Konfety

Gavin Reid
CISO

Lindsay Kaye
VP Threat Intelligence

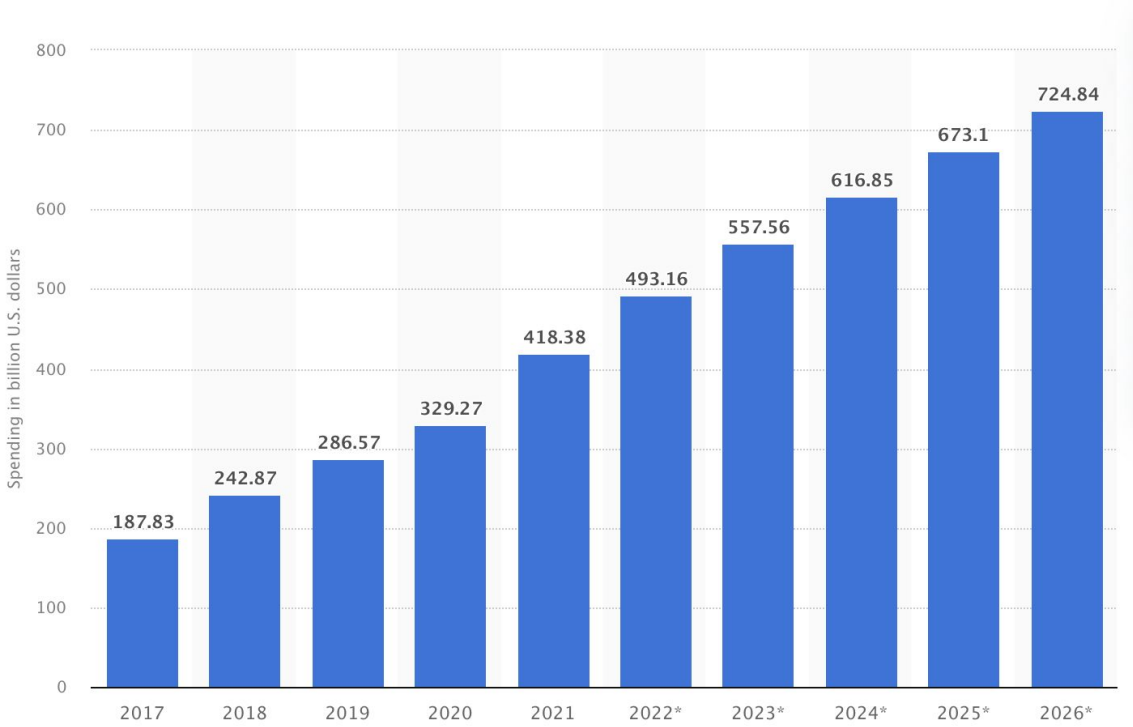
whoami

Gavin Reid
CISO

Lindsay Kaye
VP, Threat Intelligence

The Well

Global programmatic advertising spending from 2017 to 2026
(in billion U.S. dollars)



What is Ad Fraud?

Ad fraud refers to deceptive practices that manipulate digital advertising to generate revenue illegally.

Fake impressions or clicks

Domain or app spoofing

Install or attribution fraud

Malvertising and malware distribution

Data manipulation and traffic laundering

So how did they siphon money from that well?

Ad Fraud Type	Description	Used in Konfety?
Impression Fraud	Fake ad views to inflate revenue.	✅
Click Fraud	Simulated clicks to charge advertisers.	✅
App Spoofing	Faking legitimate app identities to mimic real traffic.	✅ (Evil Twin apps)
Malvertising	Using ads to deliver malware or direct installs.	✅

Why is it so easy?

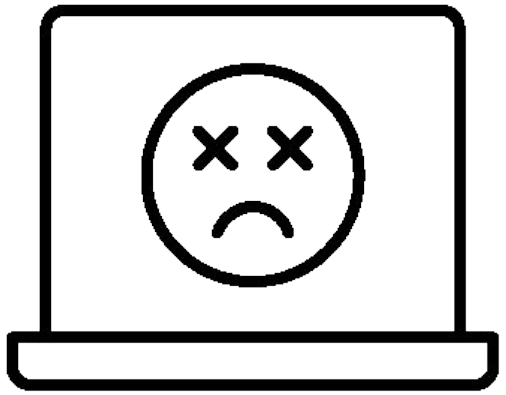
- **Enormous profits** – small frauds X billions of transactions can generate millions.
- **Complex ad ecosystem** – many intermediaries hide activity.
- **Lack of transparency** – poor visibility and inconsistent application of standards
- **Sophisticated bots** – mimic real users and avoid detection.
- **Mobile & CTV** – newer platforms are under-protected.
- **Low legal risk** – prosecution is rare and difficult.
- **Industry complacency** – inflated metrics benefit some players.

