

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

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

Islamabad 2 Nov 2020

Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No. 19)**

1. **Introduction.** A malware has been found spreading through emails and social engineering that is specially designed to target Pakistan's army/ defense / intelligence organizations as well as DAs abroad in a well-planned targeted manner. These emails portray a legitimate looking document on "**Poland and Pakistan together for Security**". Downloading and clicking on fake document executes a malware in background which will compromise victim's machine.

2. **Summary of Malicious Email**

- a. **Email Subject.** Poland and Pakistan together for Security
- b. **MD5 Hash.** 1cf37a0a8a5f5704a3df692d84a16a71
- c. **Vulnerability ID.** CVE-2017-11882
- d. **Malware APT Group.** SideWinder
- e. **Download File.** Protocol.doc
- f. **Antivirus Detection Rate.** Low
- g. **File Size.** 702 KB
- h. **File Extension.** .doc
- i. **C&C Servers**

Ser.	URL	IP Address	Country
(1)	fqn-cloud.net	185.99133.58	New Zealand

3. **Indicators of Compromise**

- a. Files downloaded or rewritten from another process: -
  - (3) C:\ProgramData\SyncFiles\rekeywiz.exe
  - (4) C:\ProgramData\SyncFiles\Duser.dll
- b. Changes auto run value in registry: -
  - (1) HKCU\Software\Microsoft\Windows\CurrentVersion\Run with key Sync and value C:\ProgramData\TVFiles\rekeywiz.exe

4. **Capabilities of Malware**

- a. The RTF based malware is specially designed for targeted attacks and can steal files and keystrokes (along with stored usernames / passwords) from Windows system and browsers.
- b. The attacker can gain remote access of the system and can execute additional payload from it and run Microsoft certified files to evade antivirus detection.

*[Signature]* 4/11/22 SSL (IT)

03 NOV 2020

M(A)

~~M(IT)~~

A.S (Rev. Div.)

Chief (IT)  
CIO

FRK eDOX No. 1966478  
 Received in Member (IT)  
 4/11/2020

FRK eDOX No. 1966478  
 Received in Member (IT)  
 4/11/2020

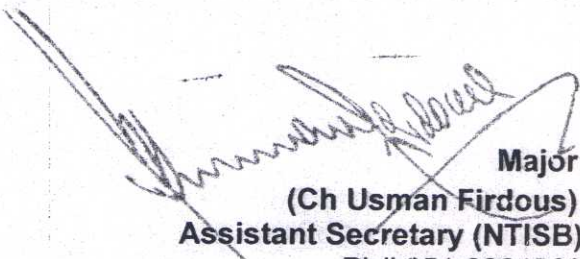
03 NOV 2020

- c. The adversary gets persistence through hooking by changing auto run value in the registry.

5. **Recommendations**

- a. **Regularly update well reputed antiviruses** such as Kaspersky, Avira, Avast etc. and scan system regularly.
- b. Update all software including Windows OS, Microsoft Office and all other on regular basis.
- c. Uninstall all **not in use applications and software** from system and personal phone.
- d. **Do not download attachments from emails unless you are sure about the source.**

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

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

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

**Copy to: -**

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-II, Cabinet Division, Islamabad
5. Secretary, NTISB, Cabinet Division, Islamabad
6. Deputy Secretary, NTISB, Cabinet Division, Islamabad
7. Director (IT), Cabinet Division, Islamabad