Subject:- **Advisory - Prevention Against Cyber Espionage (Advisory No 14 July 2016)**

1. **Introduction.** A malicious email titled as **"Unable to deliver your item,#00507979"**is being sent to officers and staff of Government departments. The email is a **zip file** that contains a **JavaScript malware.** Downloading and extracting the file, executes malware in the background that results in hacking of the computer.

2. Summary of Malicious Email

a. **Subject.** Unable to deliver your item,#00507979.

b. **File Name.** Label_005079797.zip.

c. **File Type.** Archive File Format **(.zip)**

d. **Malware Type.** JavaScript Based exploit

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

Ser	URL	IP	Country
a.	webcluster233.one.com	46.30.212.233	Denmark
b.	turabiruggallery.com	67.231.240.143	USA
c.	originsweden.com	46.30.212.233	Denmark
d.	hoppersindoorsportz.net.au	43.229.63.14	Australia
e.	xn--b1amg7e.xn--p1ai lovimoment77.ru		

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

a. C:\Users\admin\AppData\Local\Temp\7581012.exe

b. C:\Users\admin\AppData\LOcal\Temp\7581011.exe

c. C:\Users\admin\AppData\Local\<rand.no>**<rand.no .bat>**

d. C:\Users\admin\AppData\LocaR<rand.no>\**<rand.no .exe>**

5. Capabilities of Malware.

a. Upon opening the **.js** file, malware launches a script in the background.

b. The malware downloads numerous executables from its C&C servers and tampers with windows registry to make itself non-deleteable.

c. The malware uploads .IP address, Computer name , Network Settings and operating system details to its C&C servers.

d. The malware steals passwords from victim's browsers and uploads victim's files to its C&C server.

e. The malware communicates with a huge pool of random C&C servers but has a high detection ratio.

f. The malware has ability to make itself dormant to avoid detection and , registers itself via Microsoft Reg. Server. **(regsvr32.exe)**

g. The malware also sometimes acts like a **fake ransomware** to lure the victim into downloading more malicious executables from its C&C server.

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 3 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.