

**Regional Forum on Cybersecurity in the Era of Emerging Technologies &
the Second Meeting of the “Successful Administrative Practices”-2017
Cairo, Egypt 28-29 November 2017**



ITU WTDC
BUENOS AIRES 2017
9-20 October

SMART PHONE SECURITY THREATS

Eng. Ahmed Mohamed El-Sayed
Head of Multimedia & Creative Education of Science Unit
Academy Of Scientific Research & Technology



CELEBRATING
25 YEARS
OF ACHIEVEMENTS

**YOUR MOBILE PHONE IS WATCHING YOU ...
AND HACKERS WATCHING YOUR MOBILE PHONE ...
SO THEY WATCHING YOU ... BY HACKING YOUR BEHAVIOR**

This study is based on a sample of

1.5 Million

Most Recent Single
Applications

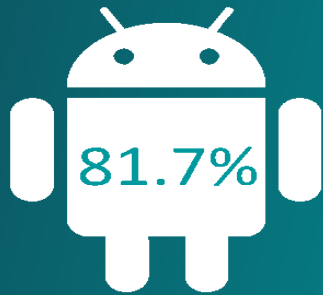


**YOUR
PHONE
IS
WATCHING
YOU**



ANDROID / iOS

99.6% of new smartphones
run Android or iOS



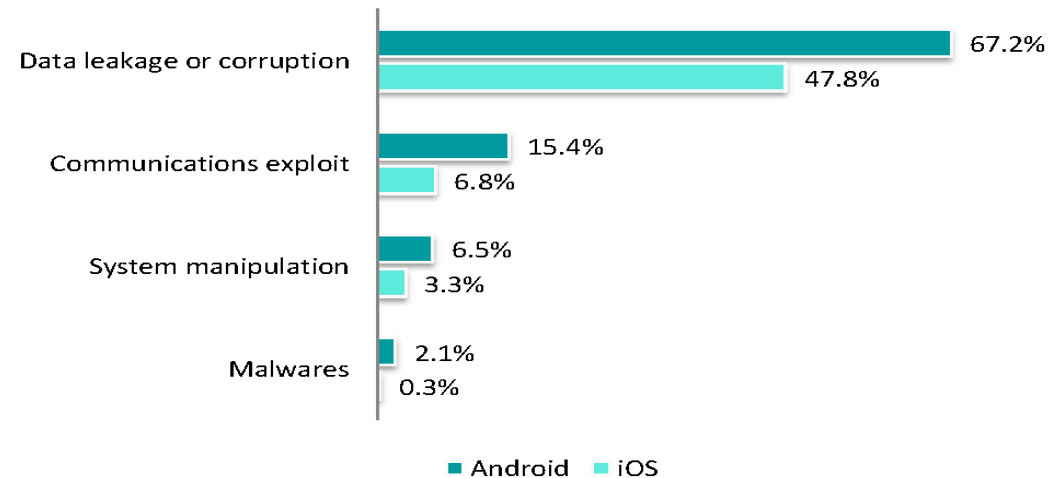
Gartner's Q4 2016 figures

WHAT IS DIFFERENT?

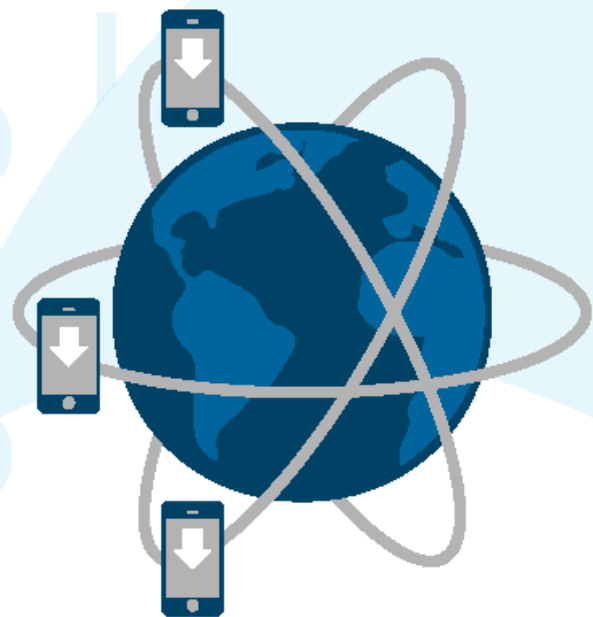
Android turns out to be a privileged threat landscape.

More permissive than iOS, Android is an easier playground for hackers with a higher propagation rate because of its widespread use. iOS requires more complex hacking techniques to bypass Play store's and user's checks. However, data leakage and corruption also hits a high ratio with 47.8% of Applications. In addition, iOS malwares, though less numerous than Android, still represent an important threat in terms of damages.

% Applications featuring a malicious or an intrusive behaviors for Android and iOS



Take a comprehensive approach to securing the mobile enterprise



By 2016 there will be over **2 billion smart-phone users**¹ with over **268 billion mobile downloads** by 2017²



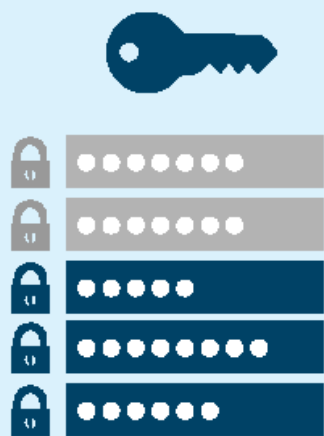
There are **387 new threats every minute** or more than six every second.³ **97%** of top paid **Android apps** and **87%** of top paid **iOS apps have been hacked**⁴



97% say some portion of workforce **uses mobile devices** in their job today⁵



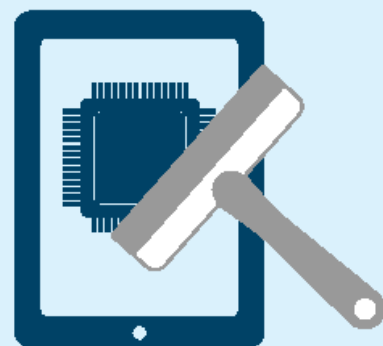
Protect devices



60% use passcodes for device security⁵



32% say lost/stolen devices are leading cause of mobile security incidents⁵



Every three minutes an enterprise wipes a mobile device⁶



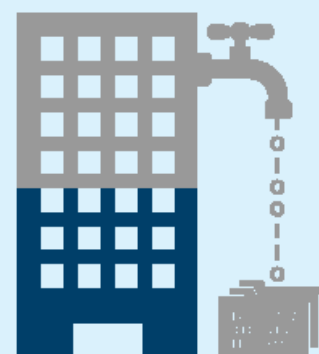
Secure content & collaboration



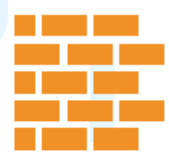
60% of employees **access content from outside** the office⁷



64% of decision-makers read their email via mobile devices⁸



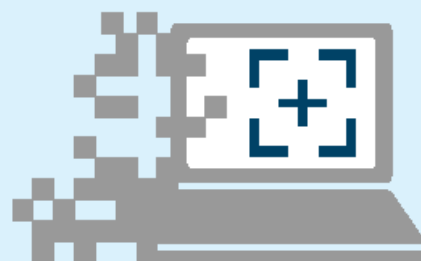
50% of organizations say content theft and leakage are their top concerns⁵



Safeguard applications & data



On average, **companies test less than 50%** of the mobile apps they build⁹



2.2 billion malicious attacks on computers and mobile devices were **blocked** in Q1 2015¹⁰



Through 2017, **75%** of all mobile security breaches **will be through apps**¹¹



Manage access & fraud



76% of organizations plan to invest more in mobile technologies in 2016–2017¹²



32% are concerned about fraudulent transactions, only **18% can detect** malware/jailbreaks⁵



The annual U.S. cost of a cyber-crime is **\$11.56 million per organization**¹³

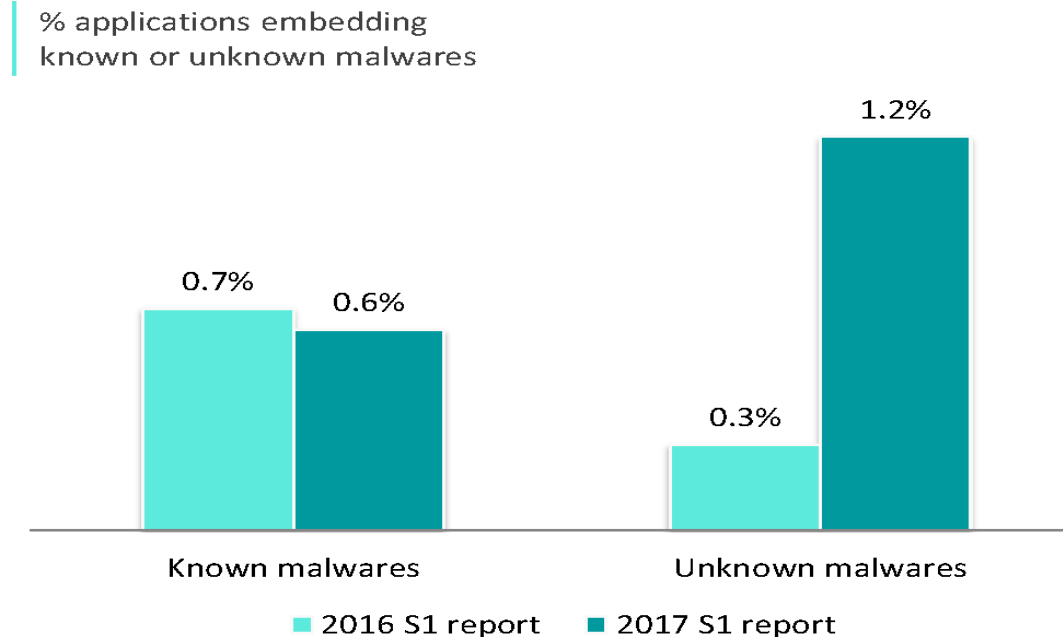
MALWARES TREND

Unknown malwares are on the rise

4X More applications embedding
Unknown malwares

whereas

Known malwares
maintain the same ratio



Known malwares represent applications identified as malicious from their viral signature. From S1 2016 to S1 2017, the volume of applications infected by known malware remain stable whereas unknown malwares quadrupled.

This trend reflects the evolution of the mobile cyber-criminality and the incapacity of an antivirus to properly counter and stop mobile threats. Hackers keep on developing unknown and advanced threats and easily bypass traditional antivirus protections.

