

Subject:- **Updated List of Malicious Application (Advisory No. 44)**

Sequel to already identified malicious applications intimated vide NTISB advisory No. 14, dated 25<sup>th</sup> April, 2022 and advisory No. 01, dated 9<sup>th</sup> February, 2023, 13x new malicious applications being used by HIAs for espionage/information gathering operations have been identified and fresh list of 133x identified malicious applications is attached at **Annex-A**. The newly identified applications are developed by Hostile Intelligence Agencies (HIAs) to trap individuals and extract sensitive information through technical and coercive means.

2. Above in view, individuals who have accidentally installed any of malicious apps 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.** In addition, users are advised to adhere to the following best practices (but not limited to):

- a. Always check application permissions before installation of application and install applications from Google/Apple Play Store only.
- b. Under command/civil staff 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. After installation, scan the suspected device with antivirus solutions to detect and clean infections.
- 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 CSO.
- h. Avoid using insecure and unknown Wi-Fi networks 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.
- k. List/names of malicious apps be disseminated to all ranks at priority for their awareness.

**LIST OF IDENTIFIED MALICIOUS APPLICATIONS**(As on 25<sup>th</sup> Jul 2023)

<b>Ser</b>	<b>Malicious Appl Name</b>	<b>Ser</b>	<b>Malicious Appl Name</b>	<b>Ser</b>	<b>Malicious Appl Name</b>
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.	Chirrup	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)

Ser	Malicious Appl Name	Ser	Malicious Appl Name	Ser	Malicious Appl Name
58.	ZangiV2	59.	Media Services	60.	CrazyChat
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	86.	Yooho Chat	87.	Howdee
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	120.	Live Talk Video Call

Ser	Malicious Appl Name	Ser	Malicious Appl Name	Ser	Malicious Appl Name
			Video Chat		
121.	Quick Chat	122.	Let's Chat	123.	Ludo King
124.	Gupta Racing	125.	Glow Chat	126.	ROIX
127.	Meet Up	128.	IKKias VPN	129.	Media Provider
130.	iRecorder - Screen Recorder	131.	YouTube Premium	132.	VaultCloud
133.	mSureChat				