Malware in Google Play: Latest tactics used to penetrate the official app store

Corneliu Nitu
Security Researcher
Nokia Threat Intelligence Lab

Presentation Outline

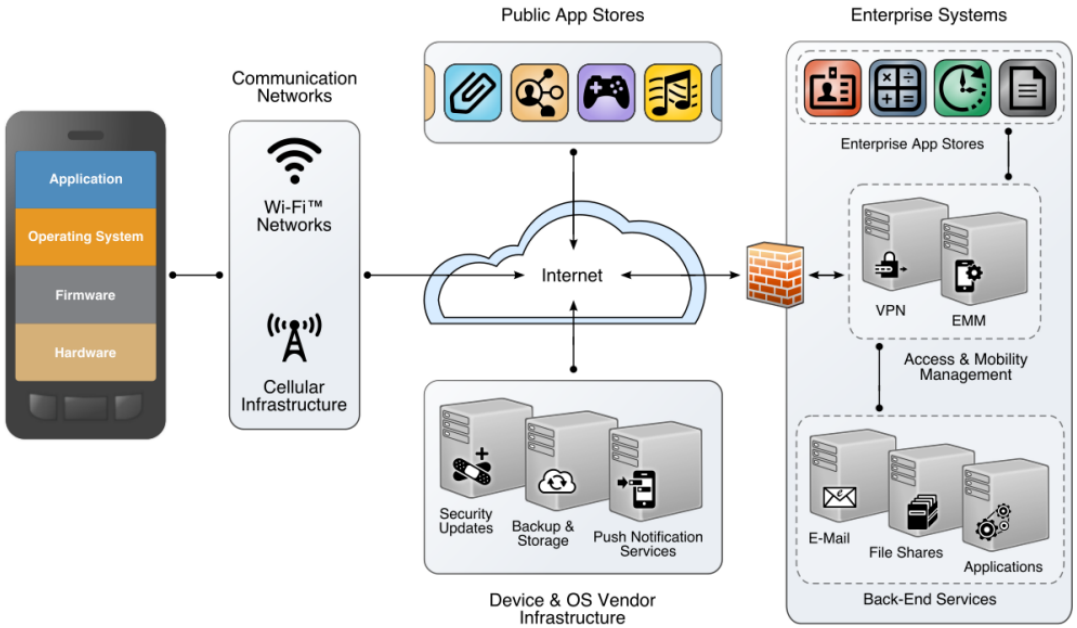
1. Objectives
    > Focus on Google Play security
2. Mobile application ecosystems
    > Architecture, security goals
3. Mobile vulnerabilities and attacks landscape
    > Focus on Mobile Applications Security
4. Google Play
    > Security considerations
5. Malware in Google Play
    > Major categories with concrete examples
6. What can be done to improve security
    > Responsibilities of each player

Official App Store in Focus

- Mobile security is important:
  - Protect devices and the local user data
  - Guard the gateway to cloud
- Mobile application security: one of the main components of mobile security
- Theoretically, mobile application security is under control:
  - use well developed, security proofed apps from tightly controlled repositories (app stores) that communicate securely with the cloud.
- However: recurring cases of malicious applications that gain widespread circulation
- Critical: ensure that malware doesn’t penetrate the official app store

Mobile application ecosystems

- More than mobile devices and apps (the visible part of the ecosystem)
- Integrated system serving the goal of creating a seamless, end-to-end experience
- Multitude of players, processes and assets
- Each player has certain responsibilities



Credit: National Institute of Standards and Technology [NISTIR 8144]

Mobile application ecosystems (cont.)

