Subject: **Prevention Against Info Stealing Malware (Advisory No. 21)**

1. **Introduction**. Several phishing **emails purporting to be originated from FBR (Federal Bureau of Revenue)** have been sent as part of a malware campaign to compromise data rich servers / systems. Downloading / opening such attachments from email executes malware in background and displays a fake FBR document in front screen.

2. **Summary of Malicious Emails**

   a. **Email Subject**. Circular: 24-Sep-2019

   b. **Attachment Name**. Detail Annfdp.exe

   c. **Malware Type**. Information Stealing Trojan

   d. **Antivirus Detection Rate**. 9/56 (**Very Low**)

   e. **C&C (Command and Control) Servers.** Following C&C servers have been identified in this malware campaign:-

| Ser | C&C URL | IP Address | Remarks |
|---|---|---|---|
| (1) | http://rightapps.net/sms/securimage/fbr_notification.php | 151.106.12.34 (France) | Domain hacked earlier |
| (2) | http://dailyeasyenglish.com.pk | 192.198.81.234 (USA) | Domain hacked earlier |
| (3) | http://212.114.52.148 | 212.114.52.148 (Germany) | Malicious payload hosting & C&C server |
| (4) | en-content.com | 178.62.188.63 (Netherlands) | C&C server |

   f. **Indicators of Compromise (IOC)**

      (1). C:\Users\<Acct. Name>\Adobe\Driver\pdf**Down_LinkLog.vbs**

      (2) C:\Users\<Acct. Name>\Adobe\Driver\pdf**pid.txt**

      (3) C:\Users\<Acct. Name>\Adobe\Driver\pdf**wilog.exe**

3. **Capabilities of Malware**

   a. Malware collects information about **computer name, IP address, network adopter settings, time zone settings** and **drops a payload from its C&C server**.

   b. It can extract stored **usernames, passwords in web browsers** and **automatically executes itself on windows restart**.

   c. Malware grants remote access to the attackers **to execute commands**.

4. **Recommendations.**

a. Use 2x factor authentication on **email, banking** and **social media accounts.**

b. Don't download / open attachment from untrusted email **and immediately report suspicious e-mail to iCSIRT**.

c. If **IOCs (Para 2f) are found,** in your system then immediately **disconnect it from internet and reinstall windows**.

d. **Network administrator should seep check of traffic flow** from endpoints domains mentioned in para2(e).

e. **Software Restriction Policies (SRP)** must be implemented to block **unsigned binaries** running from **%APPDATA% and %TEMP% locations**.

f. **Block outbound network connections originating** from WindWord.ex,Powershell.exe, Powersell_ise.exe, Mshta.exe and **block inbound connections if remote access of system is not required**.

g. **Operating System should be fully updated and hardened against known threat vectors**.

5. Forwarded for perusal and dissemination of information to all concerned and under command, please.