NCA-22.102824 – National CERT Advisory: Konfety Group Targets Android Users with Evil Twin Malicious Play Store Apps

Introduction

National CERT has discovered a malicious campaign targeting Android users globally, known as the *Konfety Apps* campaign. This operation, allegedly orchestrated by the Konfety group, involves over 200 decoy Evil Twin Android applications that were previously available on Google Play Store (**Annex-A**). The primary goal of these apps is monetary gain through advertisement fraud. Although the malicious apps have been removed from the Play Store, this advisory provides details on the threat, indicators of compromise (IOCs), and recommended security measures to protect Android users.

Campaign Details

The Konfety campaign deploys modified APKs through advertising campaigns to lure users into downloading malicious applications. Once installed, these apps deploy a dropper APK, which loads an obfuscated stager and a backdoored software development kit (SDK). These decoy apps appear harmless, but their Evil Twin counterparts engage in activities such as ad fraud, payload installation, second-stage malware deployment, and code injection.

Key Findings

- **Malware Delivery Method:** Users are tricked into downloading Evil Twin apps, which mimic legitimate applications. These malicious apps can bypass detection due to their evasive nature, making it difficult for standard anti-malware solutions to identify them.
- **Ad Fraud and Payloads:** The primary goal of these apps is to commit ad fraud by generating fake clicks and impressions. They can also install second-stage malware and execute harmful payloads, leading to further exploitation of the victim's device.
- **Obfuscation and Evasion Techniques:** The stager and backdoored SDK are heavily obfuscated, making the malware difficult to analyze or reverse-engineer.

Indicators of Compromise (IOCs)

Users should immediately uninstall any of the listed apps (Annex-A). Below are common signs that an Android device may be compromised:

- Unusual data consumption by apps.
- Slow device performance or random pop-up advertisements.

- Apps requesting unnecessary permissions.
- Unexpected network traffic.

Recommended Security Measures

1. Prevention Measures

a. **Uninstall Malicious Apps:** If any Konfety apps from the list in Annex-A are found, immediately uninstall them.

b. **Factory Reset:** Perform a factory reset of the device, but ensure personal files are backed up (excluding system and device apps).

c. **Download from Official Stores Only:** Always download apps from official stores like Google Play or Apple's App Store.

d. **Limit App Permissions:** Restrict unnecessary app permissions and set them to "only while using the app."

e. **Regular Updates:** Ensure the Android operating system and all apps are regularly updated to the latest versions.

f. **Monitor Data Usage:** Regularly check the data usage of apps on your device for any unusual activity.

g. **Use Reputable Security Software:** Install and update reputable anti-virus and internet security software on your device.

2. Detection and Response

a. **Regular Device Scans:** Use a mobile security app to run regular scans for malware.

b. **Monitor for Suspicious Activity:** Be vigilant of abnormal behavior on your device, such as slow performance or sudden pop-ups.

c. **Incident Response:** In case of confirmed infection, follow incident response procedures, including factory resetting the device, restoring from clean backups, and monitoring for further suspicious activity.

3. Best Practices

a. **Awareness Training:** Educate users on the risks of downloading unverified apps and granting unnecessary permissions.

b. **Security Patching:** Ensure timely installation of security updates for Android devices.

c. **Multi-Factor Authentication (MFA):** Enable MFA for all sensitive applications and services to add an extra layer of protection.

PKCERT

This campaign highlights the need for increased vigilance when downloading and using mobile applications. National CERT urges users to follow the recommendations provided and stay alert to emerging threats.

Annex A

LIST OF KONFETY MALICIOUS EVIL TWIN DECOY APPS

(Already Removed by Google Play Store)

Sr	App Name	Sr	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	172	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	Beat It

PKCERT