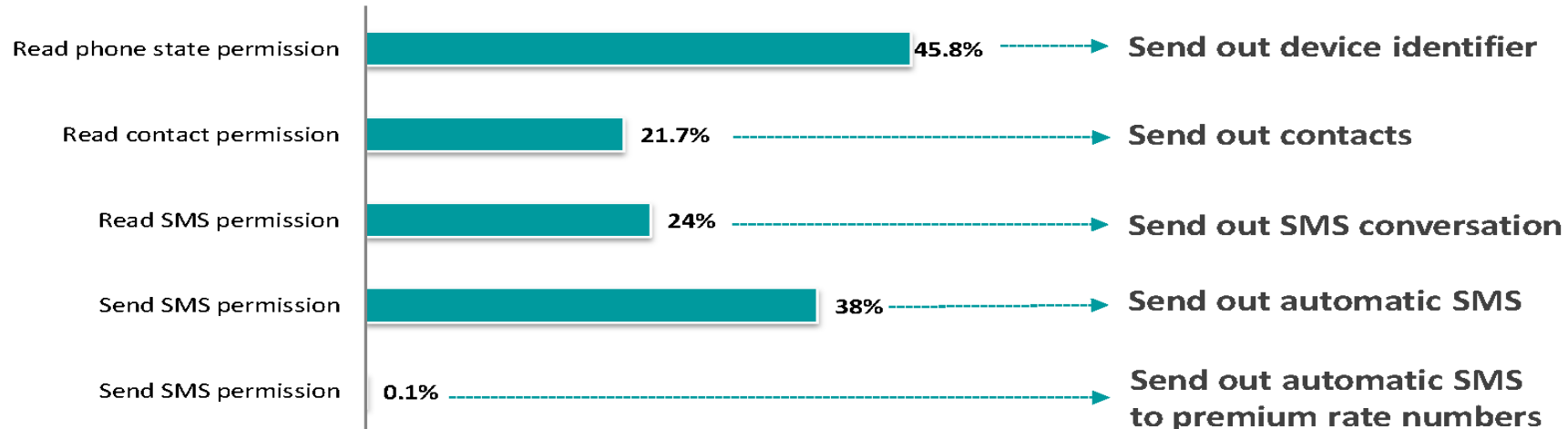
PERMISSIONS

Permeable boundaries

Despite the nature of permissions, Applications can bypass those boundaries and perform data leakage. Permissions grant the ability for an Application to manipulate a data.

Permissions cannot be considered as proper safeguards for data protection nor reflect any risk level to evaluate Applications.

% of Applications bypassing permissions and performing data leakage



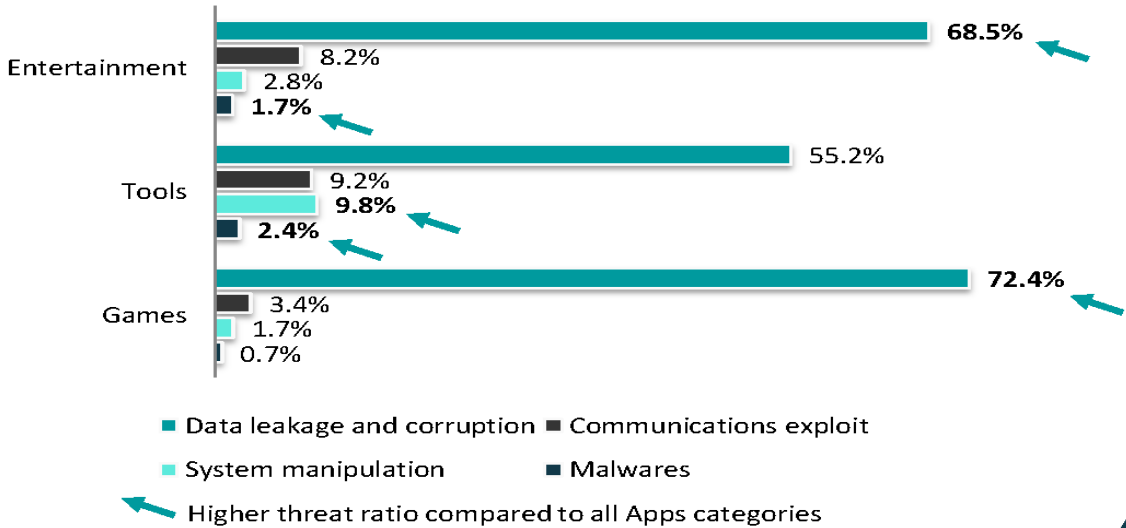
WHAT ABOUT MOST POPULAR APPLICATIONS?

Games, Entertainment and Tools

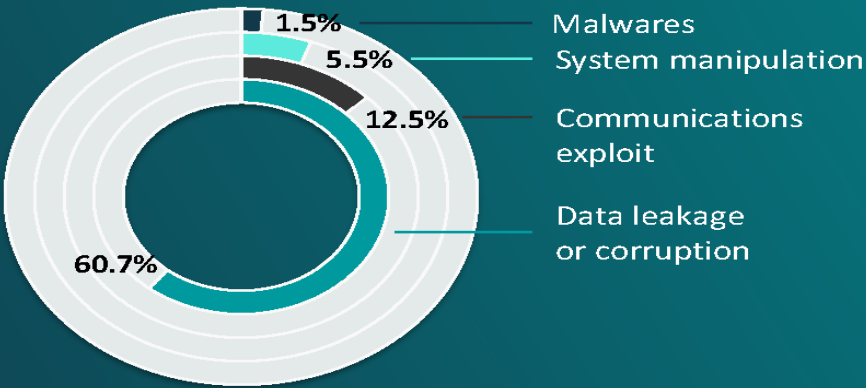
The most popular Applications are not the safest ones.

The focus on Games, Tools and Entertainment families of Applications outlines high rates of Applications presenting malicious or intrusive behaviors.

% Applications featuring a malicious or an intrusive behaviors in Games, Utilities & Tools and Entertainment categories

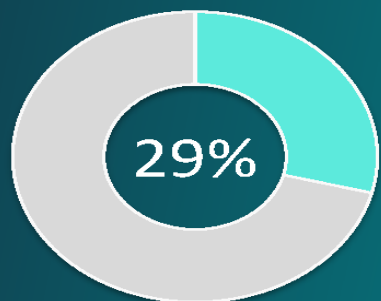


% Applications featuring a malicious or an intrusive behaviors

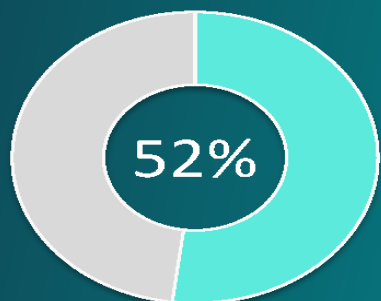


DATA LEAKAGE OR

Sending, deletion
or modification



of Applications
exploit user's
location



of Applications
manipulate
hardware
information

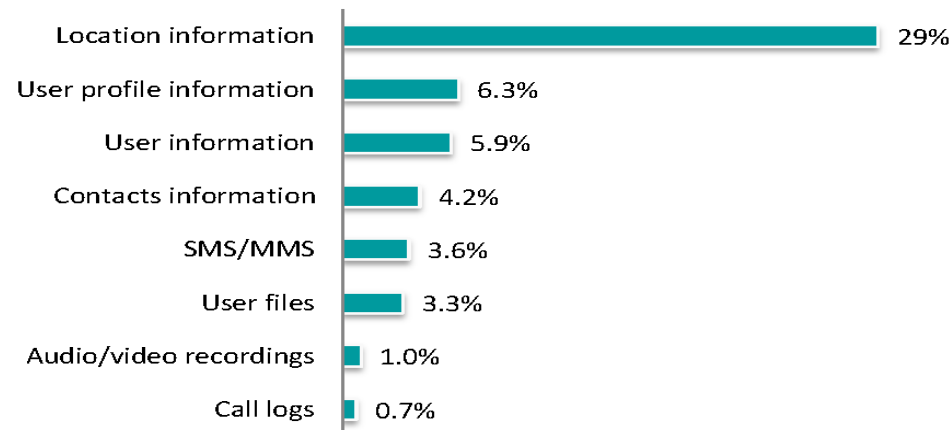
CORRUPTION

Data leakage or corruption come on top of identified threats in this study with 60.7% of Applications featuring intrusive behaviors.

This demonstrates the gap between public stores standard security policies and data protection levels expected by companies or individuals.

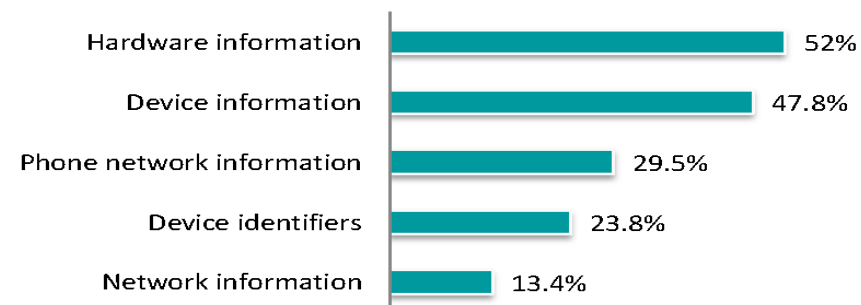
User's data

% of Applications
manipulating
user's data



Device's data

% of Applications
manipulating
device's data





Bitcoin

mBTC477.06

≈ USD112.44

21 Apr Donation for Bitcoi... +6.26

19:29, 17 April Donation for Bitcoin Wallet +13.09

17 Apr Donation for Bitcoi... +1.00

15 Apr 13tT vECF HS7D A... +0.97

14 Apr 1Bq6 P6LV 7L1K m... -1.00

12 Apr Donation for Bitcoi... +0.50

11 Apr Donation for Bitcoi... +4.22

Request Bitcoins

Requested amount (optional)

m฿7.12 €1.50

☒ Accept payment via Bluetooth for more reliable processing

Have this code scanned by the sender. Or tap an NFC enabled device.

1 2 3 -

4 5 6 ,

7 8 9 ✕

. 0 English Finished

Sweep paper wallet

You are about to sweep a paper wallet or coupon. This will move all coins from that paper to your wallet on this device. When the transaction is confirmed, the paper will be worthless and should not be re-used for safety reasons.

Start by scanning the private key of a paper wallet. Use the camera action button.

Paper wallets are most commonly used for cold storage. Some ATMs print them on their paper slip rather than sending the coins to your mobile device directly. People sometimes use pre-charged paper wallets to pass value around (not recommended).

Cancel

Decrypt

Recitiamo Santo Rosario Free

PR Solutions Lifestyle

★★★★★ 376

3+

This app is compatible with some of your devices.

Add to Wishlist

Install

SafetyNet Wireless App

FreeMo Productivity

★★★★★ 27

3+

Contains ads

This app is incompatible with all of your devices.

Add to Wishlist

Install

Car Wallpaper HD: mercedes, ferrari, bmw and audi

Artal Personalization

★★★★★ 13

3+

This app is compatible with some of your devices.

