149 New Montgomery Street
4th Floor
San Francisco, CA 94105

1,000 Mobile Apps in Australia:

Appendix A: Obfuscated Data Transmissions

September 24, 2020

A   Obfuscated Data Transmissions

In this section, we provide examples of four obfuscation techniques that we observed being used by various advertising-related SDKs[78] when transmitting user information from apps during the testing period. We define "obfuscation" as a process of encoding data that results in its presence being obscured in network transmissions. In this report, when we refer to "obfuscation techniques," we refer to methods that go beyond the recommended use of transport-layer security (TLS);[79,80] that is, these are examples of bespoke techniques that we believe are likely to obscure the transmission of user data to the casual observer, which is why we highlight them here.

---

[78]For an explanation of SDKs, see Section 4.1.2.

[79]https://en.wikipedia.org/wiki/Transport_Layer_Security

[80]https://web.archive.org/web/20200621224406/https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html

---

A.1   AppLovin

AppLovin is a mobile marketing platform. They encode their traffic using naïve cryptographic means, which we were able to decode. Figure 23 shows an example transmission. The data itself is encoded using "base64", a standard for encoding binary data as plain text.[81] The decoded data, however, needed to be further decrypted by our automated testing tools. An example decrypted transmission is shown in Figure 24.

The specific encoding is as follows. First, a developer key is found for each app, which is unique to the developer and AppLovin. These are found either in transmitted data, or as part of a filename on the filesystem (`com.applovin.sdk.preferences.<developer key>.xml`). The developer key must be base64 decoded, and the first 8 bytes of it are taken as an XOR-mask to decrypt a per-payload random seed that appears as the first eight bytes of the transmitted data.

The remaining bytes of the encrypted data are doubly encrypted with a Vernam-style XOR mask.[82] First, the first eight bytes of the developer key is XORed with the encrypted data. Then, at every eight-byte interval, the random seed and current offset in the stream is used to compute another eight-byte number that is also XORed to the encrypted data to reveal the decrypted data. The pseudocode to compute this number is as follows:

```
int64_t seed_offset(int64_t seed, size_t pos) {
        int64_t cur = seed + pos;
        cur ^= (cur >> 33);
        cur *= -4417276706812531889;
        cur ^= (cur >> 29);
        cur *= -8796714831421723037;
        cur ^= (cur >> 32);
        return cur;
}
```

---

[81]https://en.wikipedia.org/wiki/Base64
[82]https://en.wikipedia.org/wiki/Gilbert_Vernam#The_Vernam_cipher

```
POST /2.0/device?p=1:96943fdea087a1d759e08734fce0068af23ef96e:47UideV...** HTTP/1.1
Content-Type: application/json; charset=utf-8
Content-Length: 910
User-Agent: Dalvik/2.1.0 ...
Host: d.applovin.com
Connection: Keep-Alive
Accept-Encoding: gzip

1:96943fdea087a1d759e08734fce0068af23ef96e:47UideVFAWW-CPU_QsgyoqDNFdkAiJvwcOrzMVzt
i-ocffCnOIKBxg:uqFkRop8LuP2RcJL1M_ox-_n325LM43metv49ew1onZ3WhoLxKJ9iifJh4e6lXyMx...
```

Figure 23: Example (truncated and redacted) packet transmission from the Be Closer app to Applovin (`d.applovin.com`). The payload of the data beginning at `uqFkR` is encrypted.

```
{
  "app_info": {
    "app_name": "be closer",
    "app_version": "2.4.1",
    "applovin_sdk_version": "9. 2.1",
    "first_install": "true",
    "installed_at": "XXXXXXXXXXXXX",
    "installer_name": "",
    "package_name": "com.becloser",
    "tg": "31"
  }
  "device_info": {
    "adns": "2.75",
    "adnsd": "440",
    "adr": "0",
    "brand": "Google",
    "brand_name": "Android",
    "dnt": "false",
    "fs": "XXXXXXXXXX",
    "gy": "1",
    "hardware": "sargo",
    "idfa": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
    "locale": "en_US",
    "model": "AOSP on sargo",
    "orientation_lock": "portrait",
    "os": "9",
    "revision": "sargo",
    "sdk_version": "28",
    "sim": "0",
    "tv": "0",
    "type": "android",
    "tz_offset": "-7",
    "volume": "53",
    "wvvc": "0"
...
```

Figure 24: Decrypted payload from the example packet transmission from the Be Closer app to Applovin (`d.applovin.com`). The line beginning with `"idfa"` contains the AAID.

