

Chasing the Joker

About Me



Ahmet Bilal Can

 0xabc0

Android, malware, frida

Invictus

Choker



What is Joker anyway ?

Found by @s_metanka and his team

An Android SMS Subscription Bot

Silently subscribes users to paid services (weekly/monthly)

In initial report total number of download was 472,000 and 24 apps

What is Joker anyway ?

Different types of apps:

- Camera
- VPN
- Lock
- Wallpaper
- SMS
- ..

Chase begins

How to chase apps?

→ Think as a threat actor

Chase begins

How to chase apps?

- Think as a threat actor
 - Different types of apps? Should I write the each app from scratch ?

Chase begins

How to chase apps?

- Think as a threat actor
 - Different types of apps? Should I write the each app from scratch ?
 - How will I distribute my apk ? (lots of installs in first days)

Chase begins

How to chase apps?

- Think as a threat actor
 - Different types of apps? Should I write the each app from scratch ?
 - How will I distribute my apk ?
 - If you can't distribute fast, people will complain and app will be removed from GP

Chasing the Joker



Distribution of Apps:

→ Saw @sh1shkova's tweet

Chasing the Joker

Distribution of
→ Saw @



Tatyana Shishkova @ Botconf · 08 Nov

More #Joker Trojans on Google Play:
[play.google.com/store/apps/details...](https://play.google.com/store/apps/details?id=com.lancegriggs.bobcamera)
[play.google.com/store/apps/details...](https://play.google.com/store/apps/details?id=com.samanthaferguson.crazyclean)

Bob Camera
LANCE GRIGGS Photography
This app is compatible with your device.
Add to wishlist **Install**

HD Camera Live Stickers Live Filters Photo

Bob Camera is an excellent fast camera app that turns your phone into a professional camera.

Special feature
• Face detection / face recognition
• Flood HD images

Crazy Clean
Samantha Ferguson Tools
This app is compatible with your device.
Add to wishlist **Install**

Clean My Phone Junk Files Battery Saver APP

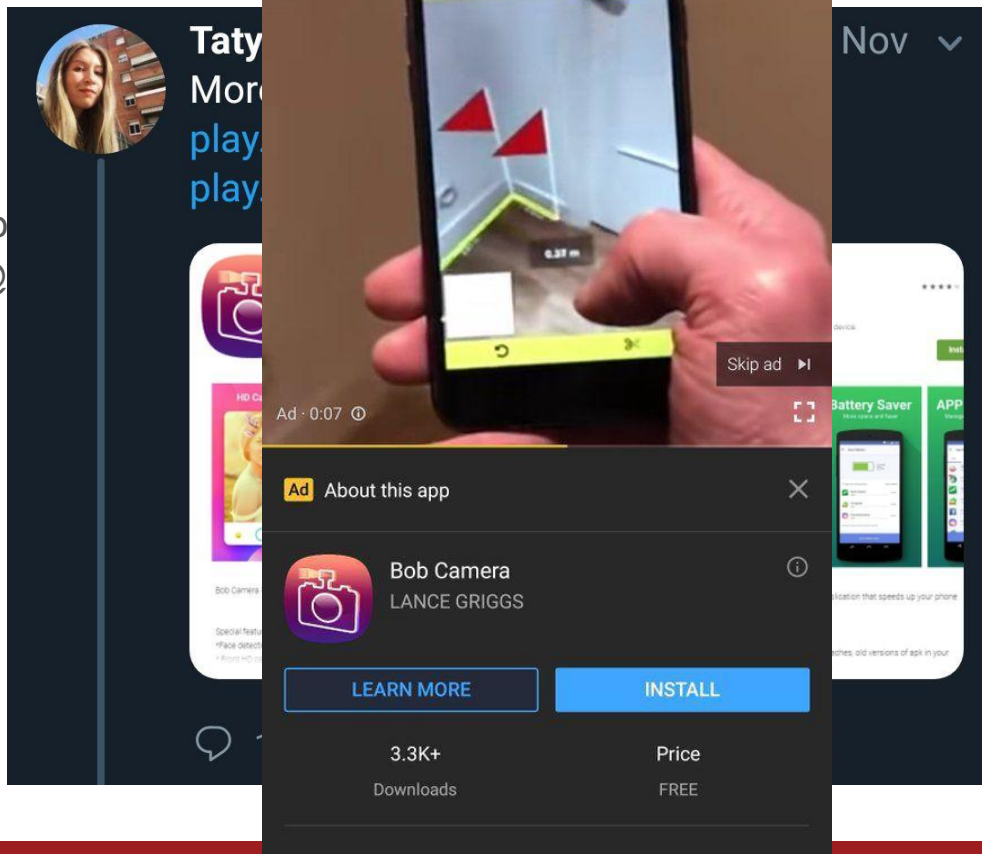
Crazy Clean is a professional and efficient Android cleaning application that speeds up your phone and continually scans and rejects junk files.