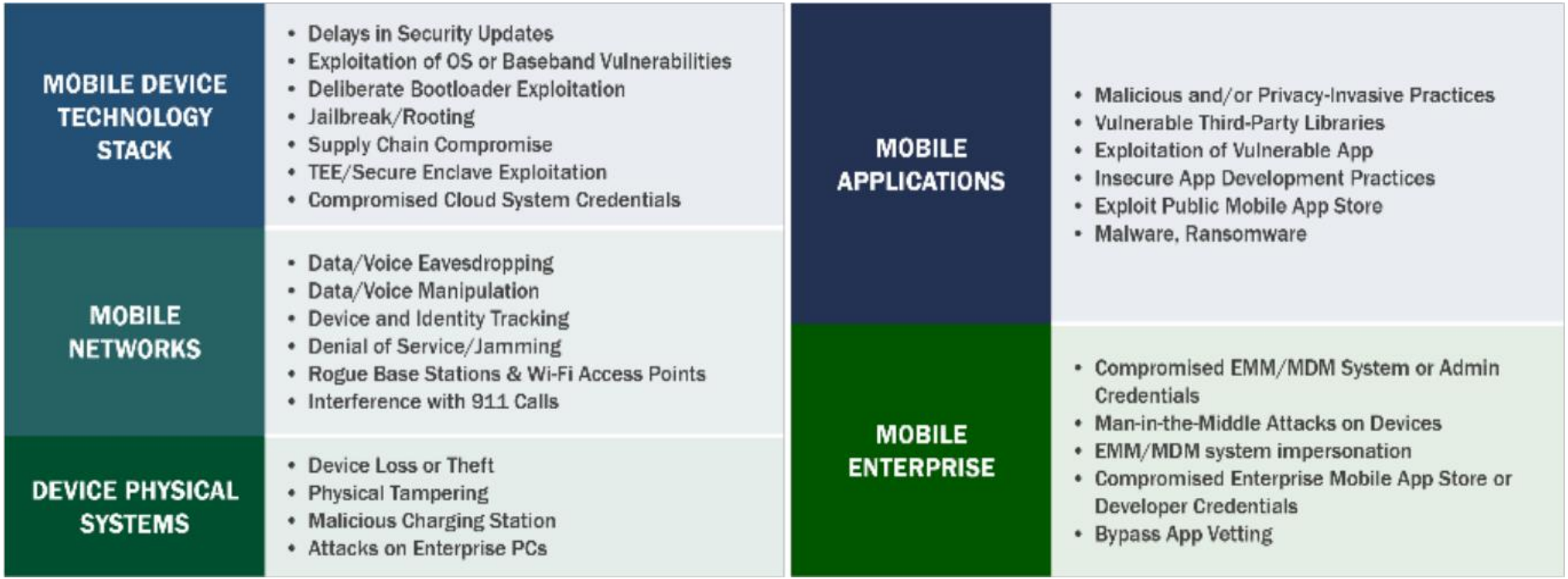
Mobile Security is centered on the security of private information across the ecosystem.

Goals:

- Protect local data stored on the mobile device (sensitive information like home address, telephone number, medical information and credit card numbers to authentication information (users & passwords))
- Protect identity, as identity theft can be used to gain unauthorized access to information (in the cloud) that can then be compromised or stolen.

Mobile vulnerabilities and attacks landscape

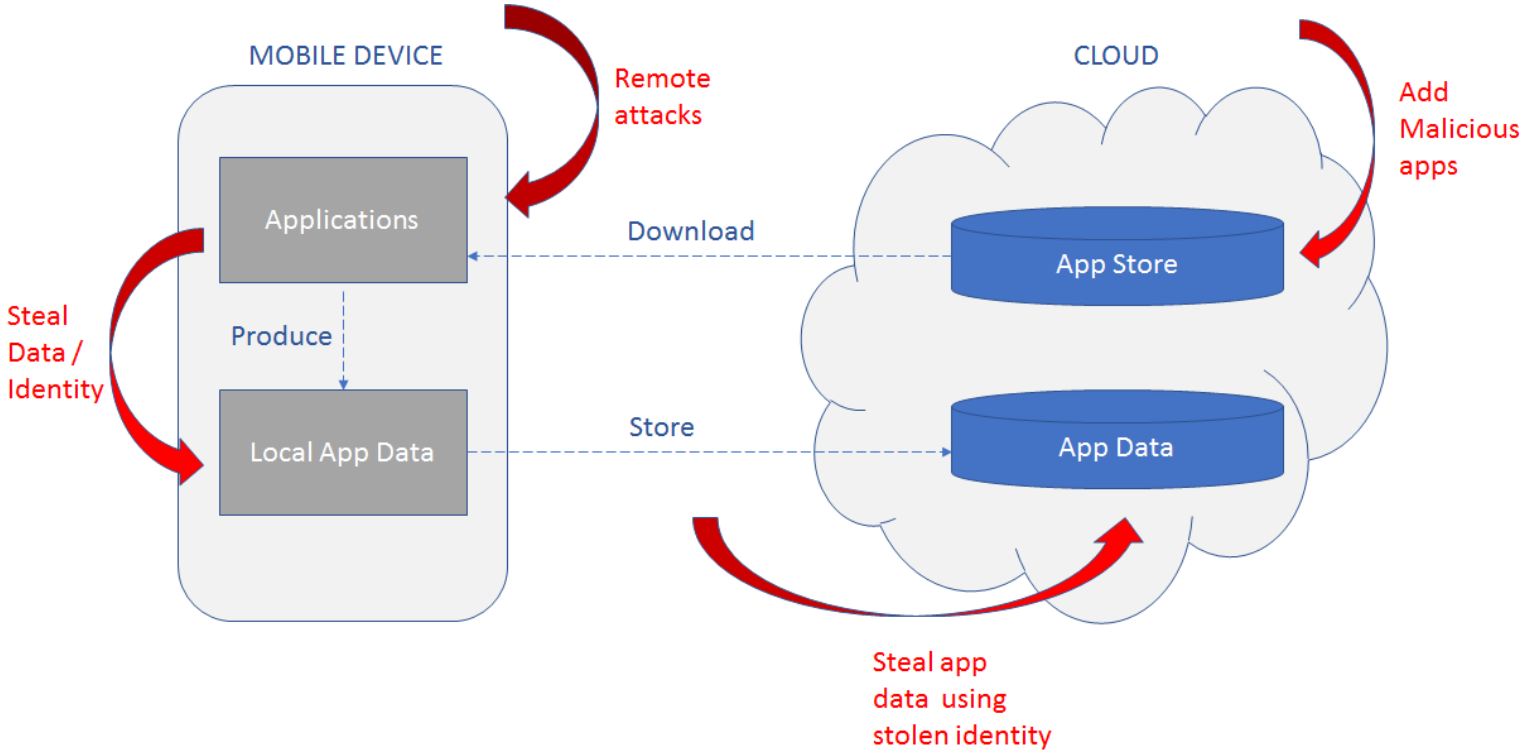
Homeland Security: Mobile Security Threats by Category



