

F. No. 3(5)/2023-NTISB-EW
Government of Pakistan
Ministry of Science & Technology

Islamabad, the 23rd February, 2024

- | | | |
|---|---|--|
| 1. The Chairman,
PCSIR, <u>Islamabad.</u> | 2. The Chairman,
PSF, <u>Islamabad.</u> | 3. The Chairman,
PCST, <u>Islamabad.</u> |
| 4. The Chairman,
PEC, <u>Islamabad.</u> | 5. The Chairman,
CWHR, <u>Karachi.</u> | 6. The Rector,
CUI, <u>Islamabad.</u> |
| 7. The Rector,
NUST, <u>Islamabad.</u> | 8. The Rector,
NUTECH, <u>Islamabad.</u> | 9. The Director General,
PNAC, <u>Islamabad.</u> |
| 10. The Director General,
PCRET, <u>Islamabad.</u> | 11. The Director General,
NIE, <u>Islamabad.</u> | 12. The Director General,
PHA, <u>Islamabad.</u> |
| 13. The Director General,
PSQCA, <u>Karachi.</u> | 14. The Director General,
NIO, <u>Karachi.</u> | 15. The Managing Director,
STEDEC, <u>Lahore.</u> |

Subject: Cyber Security Advisory – Fake/ Malicious Website Spoofed as Legitimate Government Website (MoIT&IT /FIA) (Advisory No. 01).

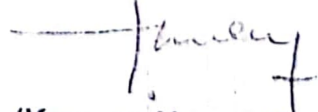
Cyber Security Advisory – Apple Products Zero Day Attack Latest Mitigation Measures (Advisory No. 02)

Pakistan's Digital Blackout – Fake Propaganda and Response Initiative at Financial Sector (Advisory No. 03).

Dear Sir/ Madam,

Please find enclosed herewith the subject advisories received from National Telecom and Information Technology Security Board (NTISB) Cabinet Division, for information and strict compliance.

Encl: As above


(Kamran Nawaz Khan)
Deputy Electronics Adviser-I
051-9216304

Copy for Information to:

- i. APS to JEA, MoST.
- ii. Network Administrator, MoST.

**GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)**

F. No. 1-5/2003/24(NTISB-II)

Islamabad, the 13 February, 2024


Subject: - Cyber Security Advisory – Fake/Malicious Website Spoofed as Legitimate Government Website (MoIT&T/FIA) (Advisory No. 01)

Introduction. A new spoofed website impersonating as legitimate government website (MoIT&T/FIA) used for hacking purposes (spreading via SM channels) by hacker groups has been identified. Details of spoofed websites are as follows:

Ser	Website	Purpose	C&C/IP	Linkage
a.	https://moitt-govv-pk.fia-gov.net	Hacking bait via spoofing	77.83.196.59 (HZ Hosting Ltd, Poland, Europe)	SideWinder APT (India)
b.	https://moitt-gov-pk.fia-gov.net/364896null/file.rtf			

2. **Mitigation.** Above in view, please avoid opening/testing above mentioned websites. Also, IT administrator are requested to blacklist said website/C&C servers (where applicable).

3. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.


(Muhammad Usman Tariq)
 Assistant Secretary-II (NTISB)
 Ph# 051-9204560

All Secretaries of Ministries/Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

Copy to:

1. Principal Secretary to the PM, Prime Minister's 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), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

JS (Admin)	
JS (Op)	
CSAO	
JEA	✓
JTA	
JSA (D)	
JSA (PRC)	
JSA (L&R)	

SECRETARY MOST
 Dy. No. 875
 Dated: 21-02-24

JEA
 Dy. No. 142
 Dated: 21/02/24

DEJA-IT
 DEJA-II
 2023
 JEA

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

F. No. 1-5/2003/24(NTISB-II)

Islamabad, the 13 February, 2024

Subject: - Cyber Security Advisory – Apple Products Zero Day Attacks Latest Mitigation Measures (Advisory No. 02)

Introduction. Recently, Kaspersky has introduced a lightweight method called iShutdown to detect zero click spywares e.g. Pegasus, Reign and Predator on Apple iOS devices.

2. **Technical Details.** Kaspersky analyzed Shutdown.log file present within the sysdiagnose archive further identifying anomalies during reboots linked to Pegasus. Entries in the log file indicated reboot delays caused by sticky spyware processes. The log file also showed a common infection path (/private/var/db) shown by other iOS malware families.

