Mobile Security

Dr. Eleonora Losiouk
Department of Mathematics
University of Padua
elosiouk@math.unipd.it
https://www.math.unipd.it/~elosiouk/

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

DIPARTIMENTO
MATEMATICA

Malware

- Malware is software with a malicious intent

- Relation with security vulnerabilities
  - Malware may need to use/exploit security vulnerabilities to carry on its malicious actions
  - Discussion on malware will focus on the malicious behavior per se, what's the rationale behind it, various associated techniques

Why does malware exist?

Why does malware exist?

- Why would a human being spend her time writing malicious software?

- Try to always ask "why?"

- Three main thrusts
  - Just for fun / bragging rights
  - To become rich
  - Targeted attacks

Just for fun

- Just as a prank
  - "Hey, now your wallpaper is a pic of Justin Bieber ahah so funny"
- Bragging rights
  - I hacked your phone and I spammed your entire contacts list about it
- I don't like you...
  - ... and I'll post something stupid on facebook

To get money

- This is most often the case

- Monetization is one of the biggest incentives
  - Information stealing (and selling)
    - Credentials, personal data
  - Asking you to pay (ransomware)
  - Advertisement
  - Bitcoin mining
  - Send premium SMS

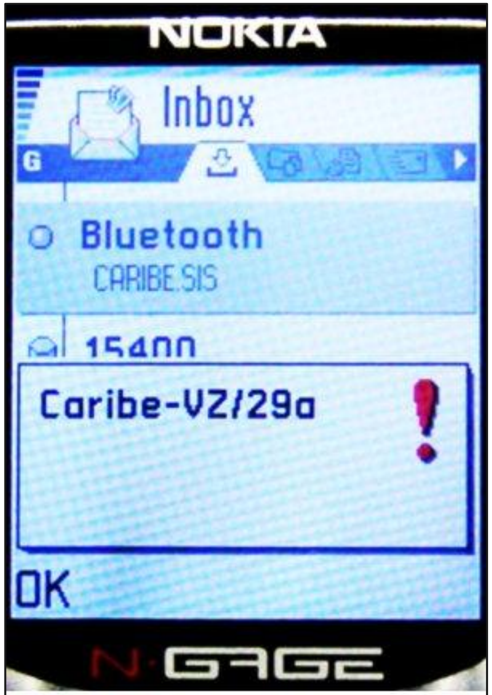
Targeted Attack

- "Targeted attacks" are those attacks meant to attack a specific, small set of individuals
    - Sometimes a specific person is targeted
- These are the most advanced, sophisticated attacks
    - People writing these (or commissioning these) have a lot of money
- Potential targets: political activists, journalists, ...

What does malware do, and why?

Cabir (2004)

- First mobile malware
- It targets Symbian OS
- The payload is a “Caribe” popup message
- Attempts propagation through bluetooth



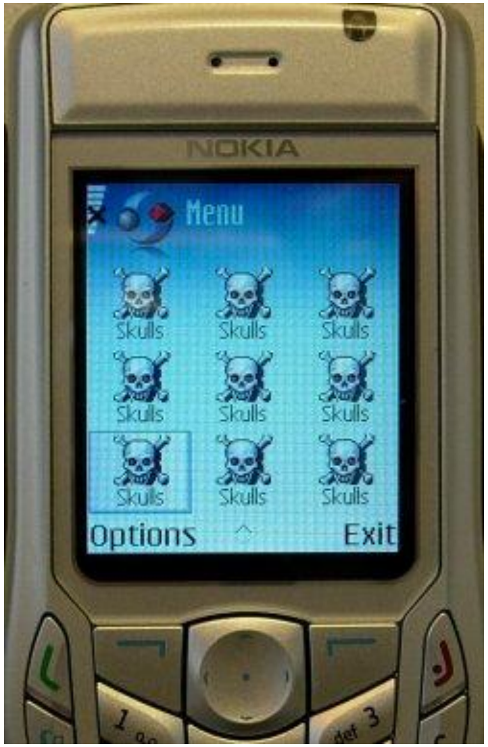
Bluetooth
CARIBE.SIS

Caribe-VZ/29a

Copyright F-Secure Corp. 2004

Skull (2004)

- The payload is slightly more annoying
- It corrupts files related to critical functionalities
  - SMS / MMS
  - web browsing
  - camera
- It replaces all icons with skulls



Malware Gets Real

- Plankton (2011)
  - Found on the Play Store
  - Leak user’s private information
    - contact list
    - bookmark
    - browser history

- Monetization strategy:
  - Private information is valuable, especially if it's about K/M+ users
  - Sell private information on the black market

Malware Gets Real

- DroidKungFu (2011)
  - Found on the Play Store
  - Root exploit
  - Bot-like capabilities

