

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

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

Islamabad, 18 August, 2018

17 AUG 2018
M(A)
M(I.T)

Subject: Advisory - Prevention Against Windows Banking Trojan "Emotet"
(Advisory No 149)

Introduction. A malware named "Emotet" has been spreading through emails, social media and targeting windows based users. This malware is highly sophisticated, undetectable banking trojan capable of stealing sensitive information causing disruption to regular operations.

A.S (Rev. Div.)

2. Technical Analysis

- a. Emotet is an advanced, modular banking Trojan that primarily functions as downloader or dropper of other banking Trojans.
- b. Malware use several methods for maintaining persistence, including auto-start registry keys and services.
- c. It uses modular Dynamic Link Libraries (DLLs) to continuously evolve and update its capabilities.
- d. Malware can also evade signature based detection mechanism due to its polymorphic design.
- e. Malware is spreading via posts on Facebook groups, malspam (emails containing malicious attachments or links) and whatsapp messages encouraging users to visit hackers-controlled fake websites.
- f. Emotet artifacts are typically found in arbitrary paths located at AppData\Local and AppDataRoaming directories.

3. Mitigation Measures. Following mitigation measures are suggested in this regard:-

- a. Use Group Policy Object to set a windows Firewall rule for restricting inbound SMB communication between client systems.
- b. Use antivirus programs, with automatic updates of signatures and software, on clients and servers.
- c. Vendors release security patches times to time, apply appropriate patches and software updates immediately.
- d. Implement filters at the email gateway to filter out emails with known indicators; such as known malicious subject lines and block suspicious IP addresses at the firewall.
- e. Formulate a policy regarding suspicious emails so that all suspicious emails should be reported to the security or IT

FBR eDOX No. 99211-R
Received in Member (IT)
Dated 28/8/18

99211-R
CC (IT)
ep
17 AUG 2018
FBR eDOX Dy. No. /Ch. Sectt
Received in

Department.

f. Provide **employees** basic **cyber security** awareness training.

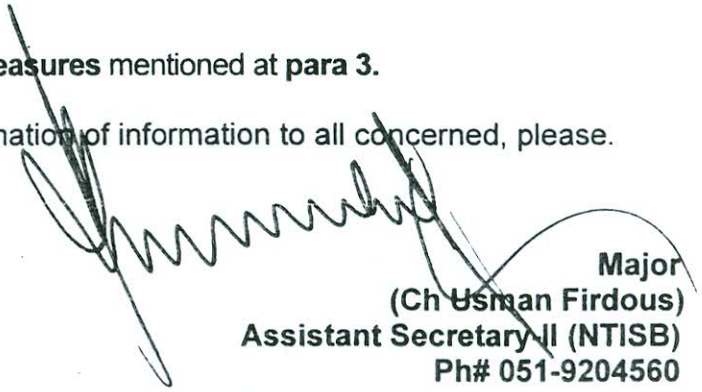
4. **Recommendations**

a. **Install** and **update** well .reputed antivirus such as **Kaspersky**,
Bitdefender, Nod32 and **Avast** etc.

b. Regularly update all software's including **Windows OS, Microsoft Office** and
all other software's.

c. Strictly follow all **mitigation measures** mentioned at **para 3**.

5. 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 Secretary, NTISB

APS Deputy Secretary, NTISB