• Clean up the garbage
It can detect unwanted junk files, application caches, system caches, old versions of apk in your phone, and clean them up to free up and optimize your storage.

1 12 16

Chasing the Job

Distribution of
→ Saw @



Visit advertiser


Cancel Done

6.37 m

Skip ad ▶

Ad · 0:07 ⓘ

Ad About this app ×

 **Bob Camera**
LANCE GRIGGS ⓘ

[LEARN MORE](#) [INSTALL](#)

3.3K+ Downloads Price
FREE

86% 12:02

Visit advertiser

Ad · 1 of 2 · 0:06

88% 11:54

Visit advertiser

Skip ad

about this app

Bob Camera
LANCE GRIGGS

LEARN MORE INSTALL

3.3K+ Downloads Price FREE

Outline Wallpaper
ASHTON WALLACE

LEARN MORE INSTALL

Nov

Battery Saver

APP





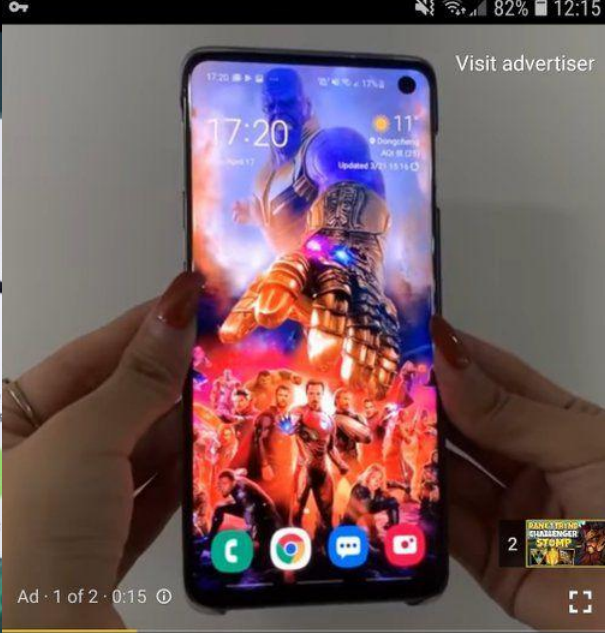
Ad · 1 of 2 · 0:06

Ad About this app



Outline Wallpaper
ASHTON WALLACE

LEARN MORE



Visit advertiser

Ad · 1 of 2 · 0:15

Ad About this app



Poetry Wallpaper
Jacqueline Coney

LEARN MORE

INSTALL

18K+
Downloads

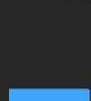
Price
FREE



Visit advertiser

Ad · 1 of 2 · 0:15

Ad About this app

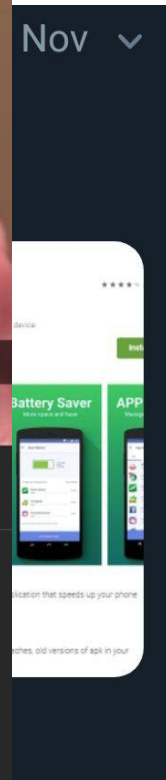


Poetry Wallpaper
Jacqueline Coney

LEARN MORE

18K+
Downloads

Price
FREE



Battery Saver

APP

More apps and games

More apps and games

More apps and games

More apps and games

More apps and games

More apps and games

More apps and games

More apps and games

More apps and games

More apps and games

More apps and games

More apps and games

More apps and games

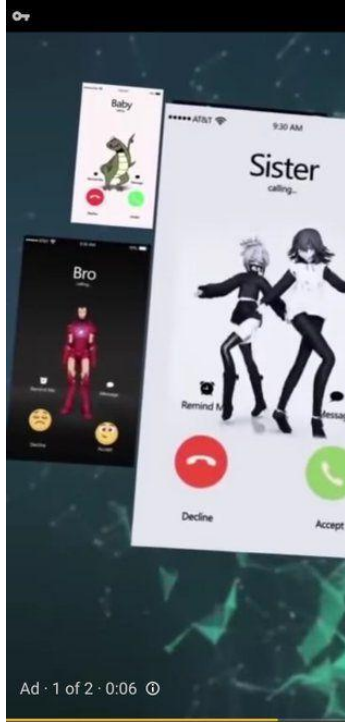
More apps and games

More apps and games

More apps and games

More apps and games






Ad · 1 of 2 · 0:06





Ad · 1 of 2 · 0:15

Ad About this app


 **Scape Wallpaper**
Patti Kiser
FREE

[LEARN MORE](#) [INSTALL](#)

 Google Play



Ad About this app

 **Outline Wallpaper**
ASHTON WALLACE

[LEARN MORE](#)

 **Poetry Wallpaper**
Jacqueline Coney

[LEARN MORE](#) [INSTALL](#)

18K+ Downloads Price FREE

Ad · 1 of 2 · 0:06

Baby
Sister calling...
Bro

Ad About this app

Outline Wallpaper
ASHTON WALLACE

LEARN MORE

Visit advertiser

17:20 11°
18%

Ad · 1 of 2 · 0:15

Ad About this app

Poetry Wallpaper
Jacqueline Coney

LEARN MORE

INSTALL

18K+ Downloads

Price FREE

Ad About this app

Scape World
Patti Kise
FREE

LEARN MORE

Visit advertiser

HOW TO LOOT?