Add to Wishlist

Install

CIA HACKING SOURCE CODE



WikiLeaks <https://wikileaks.org/vault8/>

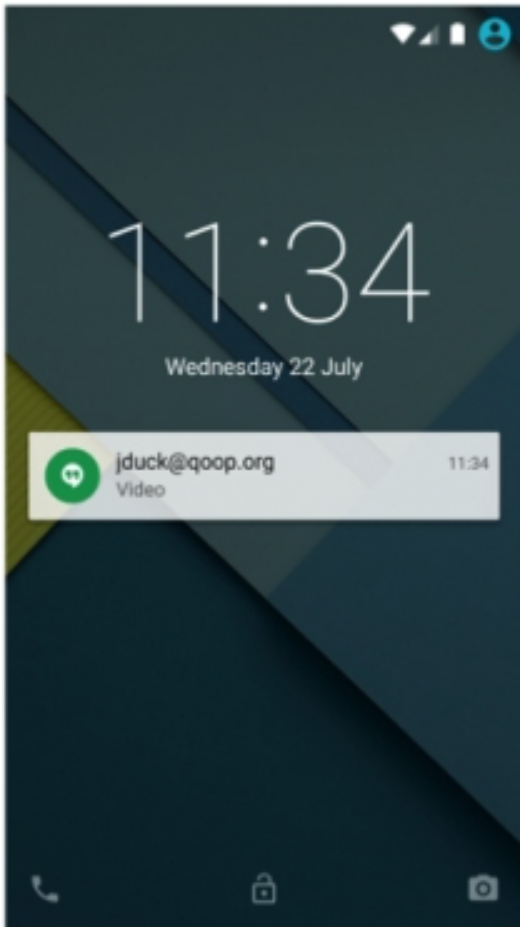
INFECTED APPS LIST



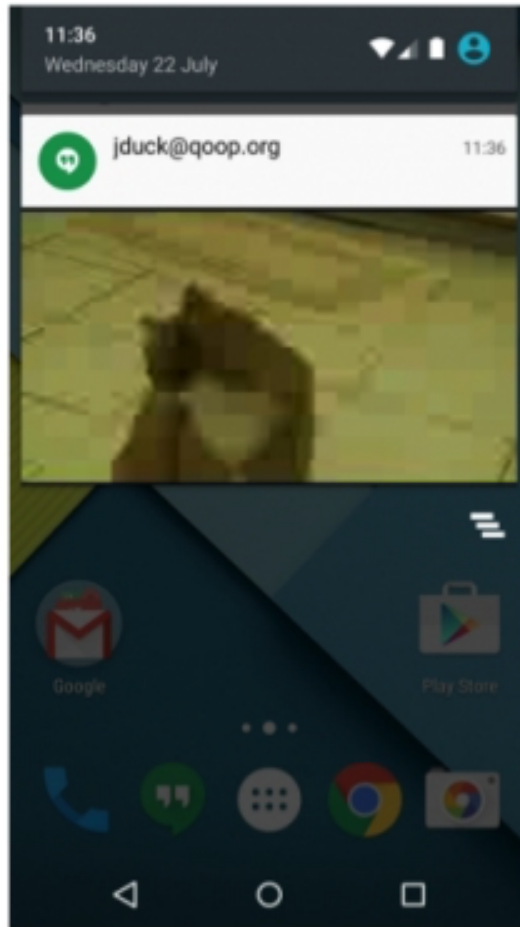
Solitaire, Classic Solitaire, Spider Solitaire, XDC Cleaner, Mobile Fonts

Package	App Name	Installs Min	Installs Max	Updated	Rating
com.pickleapps.player	Aristotle Music audio player 2017	1,000,000	5,000,000	August 17, 2017	4.5
com.musicaplayer.stonetemples	Free Music MP3 Player	1,000,000	5,000,000	July 28, 2017	4.6
com.mp3musicplayer.playmusicmp3	Free MP3 Music Download Player	500,000	1,000,000	July 28, 2017	4.4
com.densebutter.musicplayer	Quick Mp3 Music Player	500,000	1,000,000	August 9, 2017	4.1
com.airplaneapps.soundmeter	Sound/Music Volume Meter	100,000	500,000	August 4, 2017	4.3
com.dinosaursr.musicplayer	Arpeggio Music audio player 2017	100,000	500,000	August 23, 2017	4.3
com.tenuousllc.humneate	Music Downloader Player	100,000	500,000	August 25, 2017	4.2
com.astropie.musicplayer	Free Music MP3 Download Player	100,000	500,000	August 17, 2017	4.3
info.chargeshoes.videoplayer	Free MP3 Music Download Player	100,000	500,000	August 20, 2017	4.5
com.FeisalLLC.MusicPlayer	Tube MP3 Music Player	100,000	500,000	October 17, 2017	4.6
com.chopsuey.musicplayer	Volume Control for Music	100,000	500,000	October 17, 2017	4.7
com.exudedplayer.freemusicplayer	Music Album Sorter	100,000	500,000	October 24, 2017	4.6
com.kinokunya.free	Song Player	100,000	500,000	October 10, 2017	4.5
com.callsaver.doubtful	Call Saver/Downloader	50,000	100,000	August 4, 2017	4.7
com.unfestenedsail.freeapp	Simple Hearing Test	50,000	100,000	August 28, 2017	4.5
com.extendmilk.freeplayer	Free MP3 Music Download Player	50,000	100,000	August 23, 2017	4.4
com.excellentlossapps.playermusic	Great MP3 Music Player	50,000	100,000	August 27, 2017	4.5
com.callsaver.recorderfreeapp	Call Saver/Downloader	50,000	100,000	October 12, 2017	4.7
com.AliciaTech.free	Slick MP3 Music Player	10,000	50,000	September 7, 2017	4.3
com.mp3player.musicplayer.freelocalmusicplayer	Free MP3 Music Downloader Player	10,000	50,000	July 28, 2017	4.6
com.freemusicplayer.freemusicplayer.free	MP3 Music Player	10,000	50,000	July 28, 2017	4.6
com.afromusicplayer.fremediaplayer	Afro MP3 Music Player	10,000	50,000	July 28, 2017	4.6
com.freeborn.sdkintegration	MP3 Music Download Player	10,000	50,000	October 25, 2017	4.7
info.adeptly.forgoneapp	File Manager for Music	10,000	50,000	October 24, 2017	4.6
com.byunhyeong.jungfree	Media Player	10,000	50,000	October 18, 2017	4.6
info.vaskollic.jpfree	Free MP3 Music Download Player	10,000	50,000	October 17, 2017	4.5
com.unscalableapps.free	Audio Recorder	10,000	50,000	October 17, 2017	4.7
com.info_astro.glider_player	Mp3 Music Downloader	5,000	10,000	April 6, 2017	4
com.illfatednotice.humdrum	Free MP3 Music Downloader Player	1,000	5,000	August 25, 2017	3.7
com.headyowl.musicplayer	MP3 Music Player	1,000	5,000	August 20, 2017	4.3
com.checkrein.musicapp	Album Manager for MP3 Music	1,000	5,000	October 18, 2017	4.2
com.headyowl.musicplayer	MP3 Music Player	1,000	5,000	August 20, 2017	4.3
com.combustionapps.musique	Tube MP3 Music Player	1,000	5,000	October 24, 2017	4.7
com.musicgratisplayerfree.free	Music Player	500	1,000	July 18, 2017	4
Total		4,250,500	17,486,000		

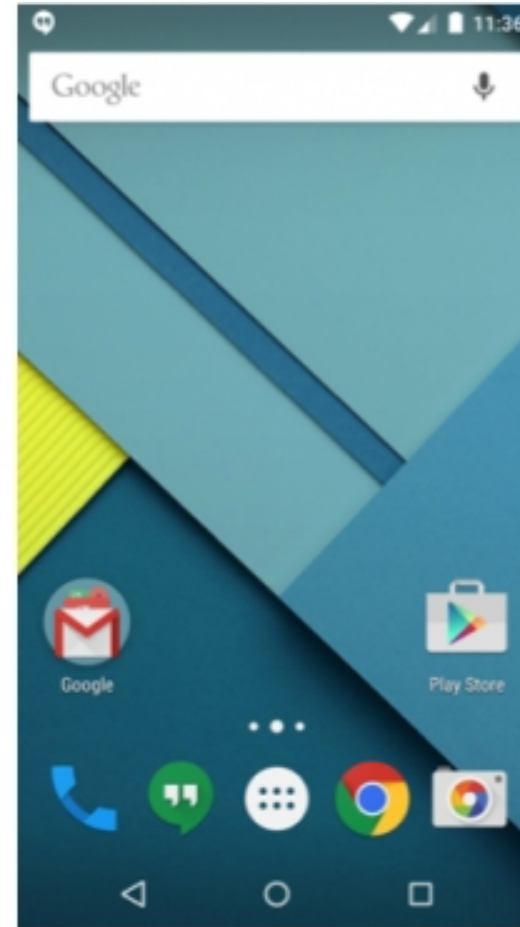
SPECIAL THREATS 01 – MMS MKV INTEGER ATTACK



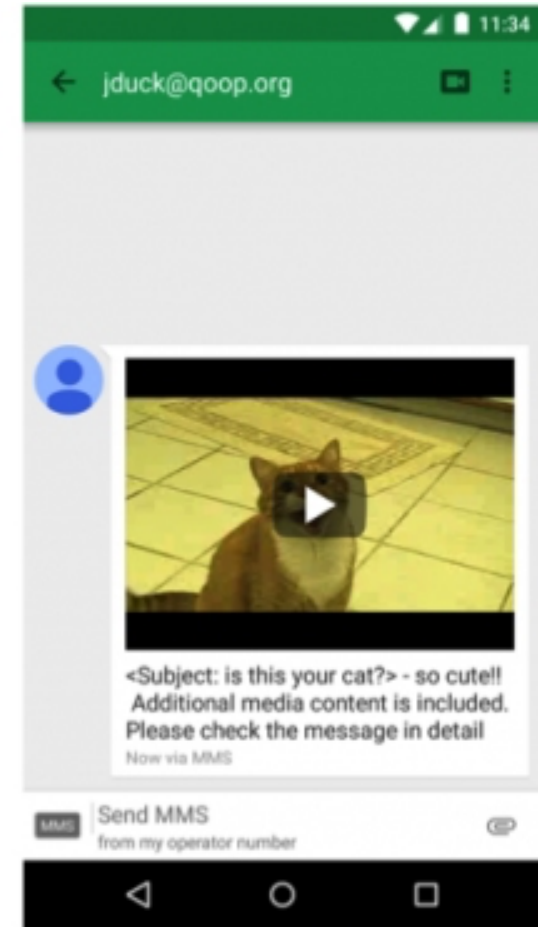
An MMS was received by Hangouts. At this point, an attacker may have already executed arbitrary code.



MMS notifications show a preview, which triggers the vulnerable code.



After unlocking the screen, no effects are apparent.



Viewing the MMS message triggers the vulnerable code again. Touching the video or rotating the screen triggers the vulnerable code again and again.



SMSecure

SPECIAL THREATS 02 – “BRICKED” DEVICES

Android system crash vulnerability affecting Google’s Bouncer™ infrastructure, one that, alarmingly, also affects mobile devices with Android OS versions 4.0 and above. We believe that this vulnerability may be used by cybercriminals to do some substantial damage on Android smartphones and tablets. The device is stuck in an endless reboot loop, or a bootloop. This can render the device unusable, which some may consider “bricking” it. ((App long name code over than “387,000 character”))

```
java.lang.RuntimeException: Package manager has died
    at android.app.ApplicationPackageManager.queryIntentActivitiesAsUs
er(ApplicationPackageManager.java:500)
    at android.app.ApplicationPackageManager.queryIntentActivities(App
licationPackageManager.java:486)
```

```
system_process  ActivityManager  Exception thrown during bind!
system_process  ActivityManager  android.os.TransactionTooLargeException
system_process  ActivityManager  at android.os.BinderProxy.transact(Native Method)
system_process  ActivityManager  at android.app.ApplicationThreadProxy.bindApplication(ApplicationT
hreadNative.java:899)
system_process  ActivityManager  at com.android.server.am.ActivityManagerService.attachApplicationL
ocked(ActivityManagerService.java:4296)
```

```
ProcessState  Using /dev/binder failed: unable to mmap transaction memory.
ProcessState  Binder driver could not be opened.  Terminating.
libc          Fatal signal 4 (SIGILL) at 0xb77a6c0d (code=2), thread 1987 (zygote)
```

Unfortunately, the process
android.process.acore has
stopped.

OK

Unfortunately, Launcher has
stopped.