How Fraud Fuels Disinformation and Risk

Fake traffic props up fake content.

It monetizes disinformation, scam apps, and clickbait.

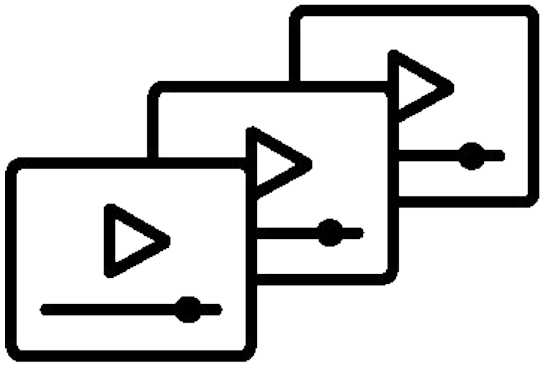
Fraud skews what users see and trust — it's not only a revenue issue.



Why Should I Care About Ad Fraud?

Most people hear “ad fraud” and assume it’s about wasted clicks and bad attribution.

But the truth is: ad fraud is **one of the biggest unmonitored capital flows on the internet** — and one of the most *heavily exploited* by cybercriminals.

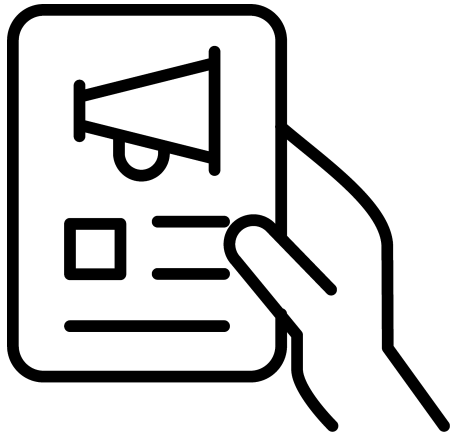


A Hidden Tax on the Digital Economy

$100 billion per year is siphoned by fraudsters.

That's money meant for real content, creators, and growth.

Fraud drains ROI, misleads attribution, and funds criminal networks.

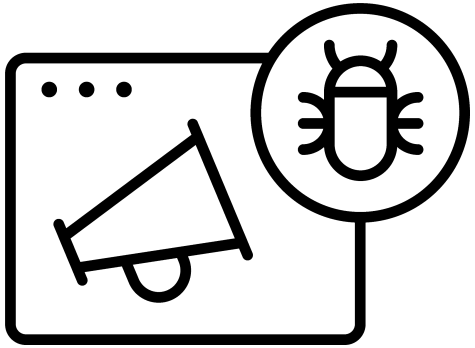


Building Blocks for Cybercrime Infrastructure

Botnets used for ad fraud also do credential stuffing, DDoS, and more.

Fraudulent traffic helps **embed malware, spoof identity, and evade detection.**

It's a soft entry point to much bigger attacks



Let's Talk About Konfety

Advertising fraud remains a threat to the integrity of digital marketing,

and threat actors' fraud campaigns are growing more sophisticated

SATORI INVESTIGATION | KONFETY

HUMAN uncovered and disrupted a campaign known as

“Konfety” — a mobile advertising fraud campaign that uses a novel “evil twin” evasion method

to operate under the radar

This “evil twin” method allowed the threat actor to **keep more than 250 decoy apps active** on the Google Play Store, and in parallel, created specially crafted **“evil twin” apps that fraudulently generated ads** using the publisher accounts from the “decoy” apps.

Konfety reached

a peak of 10 billion bid requests per day

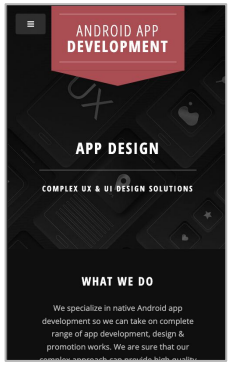
prior to disruption

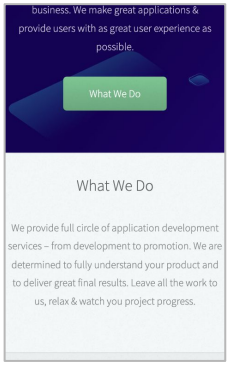
We've disrupted Konfety,
but how will it, or campaigns like it,

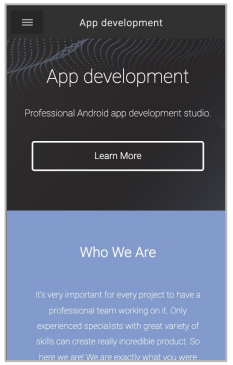
impact digital marketing and ad tech for years to come?