Table 11 lists the 75 apps that communicated with AppLovin's domains during the test-ing period, many of which we observed using this obfuscation technique.

Table 11: Apps that transmitted user information to AppLovin during the testing period.

App	Category
"C25K® - 5K Running Trainer" (com.c25k; 1,000,000 installs), developed by Zen Labs Fitness	Health
"Sleepa: Relaxing sounds, Sleep" (net.relaxio.sleepo; 1,000,000 installs), developed by Sound Sleep - Relaxing Sounds and White Noise	Health
"Sleep Sounds" (net.metapps.sleepsounds; 5,000,000 installs), developed by Sound Sleep - Relaxing Sounds and White Noise	Health
"Plant Nanny² - Your Adorable Water Reminder" (com.fourdesire.plantnanny2; 1,000,000 installs), devel-oped by Fourdesire	Health
"ABC Song - Rhymes Videos, Games, Phonics Learning" (kidzooly.rhymes; 1,000,000 installs), developed by Kidzooly - Kids Games, Rhymes , Nursery Songs.	Kids
"Be Closer" (com.becloser; 10,000,000 installs), developed by Agromart Dev	Kids
"Kids Top Nursery Rhymes Videos - Offline Learning" (kidzooly.fivelittle; 1,000,000 installs), developed by Kidzooly - Kids Games, Rhymes , Nursery Songs.	Kids
"Galaxy Attack: Alien Shooter (Premium)" (com.alien.shooter.galaxy.attack.premium; 100,000 installs), developed by ONESOFT	Kids
"Vector Full" (com.nekki.vector.paid; 500,000 installs), developed by NEKKI	Kids
"Wattpad - Read & Write Stories" (wp.wattpad; 100,000,000 installs), developed by Wattpad.com	Other
"My Talking Tom 2" (com.outfit7.mytalkingtom2; 100,000,000 installs), developed by Outfit7 Limited	Other
"Slots Casino - Jackpot Mania" (slots.hot.vegas.casino.games.free; 1,000,000 installs), developed by Grande Games	Other
"Audiomack: Download New Music Offline Free" (com.audiomack; 10,000,000 installs), developed by Audiomack	Other
"Pixel Art: Color by Number" (com.europosit.pixelcoloring; 50,000,000 installs), developed by Easybrain	Other
"Vegas Night Slots - HOT&FREE VEGAS CASINO GAMES" (com.vegas.casino.slothbunm; 100,000 installs), developed by Zengzhineng	Other
"Make it perfect" (com.game.perfection; 1,000,000 installs), developed by VOODOO	Other
"Words With Friends 2 –Free Word Games & Puzzles" (com.zynga.words3; 10,000,000 installs), developed by Zynga	Other
"Wordscapes" (com.peoplefun.wordcross; 10,000,000 installs), developed by PeopleFun	Other
"Archero" (com.habby.archero; 10,000,000 installs), developed by Habby	Other
"Happy Color™ –Color by Number" (com.pixel.art.coloring.color.number; 50,000,000 installs), devel-oped by X-Flow	Other
"Sudoku.com - Free Sudoku Puzzles" (com.easybrain.sudoku.android; 10,000,000 installs), developed by Easybrain	Other
"Weather & Clock Widget for Android" (com.devexpert.weather; 50,000,000 installs), developed by Devexpert.NET	Other
"Muslim Pro - Ramadan 2020" (com.bitsmedia.android.muslimpro; 50,000,000 installs), developed by Muslim Pro Limited	Other
"Double Win Casino Slots - Free Vegas Casino Games" (com.huge.slots.casino.vegas.android.avid...; 1,000,000 installs), developed by Free Royal Slot Casino	Other
"Slap Kings" (mobi.gameguru.slapkings; 50,000,000 installs), developed by Lion Studios	Other
"Merge Dragons!" (com.gramgames.mergedragons; 10,000,000 installs), developed by Gram Games Limited	Other
"Tellonym: Honest Q&A" (de.tellonym.app; 10,000,000 installs), developed by Callosum Software	Other

