Subject: **Advisory-Prevention Against Cyber Espionage (Advisory No 1)**

Introduction. A malicious email titled as **"US Pak Track II Naval Dialogues"** is being sent to officers and staff of Government departments. The email contains a malicious **document** file. Downloading and opening the file executes malware in the background that results in hacking of the computer.

1. **Summary of Malicious Email**
   a. **Subject.** US Pak Track II Naval Dialogues
   b. **Name of Attachments.** US Pak Track II Naval Dialogues.doc
   c. **Ma!ware Type.** RTF based Exploit
   d. **Originator of Email.** nomanbashir@hotmail.com
   e. **Affected Softwares.** Microsoft Word 2003, 2007, 2010, 2013.
   f. **Antivirus Detection Rate.** **14/55 (25%)**
   g. **C&C Servers**

Ser	URL	IP	Country	Registrant Country
(1)	http://presspublishing24.net	162.222.226.140	USA	**Mumbai, India**
(2)	http://ichoose.zapto.org	52.204.110.189	USA	Seattle, USA

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

   a. C: \Program Data \Sun18\s23.dat .
   b. C:\Users\<Computer name>\AppData\Local\Temp\xv8851.tmp
   c. C: \Users\<Computer name> \AppData \Local \Temp\ChoiceGuard.d ll
   d. C:\Users\<Computer name>\AppDatalocal\Temp\ scr8863.tmp.js

4. **Capabilities of Malware**
   a. The malware reads user information like IP address, operating system detail t and Computer Name from the victim's computer.
   b. It uploads stored usernames and passwords on victim's computer.
   c. The malware is also a key logger that records and steals usernames/ passwords of all accounts.
   d. The malware is capable to remotely control victim's computer.

5. **Recommendations**
   a. **Install and update well reputed antiviruses** such as Kaspersky, Avira, Avast etc.
   b. Block C&C Servers at para 2g in firewalls of or networks.
   c. In case if indicators of compromise (para 3) are found in the system, please disconnect the computer from Internet and reinstall Windows.
   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.