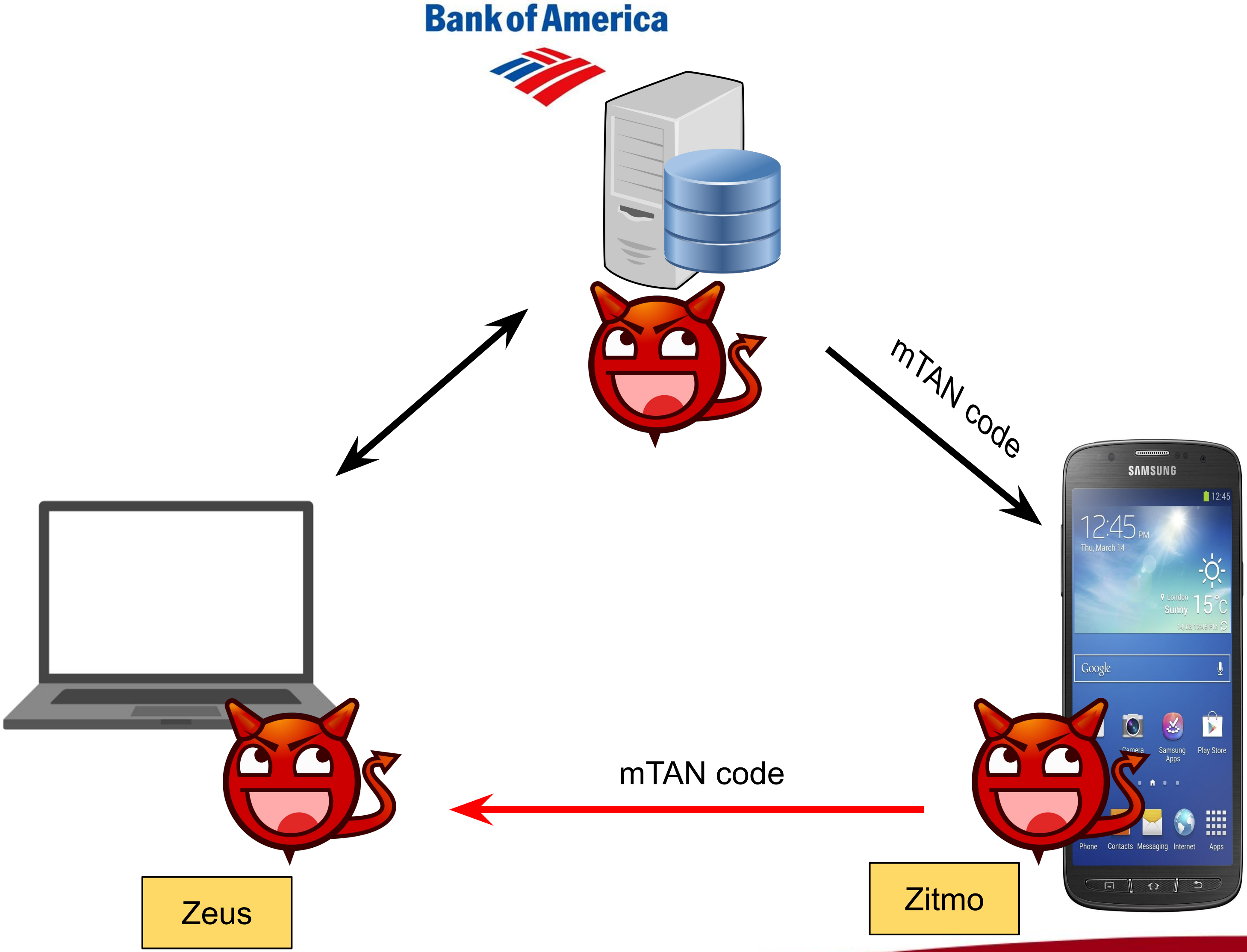
- Monetization strategy
  - Valuable: A botmaster can direct K/M+ bots to do many things
  - Examples: distributed denial-of-service attack (DDoS attack), send spam, steal data "on request", device admin and monitoring
  - Once again: these "bots" can be sold on the black market

Malware author != Malware "user"

- Different roles
    - Whoever "writes" the malicious apps ("the developer")
        - The actual coder
    - Whoever carries on the "infection"
        - Who adopts strategies to actual infect users with malware X
    - Whoever directs the malware to do XYZ ("the operator")
        - Whoever "pulls the trigger"
    - Whoever actually decides what the malware should do ("the customer")
        - "Bring website xyz.com down"

- These roles are often fulfilled by different persons

Zitmo ("Zeus In The Mobile", 2011)

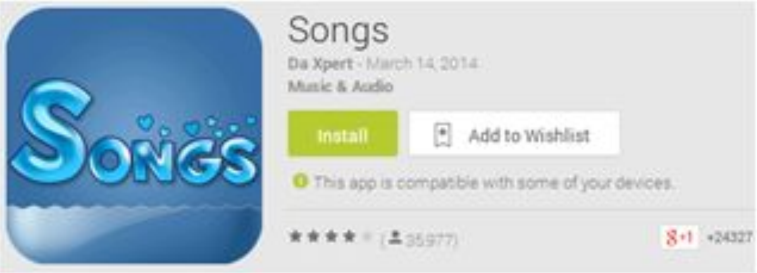


HippoSMS (2011)

- It sends SMS to premium numbers
- Stealthy: all the malware-related SMS are deleted

Bitcoin Miner (2014)

- Legitimate apps repackaged to mine bitcoins in the background
- Is it worth for the bad guys?
    - The main app is already written
    - The mining code is stolen from another app

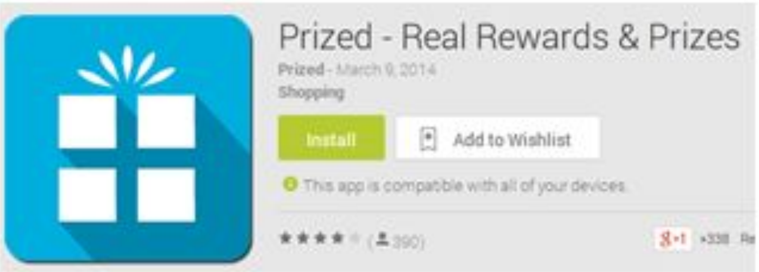


Songs

Da Xpert - March 14, 2014

Music & Audio

This app is compatible with some of your devices.

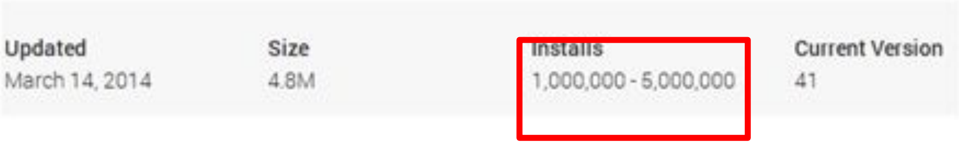


Prized - Real Rewards & Prizes

Prized - March 9, 2014

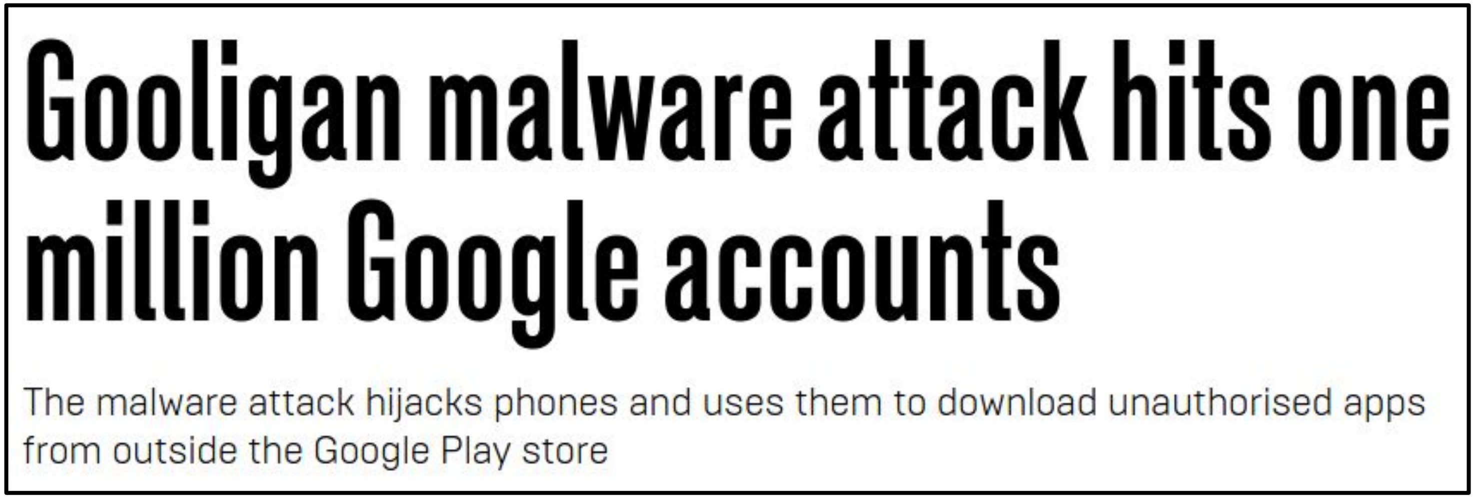
Shopping

This app is compatible with all of your devices.