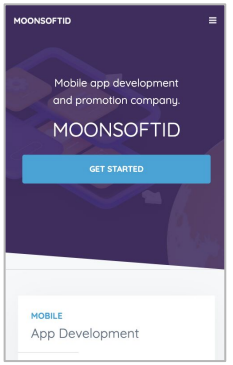
Overview of Konfety

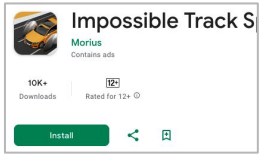
- Novel method for conducting ad fraud — no malicious apps in official app stores
- “Decoy twins” are largely generic, template-based games, app sites have nearly identical app-ads.txt
- Each “decoy twin” hosted in the Google Play Store has a corresponding “evil twin” application
- Both sets of apps used the advertising SDK CaramelAds — “evil twins” abused to conduct ad fraud
- “Evil twin” delivered via malvertising, click-baiting and drive-by attacks

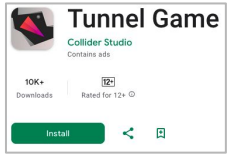






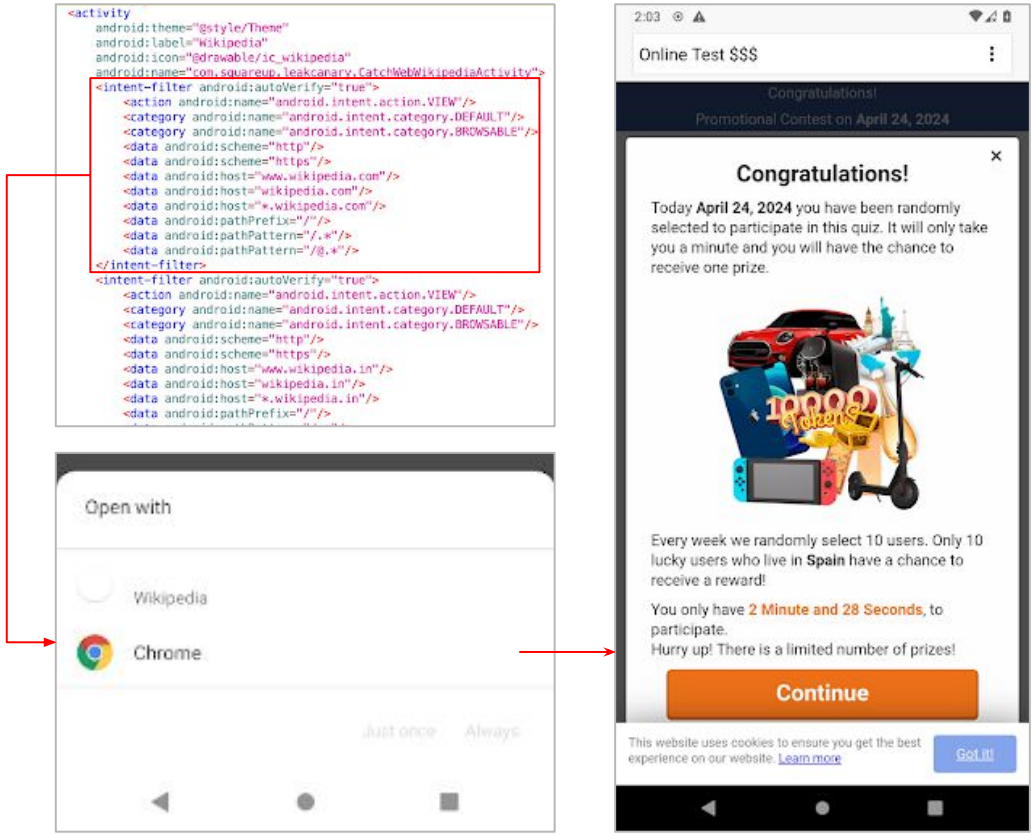




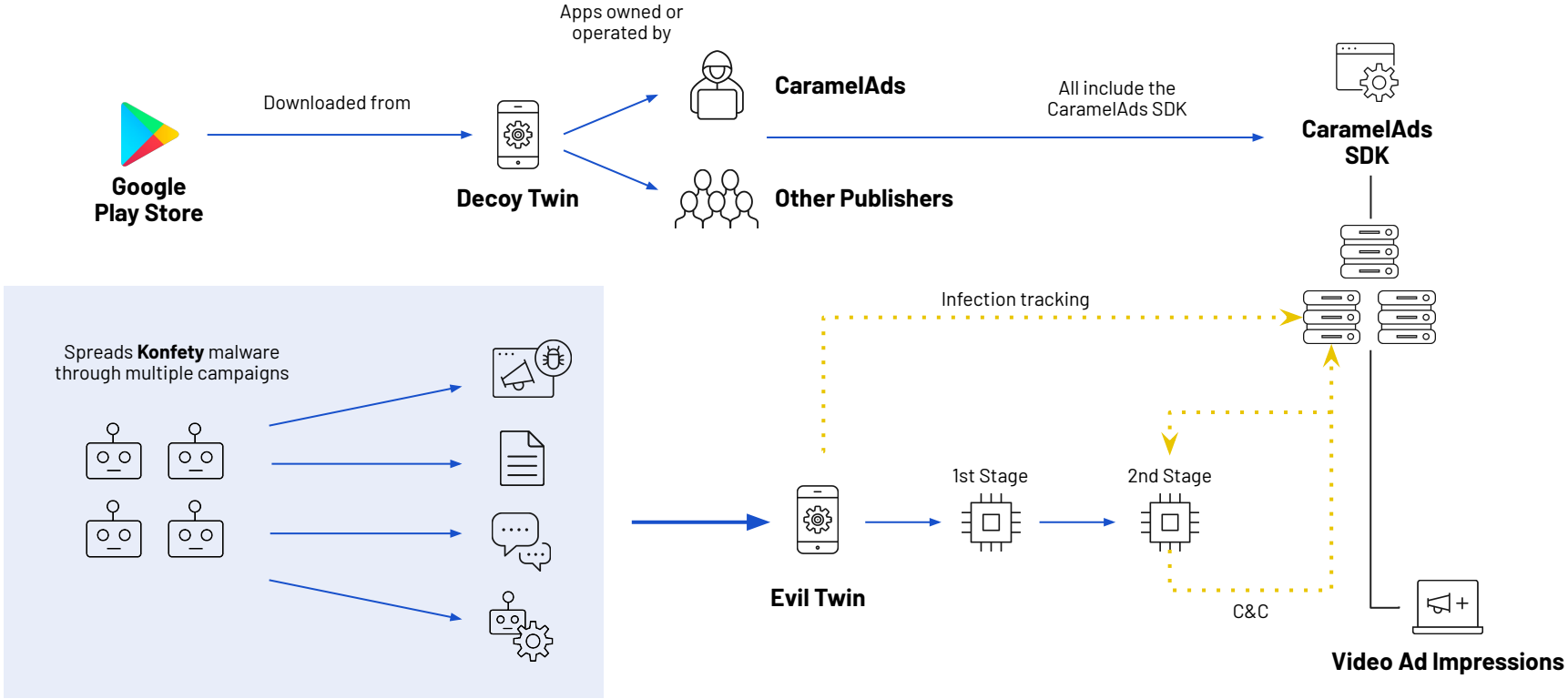


Overview of Konfety

“Evil twins” conduct other types of fraud, including browser search monitoring, code sideloading and intent filter intercepts

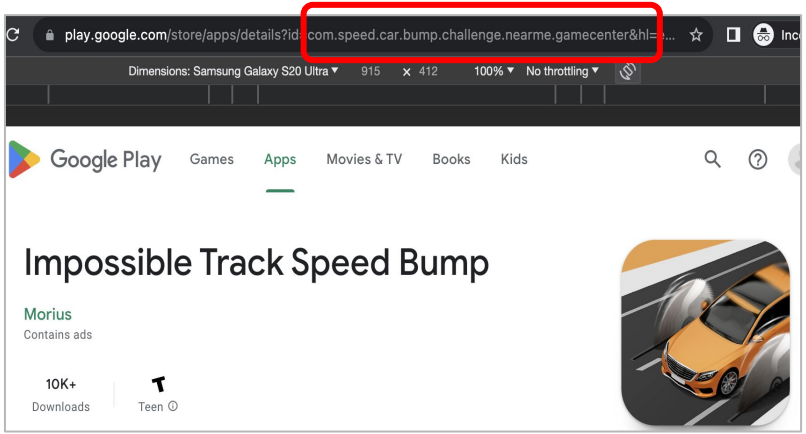


Overview of Konfety



The “Evil Twin” Method

“Evil twin” apps mimic corresponding “decoy twin” apps by copying the app ID/package names and publisher IDs from the “decoy twin” — ad traffic appears as though it is coming from non-malicious, Play Store-hosted apps



