F. No. 1-5/2003/24(NTISB-II)

Islamabad, the 12 August, 2024

Subject: **Cyber Security Advisory – Konfety Group Targets Android Users with Evil Twin Malicious Play Store Apps (Advisory No. 17)**

15 AUG 2024

M (I.T)

M (Admin/HR)

A.S (Rev. Div.)

Introduction. Recently, Google Play Store identified and thwarted an active malicious campaign targeting Android users globally. Collectively named as Konfety Apps; this campaign used 250+ Decoy Evil Twin android applications (**Annex - A**). The malicious activity is allegedly conducted by the Russian Konfety cybercrime group having ulterior motives primarily backed by monetary gains using advertisement fraud.

2. **Modus Operandi**. Attackers use advertising campaigns to promote modified APK and redirects users to download malicious apps. Konfety malware involves a dropper APK that further loads an obfuscated stager and back doored SDK, making it highly evasive hence difficult to detect. Further, the decoy twin apps used by attackers appear harmless while Evil Twin mimics them to commit ad fraud, install payloads, second stage malwares and code injection etc.

3. **Mitigation**. Although Google has removed Konfety apps from its Play Store, however, if any of the attached malicious Konfety apps found installed on smart phones, following remedial measures may be opted:

a. Immediately uninstall specific Konfety app.

b. Perform a factory reset.

c. Take a backup of personal media files (excluding device/system apps).

d. Restrict unnecessary apps permission and set to while using App only.

e. Download and install software only from official app stores like Play Store or the IOS App Store.

f. Keep your smart phone, OS and apps updated.

g. Regularly check the smart devices/Wi-Fi data usage of apps installed on smart devices.

h. Use a reputed anti-virus and internet security software package on your smart devices.

SS IT
execution

29/8/24

29.8.24

Sec (IT)

Chief IT (System)

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

Annex-A

LIST OF KONFETY MALICIOUS EVIL TWIN DECOY APPS

(Already Removed by Google Play Store)

Ser	App Name	Ser	App Name
1.	Best Status	2.	Learn English Urdu
3.	Akbar	4.	Galaxy Fighter
5.	Dream Head Soccer	6.	Drive me
7.	Sweet Candy Cream Rain	8.	Double Co
9.	Block Puzzle	10.	Goddess Photo
11.	Endless Airplane	12.	Dict En lt Free
13.	Modern Snake	14.	Santa Stuck
15.	Car Crash	16.	Street Fight
17.	Draw	18.	Tourism
19.	Spin Tunnel	20.	Jewel Puzzle New
21.	X Racer	22.	Head Soccer
23.	Skate Surfers	24.	Tunnel
25.	Tuneonn Lal	26.	Space Craft
27.	Tennis Ball Bounce	28.	Shark Hunter Hungry Fish
29.	Viking Saga	30.	Bouncy Ball
31.	Indian Border Animal	32.	Falling Blocks
33.	Downhill Bus Racing	34.	Survival Secret Agent Prison Mafia
35.	Football Cup	36.	Eye Color Editor
37.	Fruit Splash	38.	Basketball
39.	Car Chase	40.	GTi Drag Desert
41.	Max Parking	42.	Jump Ninja
43.	Tank Battle Games Free	44.	Words Play
45.	Ball Hop	46.	MP3 Cutter
47.	Monster Defense	48.	Insta Frame Pic Collage

49.	Proverbs and Sayings	50.	Swing Thru
51.	Bounce Ball 2	52.	Dvng Doggo
53.	Piano Balls	54.	High Dive
55.	Latest Punjabi Songs	56.	Tuneom Dohe
57.	Tuneonn Horror	58.	Animal Dash King
59.	Offroad Racing	60.	Tuneonn Yoga
61.	Tuneonn Jokes	62.	Personal Voice Judge
63.	Draw My Story	64.	Smart Quiz Price
65.	Zombie Apocalypse	66.	Self-Study Yoga
67.	Candy Heroes Mania	68.	Drift Tuner 2019
69.	Tuneonn Ayurveda	70.	Ni Mobile
71.	Soccer Ping	72.	Caesar Empire
73.	Color Jump	74.	Flight Sim 3D Pilot
75.	Fruit Sweet Blast	76.	Big Farm
77.	Myth Puzzle	78.	Four Pics One Word
79.	Sniper War Survival	80.	Flash Cards English
81.	R Drift	82.	Border Line
83.	Boom Rocket	84.	Aptitude Test
85.	Life Quote	86.	Fatty Ninja
87.	Destiny Photo Mixer	88.	English Status And Message
89.	English Stories	90.	Mind Quiz Brain Out
91.	UPSSSC Exam	92.	Deep Sea Adventure
93.	Bike Trail Stunt Master Racing Games	94.	Qiu Qiu Jstzs
95.	Umbrella Down	96.	Cook Book
97.	Pets Animals	98.	Back Hand Spring
99.	Furious Speed Car Stunt	100.	Fruit Juice
101.	Moto Racing Bike Stunt Traffic Racer	102.	Mao Miecz
103.	Indian Mountain Jeep Drive	104.	G Ball