Credit: Homeland Security [CYBERSECURITY ACT 2015]

Mobile vulnerabilities and attacks landscape (cont.)

Focusing on Mobile Applications Security:



Google Play: Security

- The following are explicitly prohibited from Google Play:
  - Viruses, trojan horses, malware, spyware or any other malicious software.
  - Apps that link to or facilitate the distribution or installation of malicious software.
  - Apps or SDKs that download executable code, such as dex files or native code, from a source other than Google Play.
  - Apps that introduce or exploit security vulnerabilities.
  - Apps that steal a user's authentication information (such as usernames or passwords) or that mimic other apps or websites to trick users into disclosing personal or authentication information.
  - Apps may not depict unverified or real world phone numbers, contacts, addresses, or personally identifiable information of non-consenting individuals or entities.
  - Apps that install other apps on a device without the user's prior consent.
  - Apps designed to secretly collect device usage, such as commercial spyware apps.
  - Apps that monitor or track a user's behavior on a device must comply with strict requirements

Credit: Google Play - Developer Policy Center [GOOGLE]

Google Play: Security (cont.)

Google Play Protect - automated antivirus system, scans both new and existing apps for malware:

- It runs a safety check on apps from the Google Play Store before download them.
- It checks the device for potentially harmful apps from other sources.
- It warns about any detected potentially harmful apps found, and removes known harmful apps from the device.
- It warns about detected apps that violate the Unwanted Software Policy by hiding or misrepresenting important information.
- It sends privacy alerts about apps that can get user permissions to access personal information

Malware in Google play

“A total of 172 malicious apps were detected on Google Play in September, with more than 330 million installations.” October 1st, 2019

Harmful app type	Number of apps	Number of installs
Adware	48	300,600,000+
Subscription Scam	15	20,000,000+
Hidden Ads	57	14,550,000+
SMS Premium Subscription	24	472,000+
Hidden App	7	310,000+
Banking Trojan	1	10,000+
Stalkware	1	10,000+
Fake Antivirus	1	10,000+
Credit Card Phishing	2	200+
Fake Cryptocurrency Exchanges	1	100+
Fake App	15	100+
sum	**172**	**335,962,400+**

Credit: Lukas Stefanko [ESET]

1. Commercial SpyWare - Overview

- Commercial solutions, mostly found on third-party app stores
- Insider attack: the attacker has access to the device and its credentials
- Tracking children, partners, employees.
- Allow for: Location tracking, spying on calls, text messages and e-mails, unlimited access to the address book and calendar event, remote control features,monitoring of phone’s surroundings, etc
- Google reviews apps that are submitted to ensure that the apps meet the company's standards for privacy.
- Can be detected and reported to the legitimate user

Commercial SpyWare - Examples

Removed from Google Play:

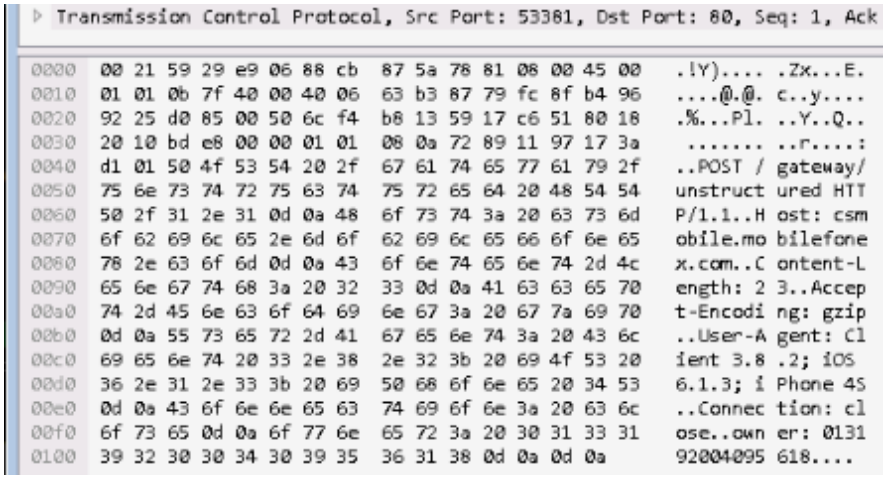
- Track Employees Check Work Phone Online Spy Free
- Spy Kids Tracker
- Phone Cell Tracker
- Mobile Tracking
- Spy Tracker
- SMS Tracker
- Employee Work Spy
- Family Employee Monitor

