"SAVE TREES & PROTECT ENVIRONMENT"

TOP PRIORITY.

042-99212223

No.E&A(FD)11-6/2012

GOVERNMENT OF THE PUNJAB
FINANCE DEPARTMENT

Dated Lahore, the 21st June, 2021.

To

- The President, Bank of Punjab, Lahore.
- The Chairperson, Punjab Revenue Authority, Lahore.
- The Chairperson, Appellate Tribunal, Punjab Revenue Authority.
- All Additional Finance Secretaries, Finance Department.
- The Chief Inspectorate of Treasuries, Lahore.
- The Provincial Director, Local Fund Audit, Lahore.
- The General Manager, Punjab Pension Fund, Lahore.

Subject:- **ADVISORY – PREVENTION AGAINST CYBER ESPIONAGE (ADVISORY NO.40).**

I am directed to refer to the subject cited above and to enclose herewith copy of circular letter No.SO(FG)3-72/2021, dated 11.06.2021 alongwith enclosure (which are self-explanatory), received from the Section Officer (FG-I), Government of the Punjab, S&GAD (I&C Wing), for information and further necessary action accordingly.

SECTION OFFICER (E&A)

C.C.

(i) PS to Finance Secretary.
(ii) PSs to Spl. Secretary Finance (B&R) & Spl. Secretary Finance (E&CF).

PAIAFS (FD)
No: 1673-L
Dated 24/6/21

22/06/2021
System Analyst

D:\1-E DATA\Steno\2021\Circulars.doc

TOP PRIORITY

35610

No.SO(FG)3-72/2021
GOVERNMENT OF THE PUNJAB
SERVICE &GENERAL ADMINISTRATION DEPARTMENT
(I&C WING)

Dated Lahore, the 11 June, 2021

To

1. The Additional Chief Secretary, Punjab.
2. The Chairman, P&D Board.
3. The Senior Member, Board of Revenue, Punjab.
4. All the Administrative Secretaries, Government of the Punjab.
5. The Inspector General of Police, Punjab.
6. All the Divisional Commissioners in Punjab.
7. The Chairman, Punjab Information Technology Board.

SSF (B&R)	✓
SSF (E&CF)	
AFS (B)	
AFS (SS)	
AFS (ES)	
AFS (PS)	
AFS (LGF)	
AFS (R)	
AFS (P&R)	
DIR (M)	
CIO'T	
HEAD-CFU	

4448
16.6.21

AFS(B)
16/6/21
PSSSF I&C R

Subject:- **ADVISORY – PREVENTION AGAINST CYBER ESPIONAGE (ADVISORY NO.40).**

I am directed to refer to the subject cited above and to enclose herewith a copy of letter No.1-5/2003(NTISB-II) dated 03.06.2021 received from Assistant Secretary-II (NTISB), Government of Pakistan, Cabinet Secretariat, National Telecom and Information Technology Security Board (NTISB), Islamabad for necessary action and further distribution to field formation for compliance, please.

AFS(B) 2029 17-6-21

FS DS(A) 17/6

11.6.21

(ZERVA SADIQ PMS)
(SECTION OFFICER (FG-I)

C.C:-

1. Assistant Secretary-III (NTISB), Government of Pakistan, Cabinet Secretariat, National Telecom and Information Technology Security Board (NTISB), Islamabad w/r/t his letter referred above.
2. PS to Secretary (I&C), S&GAD.

AS (Regt & Admn) FD
Dy. No. 1093
17-6-21

SO E&A (FD)
Dy. No. 4081
Dated 18/6/21

NO: R&I. FD
15 JUN 2021
35585
FINANCE

Special Secy. (B&R)
16 JUN 2021
1146-P
Finance

SO (E&A)	
SO (W&M)	
SO (Loans)	
SO (Imp.)	
SO (Liaison)	

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

No. 1-5/2003 (NTISB-II) Islamabad 3 June, 2021

Subject: - **Advisory - Prevention against Cyber Espionage (Advisory No.40)**

1. Recently, phishing emails containing malware links have been received at official email accounts of top ranked Civil and Military officials including posted abroad. Clicking on such malicious links / URLs may result in data breach and sensitive data leakage. Therefore, an advisory is attached at **Annexure-A** to sensitized all concerned to adopt preventive measures against phishing emails links and implement suggested guideline.

