No.10(6)/2016-Coord
Government of Pakistan
Ministry of Science and Technology
******

Islamabad, 19th September, 2022

1. The Chairman, PCSIR, **Islamabad.**	2. The Director General, NIO, **Karachi.**	3. The Director General, PSQCA, **Karachi.**
4. The Chairman, PSF, **Islamabad.**	5. The Rector, CU, **Islamabad.**	6. The Director General, NIE, **Islamabad.**
7. The Chairman, PCST, **Islamabad.**	8. The Director General, PNAC, **Islamabad.**	9. The Rector, NUST, **Islamabad.**
10. The Director General, PCRET, **Islamabad.**	11. The Chairman, CWHR, **Karachi.**	12. The Chairman, PEC, **Islamabad.**
13. The Rector, NUTECH, **Islamabad.**	14. The Managing Director, STEDEC, **Lahore.**	15 The Director General, PHA, **Islamabad.**
16. The Managing Director, NEECA, **Islamabad.**		

Subject: **CYBER SECURITY ADVISORY – WORDPRESS SITES HACKED WITH FAKE CLOUDFLARE DDoS ALERTS PUSHING (ADVISORY NO.37)**

(ii) CYBER SECURITY ADVISORY – PREVENTION AGAINST FRAUDULENT WEBSITE (ADVISORY NO.38)

(iii) PREVENTIVE MEASURES AGAINST CYBER-ATTACKS ON INDEPENDENCE DAY 22 (ADVISORY NO.39)

(iv) CYBER SECURITY ADVISORY – PLAY STORE APPS SPYING ON ANDROID USERS USING FACE STEALER (ADVISORY NO.40)

Please find enclose herewith a copy of Cabinet Division's, Cabinet Secretariat (NTISB) Letters No.1-5/2003(NTISB-II) dated 13th September, 2022 on the subject cited above for information & compliance.

Encl: As above.

(HARIS BIN TARIQ)
Section Officer (Coord)
Tel: 9202520

Copy for information to:-

i. PS to Secretary, MoST.
ii. PS to Additional Secretary, MoST.
iii. PA to Joint Secretary (Org), MoST.
iv. PA to Sr. Joint Secretary (Admn), MoST.
v. All heads of Wing's, MoST.
vi. Network Administrator, MoST.

342/DEA-III
15/09-2022

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

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

Islamabad, the 13th September, 2022

Subject: - **Cyber Security Advisory – WordPress Sites Hacked with Fake Cloudflare DDoS Alerts Pushing (Advisory No. 37)**

JEA 1421 15-9-22

Addl. SECRETARY MoST Dy. No. 6066 Date 14-9-22

Deputy Secretary (Admin) Dy. No. 7168 Date: 15-9-2022

SECRETARY MOST Dy. No: 4311 Date: 14-9-22

Context. WordPress is a free and open source content management system written in PHP, supported with HTTPS and paired with My SQL and MariaDB database. Recently, it has been observed that websites developed in WordPress are being hacked to **display fake Cloudflare DDoS protection pages**. The fake pages are used to distribute malware that install **NetSupport RAT** and **RaccoonStealer password-stealing Trojan**.

2. **Malware Details**. Working mechanism of fake DDoS protection pages is as under:-

a. **DDoS protection screens** are used for protecting sites from bots, aiming to overwhelm them with garbage traffic. These screens provided with opportunity for malware campaigns where **threat actors** are hacking poorly protected WordPress sites to add a **heavily obfuscated JavaScript payload** that displays a **fake Cloudflare protection DDoS screen**.

b. On clicking button to bypass the DDoS protection screen, will download a '**security_install.iso**' file to computer, which pretends to be a tool required to **bypass the DDoS verification**. The victims are then asked to open security_install.iso, pretending to be DDOS GUARD which is security_install.exe, which is actually a **Windows shortcut** that runs a PowerShell command from **debug.txt file**.

c. Ultimately, this causes a **chain of scripts** to run that installs NetSupport RAT and scripts downloads **Raccoon Stealer 2.0** password-stealing Trojan and launches it on the device.

d. Further, the executables acquire passwords, cookies, auto-fill data and credit cards saved in the web browsers and is capable of performing file exfiltration and taking screenshots of victim's desktop.

Dy No 929 SO (Coord) Date: 16/9/22

3. **Recommendations**

a. System Administrator must check **theme files of their WordPress** sites as this is the most **common infection point**.