Updated	Size	Installs	Current Version
March 14, 2014	4.8M	1,000,000 - 5,000,000	41

Gooligan (2016)



Gooligan malware attack hits one million Google accounts

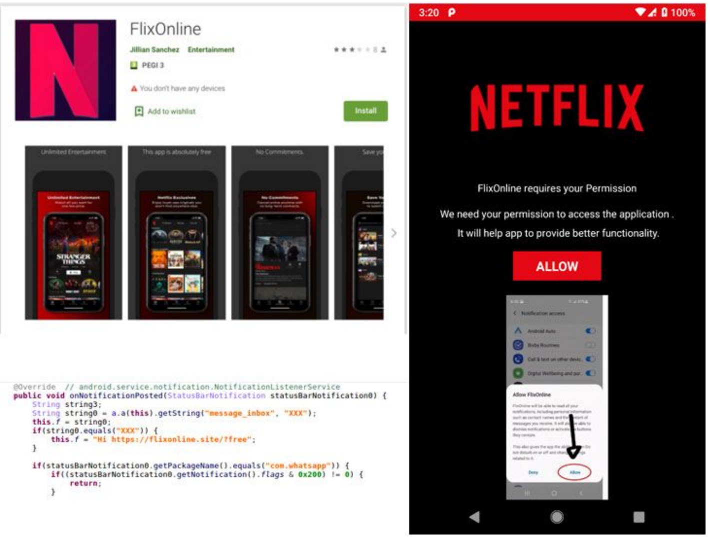
The malware attack hijacks phones and uses them to download unauthorised apps from outside the Google Play store

- Hijacked more than one million Google accounts
- Roots device, steals authentication tokens, download additional apps

More Recent Malwares

WhatsApp-based wormable Android malware spotted on the Google Play Store

April 07, 2021 Ravie Lakshmanan



FlixOnline requires your Permission

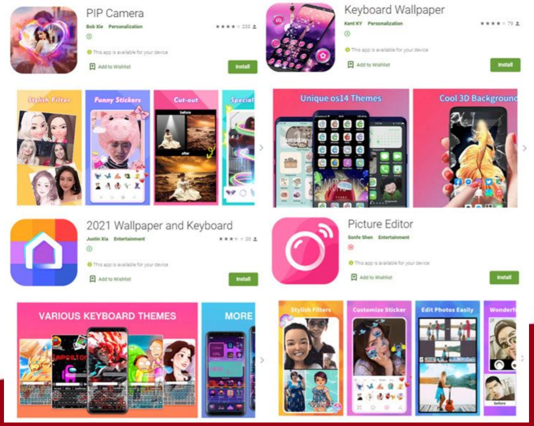
We need your permission to access the application .
It will help app to provide better functionality.

```
@Override  // android.service.notification.NotificationListenerService
public void onNotificationPosted(StatusBarNotification statusBarNotification0) {
    String string3;
    String string0 = a.a(this).getString("message_inbox", "XXX");
    this.f = string0;
    if(string0.equals("XXX")) {
        this.f = "Hi https://flixonline.site/?free";
    }

    if(statusBarNotification0.getPackageName().equals("com.whatsapp")) {
        if((statusBarNotification0.getNotification().flags & 0x200) != 0) {
            return;
        }
```

Over 750,000 Users Downloaded New Billing Fraud Apps From Google Play Store

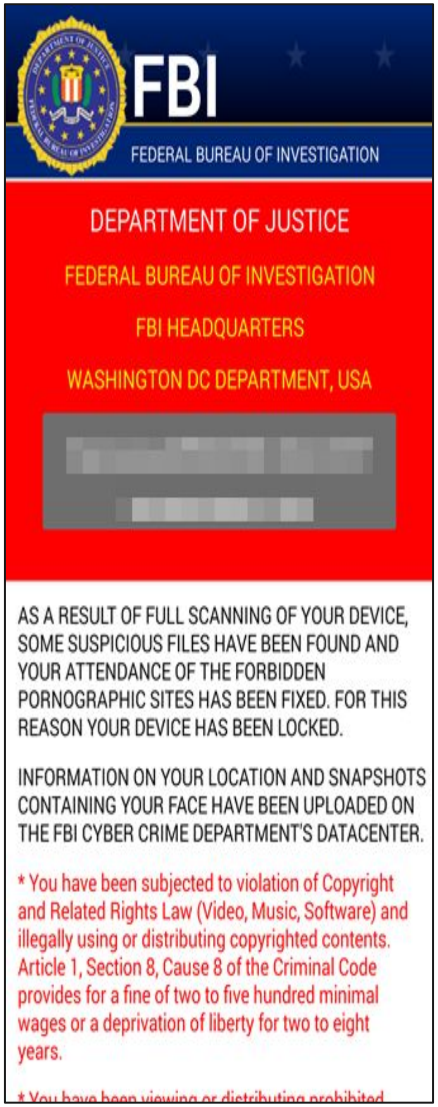
April 20, 2021 Ravie Lakshmanan



Ransomware

- It locks your device and encrypts all your data

- It asks for money (a “ransom”) to reverse its effects



DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

FBI HEADQUARTERS

WASHINGTON DC DEPARTMENT, USA

[redacted]

AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.

INFORMATION ON YOUR LOCATION AND SNAPSHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.