3. **Mitigation Measures.** To Safeguard against advanced spyware on iOS, following recommendations must be incorporated:

- a. Reboot the device daily/regularly as it causes hindrance for attacker by compelling them to infect devices each time after reboot.
- b. Enable lockdown mode on the device to block iOS malware infection.
- c. Disable iMessage and FaceTime on the device which can serve as an attractive exploitation vector.
- d. Avoid clicking on suspicious links received in messages, SMS other messengers or emails.
- e. Regularly check backups and sysdiags (system diagnosis) for potential malware.
- f. Install latest OS version and keep all applications updated.
- g. Additionally, use Kaspersky's new self-check spyware detection tool available on GitHub. (<https://www.github.com/KasperskyLab/iShutdown>)

SECRETARY MOST
Dy. No. 549
Dated 21-02-24

JEA 139
Dy. No. 31/02/24
Dated 31/02/24

JS Action	✓
JS LOG	
CFAC	
SI	✓
JIP	
JS-1	
JS-2	
JS-3	
JS-4	
JS-5	
JS-6	
JS-7	
JS-8	
JS-9	
JS-10	

DEA-I
DEA-II
DEA-III
22/2
JEA

5. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.



(Muhammad Usman Tariq)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries/Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

Copy to:

1. Principal Secretary to the PM, Prime Minister's 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), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

**GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)**

F. No. 1-5/2003/24(NTISB-II)

Islamabad, the 16th February, 2024

Subject: - Pakistan's Digital Blackout – Fake Propaganda and Response Initiative at Financial Sector (Advisory No. 03)

Resilient National Cyber Space and Critical Information Infrastructure (CII) play a significant role in the national security and economy, requiring a comprehensive framework for fail-safe protection. Pakistan's CII is vulnerable to cyber-attacks due to non-implementation of requisite cyber security (CS) measures/best practices. Hence, the existing vulnerabilities are not only exploited but also used as an add-on to launch fake propaganda by the Hostile Intelligence Agencies (HIAs).

2. A few examples depicting fake propaganda observed are as under:

- a. **Dec 2023.** An Indian hacker group "**Vanguard**" claimed to have taken down Pakistan's .gov.pk domain. Fake propaganda claims disarray of Government agencies, educational institutions and public service websites, leaving the citizens frustrated and businesses scrambling.
- b. **Jan 2024.** An Indian hacker group "**ÜCC Error 404 Team**" claimed to have hacked/defaced Pakistan's critical websites including Govt of Pak, Defence, Aviation and Banking Sector. The fake propaganda made by the hacker group co-related the attack with the Indian Republic Day (26 Jan).

3. Dark Web analysis and the above shared information depicts that threat from a number of hacker groups targeting financial/banking sector of Pakistan is imminent. In the prevailing environment, there is a dire need to ensure implementation of robust CS measures by all Federal Ministries/Divisions, CII especially SBP (in collaboration with Ministry of Finance and Banking sector). It is pertinent to mention that the following advisories on the subject have already been shared with all stakeholders:

- a. Cyber Security Advisory - Surge in Financial/Banking Scams & Prevention (Advisory No. 43, dated 4th August, 2023)
- b. Cyber Security Advisory - Prevention Against Financial Scam Activities - Impersonation as Govt Officials (Advisory No. 53, dated 8th September, 2023)

SECRETARY MOST
Dy. No. 140
Dated: 27-02-24

JEA
Dy. No. 140
Dated: 27-02-24

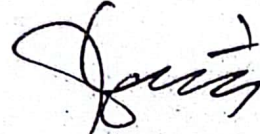
AS	
JS (Admin)	
JS (Gen)	
CPAC	
IA	✓
JIA	
JS (IT)	
JS (PAC)	
JS (Legal)	

27/2/24

JEA

[Signature]

4. All Ministries/Divisions and SBP are advised to caution affiliated setups and ensure that necessary CS measures/safeguards are in place to deter imminent threat.
5. **SBP Only.** SBP is requested to disseminate the information with the Banking Sector immediately and share certificate of compliance with NTISB (Cabinet Division) on priority.
6. This issues with the approval of the Competent Authority.



(Muhammad Usman Tariq)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

Governor State Bank of Pakistan,
SBP, Head Office, 3rd Floor,
I.I. Chundrigar Road,
Karachi.

All Secretaries of Ministries/Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

Copy to:

1. Principal Secretary to the PM, Prime Minister's 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), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad