

GOVERNMENT OF PAKISTAN  
 CABINET SECRETARIAT, CABINET DIVISION  
 NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD  
 (NTISB-II)

No. 1-5/2003 (NTISB-II)

Islamabad 1 October, 2018

Subject: ADVISORY - CYBER ATTACK ON PAKISTANI NATIONALS

FS TO CHIEF SECRETARY SINDH  
 Diary No. 25851  
 Inward Date 3/19/2018  
 Outward Date

Coordination Section-II  
 SCA&CD  
 Diary No. 3961  
 Dated 4/10/18

1. Introduction. A cyber-attack has been identified targeting Pakistani nationals' especially private firms doing contracts with Pakistan Defence Forces.
2. Attack Methodology
  - a. Target individual receives a call from an unknown Pakistani number claiming to be a Pakistani government official/ Pakistan Armed Forces. Caller Officer requests for details on defence related products being developed and provided to defence organizations.
  - b. The caller (attacker) also refers to ongoing products provided by the firms to Pakistan defence organizations to establish credibility.
  - c. Following initial telephonic conversation (on GSM and WhatsApp) emails containing malicious link are sent to the target.
  - d. Downloading and opening the file from email executes the **malware** in the background and the system is compromised/ hacked.
  - e. Attackers are using fake domain names similar to existing official domains/ websites owned by Government Institutes to convince the recipient that the emails are sent by the actual government departments. Following are the observed fake domains:-

- (1) fbrgov.com
- (2) moitgovpk.com
- (3) fpmadgovpk.com

Summary of Malicious Email

- |                             |   |                                  |
|-----------------------------|---|----------------------------------|
| a. Subject                  | : | Malfunctioning of TI Sight TK 69 |
| b. Sender's Email           | : | fatehgeeiani@gmail.com           |
| c. Malicious Link           | : | http://sharefile.site            |
| d. Downloaded Document(s)   | : | sharedfile.ccc                   |
| e. Document Signature (MD5) | : | 47E52A73F0C0CD0F3863A9CD17981F95 |

Technical Analysis of Malware

- a. Exploit. Attacker has used vulnerability in **Microsoft Word (CVE-2017-8570)** to target the victim.

[Handwritten signatures and initials]  
 3/10  
 (IEC) Home  
 I.T.

11493  
 04/10/18

[Handwritten signatures and dates]  
 04/10/18  
 SO (C-II)  
 04/10/18

- b. **Capabilities of Malware.** The malware uploads data including documents and files to C&C server.
- c. **Anti-Virus Detection.** The malware "winc.exe" is not detected by major Anti-Virus software.
  - (1) **Detection Rate.** 0/67
  - (2) **Detection Percentage.** 0
- d. **Malicious Domains/ IPs**

Ser No	Malicious URL	IP Address	Hosting Country
(1)	https://sharefile.site	23.95.9.107	United States
(2)	C&C Server	193.22.98.226	Ukraine

5 **Indicators of Compromise**

- a. **Created Files.** Malware drops 3 x files at location "VoAppDataLocal1Temp", following are the details:-
  - (1) "winc.exe", a malicious executable file with signature (MD5): 25d3508a5e887cfd7343e798d839ad5a.
  - (2) "LS4TJPBO1V00Y3A.sct", a script used to run the executable.
  - (3) "decoy.doc", a blank document.
- b. **Created processes.** Malware runs as "winc.exe" (32 Bit Application) and has a size of 6.4MB.
- c. **Persistence.** The malware creates a file "Win Setting Loader" in windows startup folder.

6. **Mitigation Methods.** Following mitigation measures are suggested in this regard:-

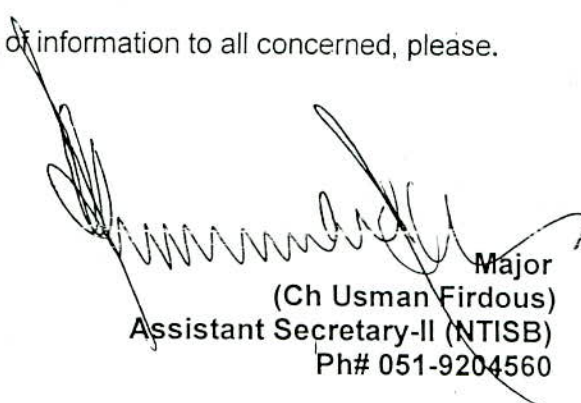
- a. Kill process "winc.exe" using Windows Task Manager.
- b. Delete the following dropped files.
  - (1) "%AppData1Local1Temp\winc.exe"
  - (2) "%AppData1Local1Temp\LS4TJPBO1V00Y3A.sct"
  - (3) "1AppData1Roaming1Microsoft1Windows1Start Menu1Programs1Startup1Win Setting Loader"
- c. Implement filters at the email gateway to filter out email with known indicators and block suspicious IP addresses at the firewall.



- for  
mei.
- d. Formulate a policy regarding suspicious emails so that all suspicious emails should be reported to the security or IT department.
- e. Provide employees basic cyber security awareness training.

7. **Recommendations**

- a. Do not respond to such fake telephone calls and avoid sharing details of products supplied to Pakistan Defence Forces.
- b. Install and update licensed and well reputed antiviruses such as Kaspersky, Avira, Avast etc.
- c. Block C&C Servers at Para 4d in firewalls of own networks.
- d. In case, if indicators of compromise (para 5) are found in the system, disconnect the computer from the internet and re-install Windows OS.
- e. Update all software including windows OS, Microsoft Office etc.
- f. Do not download attachments from emails unless you are sure about the source.
- g. Discard emails received from ambiguous/ fake domains mentioned at Para 2e.
8. Forwarded for perusal and dissemination of information to all concerned, please.

  
Major  
(Ch Usman Firdous)  
Assistant Secretary-II (NTISB)  
Ph# 051-9204560

**All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments**

Copy to :-

- SPS to Cabinet Secretary, Cabinet Division , Islamabad
- PS to AS-III, Cabinet Division, Islamabad
- APS to Secretary, NTISB
- APS to Deputy Secretary , NTISB