WEBINAR

Taking the Fight to the Fraudsters

LIFTOFF

adjust

What We'll Cover

1. The history and current methods of spoofing installs
2. Practical advice to assess if your app might already be compromised
3. Which countermeasures work - and which do not - when it comes to spoofed installs

Meet the Panelists

Andreas Naumann
Director of Fraud Prevention

adjust

Dennis Mink
VP Marketing

LIFTOFF

Matt Sadofsky
Former Head of Marketing

STUDIO

Founded in
2012

Berlin
Headquarters

Apps helped
32K

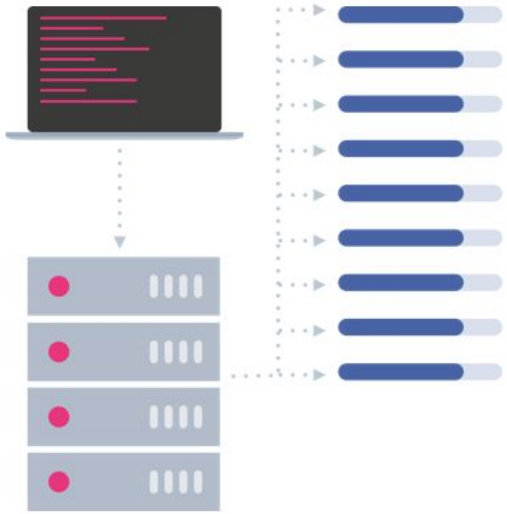
Mobile Measurement made easy: Adjust unifies all your marketing activities into one powerful platform, giving you the insights you need to scale your business.