2. Forwarded for information and dissemination 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: -

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-III, Cabinet Division, Islamabad
5. Director General (Tech), Directorate General, ISI, Islamabad
6. Secretary, NTISB, Cabinet Division, Islamabad
7. Deputy Secretary, NTISB, Cabinet Division, Islamabad
8. Director (IT), Cabinet Division, Islamabad

Annex-A

Subject: - **Advisory - Prevention against Cyber Espionage (Advisory No. 41)**

1. Recently, phishing emails containing malware links have been received at official email accounts of top ranked Civil and Military officials including posted abroad. Clicking on such malicious links / URLs may result in data breach and sensitive data leakage. The attached files in emails look legitimate but contain embedded malicious links leading to malware execution in the background. Such malware may use **DLL hijacking technique** and executables such as "**software_reporter_tool.exe**".

2. **Summary of Malicious Email.** CVE-2017-11882

   a. **APT Group.** SideWinder APT

   b. **File Name.** Building Port Resilience against Pandemics.docs

   c. **Antivirus Detection Rate.** Low

   d. The malicious files are hosted on C&C Server as under: -

Ser	URL address	IP Address	Country
(1)	Pmaesa.bahariafoundation.org	5.252.195.27	Russia

3. **Capabilities of Malware**

   a. The Rich Text Format (RTF) based malware is specially designed for targeted attacks and can steal files / stored passwords from windows system and browsers.

   b. The attack involves windows certificates alterations to reside for persistence.

   c. The malware employs sleep function as defensive technique and checks for presence of debugger.

   d. The malware uses attack techniques **DLL hijacking** and attack based on **javascript.**

   e. The attacker can gain remote access of the system and can execute additional payload from it and run through certified file "**software_rempval_tool.exe**" to evade antivirus detection.

4. **Recommendations**

   a. IT setup within the, organization should **disable Microsoft Equation Editor in Office from registry** to avoid such attacks.

Cont'd.....P/2

b. Microsoft executables including **Verclsid, Rundll32, Regsvr32, Regsvcs / Regasm, Odbcconf, MSiexec, Mshta, InstallUtil, CMSTP, ControlPanel, Compiled HTML File** to be monitored as major malware executables and must be blacklisted.

c. Do not download attachments from emails unless you are sure about the source.

d. Window Defender and Firewall of system to be kept on as recommended settings.

e. Be vigilant regarding redirected links and typing sensitive information online.

4 **Reporting of Suspicious Files / Emails.** Any malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures: -

asntisb2@cabinet.gov.pk

5. Forwarded for information and dissemination to all concerned, please.

* * * * *

TOP PRIORITY

35608

No.SO(FG)3-72/2021
GOVERNMENT OF THE PUNJAB
SERVICE &GENERAL ADMINISTRATION DEPARTMENT
(I&C WING)

Dated Lahore, the 11 June, 2021

To

SSF (B&R)	✓
SSF (E&CF)	
AFS (B)	
AFS (SS)	
AFS (ES)	
AFS (PS)	
AFS (LGF)	
AFS (R)	
AFS (P&R)	
DIR (M)	
CIOT	
HEAD-CFU	

1. The Additional Chief Secretary, Punjab.
2. The Chairman, P&D Board.
3. The Senior Member, Board of Revenue, Punjab.
4. All the Administrative Secretaries, Government of the Punjab.
5. The Inspector General of Police, Punjab.
6. All the Divisional Commissioners in Punjab.
7. The Chairman, Punjab Information Technology Board.

AFS(B)

16.6.21 PS SSF (B&R)

4449
16.6.21

Subject:- **ADVISORY – PREVENTION AGAINST CYBER ESPIONAGE (ADVISORY NO.40).**

I am directed to refer to the subject cited above and to enclose herewith a copy of letter No.1-5/2003(NTISB-II) dated 03.06.2021 received from Assistant Secretary-II (NTISB), Government of Pakistan, Cabinet Secretariat, National Telecom and Information Technology Security Board (NTISB), Islamabad for necessary action and further distribution to field formation for compliance, please.