105.	Truck Bike Racing	106.	Congratulation
107.	Ludo Star Master	108.	Ludo Legend
109.	Colo Monopoly	110.	Gravity Pipes
111.	Stic Balls	112.	Nature Puzzle
113.	Military Suit Photo Montage	114.	Subway Surf
115.	Runner Subway	116.	Tip King
117.	Pac Monoid	118.	Love Que
119.	M Food	120.	Dino Bomb
121.	Cat Run	122.	Tamil
123.	Chess Opening	124.	Space Ship
125.	Jewel Deluxe	126.	Dict En Ru Free
127.	Devil Fighter	128.	Reasoning
129.	Apple Shooter Game	130.	Bhakti Rings
131.	Fight Ord	132.	Wrapping Bubbling
133.	Test Inteligencia	134.	Enigmas
135.	Status Katta	136.	Billiard Club Deluxe
137.	Critical Strikes	138.	Devinettes
139.	Speed Car Bump Challenge	140.	GTR Redline Racing
141.	Cook From Bis	142.	Racing Girl
143.	Candy Splash	144.	Meme Katta
145.	Handled Spinner	146.	Yanggedw
147.	Racing Stunt Man	148.	Blind Zombie
149.	Pr Call Ghost	150.	Caesar Empire
151.	Dragon Hunter	152.	Retro Drag
153.	Crazy Bike Racing Simulator	154.	Kawaypk
155.	Apk Share For You	156.	Ma Mam Nq01
157.	Race and Kill	158.	Brain Ball Bash
159.	Oil Train Transporter	160.	Cartoon Quiz

161.	Candy Land	162.	Video Media Mp3 Cutter
163.	Cooking Fever Craze Expert Madness	164.	Snow Queen 2 Bird Weasel
165.	Calculator Talks	166.	Double Corks
167.	Cube Jump	168.	TSR
169.	Romantic Bells	170.	Aqua Fish
171.	Tractor Offroad	174.	Tap Soccer
173.	Flappy Bee	174.	Bistro Cook
175.	Selfi Cam Beauty	176.	Waheguru Ji Tone Mp3
177.	Acertijo	178.	Hindi Grammar
179.	Japan Race	180.	Buyaocc2
181.	Kick It	182.	Gongfu Hcrwz
183.	Missiles	184.	Huochai Rjtzz
185.	Sticky Mn	186.	Fk Xrty
187.	High War Racer	188.	Fighter Two Players
189.	Real Drift	190.	Shark Hunter Hungry Fish 2
191.	Star Stell Story	192.	Learn English Tenses In Urdu
193.	Heavy Bike Racer	194.	Dict English Synonyms Free
195.	Soccer Kicks Penalty Shootout	196.	Pr Call Burger
197.	Angry Bunnies	198.	Diving Doggy
199.	Tonne For Arabs	200.	Rubicon Car Stunts
201.	Drawing the Path	202.	Adriver Jyeghz
203.	Train Simulator	204.	M Scary
205.	Jump One Jump	206.	Dubgeon
207.	Zigzag Highway	208.	English Flash Card Learn Word
209.	Jump Bump	210.	Jiroutr
211.	Old Movies	212.	Maze
213.	Marathi	214.	Dict En El Free
215.	Trump Talk	216.	Pet Parkour

217.	Hindi Status	218.	Plane Flight Pilot Landing Sim
219.	Window Photo Editor	220.	Play Mini World
221.	Fortress Defense	222.	Tuneonn Love Stories
223.	Monte Cristo Link To 8 Puzzle	224.	Waheguru Ji Tones
225.	Tuneonn Health Tips	226.	Xiao Jie Jahz
227.	Car Wash	228.	Zombieland
229.	Tuneonn Vastu	230.	Adriver Ezjdzz
231.	Latest Arabic Ring	232.	Chess Game
233.	Conversation	234.	Vid Fake Scary Mo
235.	Snr Near	236.	Mp3 Cutter
237.	Puzzle Classic	238.	English Toefl Learn Word
239.	Slime	240.	Dict En Hi Free
241.	Picture Game	242.	Nbzh
243.	Fallin Ball	244.	English Audio Story
245.	Flib Bottle	246.	Stickman Backflip Pro
247.	Coloring App	248.	Slime Wallpapers
249.	TSR	250.	Hidden Object
251.	Maths	252.	Dict French Free
253.	Tuneonn Hindi Stories	254.	Drawing The Path
255.	Swings	256.	Snow Queen Bird Weasel