(Table Continues)

Table 11 (Continued)

App	Category
"Cash Storm Casino - Online Vegas Slots Games" (com.cashstorm.slots; 1,000,000 installs), developed by TRIWIN	Other
"Podcast App: Free & Offline Podcasts by Player FM" (fm.player; 5,000,000 installs), developed by Player FM Podcasts	Other
"Superb Casino - HD Free Slots Games" (com.uphill.slot.classic; 1,000,000 installs), developed by SuperB Casino	Other
"BG Player" (com.music.bgplayer; 1,000,000 installs), developed by Yossef Faroh Zada	Other
"theCHIVE" (com.thechive; 5,000,000 installs), developed by Chive Media Group LLC	Other
"Nonogram.com - Picture cross puzzle game" (com.easybrain.nonogram; 10,000,000 installs), developed by Easybrain	Other
"Pedometer" (com.baidu.news.pedometer; 100,000 installs), developed by Bright Star Lab	Other
"Bible Coloring - Paint by Number, Free Bible Games" (holy.bible.biblegame.bibleverse.color.by...; 1,000,000 installs), developed by iDailybread.org	Other
"Idle Army Base" (com.neonplay.casualidlearmybase; 5,000,000 installs), developed by Neon Play	Other
"Scrabble® GO - New Word Game" (com.pieyel.scrabble; 5,000,000 installs), developed by Scopely	Other
"Word Expert" (com.pisanu.scrabbleexpert.free; 100,000 installs), developed by Pisanu Chaloemrattanaporn	Other
"Lucky Time - Win Your Lucky Day & Real Money" (playgame.realmoney.free.scratchers.win.l...; 500,000 installs), developed by Luckytime App Team	Other
"My Talking Tom Friends" (com.outfit7.mytalkingtomfriends; 1,000,000 installs), developed by Outfit7 Limited	Other
"Vegas Friends - Casino Slots for Free" (com.funtriolimited.slots.casino.free; 500,000 installs), developed by Grande Games	Other
"Happy Wheels" (com.fancyforce.happywheels; 5,000,000 installs), developed by James Bonacci	Other
"Super Flashlight" (com.superapp.xincheng; 100,000 installs), developed by Craig's Hub	Other
"Slot Machines –Slots of Immortality™ Free Pokies" (com.bi.slots.immortality; 100,000 installs), developed by Bad Ibis Games Ltd	Other
"Lucky Time - Win Rewards Every Day" (com.luckyapp.winner; 10,000,000 installs), developed by Lucky Lucky Team	Other
"TOP SEED Tennis: Sports Management Simulation Game" (com.gaminho.topseedtennis; 1,000,000 installs), developed by Gaminho	Other
"Sudoku. Logic Puzzle" (com.forsbit.sudoku; 10,000 installs), developed by Forsbit LLC	Other
"Ahri RPG" (com.DoomsdayStudio.AhriRPG; 100,000 installs), developed by DOOMSDAY Studio	Other
"Jelly Drops - Free Puzzle Games" (com.cookapps.playgrounds.ff.jellypopmani...; 100,000 installs), developed by CookApps	Other
"Spider Solitaire - Offline Free Card Games" (com.sngict.spider; 100,000 installs), developed by SNG Games	Other
"Casino Slots: Vegas Fever" (casino.slots.vegasfever; 100,000 installs), developed by AGS Interactive	Other
"My Home - Design Dreams" (com.spacegame.homedesign; 50,000,000 installs), developed by Zentertain	Other
"FUT 20 Draft, Squad Builder & SBC - FUTBIN" (com.futbin; 1,000,000 installs), developed by FUTBIN	Other
"Tycoon Casino™: Free Vegas Jackpot Slots" (com.tw.tycoon.casino; 5,000,000 installs), developed by Triwin Games	Other
"Words With Friends –Word Puzzle" (com.zynga.wwf2.free; 10,000,000 installs), developed by Zynga	Other
"Parkour Race - Freerun Game" (com.parkourrace.game; 10,000,000 installs), developed by Madbox	Other
"Pulse Cleaner - Phone Booster & Optimizer" (mobi.pulse.space.boost.cleaner; 50,000 installs), developed by pulse app studio	Other