DEA-III 15-9-22

DS(CA) 15/9/22

As	
JS (Admin)	
JS (Org)	
CFAO	
JEA	✓
JTA	
JSA (IL)	
JSA (P&C)	
AO (Legal)	

b. Always employ tile integrity monitoring systems to catch **JS injections** and prevent your site from being a **RAT distribution point**.

c. Internet users can protect themselves from such threats by **enabling script blocking settings** on their browser.

d. Place **2 Factor Authentication on all important logins** (such as bank/ social media accounts). Always deploy **Firewall/ Antivirus** for protection of website.

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

(Muhammad Usman Tariq)
Assistant Secretary (NTISB-II)
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), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

343/DEA-III
15/09-2022

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

No. 1-5/2003 (NTISB-II) Islamabad, the 13 September, 2022

Subject: - **Cyber Security Advisory – Prevention against Fraudulent Website (Advisory No. 38)**

Context. A malicious Indian domain **applyforme.pk** has been identified. The website pretends to be legitimate and advertises **MoD, Pakistan** jobs/ vacancies. Analysis reveals that the domain is operating allegedly to deceive **MoD job applicants** and extract **personally identifiable information** (**PII**). Such information can be used to entrap citizens and conduct **Cyber espionage campaigns**. Users are advised to refrain from such domains and follow **recommendations** at **Para-3**.

2. **Technical Details**. Users can sign into malicious domain by uploading their CV and PII. Details as under: -

URL	IP	Country
www.applyformer.pk	165.22.221.64	India

3. **Recommendations.** Few recommendations (**but not limited to**) are as under: -

a. The applicants, while applying for jobs must remain watchful of such fraudulent websites/ platforms. **The official websites for applying MoD jobs** is **https://mod.gov.pk/SiteImage/jobs** and **https://recuitment.mod.gov.pk**

b. **Do not reveal Personal or Financial Information on Websites**. Do not respond to website solicitation for such information.

c. Verify a link by checking domain name of the site. It helps to indicate whether the site is legitimate or otherwise.

d. Always check **security of website (https)** before sending or entering any sensitive information online.

e. **Always pay attention to website's URL**. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling of a different domain.

f. In case, a user is not sure whether the website is legitimate then **try to verify by contacting concerned organization directly**.

JEA Dy. No. 1422 Dated 15-9-22

Addl SECRETARY MoST Dy. No. 6067 Date 14-9-22

SECRETARY MOST Dy. No. 4312 Date 14-9-22

Deputy Secretary (Admin) Dy. No. 777 Date 15-9-2022

Dy No. 925 SO (Coord) Date 16/9/22

DEA-III 15-9-22

D/S (A) 15/9/22

As	
JS (Admn)	
JS (Org)	
CFAO	
JEA	✓
JTA	
JSA (IL)	
JSA (P&C)	
AO (Legal)	

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

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

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

Copy to: -

7. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
8. Secretary to the President, Aiwan-e-Sadar, Islamabad
9. Cabinet Secretary, Cabinet Division, Islamabad
10. Additional Secretary-III, Cabinet Division, Islamabad
11. Director General (Tech), Dte Gen, ISI Islamabad
12. Director (IT), Cabinet Division, Islamabad

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

No. 1-5/2003 (NTISB-II) Islamabad, the 13 September, 2022

Subject: - **Preventive Measures against Cyber-Attacks on Independence Day 22 (Advisory No. 39)**

Context. Hostile elements/ state sponsored malicious actors typically target government departments/ ministries and defence sector websites on the eve of National Days for disruption of services and defacement to tarnish the global image of Pakistan. It is likely that hostile elements may launch cyberattack on National IT Infrastructure on Defence Day (6 Sep). Accordingly, an advisory is being sent to sensitize website administrators and Service Providers to take additional security precautions (such as web server hardening, traffic/ integrity monitoring etc.) to avoid possible website defacement/ hacking attempts. Moreover, webserver administrators should be made mindful of cyber security guidelines mentioned at Para-2.