OK

INFECTED KERNEL


GOOGLE
BOUNCER

Android's
Anti-Malware Tool



SPECIAL THREATS 03 – STAGE FRIGHT


```
root@kali: ~  
File Edit View Search Terminal Help  
GNU nano 2.2.6 File: /opt/mp4.py  
#!/usr/bin/env python  
# Joshua J. Drake (@jduck) of ZIMPERIUM zLabs  
# Shout outs to our friends at Optiv (formerly Accuvant Labs)  
# (C) Joshua J. Drake, ZIMPERIUM Inc, Mobile Threat Protection, 2015  
# www.zimperium.com  
#  
# Exploit for RCE Vulnerability CVE-2015-1538 #1  
# Integer Overflow in the libstagefright MP4 'stsc' atom handling  
#  
# Don't forget, the output of "create_mp4" can be delivered many ways!  
# MMS is the most dangerous attack vector, but not the only one...  
#  
# DISCLAIMER: This exploit is for testing and educational purposes only. Any  
# other usage for this code is not allowed. Use at your own risk.  
#  
# "With great power comes great responsibility." - Uncle Ben  
#  
import struct  
import socket  
#  
# Creates a single MP4 atom - LEN, TAG, DATA  
#  
def make_chunk(tag, data):  
    if len(tag) != 4:  
        raise 'Yo! They call it "FourCC" for a reason.'  
    ret = struct.pack('>L', len(data) + 8)  
    ret += tag  
    ret += data  
    return ret  
^G Get Help      ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text      ^C Cur Pos  
^X Exit          ^J Justify      ^W Where Is     ^N Next Page    ^U UnCut Text    ^T To Spell
```



Stagefright Detector

This tool will check if your device is susceptible to dangerous vulnerabilities in Android's Stagefright Multimedia Framework. We're collecting anonymous results to gauge the status of Android update deployment.

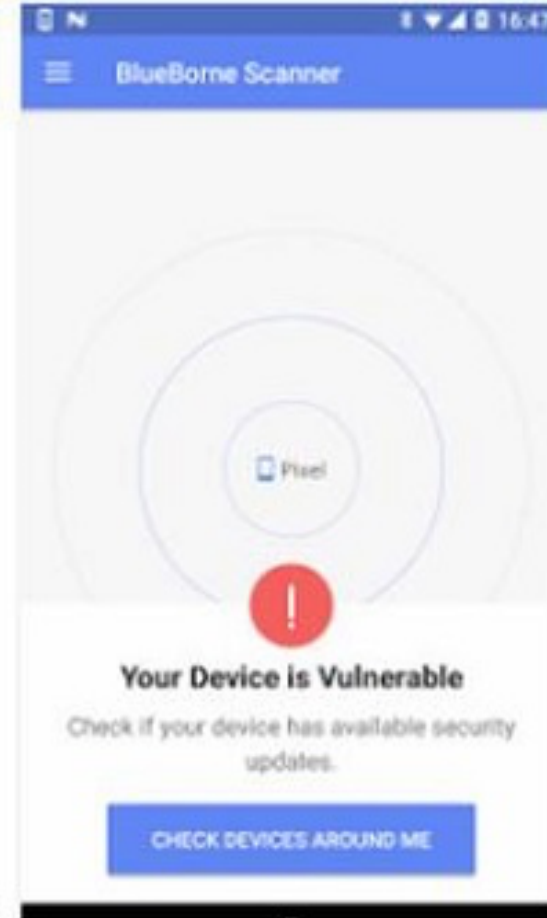
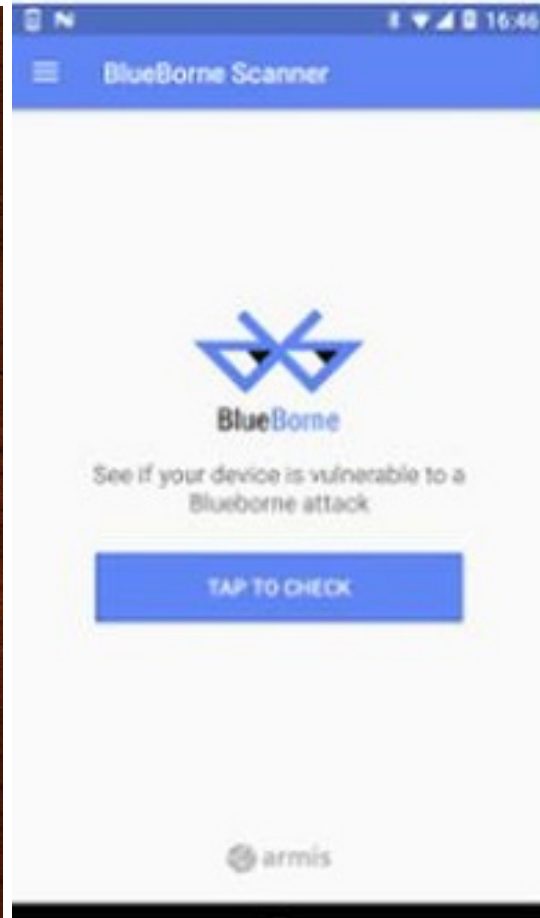
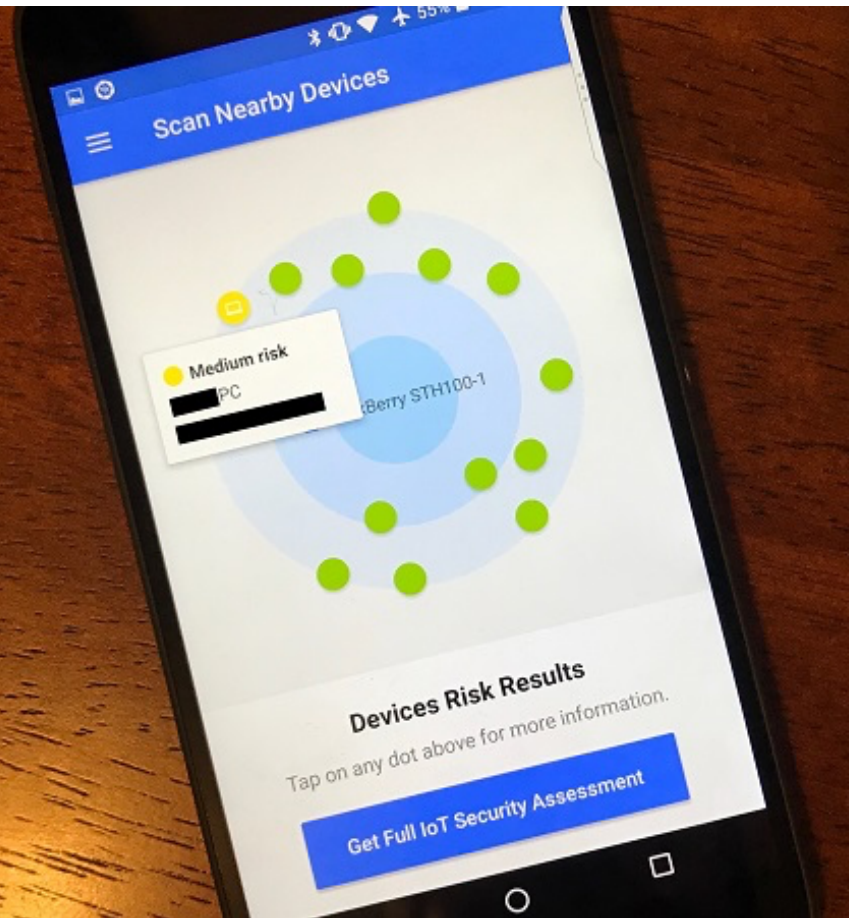
Begin Analysis



Your Android Devices at Risk Due to **stage fright** Vulnerability throw Metasploit Module by **CBHOST** , **CBPORT** if you connected to untrusted / Public WiFi or non secure network or hotspot

SPECIAL THREATS 04 – BLUEBORNE & BLUETOOTH NETWORK ENCAPSULATION PROTOCOL - BNEP

BlueBorne is an attack vector by which hackers can leverage Bluetooth connections to penetrate and take complete control over targeted devices. BlueBorne affects ordinary computers, mobile phones, and the expanding realm of IoT devices. The attack does not require the targeted device to be paired to the attacker's device, or even to be set on discoverable mode. Armis Labs has identified eight zero-day vulnerabilities so far, which indicate the existence and potential of the attack vector. Armis believes many more vulnerabilities await discovery in the various platforms using Bluetooth. These vulnerabilities are fully operational, and can be successfully exploited, as demonstrated in our research. The BlueBorne attack vector can be used to conduct a large range of offenses, including remote code execution as well as Man-in-The-Middle attacks.

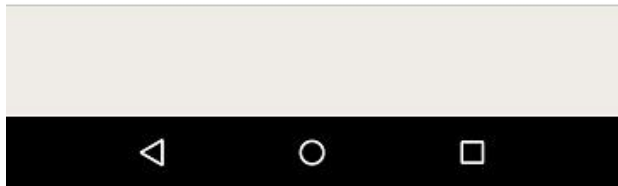
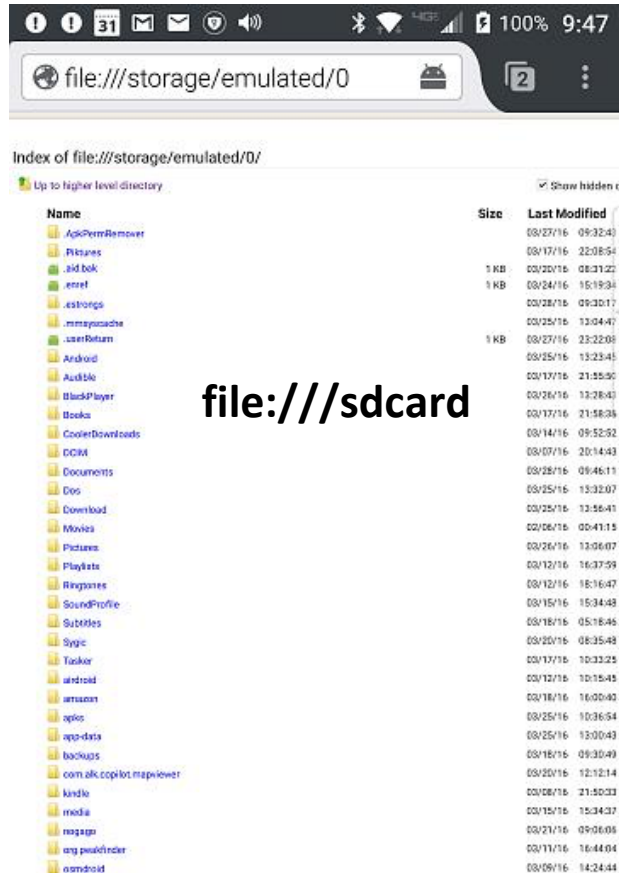