Actor-owned App on Google Play Store (decoy twin)

Drive-by download campaign delivering “evil twin” app

How Was CaramelAds Abused By “Evil Twins”?

Abuse centered on the way CaramelAds processes certain data values returned in the server response or through a malicious creative or implementation

Can modify traffic to appear as though originating from any type of device actor chooses

Can be used to open any URL using the device browser

Possible to selectively render ads

Performs no validation that the device is real, that ads are rendered correctly, or other checks common in well established networks

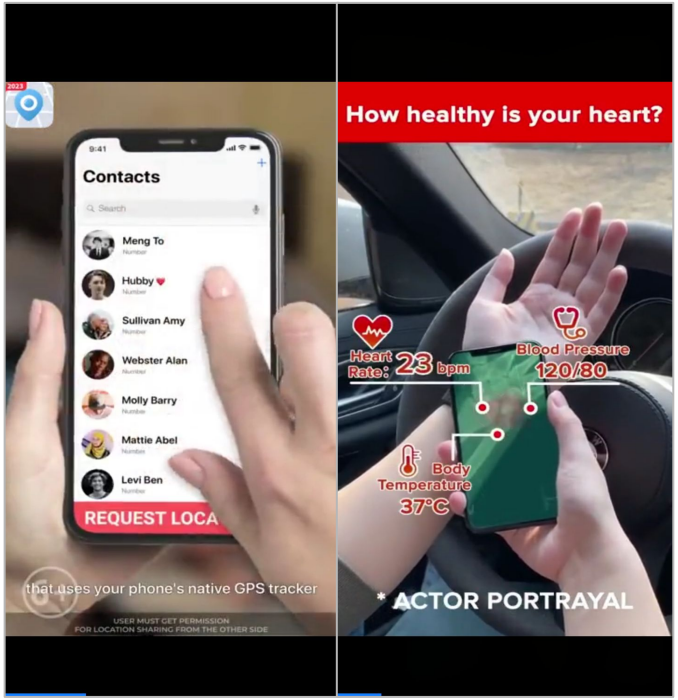
Evil Twin Malware: Ad Fraud

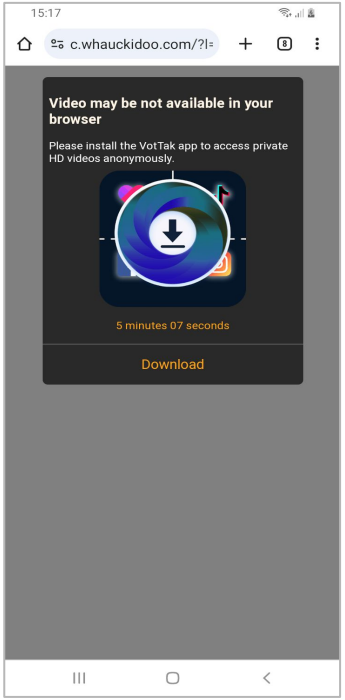
Malicious app **hijacks** the victim's **phones screen**

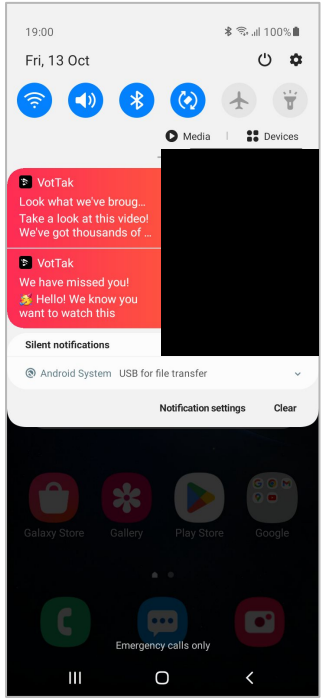
Displays **full screen, hard to escape ads** every few minutes.

At times multiple **ads stacked**.

App also **exploits notifications** to engage with victims.