2. **Cyber Security Best Practices for Websites Protection**

a. **Upgrade OS** and **webservers** to latest version.

b. Website **admin panel** should only be accessible via **white-listed IPs.**

c. Defend your website against SQL injection attacks by using input validation technique.

d. Complete analysis and penetration testing of application be carried out to identify potential threats.

e. Complete website be **deployed on inland servers** including **database** and web infrastructure.

f. **HTTPS** protocol be used for communication between client and web server.

g. **Application** and **database** be installed on **different machines** with proper security **hardening**.

h. Sensitive data be stored in **encrypted** form with **no direct public access**.

i. DB users privileges be minimized and limited access be granted inside programming code.

j. Proper **security hardening of endpoints** and servers be performed and no **unnecessary ports** and applications be used.

k. Updated **Antivirus tools/ Firewalls** be used on both endpoints and servers to safeguard from potential threats.

l. Enforce a strong **password policy**.

m. Remote management services like **RDP** and **SSH must be disabled** in production environment.

DEA-III

15-9-22

DSCA)

15/9/22

341/DEA-III 15/09/2022

JEA Dy.No. 1420 Dated 15-9-22

Addl. SECRETARY MoST Dy. No. 6069 Date 14-9-22

Deputy Secretary (Admin) Dy. No. 7170 Date 15-9-22

SECRETARY MOST Dy. No: 4314 Date: 14-9-22

Dy No. 942 SO (Coord) Date: 15/9/22

As	
JS (Admin)	
JS (Org)	
CFAO	
JEA	✓
JTA	
JSA (IL)	
JSA (P&C)	
AO (Legal)	

n. Deploy **web application firewalls** (**WAF**) for protection against web attacks.

o. Employ **secure coding practices** such as parameterized queries, proper input sanitization and validation to remove malicious scripts.

p. Keep **system** and **network devices** up-to-date.

q. **Log retention policy** must be devised for at least 3x months on separate device for attacker's reconnaissance.

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

(Muhammad Usman Tariq)
Assistant Secretary (NTISB-II)
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), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

No. 1-5/2003 (NTISB-II) Islamabad, the 13 September, 2022

Subject: - **Cyber Security Advisory – Play Store Apps Spying on Android Users Using Face Stealer (Advisory No. 40)**

Context. Recently, more than 200 Android apps **masquerading as benign** apps have been observed distributing spyware called '**Facestealer**' to gather user credentials and other valuable information.

2. **Categories**. Of the 200 apps; **42** are **VPN services, 20x camera** and **photo editing applications** and **152** are apps masquerading as **fitness** and **puzzle apps**/ others. Though, Google has removed these apps from Play Store; users who might have installed are advised to remove/ uninstall these apps (few examples at **Appendix-I**).

3. **Capabilities**. Capabilities of a face stealer app are as under:-

a. **Face stealer app** changes its code frequently, thus spawning many variants.

b. Gathers sensitive data such as **Facebook login credentials**.

c. In addition to harvesting credentials, the apps are also designed to collect Facebook cookies and **personally identifiable information** associated with a victim's account.

4. **Recommendations**. To avoid falling victim to such scam apps, users are advised to always check **reviews, verify legitimacy of developers** and **avoid downloading** apps from **third-party app stores**.

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

(Muhammad Usman Tariq)
Assistant Secretary (NTISB-II)
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), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

As	
JS (Admin)	
JS (Org)	
CFAO	
JEA	✓
JTA	
JSA (IL)	
JSA (P&C)	
AO (Legal)	

Appendix I

FACESTEALER APPS

Ser	App	Likely Purpose
a.	Daily Fitness OL	A fitness application that comes in the utilities & tools category
b.	Panorama Camera	An application for taking panorama images through your phone's camera.
c.	Business Meta Manager	An application for managing Facebook business profiles.
d.	Swam Photo	A photo editor application for Android, where it allows users to remove background and create photo collages.
e.	Enjoy Photo Editor	A photo editor application.
f.	Cryptomining Farm Your own Coin	A cryptocurrency application.
g.	Photo Gaming Puzzle	A game application.
h.	BitFunds	Crypto Cloud Mining.
i.	Bitcoin Miner	Cloud Mining.
j.	Bitcoin (BTC)	Pool Mining Cloud Wallet.
k.	Crypto Holic	Bitcoin Cloud Mining.
l.	Daily Bitcoin rewards	Cloud Based Mining System.
m.	Bitcoin 2021	-
n.	MineBit Pro	Crypto Cloud Mining & btc miner.
o.	Ethereum (ETH)	Pool Mining Cloud.