* You have been subjected to violation of Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted contents. Article 1, Section 8, Cause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

* You have been viewing or distributing prohibited

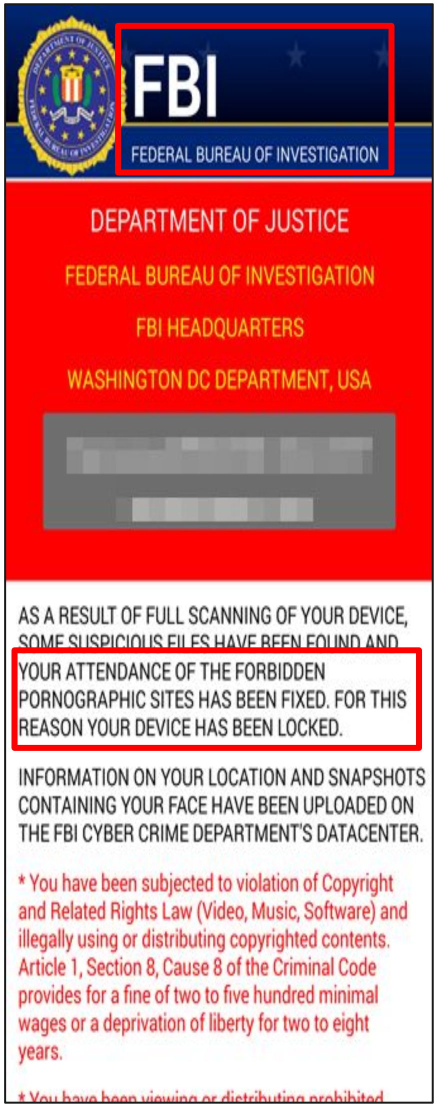
Ransomware

Università degli Studi di Padova

- It locks your device and encrypts all your data

- It asks for money (a "ransom") to reverse its effects

- Puts "pressure" on the user
  - The FBI found "Forbidden pornographic sites" on your phone!



FBI

FEDERAL BUREAU OF INVESTIGATION

DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

FBI HEADQUARTERS

WASHINGTON DC DEPARTMENT, USA

[redacted]

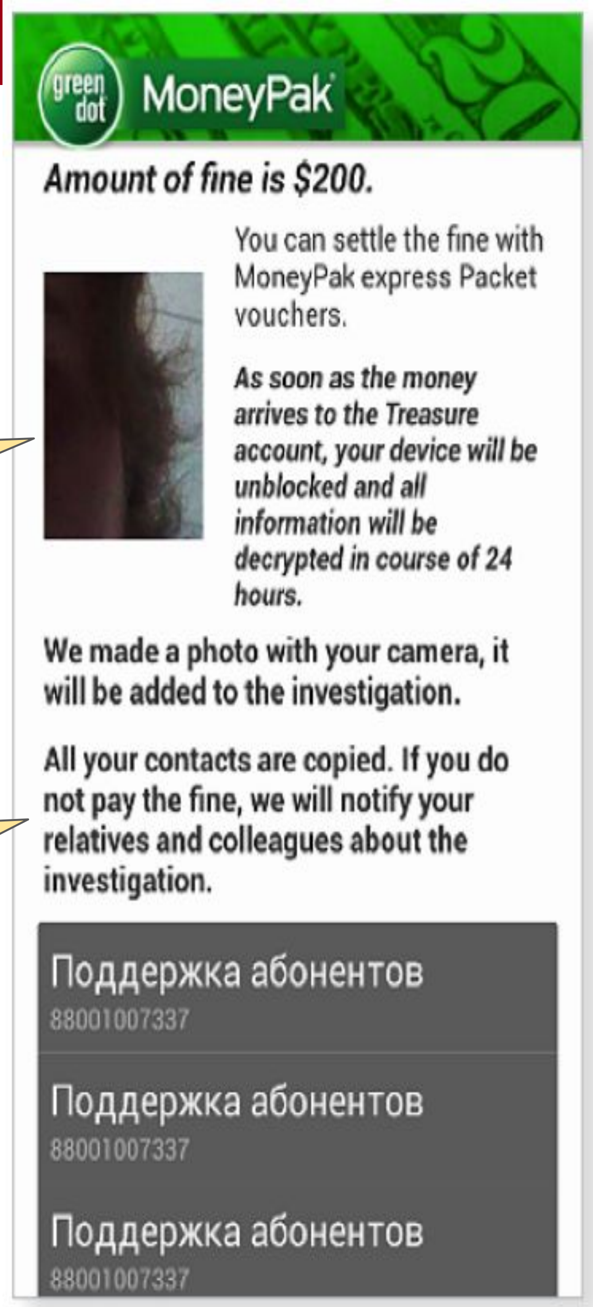
AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.

INFORMATION ON YOUR LOCATION AND SNAPSHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.

* You have been subjected to violation of Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted contents. Article 1, Section 8, Cause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

* You have been viewing or distributing prohibited

Ransomware



Amount of fine is $200.

You can settle the fine with MoneyPak express Packet vouchers.

As soon as the money arrives to the Treasure account, your device will be unblocked and all information will be decrypted in course of 24 hours.

We made a photo with your camera, it will be added to the investigation.

All your contacts are copied. If you do not pay the fine, we will notify your relatives and colleagues about the investigation.

