Government of Pakistan
Ministry of Science & Technology
******

F. No. 3(5)/2023-NTISB-EW

Islamabad, the 2nd August, 2023

Rector COMSATS University, Islamabad	Chairman, PSF, Islamabad	Chairman PCSIR, Islamabad	Chairman PCST, Islamabad
Rector NUST, Islamabad	Director General NIO, Karachi	Director General PSQCA, Karachi.	Chairman, PEC, Islamabad
Rector NUTECH, Islamabad	Chairman CWHR, Karachi	Director General PNAC, Islamabad	Managing Director, STEDEC, Lahore.
DG PCRET, Islamabad	Director General NIE, Islamabad	Managing Director NEECA, Islamabad	Director General PHA, Islamabad

Subject:

1. **Cyber Security Advisory–Microsoft Patches (132x vulnerabilities) (Advisory No. 38)**
2. **Cyber Security Advisory – Indian APT Target Pakistan Government (Advisory No. 39)**
3. **Cyber Security Advisory Apple MacOS Critical Vulnerability Migraine Patches Available (Advisory No. 40)**
4. **Personal Cyber security Guidance for Government Officials (Advisory No. 41)**
5. **Cyber Security Advisory- Threat Actors Spying on iPhones Through Zero-Click Spyware (Advisory No. 42)**

Dear Sir / Madam,

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

Encl: **As above.**

(Engr. Asif Akhtar Mughal)
Deputy Electronics Adviser-II
051-9206041

Copy for information to:

iii. Network Administrator, MoST
iv. APS to JEA, MoST

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

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

Islamabad, the 24th July, 2023

Subject:- **Cyber Security Advisory – Microsoft Patches (132x vulnerabilities) - Advisory No. 38**

Recently, Microsoft has issued patches for 132x CVEs (9x critical, 122x important and 1x medium). It includes six zero-day privilege escalation bugs being actively exploited.

2. Administrators and users of Microsoft products are advised to update their devices/applications to latest patched version from Microsoft's official support (www.support.microsoft.com).

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. 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 Islamaba
6. Director (IT), Cabinet Division, Islamabad

SECRETARY MOST 2010 Dated 25-7-23

JEA Dy No. 787 Dated 26-7-2023

DEA-III/285 26/07/2023

DEA-II 41 Dy. No 31.7.2023 Date:

For n.a. pl
DEA-III
26-7-23

Main 26/7/23
DEA/II
Asstt.
JEA
Asj. 2/8/23.

25/7/23

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

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

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

Islamabad, the 24th July, 2023

Subject:- **Cyber Security Advisory - Indian APT Target Pakistan Government (Advisory No. 39)**

Context. Recently an Indian APT group has been spotted for likely targeting Pakistan Government/Military Organizations. The threat actor uses a malicious email tilted as "Cyber Security Advisory for Government Entities (Advisory no 54)" for distribution of malware through phishing emails.

2. **Summary of Attack**

a. Attacker uses spear phishing emails to lure in users on downloading fake cyber security advisory (seemingly originated from the Prime Minister Office, **Annex-A**) and malicious attachment (file) from a website https://pakistanarmy[.]xyz, whose URL is similar to official website of Pak Army (pakistanarmy.gov.pk).

b. The fake advisory urges to download a secondary application described as advanced security application specifically designed for government entities". Downloaded attachment is a malicious XML file titled as "Security Patch.Application", once opened, it downloads another payload to compromise the victim's computer (screenshot attached at **Annex-B**)

c. Malware Type/Exploit: Trojan/Backdoor.

d. **File Behavior**. The downloaded file upon execution downloads second stage payload. The backdoor has the capability to remotely control the victim's computer and retrieve data.

e. **C2 Servers**. Following details/associated URLs have been revealed during investigation, which are recommended to be blocked at local firewalls:

Ser	Domain	IP Address
(1)	https://pakistanarmy[.]xyz	104.21.20.118 172.67.192.157

2. **Recommendations**. personal employed at various Civil/Military organizations be sensitized against falling victim to such phishing attacks

-60-

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. 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 24th July, 2023

Subject:- **Cyber Security Advisory – Apple MacOS Critical Vulnerability Migraine Patches Available (Advisory No. 40)**

Apple has recently released security updates for macOS (CVE-2023-32369; Migraine; affects OS of macOS). Non-patching of the update can be exploited by threat actors to bypass System Integrity Protection (SIP) and unauthorized access of victim devices and installation of undetectable malware. Affected products include:

a. MacOS Ventura
b. MacOS Monterey
c. MacOS Big Sur

2. Users are advised to update their devices to latest version from official support as follows:

a.	MacOS Ventura	-	Version 13.4
b.	MacOS Monterey	-	Version 12.6.6
c.	MacOS Big Sur	-	Version 11.7.7

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. 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 24th July, 2023

Subject:- **Personal Cybersecurity Guidance for Government Officials (Advisory No. 41)**

A document containing cyber security guidelines from Google reiterating social-engineering aspects and mitigation measures are as under:

a. **Personal Mobile Phones**

(1) Don't bring smartphone to meeting where most confidential or critical conversation or meeting is happening.