Available from third-party app stores:

Commercial SpyWare - Details

- FlexiSpy: One of the most well-known forms of stalkerware
- Slogan: "It takes complete control of the device, letting you know everything, no matter where you are."
- Able to: listen in on calls, spy on apps (Facebook, Viber, and WhatsApp) turn on the infected device's microphone covertly, record Android VoIP calls, exfiltrate content such as photos, and intercept both SMS messages and emails.

```
alert tcp $HOME_NET any -> $EXTERNAL_NET
$HTTP_PORTS (msg:"MobileSpyware.FlexiSpy -
Sending Personal Data to Cloud Service";
flow:established,from_client;content:"POST";ht
tp_method;content:"/gateway/unstructured";http
_uri;fast_pattern;content:"Host|3A
20|csmobile.mobilefonex.com";http_header;pcre:
"/User-Agent: Client.* iOS.*/";
content:"owner|3A
20|";http_header;classtype:MobileSpyware;
sid:515060860; rev:1; )
```



2. Government spyware - Overview

- Operate outside the lawful interception framework
- Used by governments to boost surveillance capabilities
- Placing trojenized apps in Google Play is just one of the many ways to gain access to private information

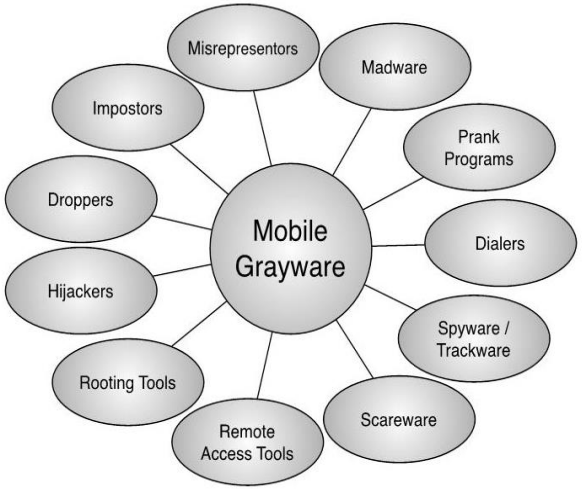
Government spyware - Example

Exodus: powerful but faulty spyware disguised as apps distributed by Italian mobile operators [EXODUS]

- Apparently purchased from a company that sells surveillance cameras
- Extensive abilities for data collection and exfiltration: installed apps, browsing history, address book, Facebook contacts and GPS coordinates, switch on and listen via the microphone and take photos with the camera, retrieve all SMS messages, extract messages and the encryption key from Telegram, dump data from Viber, extract logs and retrieve any media exchanged via WhatsApp, and extract logs, contacts and messages from Skype, etc.
- Works in two stages:
  - Exodus One: works as a decoy, loads and executes a payload of Exodus Two
  - Exodus Two: handles data collection and exfiltration
- More than 20 malicious apps in the Exodus family went unnoticed by Google over the course of roughly two years
- Google confirmed removal of all of the Exodus apps

3. PUAs (grayware) - Overview

- Apps that pose high risk or have negative impact on user security and/or privacy.
- The user expects negative side-effects, but accepts those as the price of getting what they want
- PUAs do not explicitly and completely state their functions and purpose
- Typical behaviour:
  - Advertising – excessive/aggressive advertisements, even when the app doesn’t run
  - Information collection without users' consent
  - Runs unwanted processes or applications that consume computing resources
  - Bundling – There are applications that, when installed in a device or a computer, installs other applications (bundled software) that users may not want.

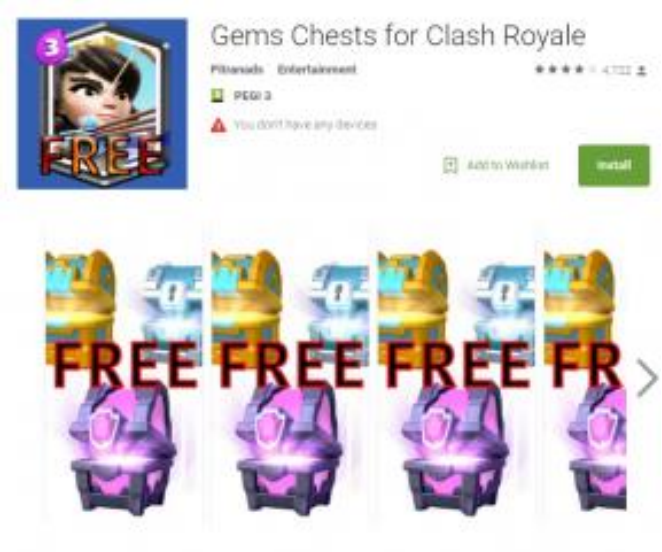


Credit: NC State University [GREYWARE]

