

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

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

Islamabad 03 Dec, 2020

Subject: Advisory - Prevention Against Cyber Espionage (Advisory No. 25)

1. A malware is being spread through **social engineering tactics** targeting civil / military / intelligence organizations including DAs abroad in a well-planned targeted manner. For this purpose, attackers have crafted a malicious MS-Word file that looks like a legitimate document. Downloading and clicking on the fake MS-Word document executes a malware in the background on the target system / computer; eventually, the victim machine is compromised and becomes prone to data exfiltration. The crafted MS-Word document mimics as a verified Microsoft software thus rendering it undetectable through anti-virus.

2. Summary of Malicious Email

- a. **Subject.** Advisory-III - Postponement of Short Duration Training Courses due to COVID-19.
- b. **MD5 Hash.** bc7cb0f6bfcd3ble69fd630c2bbd5645
- c. **Download File.** Advisory-III.docx
- d. **Sender's Email.** ibrar.hussain.pak@gmail.com
- e. **Malware APT Group.** SideWinder
- f. **Vulnerability ID.** CVE-2017-11882
- g. **Antivirus Detection Rate.** Low
- h. **File Size.** 11 Kbs
- i. **File Extension.** .docx
- j. **C&C Servers**

Ser	URL addressIP	Address	Country
(1)	hashcheck.xyz	78.47.146.220	Germany

3. Indicators of Compromise

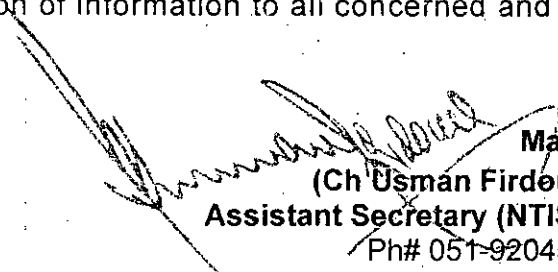
- a. Files downloaded or rewritten from another process: -
 - (1) C:\Users\admin\appdata\Local\Temp\bvm.t (581kb)
 - (2) C:\Users\admin\appdata\Local\Temp\pred.dll. (313kb)
- b. Creates Task scheduler for persistence: -
 - (1) Key \ byurt with description as JacaRg.dll and value as C:\Users1<admin>\Appdata\Roaming\Msolusn\Vtyrei.dll

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.
- c. The attacker runs malware through Equation Editor that read other registry keys for execution and transferred information through temporary files.
- d. The malicious files are customized libraries and turning source code files that execute through verified Microsoft programs.

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, Awan-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