4. For any query or reporting malware/cyber incident, please forward the same on following email addresses: -

a. Falcon1947@proton.me
b. asntisb2@cabinet.gov.pk

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-II (NTISB)
Ph# 051-9204560

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

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

(10) Always type URLs in browser rather than clicking on links.

(11) Always open websites with https and avoid visiting http websites.

b. **<u>Anti-Masquerading Guidelines</u>**

(1) **<u>Administrators</u>**

(a) Restrict incoming traffic and user's permissions to maximum extent by implementing system hardening at OS, BIOS and application level.

(b) Unauthorized USB and storage media be blocked via hardening. Also, format USb every time before suing to ensure no malware is propagated from one system to another.

(c) Monitor networks including file hashes, file locations, logins and unsuccessful login attempts.

(d) Use reputed anti-virus, firewalls, IPS/IDS and SIEM solutions.

(e) Use separate servers/routing for offline LAN and online networks.

(f) Allow internet access to specific users on need basis and restrict data usage/ applications rights.

(g) verify software and documents before downloading via digital code-signing technique.

(h) Implement MFA in mailing systems administrator controls and other critical systems.

(i) Always maintain back up of critical data periodically

(j) Regularly change passwords at administrator level

(k) Regularly patch and update all OS, applications and other technical equipment.

c. **<u>Users</u>**

(1) Always re-verify trusted user who has sent email/attachment via secondary means (call, SMS, verbal) before downloading.

(2) Report any suspicious activity to Administrator immediately.

(3) Never keep critical data on online systems and store it in standalone systems.

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

No. 1-5/2003/24(NTISB-II) Islamabad, the 10 February, 2023

Subject: - **Cyber Security Advisory – Dark Pink APT (Advisory No. 03)**

Context. Dark Pink (origin unknown) is a new APT group operational since mid-2021 targeting Asian governments and military setups. Recently, analysis of attack on Malaysian Armed Forces (MAF) reveals use of phishing emails and sophisticated attacks on email network by Dark Pink. The APT group uses sophisticated Tactics, Techniques and Procedures (TTPs) that warrants employment of proactive Cyber Security monitoring/mechanism in own government and military setups. In this regard, guidelines are provided in ensuing paras for compliance.

2. **TTPs - Dark Pink APT**. Dark Pink uses techniques such as USB infection and DLL exploitation to exploit systems. Primary means of compromise (unauthorized intrusion and access) is phishing emails.

3. **Guidelines/Preventive Measures**. An APT group may frequently change its techniques, tactics and procedures. Whoever, few preventive measures (but not limited to) are as follows: -

a. **Anti-phishing E-mail Guidelines**

(1) Never open unknown and suspicious emails, link and attachments.

(2) Use email service provider anti-virus scanner before downloading any attachment (trusted ones too)

(3) Timely update all applications and Operating Systems (PC and mobile etc)

(4) Use well reputed and updated anti-virus/anti-malware.

(5) Regularly review applications permission, system running processes and storage utilization

(6) Use separate and complex passwords for each system, mobile, SM accounts, financial and mailing accounts etc.

(7) Never use personal accounts on official systems

(8) Use multi-factor authentication (MFA)/two-factor authentications where possible.

(9) Never share personal details and credentials with unauthorized/suspicious users, websites, applications etc.

JEA-165
13-2-23

DEA-III/53
13/2/2023

SECRETARY MOST
Dy. No: 629
Date: 13-02-23

Deputy Secretary (Admin)
Dy. No: 490
Date: 13-2-23

Dy No 240
SO (Coord)
Date: 14-2-23

SO (Coord)

14/02

14/02/23

DS(A)

DEA/III

13/2

13-2-23 JEA

13/2

AS	
JS(Admin)	
JS (Org)	
CFA&	
JEA	✓
ITA	
JSA (IL)	
JSA (PAC)	
AO (Legal)	

Ser	Malicious Appl Name	Ser	Malicious Appl Name	Ser	Malicious Appl Name
61.	Chat 24/7	62.	Zapme	63.	Chat Pt
64.	Kakao Talk	65.	ZongBoost	66.	Audio & Video Recorder
67.	ISPRNews	68.	Love Bae	69.	Easy Chat
70.	Zepp	71.	Boss	72.	ChitChat Box
73.	Hideme	74.	Skymate	75.	Triover
76.	Peppyz	77.	LionVPN	78.	Paigham Chat
79.	Friend Chat	80.	Pink WhatsAp	81.	Dosti Chat
82.	Star Talk	83.	Gossip	84.	Mobile Chat
85.	Click (aval on Goggle Play store)	86.	Yooho Chat	87.	Howdee (aval on Goggle Play store)
88.	Pryvate	89.	Exodus	90.	TalkU
91.	Pakistani Mili Naghmee	92.	Ab Talk	93.	Text on Photos
94.	Pakistani Chat Rooms	95.	Imo	96.	Stripchat X
97.	Text on Photos	98.	Skype Lite	99.	Woo Plus
100.	Intimo	101.	Chat Privacy	102.	Android Services
103.	Android System Services	104.	Im Secure Chat	105.	**Bigo Live Lite**
106.	**Live Chat Video Call-Whatslive**	107.	**MeetU**	108.	**Milli-Live Video Call**
109.	**JOJOO-Live Video Chat**	110.	**Gibber-Live Video Chat**	111.	**BunChat Pro Video Chat**
112.	**iBlink-Live Video Chat**	113.	**Online Live Adult Video Chat**	114.	**Video Chat With Strangers**
115.	**Charm-Match with Singles**	116.	**Sexy Girl Video Call**	117.	**XV Random Video Chat**
118.	**Bubble for chat**	119.	**18Live: Live Random Video Chat**	120	**Live Talk Video Call**