PUAs (shady apps) - Examples

“Gems Chest for Clash Royale” - game cheats

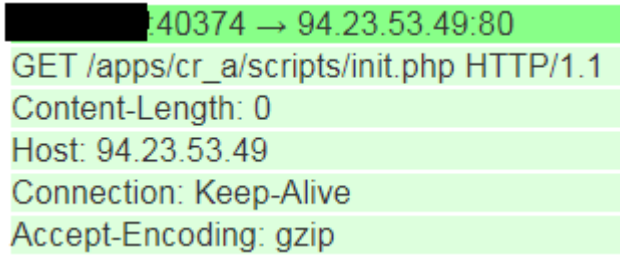
- Up to 500,000 downloads, good ratings
- Contains a new Android malware called CallJam
- CallJam malware includes:
  - A premium dialer to generate fraudulent phone calls: C&C remotely initiates calls to premium numbers
  - A rough adnet to display ads forcibly to its victims: redirects victims to malicious websites that generate fraudulent revenue for the attacker.



PUAs (shady apps) - Details

Detection of CallJam:

```
alert tcp $HOME_NET 1024: -> $EXTERNAL_NET $HTTP_PORTS (msg:"Android.Trojan.CallJam -
Communicating With Command and Control Server"; flow:established,from_client;
content:"GET"; http_method; content:"/apps/cr_a/scripts/init.php"; fast_pattern; http_uri;
content:"Content-Length|3A 20|0"; http_header; content:!"User-Agent|3A 20|"; distance:0;
http_header; reference:apknviso,2016ea74f15f4d0b98b7c50b05dacd09;
reference:url,blog.checkpoint.com/2016/09/08/calljam-android-malware-found-on-google-
play/; reference:url,androidcommunity.com/calljam-malware-now-in-google-play-racks-up-
cash-for-hackers-thru-premium-calls-20160910/;  classtype:Trojan; sid:516101701; rev:1; )
```



4. Corrupted libraries - Overview

- Reputable apps from reputable development firms
- Un-intentionally, development firms use libraries that are or turn malicious
- Affects large swaths of applications
- Libraries require extensive permissions but don’t disclose how they are used
- Possibility for intra-library collusion: library leverages the combined set of permissions available to it

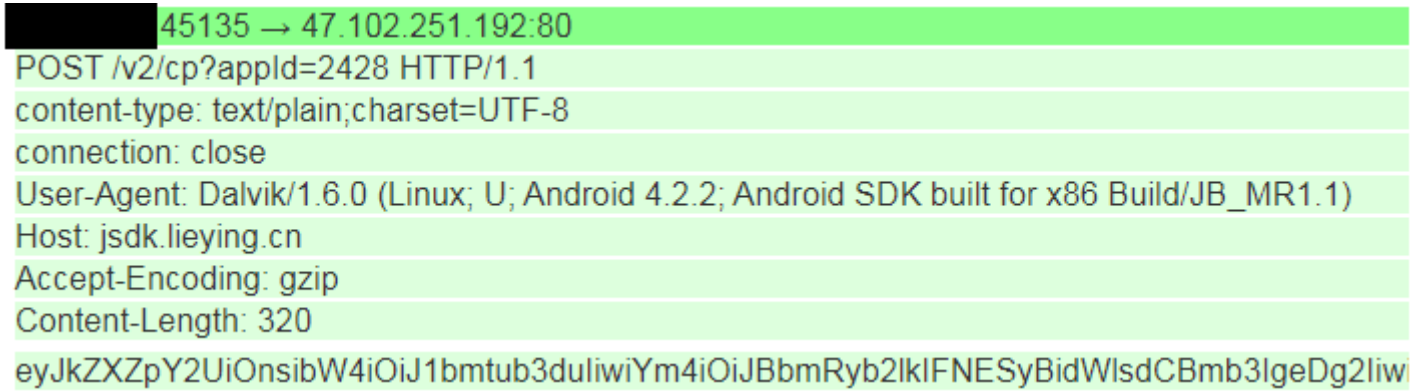
Corrupted libraries - Examples

- CamScanner: PDF creator and optical character recognition (OCR)
- Malicious component detected as *Trojan-Dropper.AndroidOS.Necro.n*
  - Decrypts and executes the malicious code contained in the mutter.zip file in the app resources.
  - Configuration file “comparison” is decrypted. Obtains addresses of the attackers’ servers
  - Dropper downloads an additional module and executes it
  - Owners of the module can use an infected device: showing the victim intrusive advertising & stealing money from their mobile account by charging paid subscriptions.
- Malicious component was introduced into their app's codebase via a third party SDK provided by AdHub.
- Application was removed from Google Play
- Updated version exists and is pending reintroduction in Google Play