SPECIAL THREATS 05 – PRIVACY ATTACK

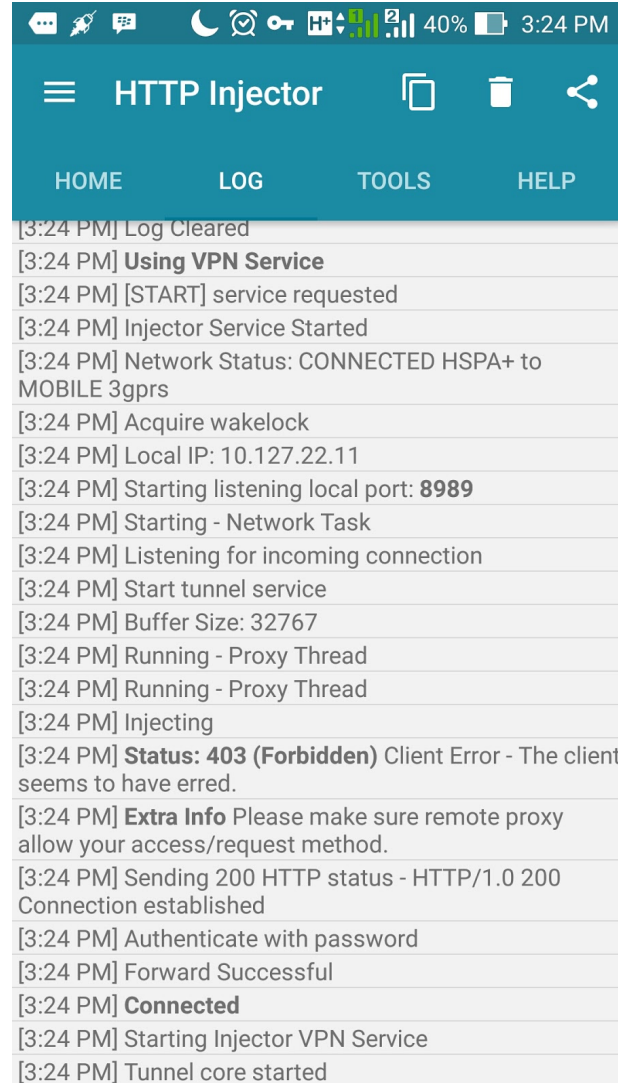
Application Locker Exploit



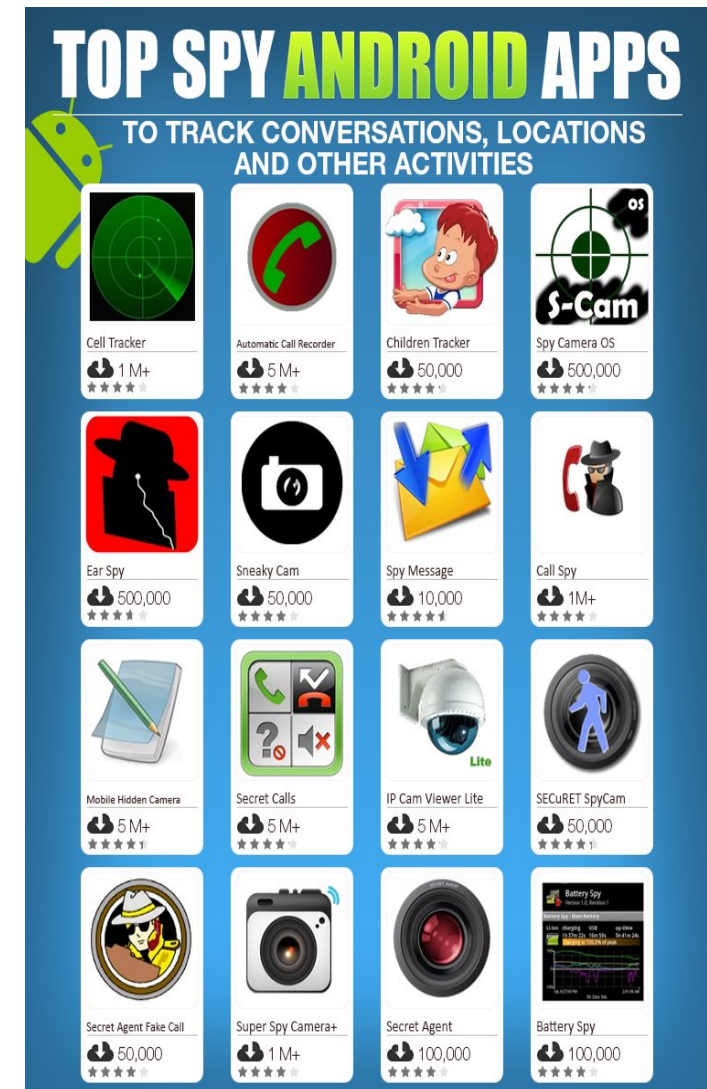
Web browser Exploit



Http Injector Exploit



Spy Apps To Spy you



RECOMMENDATIONS

1. Keep your system updated

An update is available? Install it right away; it probably holds corrections of your current version's detected breaches.

2. Don't download applications outside official stores

The App Store and the Google Play Store provide both a first level security evaluation, prior to publishing the App on their stores. In opposition to third party stores, on which a great part of their available applications are malwares.

3. Verify applications' permissions

Asking a permission should be related with the app's main purpose. For instance, an App that is meant to edit pictures shouldn't have access to your microphone.

4. Don't do sensitive operations through open networks

You have to transfer money to an important supplier's bank account? Doing so during your lunch break while connected to the restaurant's Wi-Fi might expose you to an attack such as a man-in-the-middle. You should wait to be connected to a secured network.

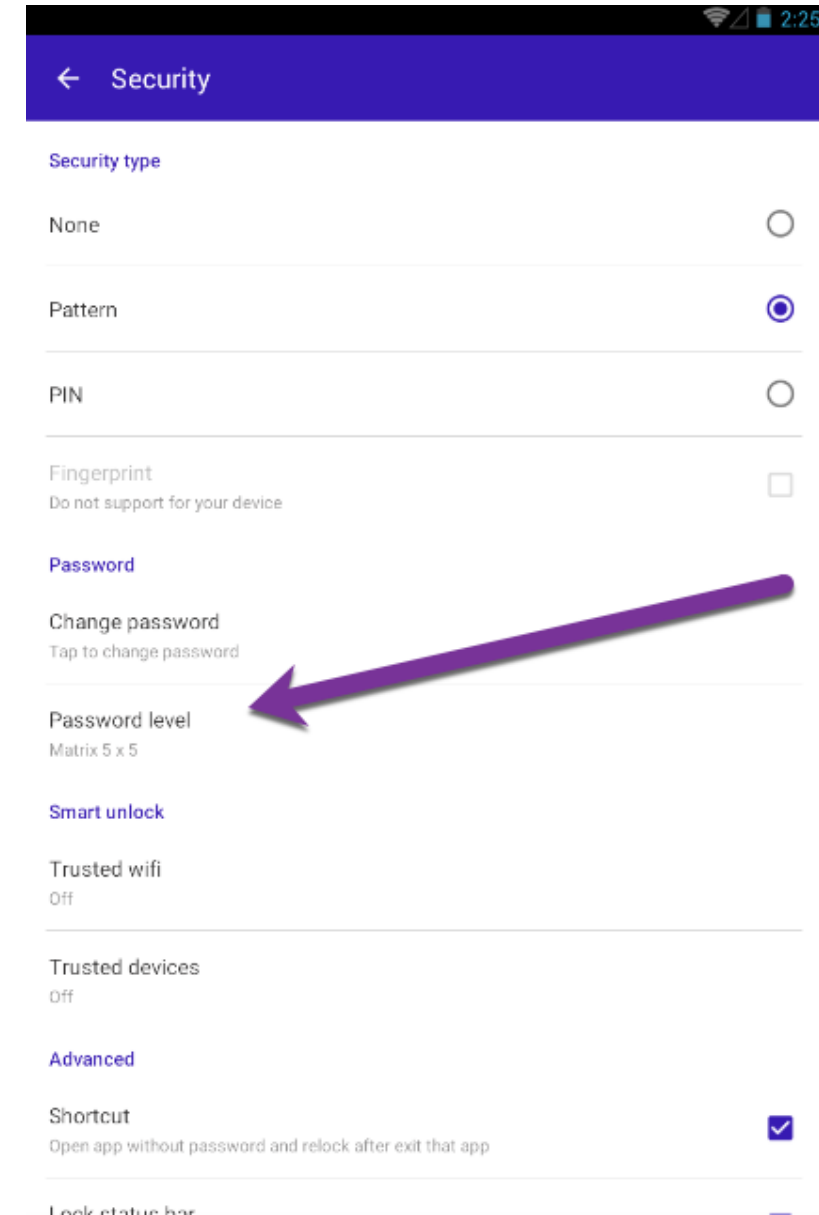
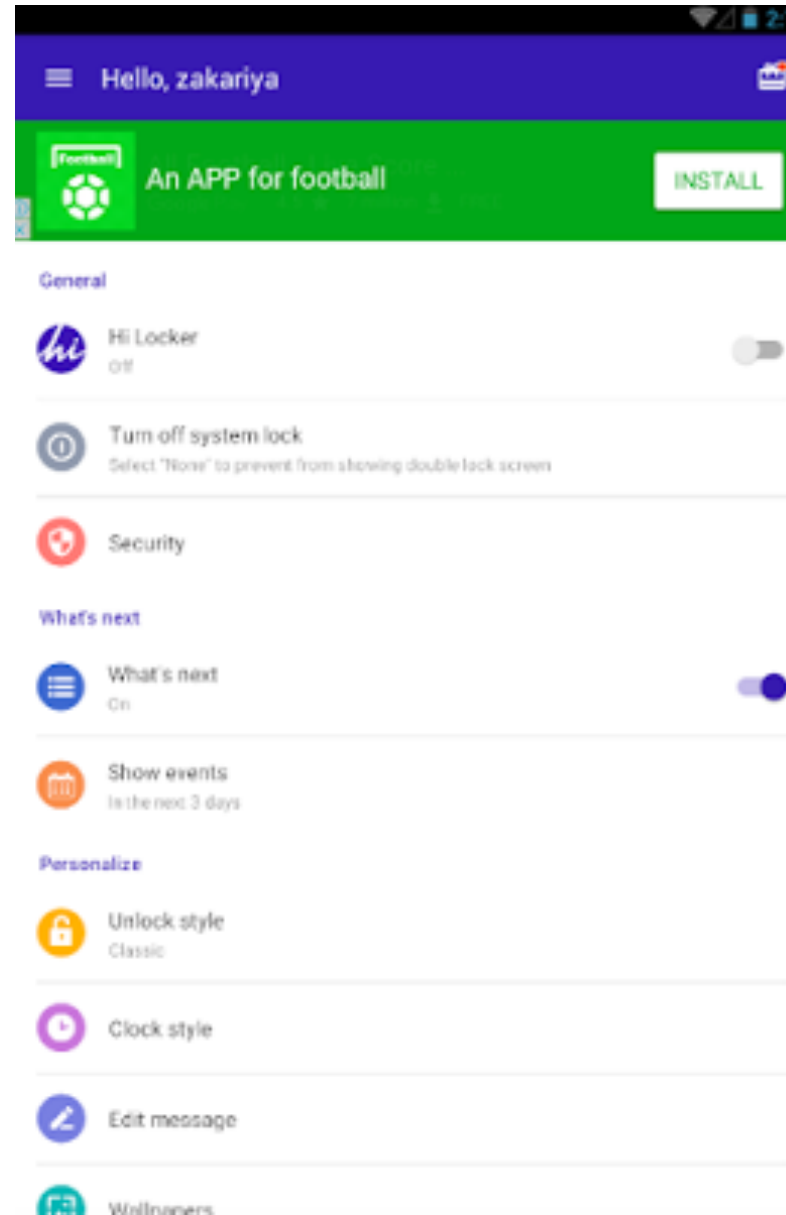
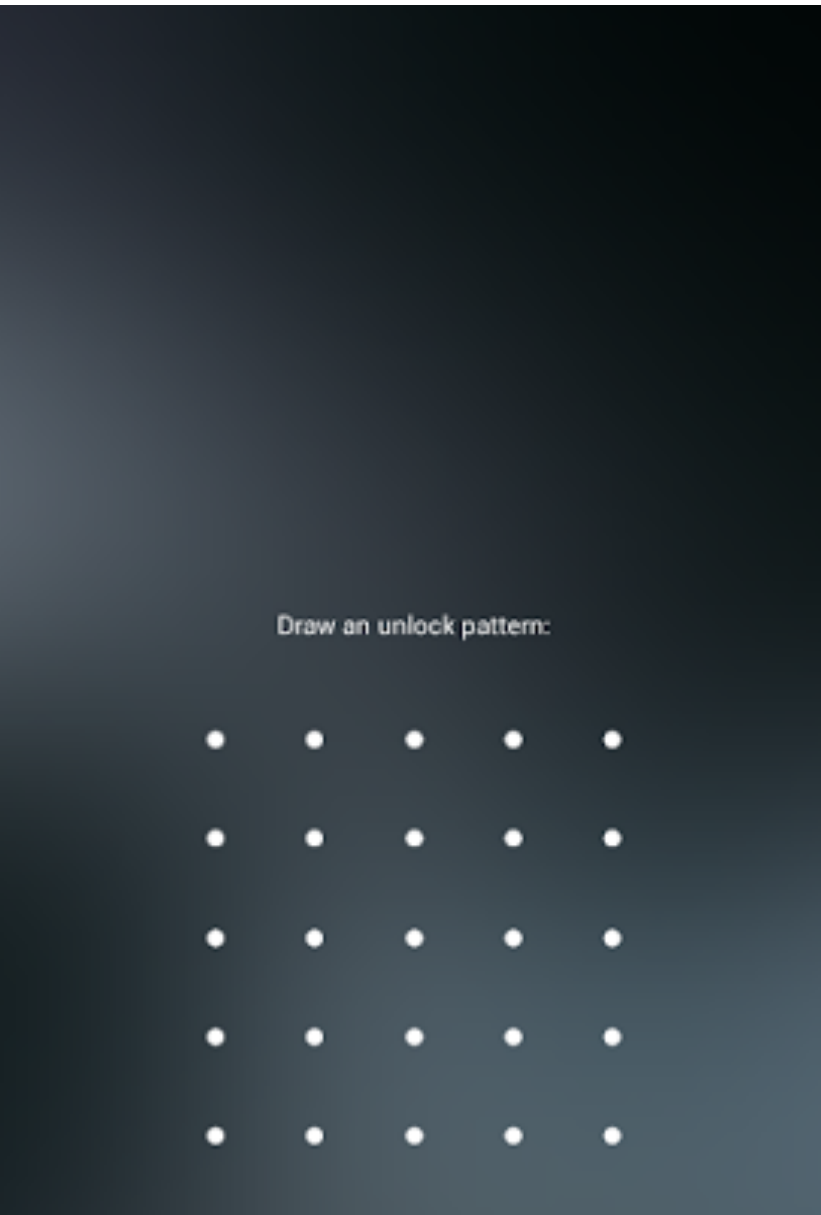
5. Don't root / jailbreak your device

