

**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. 20)

1. **Introduction.** Recently, a malware is spreading through social engineering that is targeting army / defense / intelligence organizations as well as DAs abroad in a well-planned targeted manner. These emails portray a legitimate looking **MOUs document regarding Pakistan-Philippines Agreement**. Downloading and clicking on fake document executes a malware in background that will compromise victim's machine.

2. **Summary of Malicious Email**

- a. **Subjects.** Pakistan-Philippines Agreement! MoU's.doc
- b. **MD5 Hash.** 2ba61596f9ec352eebe6e410a25867f6
- c. **Download File.** MoU's.doc
- d. **Vulnerability ID.** CVE-2017-11882
- e. **Malware APT Group.** SideWinder
- f. **Antivirus Detection Rate.** Low
- g. **File Size.** 806 Kbs
- h. **File Extension.** .doc
- i. **C&C Servers**

Ser.	URL	IP Address	Country
(2)	cdn-sop.net	172.93.188.161	Hong Kong

3. **Indicators of Compromise**

- a. Files downloaded or rewritten from another process: -
 - (1) C:\ProgramData\SyncFiles\rekeywiz.exe
 - (2) 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\SyncFiles\rekeywiz.exe**
- c. Creates Task scheduler for dual persistence: -
 - (1) Key UpdateService with value C:\ProgramData\SyncFiles\rekeywiz.exe

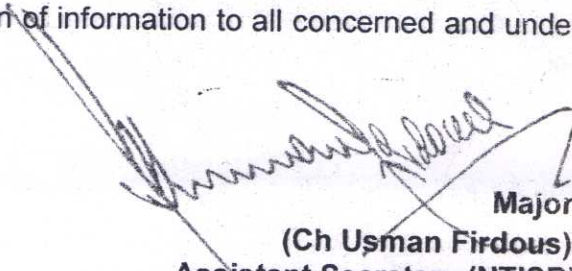
4. **Capabilities of Malware**

- a. The Rich Text Form (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.

03 NOV 2020
 M(A)
 M(IT)
 A.S (Rev. Div.)
 Chief (IT)
 CIO
 4/11/20
 196295-R
 0707 NOV 2020
 196295-R

4/11/22 SS(IT) -

- 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.
 - 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