(2) Disable Bluetooth when not in use; don't pair unknown devices.

(3) Be Judicious while connecting Public WiFi networks, try to connect with networks which are secure and are personally under your control.

(4) Ensure usage of strong password; use password manager (if exists) to generate random, unique and strong password generation.

(5) Ensure that device auto lock policy is applied after 10 consecutive failed password attempts and automatically lock after 5 minutes.

(6) Avoid software or hardware modifications such as Jailbreaking or rooting.

(7) Install applications from trusted source.

(8) Plan a contingency plan in case of loss or theft e.g. Activation of mobile tracking feature "Find My Mobile" and backup storage place (Alternative Digital Device/Cloud) for your data.

(9) Do not print official documents from home printers or share those on public media/applications or conduct sensitive meetings from home.

b. **Personal Machines and Networks**

(1) Upgrade to latest Operating System/Web Browser and keep it updated.

(2) Use Multi-Factor Authentication whenever possible; most online services provide an option of MFA.

(3) Leverage security software that provides layered defense via Antivirus, Anti-Phishing, Anti-Malware, Safe Browsing and Firewalls capabilities.

(4) Disable listening devices when not in use e.g. smartphone microphones, software voice assistants, baby monitors, CCTVs, home cameras etc.

(5) Use secure networks for official and personal communications by ensuring following:

(a) Network Address Translation (NAT) protocol is enabled.

(b) Change the default Service Set Identifier (SSID).

(c) If the ISP supports IPv6, ensure the router supports IPv6.

(d) Disable Universal Plug-n-Play (UPnP).

(e) Use strong passphrases of 20 characters to secure network connecting devices.

c. **General Online Safety**

(1) **Email Security**

(a) Avoid opening attachments or links from unsolicited emails.

(b) To prevent the reuse of any compromised passwords, use different password for different accounts.

(c) Always use secure email protocols (Secure IMAP or Secure POP3).

(d) Never open emails that make unusual claims "offer too good to be true".

(2) **Social Media**

(a) Avoid posting personal information such as home address, phone number, CNIC, place of employment and other personal information that can be used to target or harass.

(b) Limit access of your information to "friends only" and always verify any friend requests outside of social networking.

(c) Review of security policies and settings available from your social network providers quarterly or when the site's terms of use/policy changes.

(d) Opt for not exposing personal information to search engines.

(3) **Online Payments**. When shopping online, use a virtual card, instead of sharing your actual card number with the merchant. Google creates a virtual number that is shared with merchant to process your transaction.

(4) **Online Services**. Meta (Facebook, WhatsApp, Instagram) also provides a set of security tips for government officials available on the link "https://www.facebook.com/gpa/resources/basics/security".

2. 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. 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 24th July, 2023

Subject:- **Cyber Security Advisory – Threat Actors Spying on iPhones Through Zero-Click Spyware (Advisory No. 42)**

Context. Reportedly, threat actors are targeting iPhones with zero-click spyware; multiphase polymorphic and self-destructive malware. The campaign is considered as part of sophisticated and long-running mobile espionage and data exfiltration activity termed as ***Operation Triangulation***.

2. **International View Point.** Operation Triangulation has recently been unearthed, however, it was running since 2019. Russia has accused USA and Apple for facilitating spying activities, though Apple has denied such allegations. It may be inferred that the operation is to spy Russian officials iPhones.

3. **Modus Operandi.** Technical details and modus operandi of Operation Triangulation are as follows:

a. During initial phase, victims are infected using zero-click exploits via the iMessage platform. Malware runs with root privilege, gaining complete control of the victim's devices and data.

b. Attack begins with iOS devices receiving a message via iMessage containing malicious attachment.

c. As it is a zero-day, the message triggers malware execution automatically without any user interaction and notice.

d. The malware downloads payloads from download server and further exfiltrates victim's data to under mentioned remote servers:

(1) backuprabbit.com
(2) businessvideonews.com
(3) cloudsponcer.com
(4) mobilegamerstats.com
(5) snoweeanalytics.com
(6) tagclick-cdn.com
(7) topographyupdates.com
(8) unlimitedteacup.com
(9) virtuallaughing.com
(10) web-trackers.com

(11) growthtransport.com
(12) Addatamarket.net
(13) datamarketplace.net
(14) anstv.net
(15) ans7tv.net

e. In the final phase, both the initial iMessage text and malicious attachment are deleted automatically to erase traces (crafted evasion). Most recent version, which has been successfully targeted is iOS 15.7.

4. **Recommendations**

a. All iPhone users are advised to update to latest versions (iOS 16.4.1 or above).

b. Keep iMessages off/blocked.

c. Avoid storing official data/correspondence in mobile phone.

d. Remote C&C servers domains/URLs at Para 3d (serial 1 to 15) be blocked at firewall by administrators.

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. 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