A "cracked" device gives an easier access to the information it contains and increases its vulnerability.

6. Get a security solution

Make sure that you are using a solution that will help you assure apps legitimacy and protect from "zero-day" attacks.

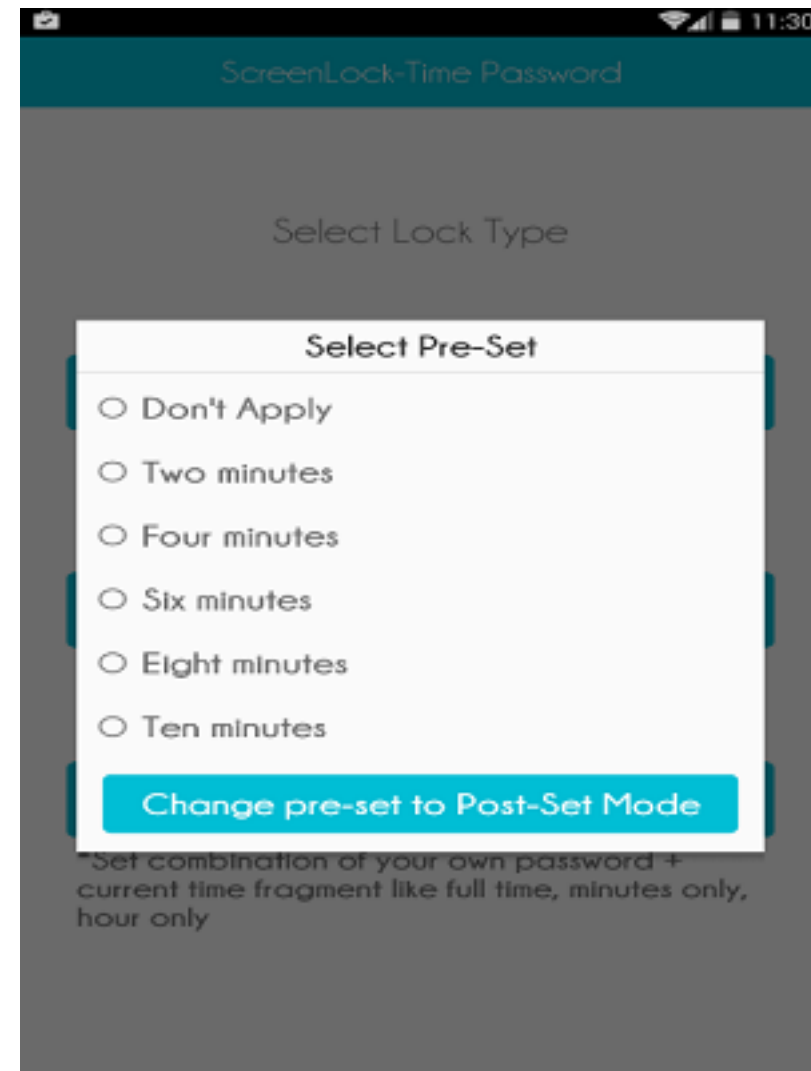
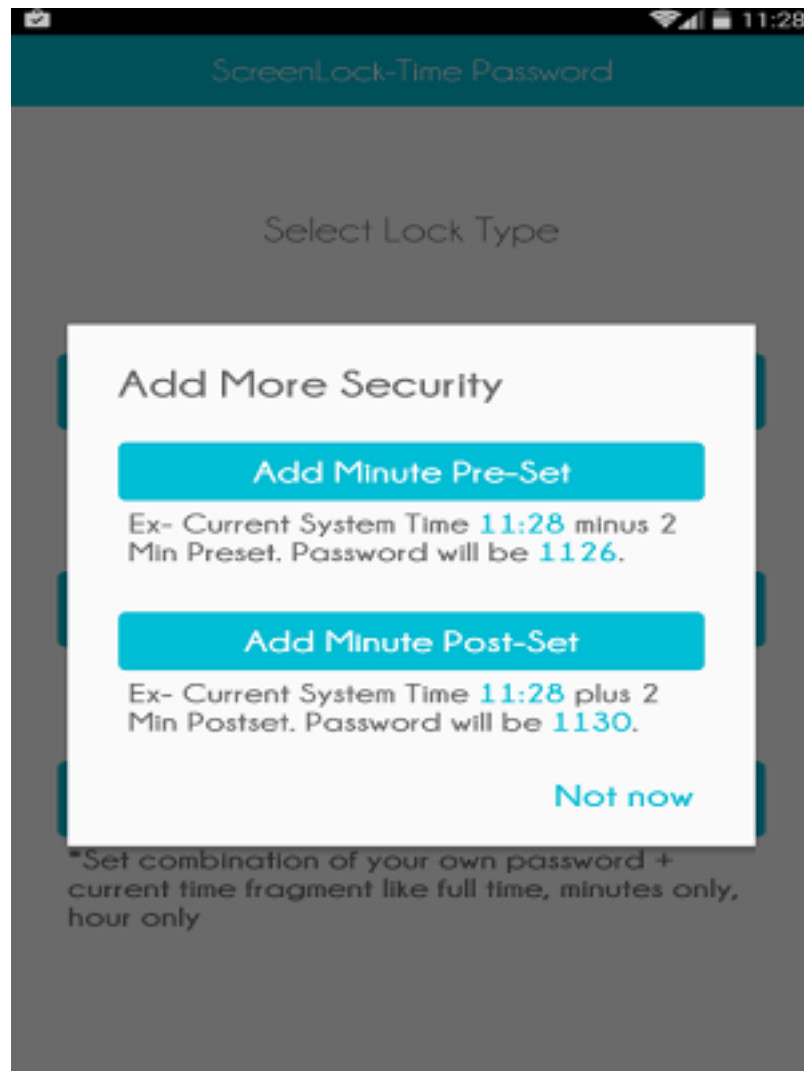
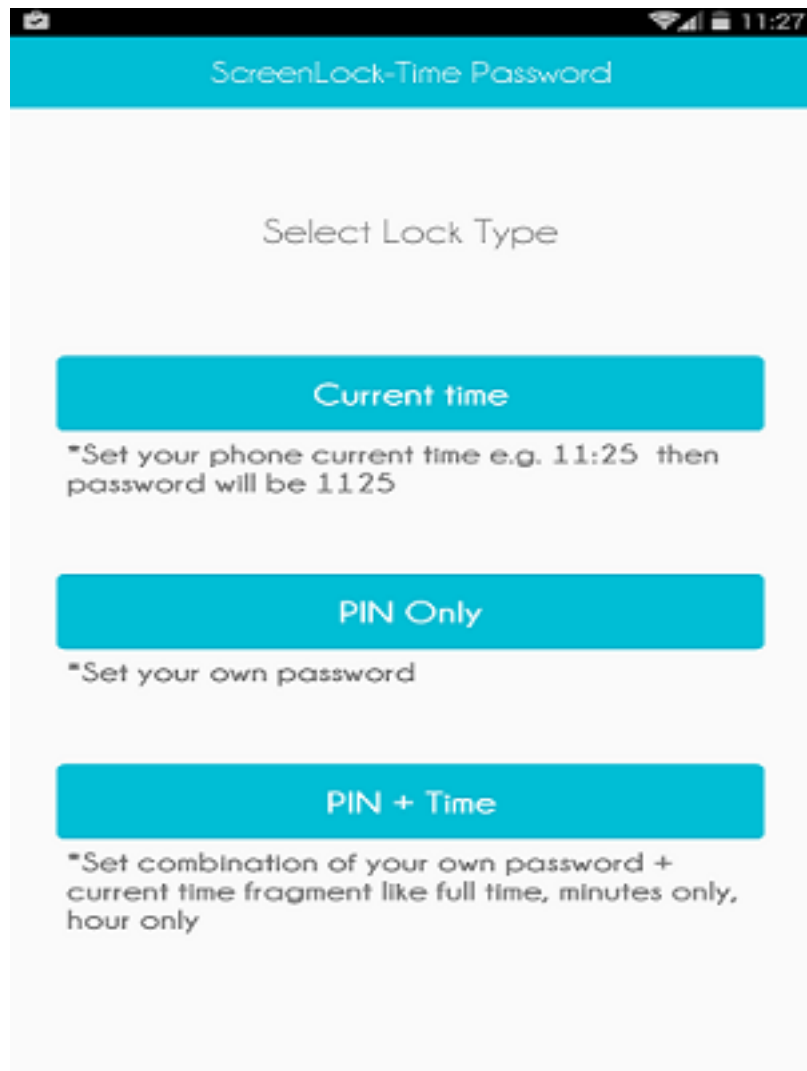
HI LOCKER PANTALLA DE BLOQUEO



SCREEN LOCK - TIME PASSWORD

Are you worried about exposing your PIN while you unlock your phone?

