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

No. 1-5/2003 (NTISB-II) Islamabad 25th June 2019

Subject: **Advisory – Prevention Against Targeted Malware Campaign (Advisory No. 17)**

M(A)

M(I.T)

A.S(Ra. Div.)

1. **Introduction.** A targeted malware campaign titled as **"Advance Salary For All MOFA Members"** is being sent to officers and staff of **civil, Defense / Government organizations** via spoofed email. The email contains a link to a **temporarily hacked website** to download a malicious excel attachment. Downloading and **enabling macros** from the **file executes malware in background** that results in hacking of the system.

2. **Summary of Malicious Email Attack**

a. **Subject.** Advance Salary For All MOFA members

b. **Name of Attachments.** Credit _Score.xls, Advance_Salaries.xls

c. **File Size.** 125.02 KB

d. **File Extension.** Microsoft Execel File Format (.xls)

e. **Malware Type.** Macro based Malware

f. **Spoofed Email.** Secure.service.net@gmail.com

g. **Antivirus Detection Rate.** 09/71 (12.67%)

h. **Threat Level.** Critical

i. **C & C Services**

Ser	C & C URL	C & C IP address	IP Location
(1)	Servicejobs.life	179.43.170.155	Switzerland

Send to FATE
As per practice Uploaded on website for info
1.7.2019

Chief IT/BD

j. **Malware Hash**

(1) 23b4dbbe5f3a44798312c1fd66117221 **(Advance_Salary.xls)**

(2) dc94af615c0baf3bcbbb71750917fc **(Credit_score.xls)**

S/S-IT
Send to fate ung

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

a. C:\Users\<admin>\DriveData\Wins\yldss.exe

b. C:\Users\<admin>\DriveData\Wins\x6teyst.txt

c. C:\Users\<admin>\AppData\Roaming\x6teyst.bat

d. C:\Users\<admin>\DriveData\Files\win.txt

4. **Capabilities of Malware**

a. Malware can read user's **system information** i.e. operating system details, network, IP, route & interfaces details, Windows Services Information, System Information, Computer Name, processes information from the victim's computer and uploads it to C & C server.

b. After fetching **basic information** about the system, it acts as a **backdoor** and has the capability **for file listing, uploading of data and key logging**.

c. The malware is preprogrammed **to run after every 1 hour to flush data onto its C & C server**.

5. **Recommendations.** In order to safeguard from this targeted malware espionage attempt, following measures are recommended: -

a. **Use a botnet detection tool** from **https://tiny.cc/agh56y** to detect the presence of **this particular malware**. If found infected, then please contact your system administrator or **backup your data and reinstall windows. In case if indicators of compromise (para 3) are found in the system, please disconnect the computer form internet and reinstall Windows**.

b. **Install and regularly update well reputed licensed anti-malware solutions. Software Restriction Policies (SRP) must be implemented to block binaries executing from %APPDATA% and %TEMP% locations as most malware runs from these paths.**

c. **Monitor and block** malicious connections with IPs mentioned in para2(i) **for detection of infected client machines.**

d. **Users are advised to disable RDP (Remote Desktop Protocol) if not in use**, if required it should be accessed **through firewall**.

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

Major
(Ch Usman Firdous)
Assistant Secretary-II (NTISB)
Tel#051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Government.

5. SPS to Cabinet Secretary, Cabinet Division Islamabad
6. PS to AS-III, Cabinet Division Islamabad
7. APS to Secretary, NTISB, Cabinet Division Islamabad
8. APS to Deputy Secretary, NTISB, Cabinet Division Islamabad