Ad · 1 of 2 · 0:12

TRY

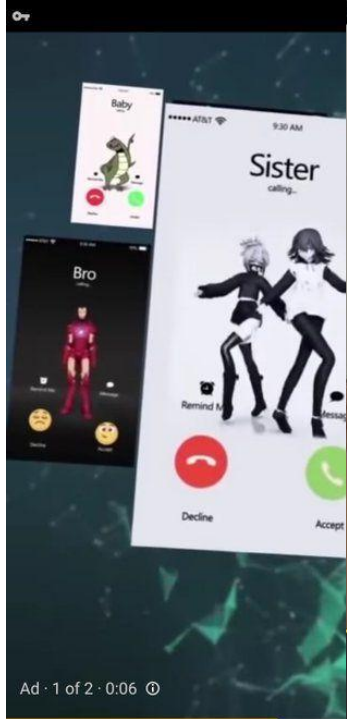
Ad About this app

Grow Game
Butterman Texas
FREE

LEARN MORE

INSTALL

Google Play



Ad · 1 of 2 · 0:06

Ad About this app

 **Outline Wallpaper**
ASHTON WALLACE

LEARN MORE



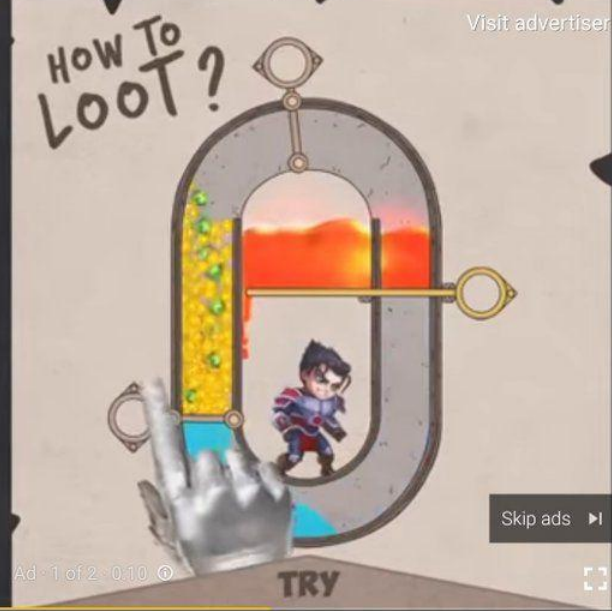
Ad · 1 of 2 · 0:15

Ad About this app

 **Poetry W**
Jacqueline

LEARN MORE

18K+
Downloads



Ad · 1 of 2 · 0:10

Ad About this app

 **Step Box**
karen lappin

LEARN MORE

2.4K+
Downloads



Ad · 1 of 2 · 0:12

Ad About this app

Grow Game
Butterman Texas
FREE

LEARN MORE

INSTALL



CTUS
O P E

Ad - 1 of 2 - 0:06

Decline

Remind Me

Visit advertiser

Ad - 0:12

Path Anchor Geometric Remove Speed Freeze Unfreeze

Visit advertiser

Skip ads

Visit advertiser

Ad - 0:12

TRY

Ad About this app

Eulogize Camera
Lauren Michaud
FREE

LEARN MORE INSTALL

Google Play

Ad About this app

Grow Game
Butterman Texas
FREE


LEARN MORE INSTALL

Price
FREE

Google Play

Ad - 1 of 2 - 0:06


Ad About this app

 Outline Wallpapers
ASHTON WALL

[LEARN MORE](#)

Ad - 0:12


Ad About this app

 Eulogize
Lauren Mi
FREE

[LEARN MORE](#)

Ad - 1 of 2 - 0:06


Ad About this app

 Boost Wallpaper
Anita B Bailey


[LEARN MORE](#)

Ad - 1 of 2 - 0:21

Ad About this app


 Fun Camera
Pamela Burfor
FREE

[LEARN MORE](#) [INSTALL](#)

 Google Play

Ad - 1 of 2 - 0:21

Ad About this app

 Angry Birds

[LEARN MORE](#) [INSTALL](#)

Ad · 1 of 2 · 0:06

Bro

Remind Me

Decline

Ad About this app

Outline Wallpapers
ASHTON WALL

LEARN MORE

Sister calling...