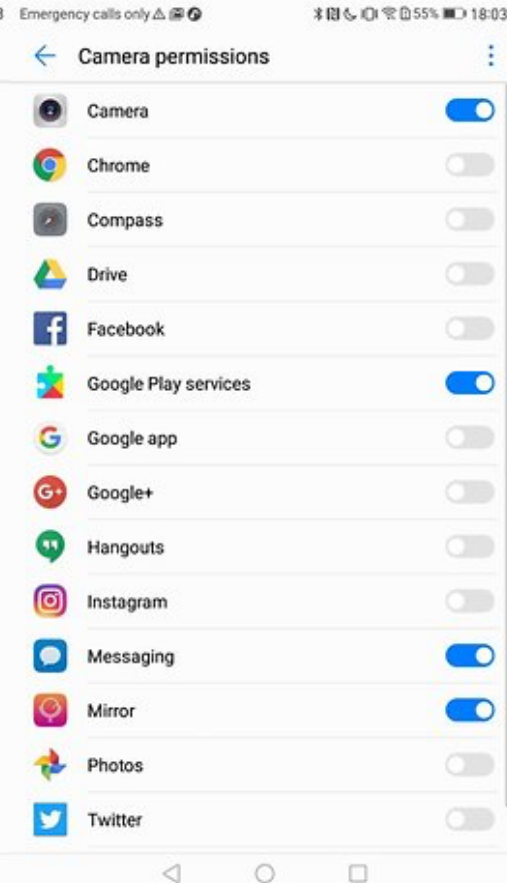
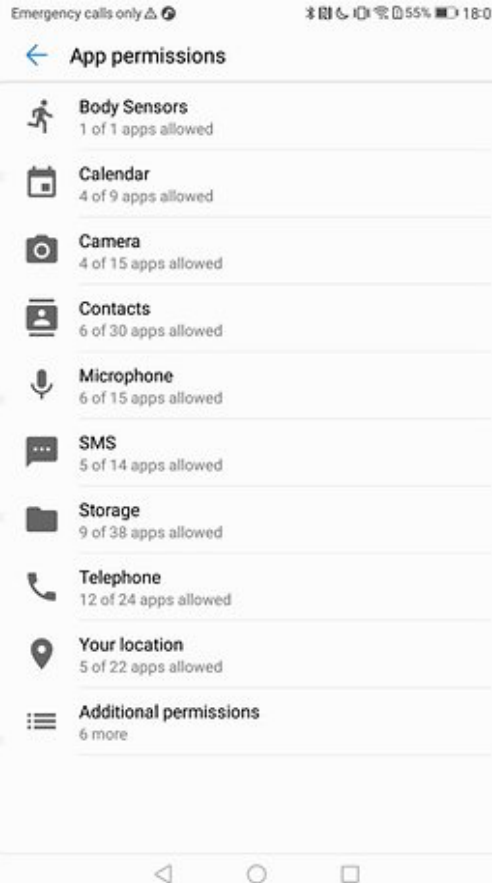
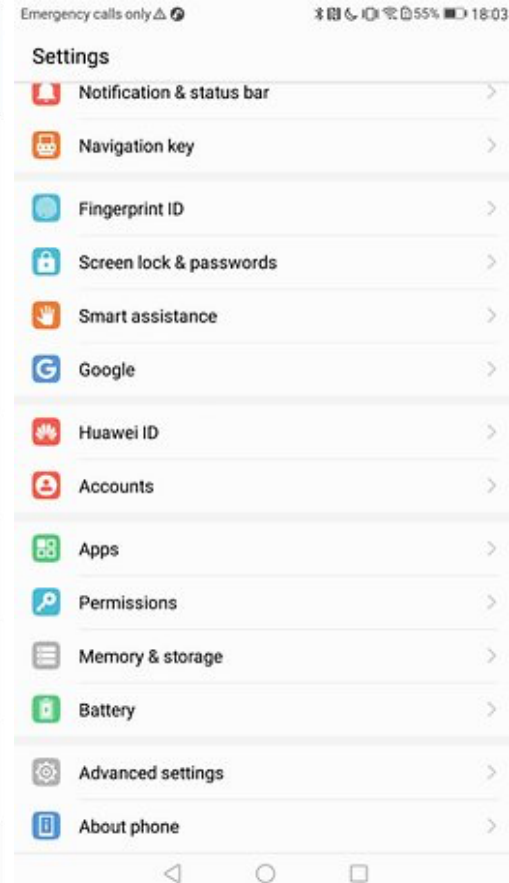
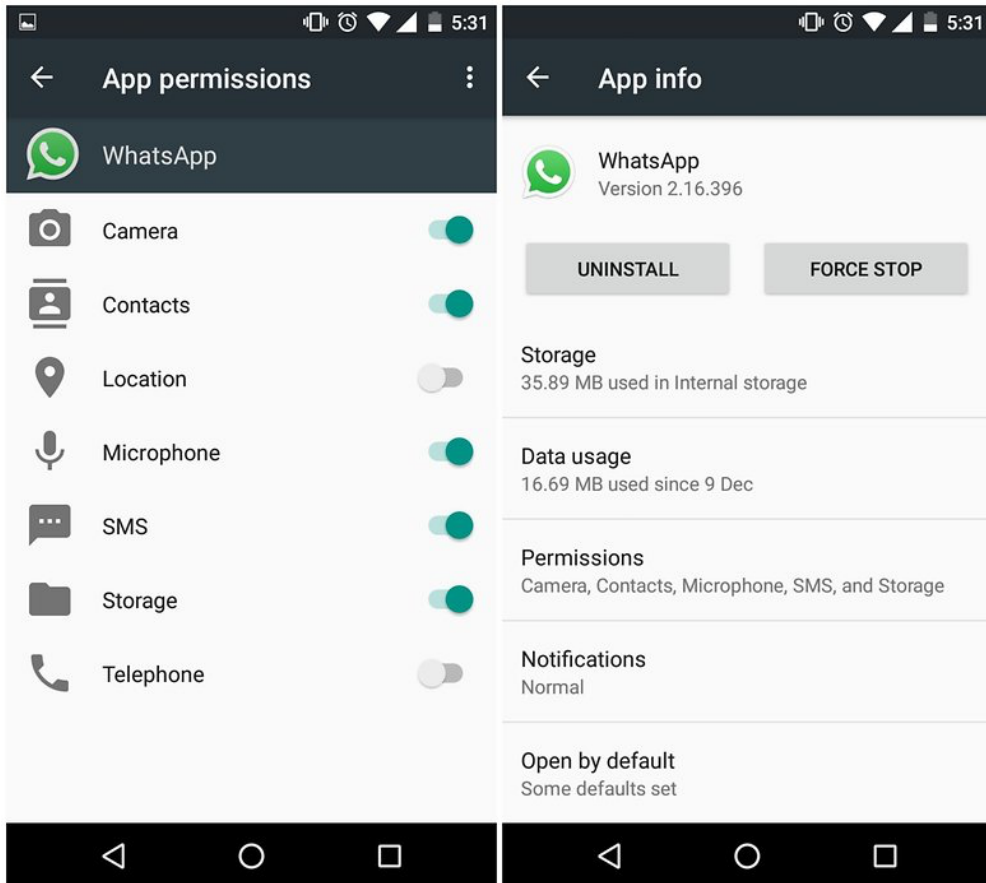
Here comes Screen Lock - Time Password (Dynamic Password) for the rescue. You can make your phone current time its lock screen password. And time changes every minute, so does the password too, so no one can even guess it.



MANUAL PERMISSION EDIT

SECURE

Android



APK PERMISSION REMOVER

✓
Keep

modify phone state

android.permission.MODIFY_PHONE_STATE
Allows the app to modify the phone state with this permission can switch networks, turn the phone on and off and the like without ever notifying you.



Freely Remove sensitive permissions!

directly call phone numbers

android.permission.CALL_PHONE
Allows the app to call phone numbers without your consent. This may result in unexpected charges or calls. Note that this permission doesn't allow the app to call emergency numbers. Using this permission may cost you money by making calls without your consent.

✗
Remove

Your messages

receive text messages (SMS)

android.permission.RECEIVE_SMS
Allows the app to receive and process SMS messages. This means the app could monitor or delete messages.

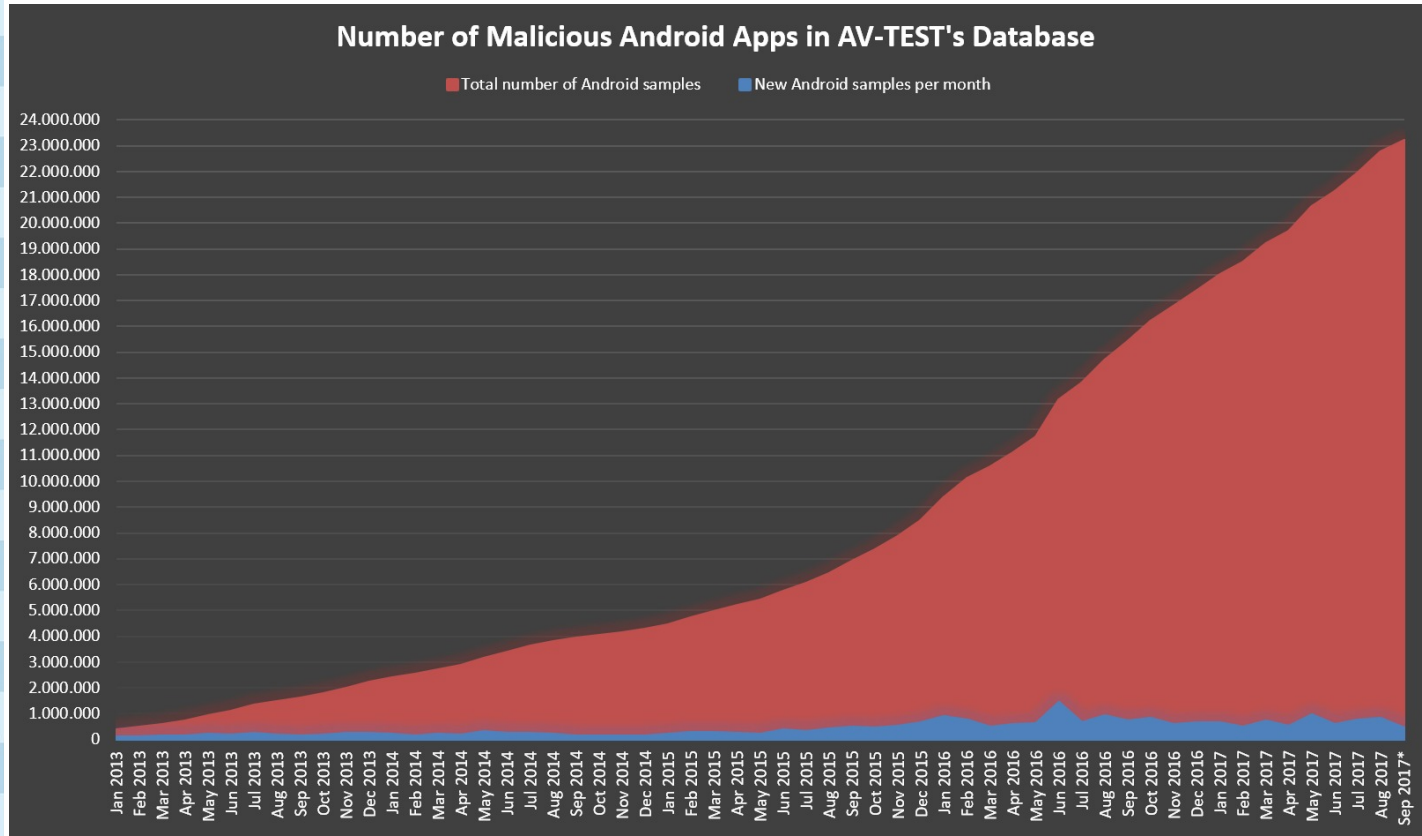
✗
Remove



The Best Malware Protection for Android Mobile Devices



Manufacturer	Product	Detection Rate Real-World-Testing	Detection Rate Reference Set
AhnLab	V3 Mobile Security	99.8%	100.0%
Alibaba	Mobile Security	99.3%	99.9%
Antiy	AVL	100.0%	100.0%
Avast	Mobile Security	99.8%	100.0%
Bitdefender	Mobile Security	100.0%	100.0%
Cheetah Mobile	Security Master	100.0%	100.0%
ESET	Mobile Security & Antivirus	99.5%	99.8%
F-Secure	SAFE	81.9%	99.5%
G Data	Internet Security	99.8%	100.0%
Google	Play Protect	65.8%	79.2%
Ikarus	mobile.security	97.5%	99.6%
Kaspersky Lab	Internet Security for Android	99.8%	100.0%
McAfee	Mobile Security	99.9%	100.0%
NSHC	Droid-X 3	82.4%	93.5%
PSafe	DFNDR	99.7%	100.0%
Qihoo 360	360 Security	86.6%	95.7%
Quick Heal	Mobile Security	98.2%	99.9%
Sophos	Mobile Security	100.0%	100.0%
Symantec	Norton Mobile Security	100.0%	100.0%
Tencent	WeSecure	99.9%	100.0%
Trend Micro	Mobile Security	100.0%	100.0%