Spoofing

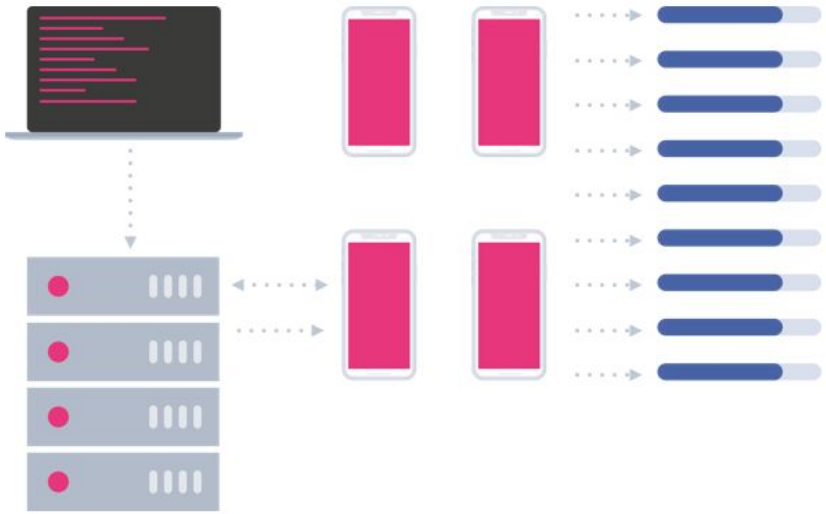
Andreas Naumann

adjust

Fake Installs



Spoofed Installs



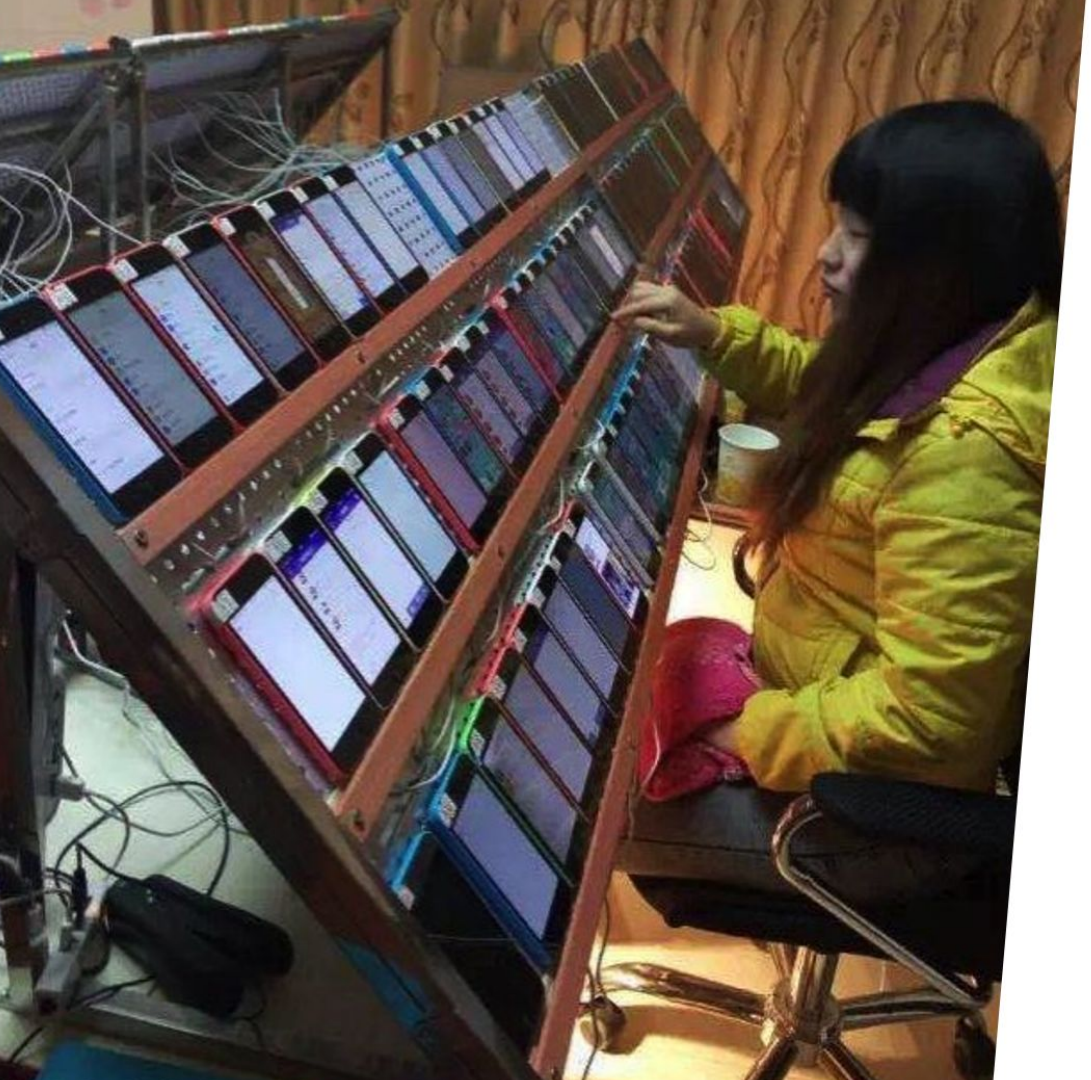
Fake Installs

Everything is fake

- Ad engagement
- User
- Device
- Install
- Post install behaviour

Perpetrators MO

- Manual
- or Instrumented
- or Emulation in Virtualized environment



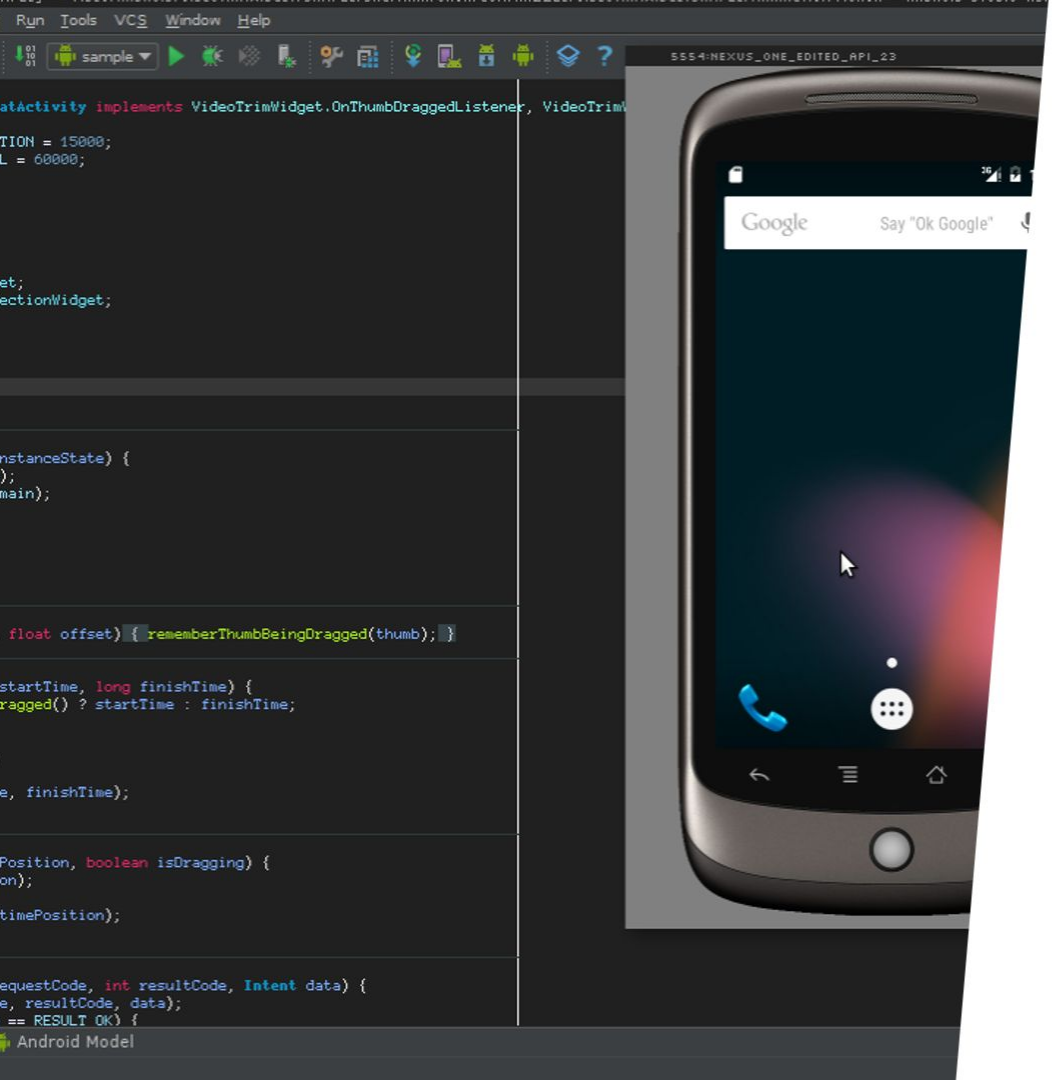
Manual fake installs

- Doesn’t scale
- Expensive to run
- Hard to detect

adjust LIFTOFF

Instrumented fake installs

- Doesn’t scale well
- Still expensive to run
- Easier to detect



Emulated fake installs

- Unlimited scale
- Cheap to run
- Easiest to detect

