Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No 57) Nov 18**

Introduction. An online malware campaign has been identified that is targeting officers and staff of government department on a large scale by using the names of national organizations i.e. NADRA, FBR and NDU. These URLs lure the target to download malicious document files. Downloading the file executes an exploit that further downloads additional malware in background which results in hacking of the computer.

2. **Summary of Malicious attack Campaign.**

a. **Attack Vector.** Usage of pushing emails to direct the user on an official looking website with very similar URL that is hosting harmful files.

b. **Malware Type.** RTF Based Word Exploit CVE 2017-11882=1 followed by a Payload download.

c. **Antivirus Detection Rate.** 03/55 (5.45%).

d. **C&C Servers.**

Ser	URL Address	IP Address
(1)	winsvs.ddns.net/glossary/nefarious.php	94.156.174.35
(2)	fbr. press	5.104.226.126
(3)	nadra-id.com	
(4)	pkgov.com	
(5)	nduinfo.org	185.140.248.200
(6)	offers.serenahotelliers.com	
(7)	hajpilgrim.org	89.47.163.211
(8)	ms-office-updater.com	
(9)	Jashneazadi.store	158.69.218.55
(10)	Pieupdate.online	
(11)	filishares.online	
(12)	firsout.org	51.68.173.62
(13)	ndualumini.club	
(14)	sty6.net	
(15)	nayapak.news	23.95.9.107
(16)	Adhath-learing.com	95.211.135.168
(17)	-	193.22.98.226
(18)	-	51.104.226.126

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

a. C:\Users\<admin>\AppData\Roaming\MicrosoftWindows\StartMenu\Programs\Startup**Network Controller**.

b. C:\AUsers\<admin>\AppData\Roaming**srctrls.exe**.

4. **Capabilities of Malware**

a. The malware reads user information like IP address, MAC address, operating system details and Computer Name from the victim's computer.

b. It uploads stored usernames and passwords present on victim's computer.

c. The malware is also a key logger that records and steals usernames / passwords of any account that victim logs in.

d. The malware has the capability to gain persistence in victim's computer by setting a shortcut of the payload in windows startup.

5. **Recommendations**

a. **Network and website administrators of sensitive government and banking organizations should regularly check their domain name permutation to detect typosquatting, phishing, malware campaigns and cooperate espionage**.

b. Always **verify lock symbol and https:// on the top left of a URL**, before logging in on a sensitive website like internet banking of social media website.

c. **Don't share your CNIC information, Online Account details, Passwords, PINs and OTPs with anyone.**

d. **Always make sure that you have enabled two factor authentication on all email account.**

e. **Install and update well reputed antiviruses** such as Kaspersky, Avira, Avast etc.

f. Avoid installation of plugins from adware websites and popups.

g. In case if indicators of compromise (para 3) are found in the system, please disconnect the computer from internet and reinstall Windows.

h. Update all software including Windows OS, Microsoft Office and all other software.

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