Ad About this app

Mars Game
SHERITTA YOUNG

LEARN MORE

INSTALL

4.6K+ Downloads

Price FREE

Ad About this app

Boost Wallpaper
Anita B Bailey

LEARN MORE

INSTALL

Visit advertiser

Erase

Restore

Insert

Shape

2

INSTALL

Ad About this app

Erase

Price FREE

LEARN MORE

INSTALL

Visit advertiser

1

INSTALL

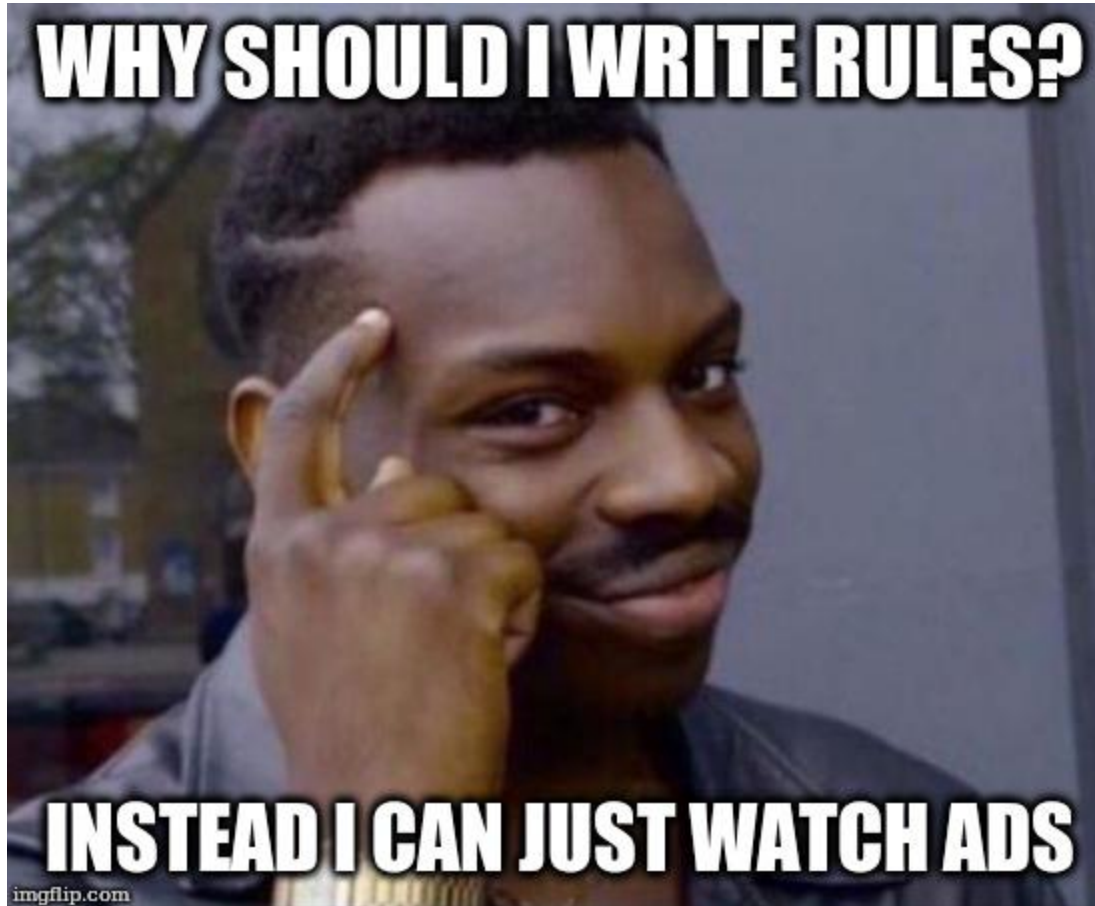
Ad About this app

Erase

Price FREE

LEARN MORE

INSTALL



Chasing the Joker

Distribution of Apps:

- Saw @sh1shkova's tweet
- They were definitely using Youtube ads
- Watching Youtube Ads to get Trojan :D

Chasing the Joker

Different types of Apps:


- Permissions will differ but my intentions will stay same
- Same subset of permissions:
 - ◆ `perm:android.permission.GET_ACCOUNTS` AND
`perm:android.permission.CHANGE_WIFI_STATE` AND
`perm:android.permission.READ_PHONE_STATE`

Chasing the Joker

apklab.io comes to help



Chasing the Joker

BETA
APK
LAB
HOME SAMPLES BATCHES NEWS ?  AHMET BILAL

SEARCH

f:CheckForSuperuserBinary AND f:GetDefaultSMSPackage AND perm:android.permis... ★

OR AND av: C

Tip: You can use fil

Showing 20 of ???.

START TIME | DESC ▼

Tools ▼

```
f:CheckForSuperuserBinary AND f:GetDefaultSMSPackage AND
perm:android.permission.GET_ACCOUNTS AND perm:android.permission.CHANGE_WIFI_STATE AND
perm:android.permission.READ_PHONE_STATE AND f:ExecutesExternalCodeDexClassLoader
activity:projekt.launcher.ProjektLauncher
activity:com.spr.racwe.MainActivity
activity:com.example.grapgame.antivirus.ui.SplashActivity
activity:com.andronicus.coolwallpapers.ui.Activity_Splash
activity:com.zentertain.photoeditor.SplashActivity
```

Chasing the Joker



Different types of Apps:

- Permissions will differ but my intentions will be same
- Same subset of permissions:
- Add malicious code to legitimate apps.
 - ◆ Trace back from legitimate apps ???