Поддержка абонентов
88001007337

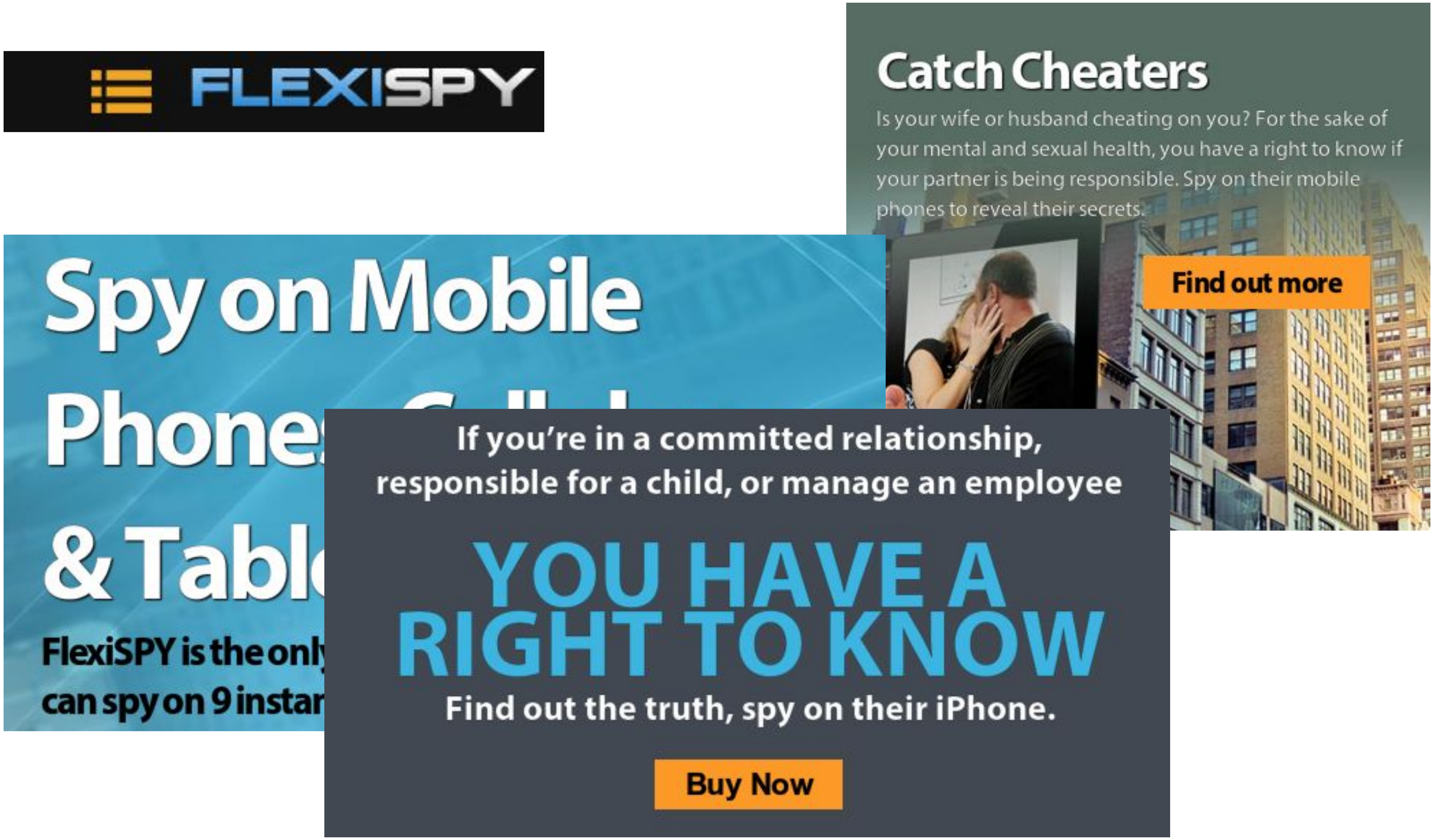
Поддержка абонентов
88001007337

Поддержка абонентов
88001007337

User's photo!

Contacts notification!

Spyware



FLEXISPY

Catch Cheaters

Is your wife or husband cheating on you? For the sake of your mental and sexual health, you have a right to know if your partner is being responsible. Spy on their mobile phones to reveal their secrets.

Find out more

Spy on Mobile Phone

& Tabl

FlexiSPY is the onl

can spy on 9 instar

If you're in a committed relationship, responsible for a child, or manage an employee

YOU HAVE A RIGHT TO KNOW

Find out the truth, spy on their iPhone.

Buy Now

FlexiSPY

- Features:
  - Call logs/recordings, Facebook/WhatsApp/Skype call logs/recordings
  - Email recording, Calendar, Location tracking, SIM changed notification
  - Keylogger, Application Screenshot
  - Remote photo acquisition
- Some features require root: they provide assistance!
  - "Installation Service"
- Quite expensive:
  - Premium: $99 / 3 month
  - Extreme: $199 / 3 months

AndroidRCS

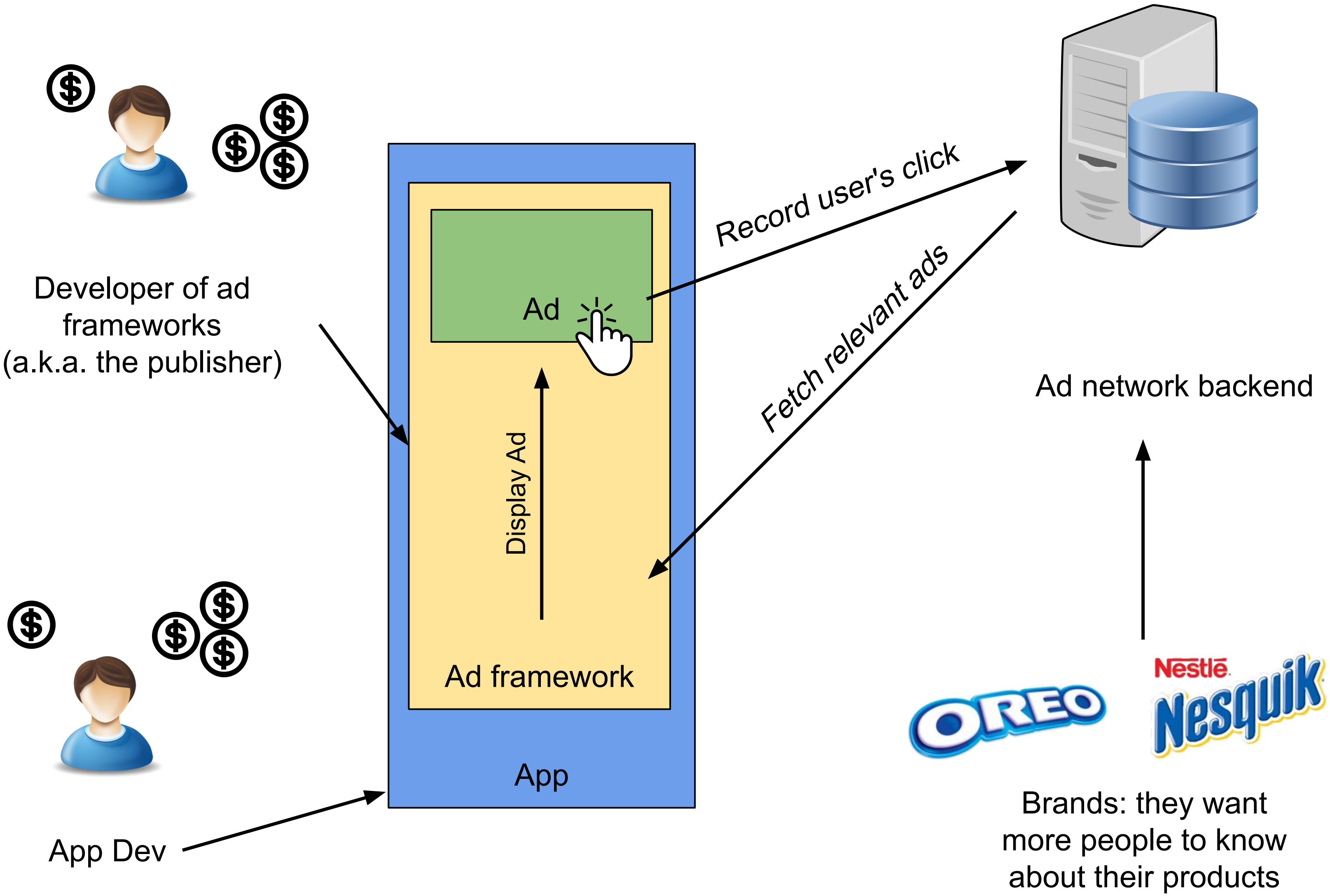
- Sophisticated malware used for "targeted attacks"
  - State-sponsored attacks, Advanced Persistent Threat (APT)
- Developed by HackingTeam
  - Italian security company, selling their products to (shady?) governments
  - Irony points: they got hacked, all private emails/info on wikileaks
- Long list of SMS-controllable “features”
  - Leak the victim’s private conversations, GPS location, and device tracking information, capture screenshots, collect information about online accounts, and capture real-time voice calls