Note: **Applications highlighted in bold are newly identified having malicious behaviour.**

Appendix I

LIST OF IDENTIFIED MALICIOUS APPLICATIONS

(AS ON 10 JAN 2023)

Ser	Malicious Appl Name	Ser	Malicious Appl Name	Ser	Malicious Appl Name
1.	Rocket Chat	2.	Safe Dialler	3.	Phub
4.	Omegle	5.	U & Me	6.	Babble V3
7.	Privatechat1	8.	Filos	9.	Chat It
10.	Rapid Chat	11.	YoTalk	12.	Porn Hub
13.	Photo Edition	14.	Crypto Chat	15.	TeleChatty
16.	ZoIPER	17.	Babble	18.	Face Call
19.	Buzz	20.	Tweety Chat	21.	VIBES
22.	Converse	23.	Lite It	24.	Hex Chat
25.	Xpress	26.	Chat On	27.	Vmate
28.	Chirrups	29.	Link Up	30.	Safe Chat
31.	Graphic Version	32.	Secure Chat	33.	Lite Chat
34.	Pvt Chat	35.	Guftagu	36.	Cheerio
37.	Free VPN V3	38.	Twin Me	39.	Philions Chat
40.	Just You	41.	CuCu Chat	42.	FM WhatsApp
43.	Quran.Apk	44.	Fruit Chat	45.	Islamic Chat
46.	SecureIt	47.	ZanigV4	48.	Spitfire
49.	FaceChat	50.	Seta / SA News	51.	Wire
52.	FireChat	53.	Cable-1	54.	Privee Chat
55.	Buddy Chat	56.	Stumped	57.	Zong Chat (Beta)
58.	ZangiV2	59.	Media Services	60.	CrazyChat

d. Before downloading/ installing apps on Android devices, review the app details, number of downloads, user reviews/ comments and "ADDITIONAL INFORMATION" section.

e. In mobile settings, do not enable installation of apps from "Untrusted Sources".

f. Install Android updates and patches as and when available from Android device vendors.

g. Do not download or open attachment in emails received from untrusted sources or unexpectedly received from trusted users and forward them to government officials.

h. Avoid using insecure and unknown Wi-Fi network as hostile elements use Wi-Fi access points at public places for distributing malicious applications.

i. Use two-factor authentication on all Internet Banking Apps, WhatsApp, social Media and Gmail Accounts.

j. All officers/staff must be guided to adhere recommended cyber security measures at personal smart appliances.

9. 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-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. 1-5/2003/24(NTISB-II) Islamabad, the 10 February, 2023

Subject: - **Cyber Security Advisory – Dubious Adult Chat Applications OV2600T (Advisory No. 02)**

In continuation of Cabinet Division's NTISB letter No. 1-5/2003/24(NTISB-II), dated 25th April, 2022 (Advisory No. 14).

Introduction. Sequel to already identified 104 x malicious apps, 16x new malicious apps are being used by Hostile Intelligence Agencies (HIAs) for espionage/information gathering. Newly identified applications are chat-cum-hacking apps, which are used to trap government officials to extract classified information through technical/coercive (blackmailing) measures.

2. Individuals who have accidently installed any of malicious apps mentioned in **Appendix-I** must immediately perform following actions: -

a. Note down contact details (WhatsApp number/Facebook ID etc) of suspected individual who shared the link for downloading the application for reporting the same to CSO of own organization/ department.

b. Immediately switch off infected mobile phone; remove battery & SIM and disconnect from internet.

c. Share subject information/incident with all persons/saved contacts for their security.

3. **Recommendations**. Above in view, following best practices are recommended: -

a. Always check application permissions before installation of application and install applications from Google Play Store only.

b. Under command should regularly be sensitized about malicious actors' tactics, techniques and procedures, moreover, all personnel (officers/ staff) be sensitized to refrain from engaging in activities that may lead to exploitation.

c. Install and update reputed antivirus solution on Android devices like AVAST or Kaspersky. After installation, scan the suspected device with antivirus solutions to detect and clean infections.