Corrupted libraries - Details

Detection of CamScanner's communication with its C&C server:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS
(msg:"Android.Hijacker.CamScanner - Sending System Information to Command and
Control Server"; flow:established,from_client; content:"POST"; http_method;
content:"/v2/cp?appId="; fast_pattern; http_uri; content:"Android"; http_header;
content:"eyJkZXZpY2"; http_client_body; depth:10; classtype:Hijacker;
sid:519092480; rev:1; )
```



5. Infected development tools - Overview

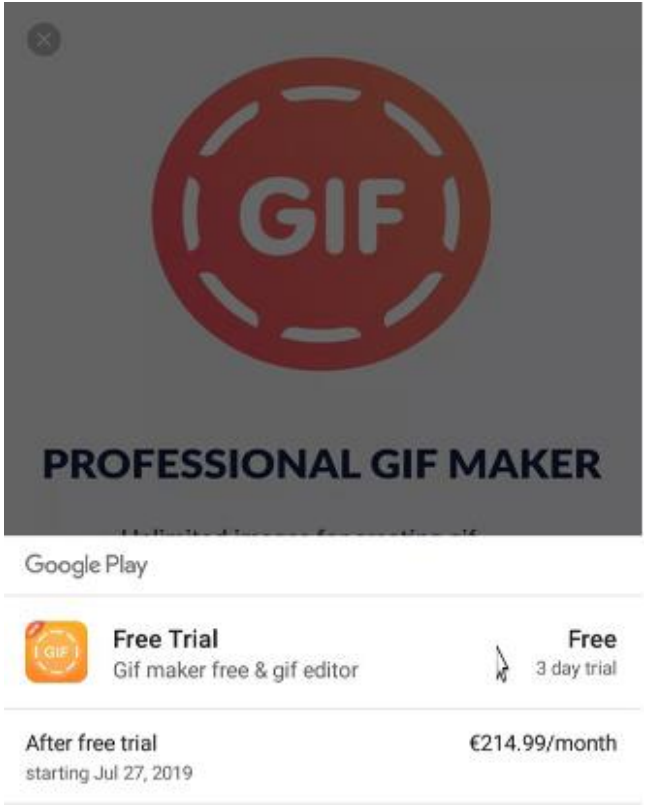
- The programming environment has some minor changes to get the malware into apps created with it
- Unbeknownst to developers
- Affects a large swaths of applications developed with the IDE
- The infected IDE is not in the official repository, but in third-party repositories
- However, the infected applications end up in the official app repository
- Not yet encountered in Google Play, however the danger exists (see XCodeGhost)

6. Fleeceware business model - Overview

- The purpose is to severely overcharge users for trivial mobile apps
- Very same functionality is available on low-cost or free apps
- Business model available within the Play Market ecosystem:
  - Users can download and use the apps at no charge for a short trial period
  - When the trial expires, if the user hasn't both uninstalled the application and informed the developer that they do not wish to continue to use the app, the app developer charges the user.
  - No way to get money back
- Practice permitted in Google Play Market, as follows the rules for in-app purchases
- The apps are clearly consumer-hostile, but are not otherwise malicious
- The apps do perform the function they claim to be able to do

Fleeceware business model - Examples

Package name	Install Count	Cost (after free trial ends)
qr.code.barcode.maker.scanner.reader	5,000,000+	€104.99
faceapp.facemystery.learnmoreaboutyourself	10,000,000+	€104.99
com.recorder.video.magic.capture.gameplay	5,000,000+	€104.99
com.ally.video.recorder	5,000+	€114.99
com.pey.old.me.face.aging	50,000+	€104.99
com.gifmaker.giffree.gifeditor	5,000+	€219.99
com.hidephotovideo.calculatorphotovault	1,000+	€104.99
com.compasspro.gpscoordinates	10,000+	€219.99
com.searchbyimage.reverseimagesearch	10,000+	€219.99



Credit: Sophos News [FLEECEWARE]

7. Outright malicious - Overview

- The apps usually perform the advertised functionality
- Covertly, they do some hidden activity
- They rely on the user accepting permissions that are clearly not needed/appropriate. Thus, they have a vaneer of legitimacy
- They are subject to removal from Google Play
- Identifiable by:
  - Reviews