Advertisement malware & frauds

Advertisement

- Several money-related malware/frauds relate to ads
- Very complex ecosystem
  - Malware authors can abuse the system in multiple ways

Ad Ecosystem



Developer of ad frameworks (a.k.a. the publisher)

App Dev

App

Ad framework

Ad

Display Ad

Record user's click

Fetch relevant ads

Ad network backend

Brands: they want more people to know about their products

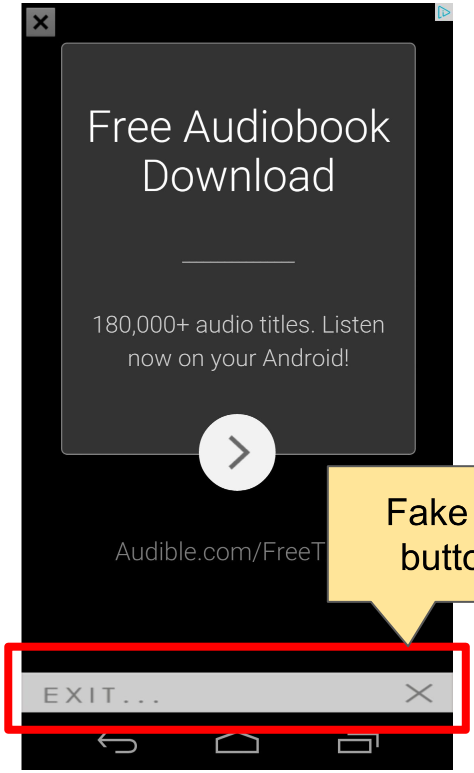
Advertisement

- Ad frameworks
  - Google's Admob, InMobi, Flurry, LeadBolt, AirPush, ...
- They differ from many aspects
  - money they pay to the app developer
  - the cost for the advertizer
  - how aggressively the ad is delivered (which technique?)
  - the level of "retargeting" they can offer
- Some have VERY shady/annoying practices

Adware

- Aggressive advertisement techniques
  - Notifications (sticky), shortcuts, overlays, in-app & abstract banners
  - Ads that pop out "out of nowhere" so you don't know which app is responsible for which ad
  - Ads in the "lock screen" view
- This is not technically a fraud, but it's annoying
- Net result: the user gets annoyed
  - but she is more likely to click on an ad ~> more money
  - if she is too annoyed & she finds the culprit app ~> uninstall

"Annoyware"



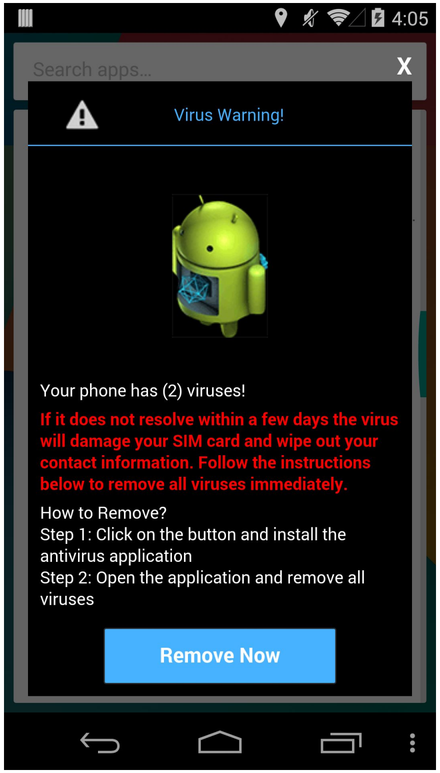
Free Audiobook Download

180,000+ audio titles. Listen now on your Android!

Audible.com/FreeT

EXIT...

Fake "X" button!



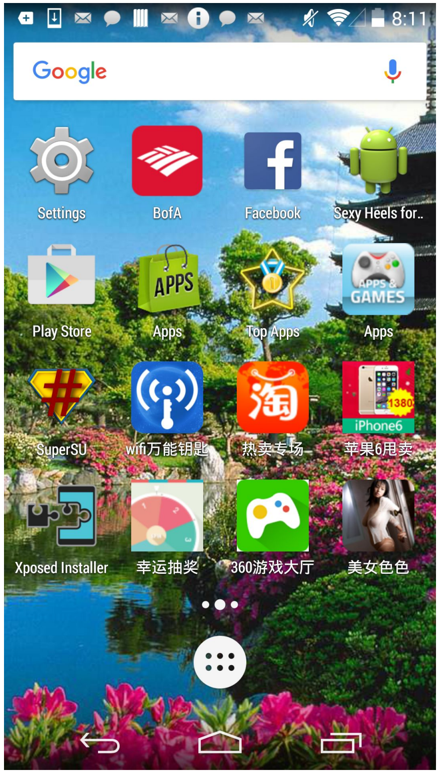
Virus Warning!

Your phone has (2) viruses!

If it does not resolve within a few days the virus will damage your SIM card and wipe out your contact information. Follow the instructions below to remove all viruses immediately.

How to Remove?
Step 1: Click on the button and install the antivirus application
Step 2: Open the application and remove all viruses

Remove Now



Ad click fraud

- An app embeds ads and it simulates user's clicks
  - App and ad views live in the same sandbox!
- To the ad network, it seems that the user clicked on ads!
- App developer gets money
  - The ad framework / the publish gets money as well!
- Net result
  - The advertizer/brand gets scammed
  - The advertizer loses trust in the publisher
    - It's in the publisher's best interest to show they detect/combat frauds!

Automatic traffic detection

- Automatic clicks are/were easy to detect
  - Very simple interactions, "easy" to distinguish user vs. bot
- Bots are now simulating real user's behavior
  - They can simulate users filling forms and watching videos
- Recent massive ad fraud: link
  - Millions of users "infected" and "tracked"
  - "By copying actual user behavior in the apps, the fraudsters were able to generate fake traffic that bypassed major fraud detection systems."

