

5. **Recommendations**

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

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

c. Install and update well reputed antiviruses such as Kasperslry, 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.