Subject:- **Prevention Against Promotion List Malware - Advisory No 13 March, 2018**

1. **Introduction.** A malicious email titled as **"Promotion List'** is being sent to officers and staff of Government departments. The email contains a malicious **,doc** file. Downloading and opening the file executes malware in the background that results in hacking of the computer.

2. **Summary of Malicious Email**

   a. **Subject.** Promotion List.

   b. **Name of Attachments.** promotion.docx.

   c. **Subject.** Promotion List.

   d. **Malware Type.** Trojan based Exploit.

   e. **Malware Detection Ratio.** 10/54 **(18.5% Very Low).**

   f. **C** & **C Servers**

Ser	IP Address	Registration	Countr	Hosting
a.	185.203.118.11	April 18,2016	Bulgari	Sofia DataBox

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

   a. CAUsers\<Admin>\AppData\Localgemp\edg499.dat.

   b. CAUsers\<Admin>\AppDatalocal\Temp\TPX498.dat

   c. CAUsers\<Admin>\AppDatalocal\Temp\9PT568.dat.

4. **Capabilities of Malware**

   a. The malware is capable of getting system IP, user location, network configuration details and upload itself on its C&C server mentioned in para 2e.

   b. The malware has the ability to steal the usernames and passwords of infected systems.

   c. The malware can copy itself into windows startup location and it automatically execute itself on windows boot.

   d. The malware has a **very low detection ratio (18.5% only).**

5. **Recommendations**

   a. **Install and UPDATE well reputed antiviruses** such as Kaspersky, Bitdefender, Nod 32, Avast etc.

   b. Block C&C Servers at para 2e on firewalls of own networks.

   c. In case if indicators of compromise (para 3) are found in the system, please disconnect the computer from Internet and share information with iCERT.

   d. Update all softwares including Windows OS, Microsoft Office and all other softwares.

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