Chasing the Joker

```
<uses-permission android:name="com.petalwallpaper.wpslow.permission.C2D_MESSAGE" />
<application android:theme="@style/MyMaterialTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher"
  <meta-data android:name="io.fabric.ApiKey" android:value="" />
  <activity android:label="@string/app_name" android:name="com.andronicus.coolwallpapers.ui.Activity_Splash">
    <intent-filter>
      <action android:name="android.intent.action.MAIN" />
      <category android:name="android.intent.category.LAUNCHER" />
    </intent-filter>
  </activity>
  <activity android:label="@string/app_name" android:name="com.andronicus.coolwallpapers.ui.Activity_Main" android:co
    <intent-filter>
      <action android:name="android.intent.action.MAIN" />
      <category android:name="android.intent.category.DEFAULT" />
    </intent-filter>
  </activity>
</application>
```

Chasing the Joker

Q Search...  

OR AND av: C

Tip: You can use fil

f:CheckForSuperuserBinary AND f:GetDefaultSMSPackage AND
perm:android.permission.GET_ACCOUNTS AND perm:android.permission.CHANGE_WIFI_STATE AND S
perm:android.permission.READ_PHONE_STATE AND f:ExecutesExternalCodeDexClassLoader

activity:projekt.launcher.ProjektLauncher	S
activity:com.spr.racwe.MainActivity	S
activity:com.example.grapgame.antivirus.ui.SplashActivity	S
activity:com.andronicus.coolwallpapers.ui.Activity_Splash	S
activity:com.zentertain.photoeditor.SplashActivity	S
activity:com.radialapps.antivirus.battery.appbooster.cleaner.activities.SplashActivity	S
activity:com.soda.gambox.boost.SplashActivity	S
activity:info.androidstation.qhdwallpaper.activities.SplashActivity	S
activity:hd.uhd.wallpapers.best.quality.activities.SplashScreenNew	S

Tools ▼

SEARCH


START TI

Chasing the Joker




In the end lots of people protected. Samples are reported to Google and removed from Google Play Store


Only in November 60 apps with over 1.000.000 installations




Wonder Puzzle
Jessica Graham Entertainment
PEGI 3
This app is compatible with all of your devices.



Warmine Messages
Vanessa Campbell Personalization
PEGI 3
This app is compatible with some of your devices.




Scale Photo Editor
Kristi R Robinson Photography
PEGI 3
This app is compatible with all of your devices.




Forum Wallpaper
Robin Francis Personalization
PEGI 3
This app is compatible with all of your devices.




Suit Game
Gary L Belcher Entertainment
PEGI 3




Meet Messages
Robin Sypoltr Communication
PEGI 3
This app is compatible with some of your devices.



Peculiar Photo Editor
Shirley Hargrove Personalization
PEGI 3
This app is compatible with all of your devices.




Deposit Photo Editor
gaylene sakiestewa Personalization
PEGI 3
This app is compatible with some of your devices.




Hilarious Camera
eirehamene1 Entertainment
PEGI 3
Contains Ads
This app is compatible with all of your devices.




Space Photo Editor
Paula Edwards Photography
PEGI 3
This app is compatible with all of your devices.



Alien
Matthew Thorpe Tools
PEGI 3
This app is compatible with all of your devices.




Go SMS
Matt Bland Communication
PEGI 3
This app is incompatible with all of your devices.



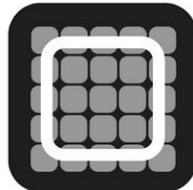
Demand Photo Editor
Joshua Lambrou Photography
PEGI 3
This app is compatible with some of your devices.



Timbre Clean
PATRICIA Tools
PEGI 3
This app is compatible with all of your devices.



Demand Wallpaper
Edward C Butterworth Personalization
PEGI 3
This app is compatible with all of your devices.



Step Box
karen lappin Entertainment
PEGI 3
This app is compatible with all of your devices.

Thanks for listening



Ahmet Bilal Can

 0xabc0