Spoofed Installs

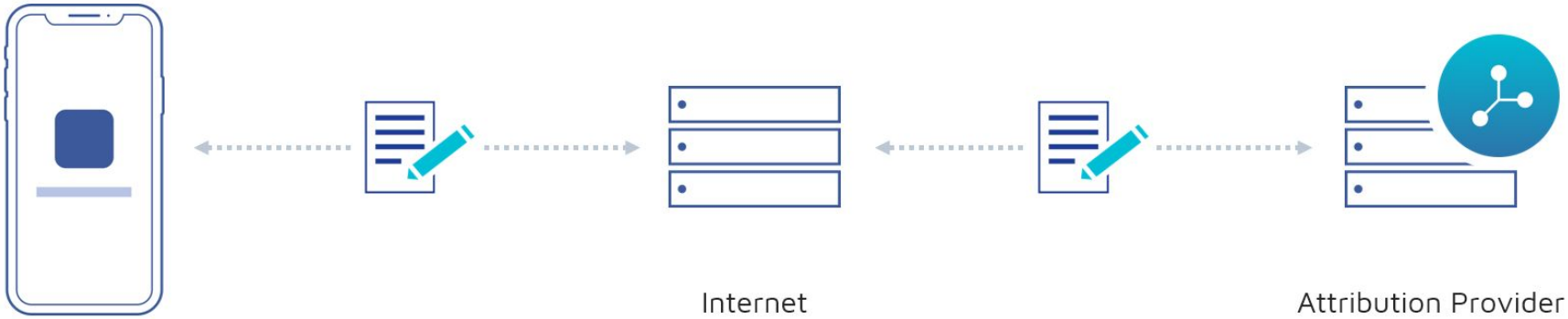
Everything is fake

- Ad engagement
- User
- Device
- Install
- Post install behaviour

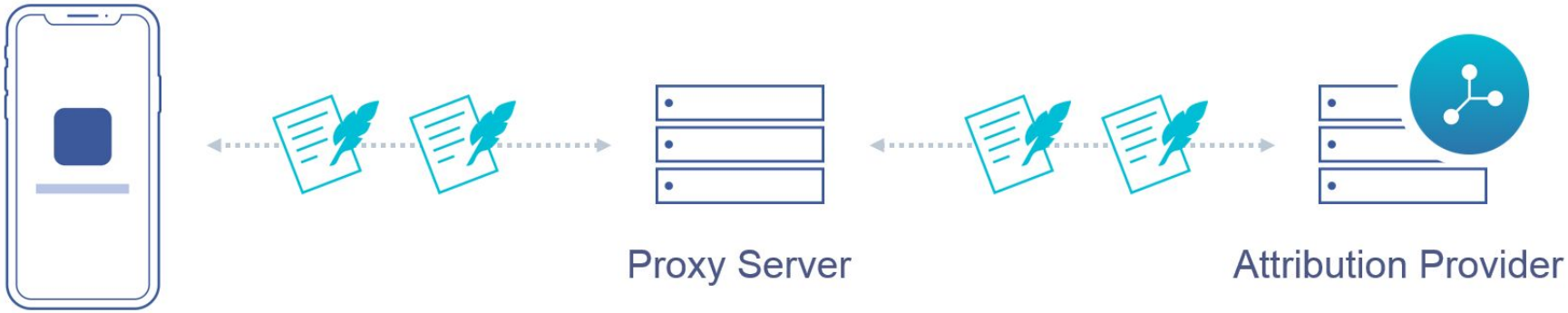
Perpetrators MO

- Evolved from emulation
- MITM Attack to circumvent SSL
- Studying tracking URLs
- Static and dynamic parameters uncovered
- Replay attacks
- Own app acts as proxy

Common data transfer



Proxy traffic



MITM Attack

Replay attack / spoofing

adjust LIFTOFF

Spoofed installs

- Unlimited scale
- Cheap to run
- Hardest to detect
- Real apps collect data used in spoofing attack

Q&A

Taking the Fight to the Fraudsters

Thank you!