Click Farms

- "Large groups of low-paid workers whose job is to click on ads"
- We are talking about "actual humans"
- "Inside of A Chinese Click Farm (10K+ phones)"

Hiding ads

- The app uses multiple ad frameworks
- Some ads are "hidden"
    - "Ad stacking": multiple ads one on top of each other
    - "Pixel stuffing": ads fit in 1x1 pixel views
- The publisher & advertiser think "the ad was shown"

Installation referrals stealers

- Big story
  - Multi million dollar scam: Buzzfeed's Cheetah scandal
  - Eight apps with a total of more than 2 billion downloads
  - There is controversy:
    - Cheetah started replying to accusations with "we don't have control over ads SDKs"
    - "The Chinese company has condemned Kochava’s “misleading statements” in a press release, adding that it plans to take legal action against the firm."
    - Details on updates here

Installation referrals stealers

- App developers pay 50 cents ~> $3 to partners that help drive new installations

- Mechanism based on "Installation referrals"

- A just-installed app can "look back" and check "which device / app / ad framework" should be thanked for the installation

Installation referrals stealers

- The fraud: Click flooding and click injection

- Steps
  - The Cheetah apps listen for when a user downloads a new app
  - As soon as a new download is detected, the Cheetah app sends off clicks to ensure it gets "the last click"
  - It wins the bounty (even though it had nothing to do with the app being downloaded)
  - This is true even in cases when no ad was served and they played no role in the installation

Installation referrals stealers -- Bonus points

- It starts the just-installed app w/o the user’s knowledge
  - This helps increasing the odds that it will receive credit for the app install, as the bounty is only paid when a user opens a new app.
  - "They passed the attribution through many ad networks to hide the fact that so many attribution wins are coming from these apps"

- "Kika keyboard" app
  - It tracks keywords typed by users when they are searching for apps
  - It generates a series of clicks in an attempt to claim the bounty of potential future installations

Installation referrals stealers

- The scale of the fraud
  - Eight apps with a total of more than 2 billion downloads
  - "AppsFlyer analyzed 1 billion app installs over the past year and found 25% were fraudulent ~> an estimated $1.7 billion was stolen"

Ad targeting

- One of the main ad frameworks "feature": ad targeting
- Ad targeting: "the ability of tailoring which ads are shown to which user"
- Ad framework builds a "profile" of each user
  - Profile ⇔ "User X likes Nesquik"
  - This is one of the key feature of Facebook
    - They know everything about you from your "likes", "pages you visit", "websites you visit"
  - From Android O, "ANDROID_ID" is unique per device / per signing key

Cross-Device Tracking (XDT)

- The problem
  - Users browse the web via their laptop and via their mobile devices
  - "Chrome on laptop" profile is not linked with "Android device" profile
- Cross-Device Tracking (XDT)
  - Wouldn't it be great if users could be tracked across different devices?
- Concept: attempt to "link" users behind many devices

Cross-Device Tracking (XDT)

- XDT enables "Ad re-targeting"

- Scenario
  - User is in front of her television, and an ad about Nesquik is shown
  - The user's mobile device "detects" that Nesquik ad was just shown
  - Ad framework within mobile app pops out with a Nesquik-related ad

- Extremely creepy

Cross-Device Tracking (XDT)

- How can it be done?

- Google can track you across devices because most users are "logged in" in all of them
    - Example: users are logged in their chrome browser on their laptop and on their Android devices: Google can establish a link

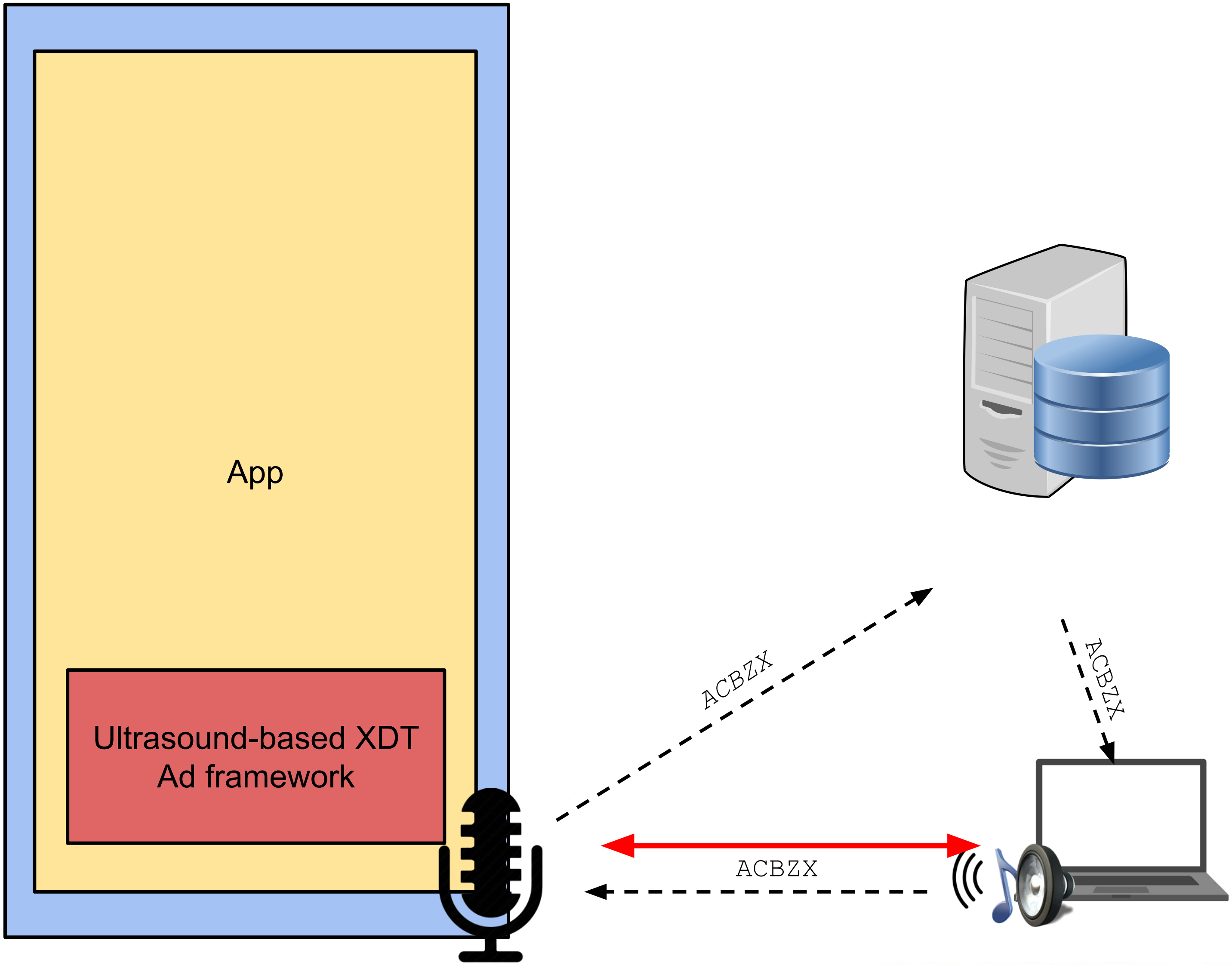
- But what about other companies? And other "devices"?