  - Number of downloads
  - Side effects, e.g. degraded performance

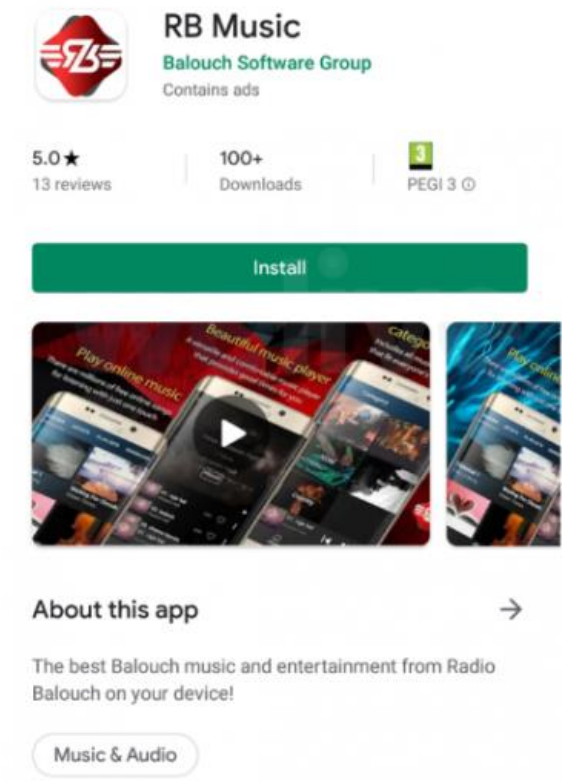
Outright malicious - Examples

Radio Balouch aka RB Music, is actually a fully working streaming radio app for Balouchi music enthusiasts.

It is built on the foundations of AhMyth open-source espionage tool:

- Steals contacts
- Harvests files stored on the device
- Sends SMS messages from the affected device
- Steals SMS messages stored on the device
- Might get further functions in the future via an update.

Removed from Google Play after appearing twice



Outright malicious - Examples

Study case Flashlighs

Normal permissions needed by these apps:

- Access the phone's flashlight
- Access the Internet, for in-app ads
- Access to the lock screen

Permission	Number of Apps
GET_TASKS	389
KILL_BACKGROUND_PROCESSES	282
READ_CONTACTS	180
CALL_PHONE	155
ACCESS_FINE_LOCATION	131
BLUETOOTH_ADMIN	100
GET_ACCOUNTS	100
PROCESS_OUTOING_CALLS	98
RECEIVE_SMS	82
RECORD_AUDIO	77
ANSWER_PHONE_CALLS	63
AUTHENTICATE_ACCOUNTS	59
DOWNLOAD_WITHOUT_NOTIFICATION	24
WRITE_CONTACTS	21
PROCESS _INCOMING_CALLS	8

Credit: avast.io [FLASHLIGHTS]

937 flashlight Android applications,

- 408 of the apps need just 10 permissions or less
- 262 apps require 50 permissions or more

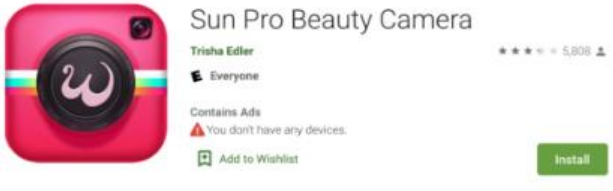
No.	App Name	Permissions Count	Number of Downloads
1	Ultra Color Flashlight	77	100,000
2	Super Bright Flashlight	77	100,000
3	Flashlight Plus	76	1,000,000
4	Brightest LED Flashlight — Multi LED & SOS Mode	76	100,000
5	Fun Flashlight SOS mode & Multi LED	76	100,000

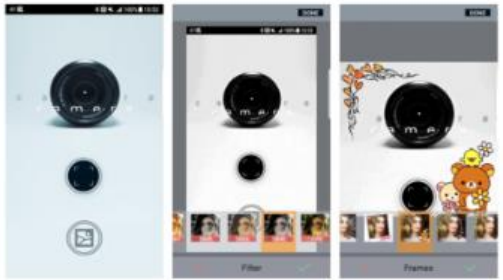
Outright malicious - Examples

Apps that are not spying on users, but aggressively pushing adware that cover the entire screen:

- Sun Pro Beauty Camera, with more than one million installations
- Funny Sweet Beauty Selfie Camera, installed over 500,000 times.

Worrying permissions RECORD_AUDIO, SYSTEM_ALERT_WINDOW





Outright malicious - Examples

XGEN.PI: Malware that bypasses the normal app upgrade mechanism.

Network traffic used to check for a payload update, followed by download of zip files containing .dex files:

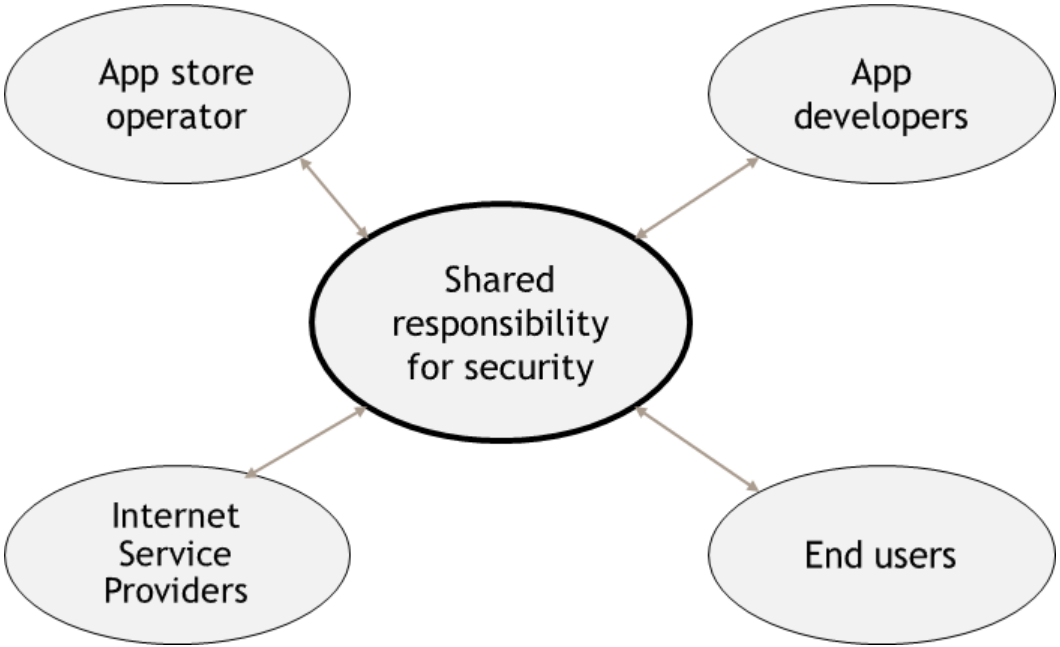
```
GET /update/check?
pkey=1008&ts=1558710080420&data=ybPol8bQ2eKgQpP037%2BURhA8EUXmLh49qozplF9SRygCcS0UrKiZEXgxbozxIU0PRaqrxUwdh7hWHOkCzwrerq9GZ7pIeoXJaHo6vs3OLD
...
%2FGYhk2RlZMsHjNrrsB7IbcR1AQ%3D%3D&secret=01a36e35312c41edd77174c2b42d912c&isencry=1 HTTP/1.1
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.4.3; Nexus 5 Build/KTU84M)
Accept-Encoding: gzip
Host: cat.moyumedia.com
Connection: Keep-Alive
```

Network traffic used to download a new version of the payload (truck.moyumedia.com):