2081
17-06-21

FS. DS(A)

11.6.21

(ZERVA SADIQ PMS)
(SECTION OFFICER (FG-I)

C.C:-

1. Assistant Secretary-II (NTISB), Government of Pakistan, Cabinet Secretariat, National Telecom and Information Technology Security Board (NTISB), Islamabad w/r/t his letter referred above.
2. PS to Secretary (I&C), S&GAD.

NO: R&I, FD(I)
15 JUN 2021
35582
FINANCE

Special Secy. (B&R)
16 JUN 2021
1147
Finance

SO (E&A)	
SO (W&M)	
SO (Loans)	
SO (Imp.)	
SO (Liaison)	

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

No. 1-5/2003 (NTISB-II) Islamabad 3 June, 2021

Subject: - **Advisory - Prevention against Cyber Espionage (Advisory No.40)**

1. Recently, phishing emails containing malware links have been received at official email accounts of top ranked Civil and Military officials including posted abroad. Clicking on such malicious links / URLs may result in data breach and sensitive data leakage. Therefore, an advisory is attached at **Annexure-A** to sensitized all concerned to adopt preventive measures against phishing emails links and implement suggested guideline.

2. Forwarded for information and dissemination 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: -

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-III, Cabinet Division, Islamabad
5. Director General (Tech), Directorate General, ISI, Islamabad
6. Secretary, NTISB, Cabinet Division, Islamabad
7. Deputy Secretary, NTISB, Cabinet Division, Islamabad
8. Director (IT), Cabinet Division, Islamabad

Annex-A

Subject: - **Advisory - Prevention against Cyber Espionage (Advisory No.4/21)**

1. Recently, phishing emails containing malware links have been received at official email accounts of top ranked Civil and Military officials including posted abroad. Clicking on such malicious links / URLs may result in data breach and sensitive data leakage. The attached files in emails look legitimate but contain embedded malicious links leading to malware execution in the background. Such malware may use **DLL hijacking technique** and executables such as "**software_reporter_tool.exe**".

2. **Summary of Malicious Email.** CVE-2017-11882

   a. **APT Group.** SideWinder APT

   b. **File Name.** Building Port Resilience against Pandemics.docs

   c. **Antivirus Detection Rate.** Low

   d. The malicious files are hosted on C&C Server as under: -

Ser	URL address	IP Address	Country
(1)	Pmaesa.bahariafoundation.org	5.252.195.27	Russia

3. **Capabilities of Malware**

   a. The Rich Text Format (RTF) based malware is specially designed for targeted attacks and can steal files / stored passwords from windows system and browsers.

   b. The attack involves windows certificates alterations to reside for persistence.

   c. The malware employs sleep function as defensive technique and checks for presence of debugger.

   d. The malware uses attack techniques **DLL hijacking** and attack based on **javascript.**

   e. The attacker can gain remote access of the system and can execute additional payload from it and run through certified file "**software_rempval_tool.exe**" to evade antivirus detection.

4. **Recommendations**

   a. IT setup within the, organization should **disable Microsoft Equation Editor in Office from registry** to avoid such attacks.

Cont'd.....P/2

b. Microsoft executables including **Verclsid, Rundll32, Regsvr32, Regsvcs / Regasm, Odbcconf, MSiexec, Mshta, InstallUtil, CMSTP, ControlPanel, Compiled HTML File** to be monitored as major malware executables and must be blacklisted.

c. Do not download attachments from emails unless you are sure about the source.

d. Window Defender and Firewall of system to be kept on as recommended settings.

e. Be vigilant regarding redirected links and typing sensitive information online.

4 **Reporting of Suspicious Files / Emails.** Any malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures: -

asntisb2@cabinet.gov.pk

5. Forwarded for information and dissemination to all concerned, please.

* * * * *