ANDROID VULNERABILITY TEST SUITE - ANDROIDVTS



Build Release: 5.1.1
Build SDK: 22
Build ID: LMY48B

StageFright: cve-2015-1538-4	Passed
StageFright: cve-2015-1539	Passed
StageFright: cve-2015-3824	Passed
StageFright: cve-2015-3828	Passed
StageFright: cve-2015-3829	Passed
StageFright: cve-2015-3864	Passed
StageFright: sf-itunes-poc	Passed
StageFright: cve-2015-6602	Failed
OpenSSL509 Serialization Bug :	Passed

Build ID: LMY48M

ZipBug 9950697 **Passed**

Device Vulnerability Checker



Checking device for publicly known vulnerabilities

CVE-2014-3153/Towelroot/futex **Passed**

CVE-2014-4943/L2TP **Passed**

CVE-2015-1528/GraphicsBuffer Unflatten **Passed**

StageFright: cve-2015-1538-1 **Passed**

StageFright: cve-2015-1538-2 **Passed**

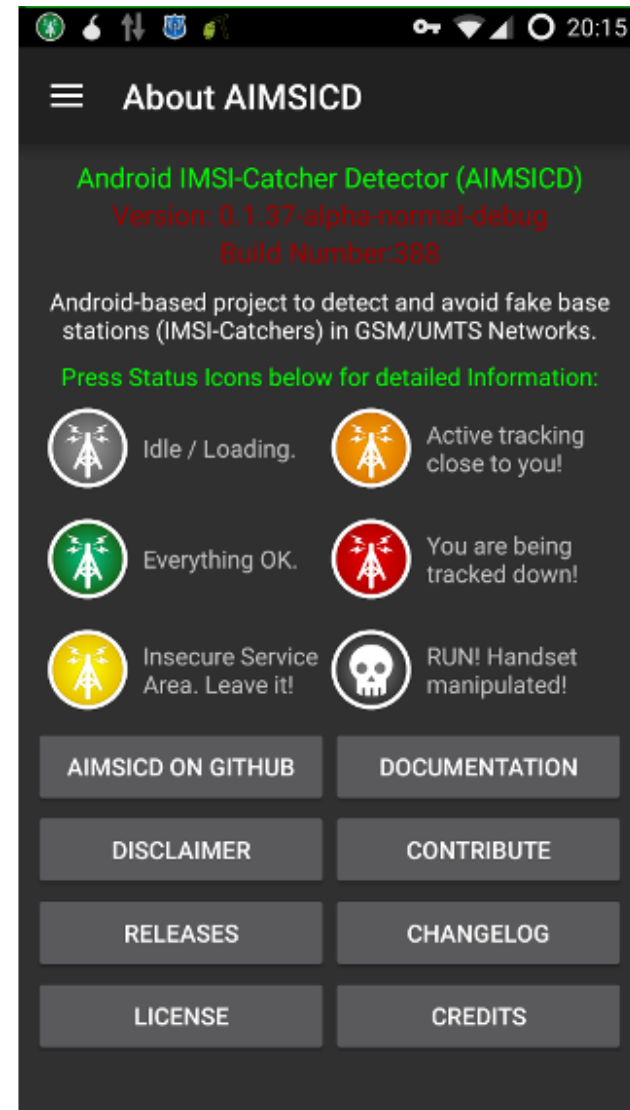
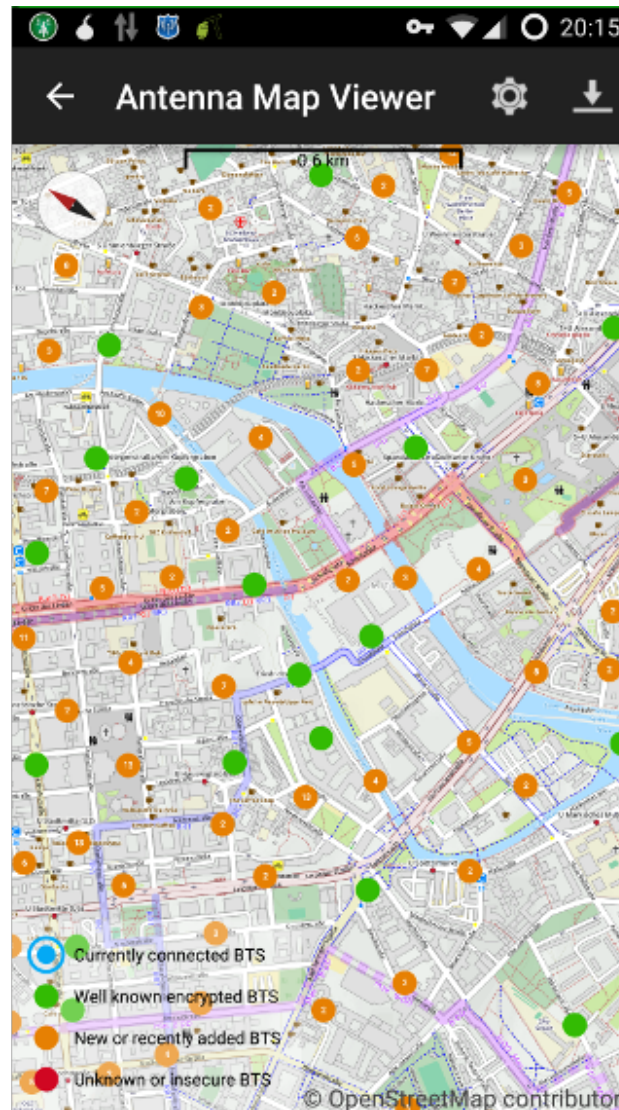
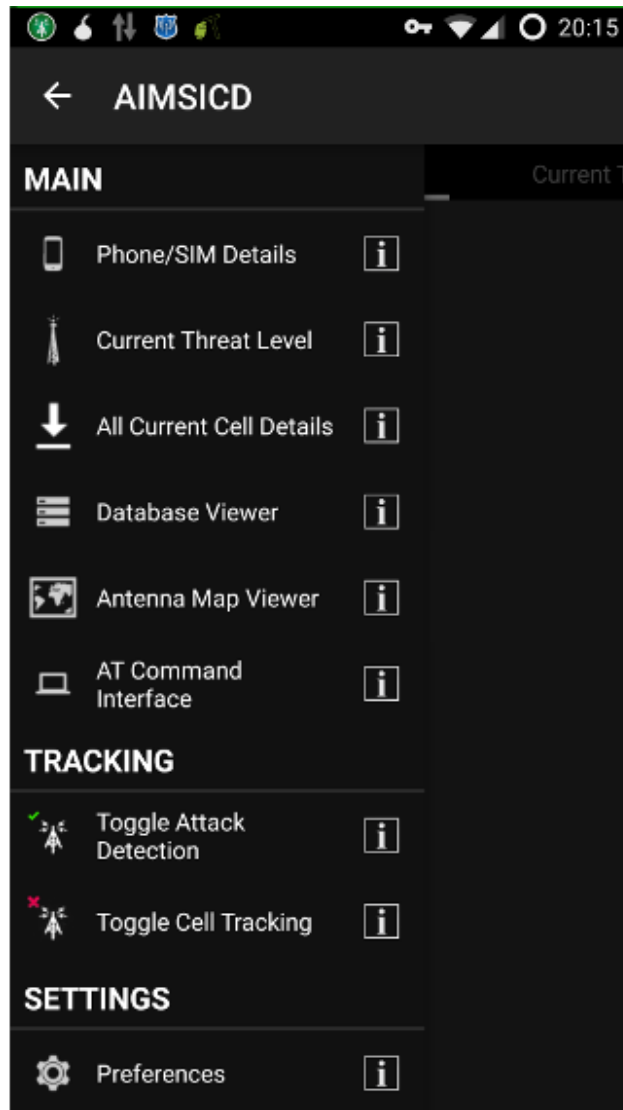
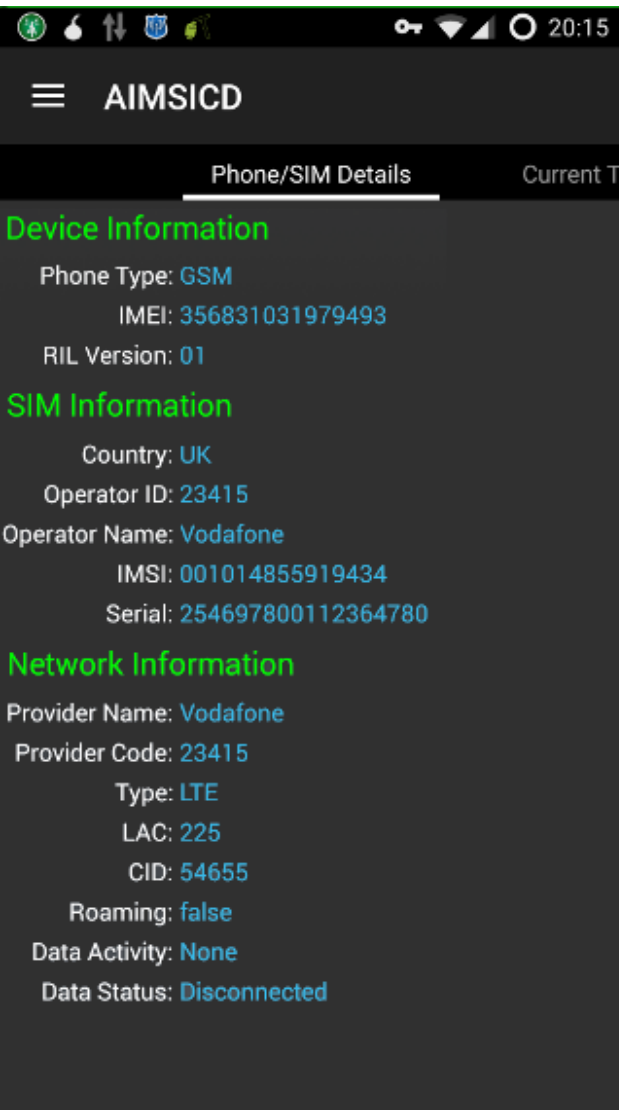
StageFright: cve-2015-1538-3 **Passed**

StageFright: cve-2015-1538-4 **Passed**

MOBILE PHONE HACKING DEVICES



AIMSICD, ANDROID-IMSI-CATCHER-DETECTOR



AIMSICD) is an Android open-source based project to detect and avoid fake base stations (IMSI-Catchers) or other base-stations (mobile antennas) with poor/no encryption



Thank You ...