```
GET /nfile/update/zkadsdex/2019032953545050.zip HTTP/1.1
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.4.3; Nexus 5 Build/KTU84M)
Host: truck.moyumedia.com
Connection: Keep-Alive
Accept-Encoding: gzip
```

What can be done?

Responsibility for mobile application security is shared between all the participants in the ecosystem:



Responsibilities of app developers

- Use vetted libraries
- Don’t let open backdoors
- Use minimum necessary of permissions
- PenTest the applications
- Operate a bug bounty program (with Google’s help)

Responsibilities of Google

Google takes mobile app security very seriously - a significant reduction in mobile malware infections was observed.
Current initiatives:

- Improve permission management - to combat abuse, starting Android 6 (Marshmallow), apps using a dangerous permission need to ask for approval at run time.
- Google Play Security Reward Program (GPSRP), and the Developer Data Protection Reward Program (DDPRP).
- Throw the security net over not just its own apps, but over all very popular third-party software.
- Encourage app makers that don’t yet have bug bounty programs to start them up.
- Scanning for malicious applications in Google Play and removal of the offending apps

Responsibilities of ISPs

- ISPs monitor traffic for attacks on subscribers and for signs of infection of subscriber’s devices
- Sometimes they share threat intelligence with end users in form of monthly protection plans
- Detect lateral movement
- Isolate/disable the worst offenders

Responsibilities of end users

- Don’t install bad apps in the first place: check the news, check permissions
- Familiarize themselves with the permissions
- Observe application behaviour, e.g. too many ads
- Subscribe for protection plan, if offered by ISP
- Stick with official sources of apps
- Install a reputable mobile security solution.
- Install an Anti Spy application

Conclusions

- No clear boundary between perpetrators and victims:
  - Good guys become involuntarily bad guys
  - Victims have a share of responsibility in the attacks that targets them
- Mobile application security - responsibility of all players of the mobile ecosystem:
  - Developers, end users, application stores operators, ISPs, etc
- Vigilance is required - the official app stores are prime targets for malicious actors

References

[NISTIR 8144] Draft NISTIR 8144: Assessing Threats to Mobile Devices & Infrastructure - The Mobile Threat Catalogue.
csrc.nist.gov/csrc/media/publications/nistir/8144/draft/documents/nistir8144_draft.pdf

[CYBERSECURITY ACT 2015] Study on Mobile Device Security - Cybersecurity Act of 2015, Title IV, Section 401

csrc.nist.gov/CSRC/media/Presentations/Study-on-Mobile-Device-Security/images-media/vs-jf-study-mobile-device-security.pdf

[GOOGLE] Google Play - Developer Policy Center: Privacy, Security, and Deception

play.google.com/about/privacy-security-deception/malicious-behavior/

[ESET] ESET: Android Security Monthly Recap #9, September 2019

lukasstefanko.com/2019/10/android-security-monthly-recap-9.html

[EXODUS] Security Without Borders:Exodus: New Android Spyware Made in Italy

securitywithoutborders.org/blog/2019/03/29/exodus.html

References

[GREYWARE] NC State University, B. Andow et al.: A Study of Grayware on Google Play

https://slideplayer.com/slide/12543616/

[FLEECEWARE] Sophos News: ‘Fleeceware’ apps overcharge users for basic app functionality

news.sophos.com/en-us/2019/09/25/fleeceware-apps-overcharge-users-for-basic-app-functionality/?cmp=30728

[FLASHLIGHTS] avast.io: Flashlight Apps on Google Play Request Up to 77 Permissions

https://decoded.avast.io/luiscorrons/flashlight-apps-on-google-play-request-up-to-77-permissions/