Ultrasound-based Cross-Device Tracking

- Super creepy technology to track users across multiple devices (smartphones, PCs, televisions)

- Idea: the microphone on your mobile device is used to "pick up" ultrasound-based "beacons" emitted by other devices around you (television, laptop, etc.)

- Main company: SilverPush (ArsTechnica article)
  - They now moved on and are doing different ad-related stuff


App
Ultrasound-based XDT Ad framework
ACBZX
ACBZX
ACBZX

How does malware get on your phone?

Multiple security mechanisms to bypass

- Google Play Store’s vetting process
- Each app needs to be manually installed
  - Why would a user install these malicious apps?
- Many security mechanisms on Android
- Permission system: the user is asked for everything

Google's Vetting Process

- Google scans each APK submitted to the Play Store
- The app needs to pass security checks
- Only after the app has passed all the checks, it is accepted to the store and users can start downloading it

Google's Vetting Process Security Checks

- Static program analysis
  - It consists in trying to understand what the app is doing without running it
  - It looks for common "malicious" patterns
- Dynamic program analysis
  - Same goal, but it actually runs the app (~5 min) and logs what it does
  - They run the apps within emulators (this is my understanding)
- Analysis on metadata of the app / app developer

Bypassing Google’s Vetting Process

- Bypassing static analysis
  - Code obfuscation
  - Dynamic code loading (now "against the policy", but can be undetected)
- Bypassing dynamic analysis
  - Emulators can be detected ~> malicious functionality is not executed
  - Intentionally delayed functionality
  - Check for user's presence
- Note: Google can only control the Play Store!
  - Google can't "prevent" malware to be published on 3rd-party stores

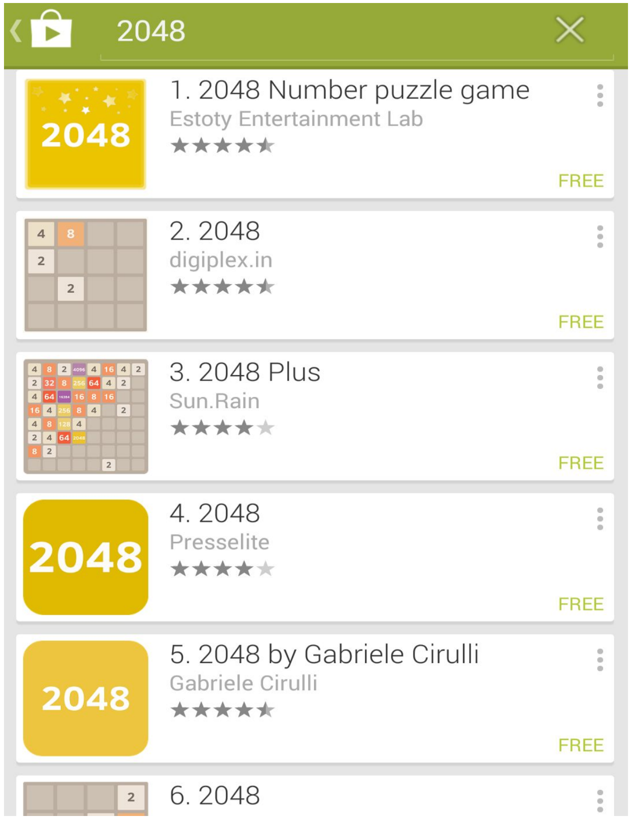
Apps are manually installed

- Once Google's vetting process is bypassed...
- ... why would a user install app X?
- Several strategies
  - Social Engineering
  - Repackaging
  - Benign-becomes-malicious aka "turning bad"

Social Engineering

- Somehow convinces the user that the app she is looking for is exactly yours
- Possible techniques
  - Upload similar-looking apps on the store and hope the user is tricked
  - Malicious ads point the user to the wrong app
  - Offer the "free" version of an otherwise "paid" app
  - Offer "extra features" with respect to the "basic" version of the app

Social Engineering



2048

1. 2048 Number puzzle game
Estoty Entertainment Lab
★★★★½
FREE

2. 2048
digiplex.in
★★★★½
FREE

3. 2048 Plus
Sun.Rain
★★★★☆
FREE

4. 2048
Presselite
★★★★☆
FREE

5. 2048 by Gabriele Cirulli
Gabriele Cirulli
★★★★½
FREE

6. 2048

Repackaging

- Repackaging steps
  - download app A
  - unpack it
  - add "feature XYZ"
  - repack it
  - upload it with slightly different name (or somewhere else)

- Very trivial from the technical standpoint!

Repackaging - Use cases

- Paid app is repackaged / re-uploaded as "free" but with
  - Advertisement ~> the 'malware' author gets ads money
  - Tracking functionality to steal user's data
  - Actual malicious functionality

- Repackaged free apps are advertised with extra features
  - These extra features may not even exist

Turning Bad

- App that is initially benign suddenly becomes malicious
  - All users will be infected at the next update (which happen automatically)

- How can this happen?
  - "Legal" change of ownership
    - The app is sold to a new "developer", who abuses the popularity of the app to start with an already big user base
  - The developer gets hacked
  - An entire software editor gets hacked (!)

XcodeGhost malware for iOS

- Xcode is a very popular code editor for Apple's macOS
- Malicious version of Xcode published on Chinese market
  - Theory: network speed is slower in China, devs looked for local copy
- All apps compiled with it are modified with malware
  - Over 4000 "benign" apps infected (including WeChat)
- Malicious behavior included
  - stealing user device information
  - read/write clipboard
  - hijack opening urls

Bypass of security mechanisms

- Even if the attacker can install an app, there are many security checks / mechanisms in place

- This is when "security vulnerabilities" kick in
    - Malware can bypass permission checks, mount privilege escalation attack, attack other user's apps, get code execution on your phone by just being on the same wifi

Questions? Feedback? Suggestions?