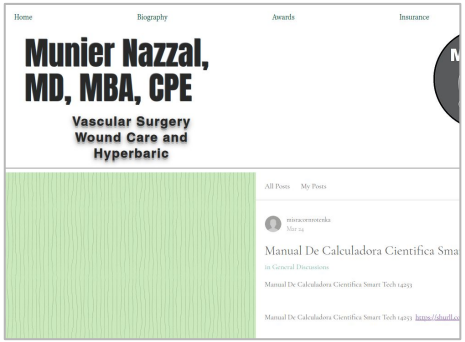


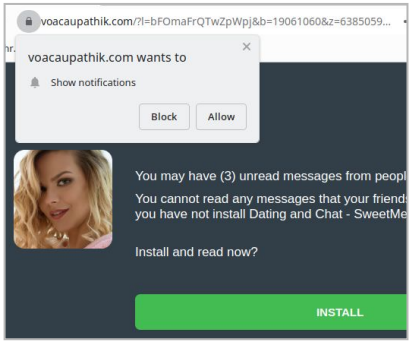


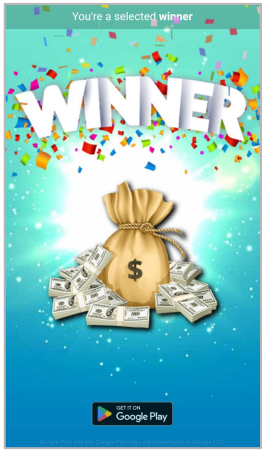


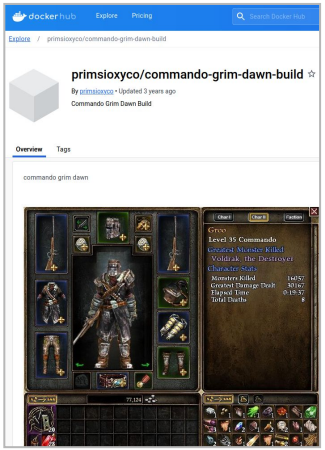
Evil Twin Malware: Distribution

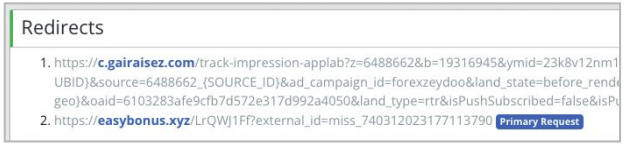
The distribution campaigns for “evil twin” apps included: malicious PDFs hosted across the web, including on legitimate domains, malicious advertising, and online questionnaires











Disrupting Konfety

HUMAN began to flag high confidence traffic from these applications as soon as the threat was identified.

Disrupting Konfety

After we deployed countermeasures, **the threat actors shifted which ad networks were targeted** by the operation to avoid HUMAN's customers

The actor also **updated the SSP servers in the SDK** to try to evade detection

Konfety Campaign Impact

Prior to disruption, **9.6 billion** fraudulent bid requests per day — now **substantially decreased**

Konfety Campaign Impact

This campaign affected **multiple entities** across the advertising ecosystem including **ad networks**, and could affect developers unknowingly using the CaramelAds SDK

Konfety Campaign Impact

The Konfety campaign demonstrates a **new, innovative way** that cybercriminals are conducting ad fraud operations; the “evil twin” method aims to **circumvent official app store rules** to enable criminal activity

Konfety Sets the Stage

Konfety is **just one ad fraud campaign** in a sea of many, but **it underscores the need for collective, industry action against this type of threat** — keeping digital marketing safe benefits all of us

Successfully demonetizing requires **collective action**

Novel method for ad fraud **complicates "takedown" procedures** for malicious apps

Increase in "sophisticated" campaigns that **cannot be solved by a singular organization alone**: Konfety and BADBOX/PEACHPIT

Konfety is Just One Campaign

Where is Ad Fraud Going?

Threat actors will continue increasing sophistication in ad fraud TTPs

Often **part of funding/cashout for a larger operation** — BADBOX 2.0

Will remain a persistent issue — highly lucrative

Where Do We Go From Here?

Demonetize Fraudulent Entities

- Digital advertising protection
- Know your partners and your partners' partners
- Make them re-tool
- Campaign-adjacent tooling?

Engage with External Partners

- Share/implement detections for malicious apps, infrastructure and TTPs
- Law enforcement engagement, where relevant

Stay Ahead of What's Next

- Threat intelligence is crucial
- HUMAN continues to track these and other campaigns

Questions?