No.DG-II/Cyber.Advisory/4/0030001/2024

GOVERNMENT OF SINDH
INFORMATION, SCIENCE & TECHNOLOGY
DEPARTMENT

Karachi dated the 28th February, 2024

Subject : **Cyber Security Advisory – Fake / Malicious Website Spoofed as Legitimate Government Websites (MoIT&T/FIA) (Advisory No.003001)**

Introduction : A new spoofed website impersonating as legitimate government website (MoIT&T/FIA) used for hacking purpose (spreading via SM channels by hacker groups has been identified . Detail 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)	Side Winder 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.

28/2-24.

(DR. RANA SHAHZAD QAISER)
DIRECTOR GENERAL-II

To,

The Secretary,

_____Department,
Government of Sindh,
KARACHI.

A copy is forwarded for information and necessary action to:-

1. The NTIS-II), Cabinet Secretariat, Cabinet Division(NTISB), Gov. of Pakistan
2. PS to chief Secretary, Sindh
3. PS to Secretary (I&C), SGA & CD, Govt. of Sindh Karachi.
4. Staff Officer to Secretary, IS&TD, Government of Sindh.
5. Webmaster, for uploading the advisory on URL http:www.sindh.gov.pk

No.DG-II/Cyber.Advisory/4/004002/2024

GOVERNMENT OF SINDH
INFORMATION, SCIENCE & TECHNOLOGY
DEPARTMENT

Karachi dated the 28th February

Subject: **Cyber Security Advisory – Apple Products Zero Day Attack Latest Mitigation Measures (Advisory No : 004002)**

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

2. **Technical Details.b** 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 again 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)

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

(DR. RANA SHAHZAD QAISER)
DIRECTOR GENERAL-II

To,

The Secretary,

_____Department,

Government of Sindh,

KARACHI.

A copy is forwarded for information and necessary action to:-

1. The NTIS-II), Cabinet Secretariat, Cabinet Division(NTISB), Gov. of Pakistan
2. PS to chief Secretary, Sindh
3. PS to Secretary (I&C), SGA & CD, Govt. of Sindh Karachi.
4. Staff Officer to Secretary, IS&TD, Government of Sindh.
5. Webmaster, for uploading the advisory on URL http:www.sindh.gov.pk

GOVERNMENT OF [illegible]
INFORMATION, SCIENCE & TECHNOLOGY
DEPARTMENT

Karachi dated the 28th February

SUBJECT: **Pakistan's Digital Blackout- Fake Propaganda and Response Initiative at Financial Sector (Advisory No; 005003)**

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 (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 to launch fake propaganda by the Hostile intelligence agencies (HIA's).

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 institution and public service Websites, leaving the citizens frustrated and business scrambling.

b. Jan 2024 — An Indians hacker group "CCC Error 404 Team" claimed to have hacked/defaced Pakistan's critical website 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)

Dark Web analysis and the above shared information depicts that threat from a number of hacker group 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 withal stakeholders .

a. cyber Security Advisory – Surge in Financial/ Banking . Scam & 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)

4. All Ministries / Divisions and SBP are advised to caution affiliated setup 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 competent Authority.

(DR. RANA SHAHZAD QAISER)
DIRECTOR GENERAL-II

The Secretary,

_____Department,
Government of Sindh,
KARACHI.

A copy is forwarded for information and necessary action to:-

1. The NTIS-II), Cabinet Secretariat, Cabinet Division(NTISB), Gov. of Pakistan
2. PS to chief Secretary, Sindh
3. PS to Secretary (I&C), SGA & CD, Govt. of Sindh Karachi.
4. Staff Officer to Secretary, IS&TD, Government of Sindh.
5. Webmaster, for uploading the advisory on URL http:www.sindh.gov.pk