Subject:- **Prevention Against A Persistent Cyber Attack Campaign (Advisory No. 05) April 2015**

Cyber-attacks against users of sensitive and military organizations are on the rise. For more than three years, a group of malware is active which uses phishing (fake) emails that portray as official emails from officers of military organizations.

2. **Common Characteristics of Malware Family**. All variants of this malware group have following common characteristics:-

a. Each new variant is not detected by any antivirus.

b. Detection rate of even known / old malware by antivirus softwares is very low.

c. Malware is sent through emails by using fake identities of military officers.

d. Icon of file looks like Microsoft Word, Power Point, Excel or Acrobat (pdf) file. However, the file is actually an executable program with extension. scr. Sample is attached for easy comprehension at Annex A.

e. On opening the .scr. file, a fake document is opened in foreground and a malware is executed in background, which performs following functions :

(1) Downloads more malware for additional hacking functions:

(2) Records keystrokes therefore everything typed on keyboard is recorded and sent to hackers. It includes all usernames and passwords.

(3) Finds all documents (word, power point, excel and pdf) on internal as well as external hard drives (USBs) and uploads the files to the servers of hackers .

(4) Gathers information even if the system is not connected to internet and steals all above mentioned information when user goes online.

3. The malware resembles and improves upon the characteristics of malware identified in Operation Hangover.

4. **Variants of Malware.** Emails with following attachment have been reported recently:

Ser	Email Attachment	File type		Sender
		Compressed	Uncompressed	
a.	43 Inf Div mnpr	.7z	.scr	Capt Kashif<mission@rediff.us.pn>
b.	17 Div Table	.7z	.scr	sajedmh@gmail.com
c.	Plan-in-pakistan-ISIS	.7z	.scr	ahmed khan <von.randy57@yahoo.com>
d.	Confidential Zone Wise list of staff	.7z	.scr	brig. tariq khan <von.randy26@yahoo.com>
e.	SPD	.7z	.scr	M. Karim Strategic plan division (SPD) Sect National Command Authority<m.karim@nca.gov.pk
f.	Final report on Nirbhay Test	.7z	.scr	K Hayat <omarhayat68@gmail.com>
g.	ISIS plan for global dominance	.7z	.scr	Sunao Yum <sophiialeafy@gmail.com>
h.	PAK-army-atlast-took-revenge-for-us	.7z	.scr	Muhammad Anwar <muhammadanwar01@yahoo.com
i.	Letter from Government of Balochistan	.7z	.scr	Twa_Anwar <twa_anwar@yahoo.com>
j.	Allies between Tallibaan and is worries PAK	.7z	.scr	Abu Zaffar <sheikhabuzaffar@gmail.com>
k.	Pak Jihadist Group ‘s plan	.7z	.scr	Waqar wkingravi@yahoo.com

5. **Recommendations**

a. Never open email from unknown source even if the subject is official or intriguing.

b. As a primary defensive measure, install software firewall.

c. Install antivirus and update it regularly.

d. Official data must not be kept on internet connected systems, even if the system is offline.

e. All software including Windows must be updated regularly.

f. In case if any of the above mentioned file or similar files (.scr) have been opened, please consult IT department for repair/recovery.