

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

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

Islamabad 16 September 2020

**Subject: Advisory - Prevention Against Cyber Espionage (Advisory No.18)**

1. **Context.** Recently, a malware has been found spreading through spoofed emails that is targeting **Army / Defense / Intelligence Organizations** as well as **Defence Attaches** abroad in a well-planned targeted manner. These emails portray a legitimate looking **Ministry of Foreign Affairs document informing the recipient about his involvement in ongoing investigation regarding a Military Coup.** 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.** CIRCULAR 209/1312/BC/1011411
- b. **Spoofed Email address.** ... compliance-helpdesk@mofa.digital
- c. **Download File.** CIRCULAR 2091312BC1011411.doc
- d. **Antivirus Detection Rate.** Low
- e. **File Size.** 83 bytes
- f. **File Extension.** MS-word (.doc)
- g. **C&C Servers.**

Ser	URL Address	IP address	Country
(1)	https://world-dnld.com	109.235.65.11	Lithuania

3. **Capabilities of Malware**

- a. The malware is specially designed for targeted attacks and **steal files and keystrokes** (along with stored usernames / passwords) from windows system.
- b. The attacker can **gain remote access** of the system and can execute additional payload from it.

4. **Recommendations.**

- a. Install well reputed antivirus (AV) on the system such as kaspersky, Avira, Avast etc. Regularly update AV and scan the system.
- b. Update all software including Windows OS, Microsoft office and all other regular basis.
- c. Uninstall all software / applications from systems which are not in use.
- d. **Do not download attachments from emails unless you are sure about the source.**

SS (IT)

23/9/20

PRAL

21 SEP 2020

Y(A)

I(I.T)

A.S (Rev. Div)

FER eBOX No. 165603  
 Received in Member (IT)  
 Date: 23/9/2020  
 Reviewed by Member's Sectt  
 on 21 SEP 2020

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

Lieutenant Colonel  
(Kamran Rashid)  
Deputy 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