

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

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

Islamabad 10 August, 2018

Subject: Prevention Against Cyber Espionage (Advisory No 147)

1. **Introduction.** A malicious email "GE 2018 final checklist-personal postal ballot assignment" is being sent to officers and staff of defense/ intelligence organizations. Email contains a malware hidden in ZIP file, containing malicious executables. Downloading and running the file, executes malware in background that results in hacking of the computer.

2. **Summary of Malicious Emails**

- a. **Subjects.** GE 2018 final checklist-personal postal ballot assignment
- b. **Name of Attachments.** ECP 2018 checklist.zip
- c. **Antivirus Detection Rate of Extracted Files**

Ser	Files extracted	Detection Rate	Percentage %
(1)	ECP emergency and complaint.xls	20/64	31.2
(2)	List ECP Alerts.xls	20/67	29.9
(3)	OFFICIALS SMS SERVICES.xls	33/67	49.2
(4)	ieflash.exe	20/67	29.9
(5)	fileman.exe	47/66	71.2

- d. **Malware Type.** Trojan based Keylogger
- e. **C&C Servers**

Ser	C&C URL	IP Address	Hosting Country
(1)	h88-150-138-77.host.redstation.co.uk	88.150.138.77	UK

3. **Technical Analysis.**

a. **Indicators of Compromise.** The malware makes following files on the infected system:-

- (1) C:\Windows\Temp\fileman.exe. (Original name is services.exe)
- (2) C:\Users\admin\AppData\Roaming\MicrosoftWindows\Start Menu\Programs\Startup\ieflash64.exe. Original name is native.exe
- (3) Registry key at Path and having Key: "TSUSERENABLED" "HKLM\SYSTEM\CONTROLSET001\CONTROL\TERMI ALSERVER
- (4) The malware is being spread through Google drive link

M(A)
M(I.T) ✓
A.S (Rev Div.)

CCD
7/3/18

FBR eDOX No. 97234-l
Received in Member (IT)
Dated: 13/8/18
97234-l
13 AUG 2018
FBR eDOX Dy. No.

Sarf
2

b. **Capabilities of Malware.**

- (1) The malware is capable of getting system **IP, user, location, network configuration details**, computer configurations and it can upload these details on its **C&C server** mentioned at **para 2(e)**.
- (2) The malware has the ability to act as a **key logger** and steal the **usernames** and **passwords** of infected systems.
- (3) The malware can Copy itself into registry and it can **automatically execute** itself on windows boot.
- (4) This trojan establishes and maintains continuous communication with its C&C server.

4. **Recommendations.**

- a. **Install and update licensed and well reputed antiviruses** such as Kaspersky, Avira, Avast etc.
 - b. Block C&C Servers at para 2(e) in **firewalls** of own networks.
 - c. In case if **indicators of compromise (para 3a)** are found in the system, please disconnect the computer from internet and **reinstall windows**.
 - d. **Update all softwares** including **Windows OS, Microsoft Office**.
 - e. **Don't download** attachments from **emails unless** you are sure about the source.
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