14/02
SO(Coord)
14/2/23
DS(A) DEA III
13-2-23 JEA

Appendix I

INDICATORS OF COMPROMISE (IoCs)

Ser	SHA-1	Filename	ESET detection name
a.	78E82F632856F293BDA86D77D0 2DF97EDBCDE918	cdc.dll	Win32/TrojanDownloader.Donot.C
b.	D9F439E7D9EE9450CD504D5791 FC73DA7C3F7E2E	wbiosr.exe	Win32/TrojanDownloader.Donot.D
c.	CF7A56FD0613F63418B9DF3E2D 7852FBB687BE3F	vdsc.exe	Win32/TrojanDownloader.Donot.E
d.	B2263A6688E512D90629A3A621 B2EE003B1B959E	wuaupdt.exe	Win32/ReverseShell.J
e.	13B785493145C85B005E96D5029 C20ACCFFE50F2	gedit.exe	Win32/Spy.Donot.A
f	E2A11F28F9511753698BA5CDBA A70E8141C9DFC3	wscs.exe	Win32/Spy.Donot.B
g.	F67ABC483EE2114D96A90FA0A3 9496C42EF050B5	gedit.exe	Win32/Spy.Donot.B

Appendix II

FAMOUS ATTACKS AND TOOL KITS

Ser	Name	Malicious Files	Timeline
a.	DarkMusical	Excel - Monthly Action Plan.xls	Jun 2021
b.	Henos	RTF file - ProtocolUpdate.doc	Feb 2021
c.	Gedit	RTF file - Quality Assurance Programme.doc	2020 - 2021
d.	Jaca	PPT - Approved Plan.pptx	2020 - 2021

minimal functionality, used to download and execute further components of DO NOT Team's toolset

7. Indicators of Compromise (IoCs) and Famous Attacks and Toolkits. Details are provided at **Appendix-I** and **Appendix-II**.

8. **Preventive Measures**. Few preventive measure (but not limited to) to defend against DO NOT APT attacks are as follows: -

a. Utilizing system hardening be ensured at all endpoints.

b. Active directory domain networks be hardened to ensure protection against Kerberos based attacks (Golden, Silver and Skeleton Key Attacks)

c. Execution of signed executable like PsExec.exe, Netcat.exe, Socat.exe and netcat.exe be blocked and monitored.

d. Execution of unsigned executables from %temp% directory and AppData directory be blocked and monitored.

e. Malware focused audit of all endpoints be conducted periodically.

f. Always use reputed anti-malware/anti-virus.

g. Establish SOC for network/host visibility at organizational level be ensured by utilizing open source XDR, EDR and SIEM solutions.

9. 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-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. 1-5/2003/24(NTISB-II) Islamabad, the 10 February, 2023

Subject: - **Cyber Security Advisory - Malware Analysis - Installation of Smart - S RADAR Onboard OV2600T (Advisory No. 01)**

Context. Indian state sponsored Cyber Threat Actors and APT groups have been targeting Pakistan's civil and military setups for espionage. DO NOT (also known as APT-C-35 & Sector E02) is a threat actor (APT group) operating since 2016. The threat actor is known for targeting organizations and individuals in South Asia with sophisticated windows and Android malware.

2. **Objective**. Do Not threat actor mainly collects and exfiltrates data to Indian intelligence agencies for cyber espionage.

3. **Current Status**. Recently, the threat actor has improvised cyberattack toolkits thus causing concerns for potential victims. The threat actor has emerged in various cyber threat intelligence watchdogs alerts. Modus operandi and preventive measures against DO NOT threat actor are mentioned in ensuing paras.

4. **Targets Countries**

a. South Asia-Bangladesh, Sri Lanka, Pakistan and Nepal (including embassies abroad).

b. International – Emerging powers.

5. **Interested Areas**

a. Government and military organizations

b. Ministries of Foreign Affairs

c. Embassies

6. **Modus Operandi**. DO NOT APT has been consistently targeting critical entities with waves of spear phishing emails and malicious attachments. It has been repeating attack patterns on same victims with advanced techniques. Few techniques are mentioned below: -

a. Macros in MS-Word, Excel, PowerPoint etc. leading to remote access.

b. Windows Framework RTF files with .doc extensions further containing links to download malware and gain shell access. This is the latest attack technique used by APT - C-35.

c. YTY Malware-Indigenously developed by DO NOT APT consists of a chain of downloaders that ultimately download a backdoor with

14/02

SO (Coord)

14/2/23

DSC(A)

DEA-III

14/2

13-2-23 JEA

13/2

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

Islamabad, 15th February, 2023

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 –(ADVISORY NO.1, 2, & 3)**

Please find enclose herewith a copy of Cabinet Division's, Cabinet Secretariat (NTISB) Letters No. 1-5/2003 (NTISB-II) dated 10th February, 2023 on the subject cited above for information & compliance.

Encl: **As above.**

(SAEED AHMED RAHOOJO)
Section Officer (Coord)
Tel: 9202520

Copy for information to:-

i. PS to Secretary, MoST.

ii. PS to Additional Secretary, MoST.

iii. APS to Joint Secretary (Admn), MoST.

iv. APS to Deputy Secretary (Admn), MoST.

v. All heads of Wing's, MoST.

vi. SO (Estt.), MoST.

vii. Networking Administrator, MoST