Subject:- **Prevention Against Cyber Espionage (Advisory No. 06) April 2015**

Email with specially drafted subject matters containing latest variants of existing malware are targeting users of sensitive and military organizations which are aimed at stealing information from the user's system. Following Emails were received recently:-

Ser	Subject	Email Sender	Attachment Name
a.	IS recruiters setting up shop in militant rich Paak.	Amjad Khan (iti_wokha@yahoo.com)	IS recruiters setting up shop in militant rich paak…! rar
b.	India' s DRDO Secret Development Info	Ijaz Akhtar (akhtar0670@gmalil.com)	DRDO. rar
c.	Raising New FC Wing	Maj Rashid (rashidkhan45th@gmail.com)	Raising new FC Wing. rar
d.	PM meets with Corps Commander and DG Rangers	Zahid Malik (zsm1971@outlook)	PM meets with Corps Commander and DG Rangers. rar

2. **Modus Operandi.**

a. Using conspicuous official details/names, the user is lured into downloading attached malware disguised as official word documents**.**

b. Opening the, executes hidden malware in background and decoy Word file in foreground. Fake Word files opened upon executing of these malware are attached as Annex "A" to "D".

c. Malware gives access to the hacker who steals sensitive information from the target PC and uploads it to servers outside Pakistan.

3. **Activity By Malware:-** Following hidden files/folders are created in infected system:-

a. C:/Config/boot/nero.bat

b. C:Config/boot/netstatic.exe

c. C:Config/boot/netstatic.exe

d. C:Config/boot/regi.exe

e. C:Config/boot/svconnect.exe

f. C:Config/boot/regprocesshost.exe

g. C:Config/boot/uplogin.exe

4. **Recommendations**. In order to prevent the leakage of sensitive/personal information, following is suggested:-

a. Avoid opening email from unknown sources specially having official subject matter.

b. Install well reputed antivirus software such as:-

(1) Bit defender Total Security

(2) Kaspersky Internet Security

(3) Eset NOD32 Internet Security

c. Avoid using VPN software such as spotflux, hotsotshield etc.

d. Find and delete the files mentioned at para 5 above.

e. Incase system is found to be infected, do following:-

(1) Disconnect from Internet.

(2) Backup the data to external drive or secondary partition.

(3) Reinstall windows to remove malware from partition, registry, startup, temporary file locations and windows services.