(Table Continues)

Table 11 (Continued)

App	Category
"Gold Fortune Casino™ - Free Vegas Slots" (triwin.casino.slots.fortune.gold; 1,000,000 installs), developed by TRIWIN	Other
"Mimi 4chan Reader" (com.emogoth.android.phone.mimi; 1,000,000 installs), developed by Mimi Reader	Other
"Jigsaw Puzzles - Puzzle Game" (com.easybrain.jigsaw.puzzles; 10,000,000 installs), developed by Easybrain	Other
"Sharpen Blade" (com.zplay.blade; 10,000,000 installs), developed by ZPLAY Games	Other
"캐시워크 - 적립형만보기첫화면" (com.cashwalk.cashwalk; 5,000,000 installs), developed by CashWalk, Inc.	Other
"Paint By Number - Free Coloring Book & Puzzle Game" (paint.by.number.pixel.art.coloring.drawi...; 50,000,000 installs), developed by Better Life - Color and Draw	Other
"Solitaire" (com.tripledot.solitaire; 1,000,000 installs), developed by Tripledot Studios Limited	Other
"Cash Mania Slots - Free Slots Casino Games" (slots.free.vegas.casino.cash.mania; 500,000 installs), developed by Galaxy Entertainment Limited	Other
"Tiles Hop: EDM Rush!" (com.amanotes.beathopper; 100,000,000 installs), developed by AMANOTES	Other
"Sniper 3D: Fun Free Online FPS Shooting Game" (com.fungames.sniper3d; 100,000,000 installs), developed by Fun Games For Free	Other
"Magic Tiles 3" (com.youmusic.magictiles; 100,000,000 installs), developed by AMANOTES	Other
"Paper.io 2" (io.voodoo.paper2; 100,000,000 installs), developed by VOODOO	Other
"Johnny Trigger" (com.time.trigger; 50,000,000 installs), developed by SayGames	Other
"Idle Miner Tycoon: Mine & Money Clicker Management" (com.fluffyfairygames.idleminertycoon; 50,000,000 installs), developed by Kolibri Games	Other
"Matchington Mansion" (com.matchington.mansion; 50,000,000 installs), developed by Firecraft Studios	Other
"Brain Test: Tricky Puzzles" (com.unicostudio.braintest; 50,000,000 installs), developed by Unico Studio	Other
"Word Stacks" (com.peoplefun.wordstacks; 10,000,000 installs), developed by PeopleFun	Other
"CodyCross: Crossword Puzzles" (com.fanatee.cody; 50,000,000 installs), developed by Fanatee, Inc.	Other

A.2 AppsFlyer

AppsFlyer is another mobile marketing platform. They encode their traffic using naïve cryptographic means, which we have examined and decoded/decrypted. Figure 25 shows an example transmission. The data itself is pure binary and omitted as it contains (encrypted) identifying information. Our tools are able to automatically decrypt this data and an example resulting transmission is shown in Figure 26.

AppsFlyer uses 128-bit AES encryption in CBC mode to encrypt its data.[83] It uses a random initialization vector (IV),[84] which it appends to the end of the encrypted message. The AES encryption key is generated deterministically from a per-developer key by using it as the password for a password-based key derivation function[85] with 10,000 iterations and 8 bytes of zeros as the IV. The developer key is often transmitted alongside or before encrypted data in either a JSON object or a HTTP GET request as the key "devkey."

```
POST /api/v5.2/androidevent?app_id=com.hotornot.app&buildnumber=5.2.0 HTTP/1.1
Content-Length: 2456
Content-Type: application/octet-stream
User-Agent: Dalvik/2.1.0 ...
Host: launches.appsflyer.com
Connection: Keep-Alive
Accept-Encoding: gzip

[ 2456 bytes of encrypted binary data ]
```

Figure 25: Example (truncated and redacted) packet transmission from the Hot or Not app to AppsFlyer (`launches.appsflyer.com`). The payload is omitted.

---

[83]https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
[84]https://en.wikipedia.org/wiki/Initialization_vector
[85]https://en.wikipedia.org/wiki/Key_derivation_function

```
{
    "af_timestamp": "XXXXXXXXXXXXX",
    "registeredUninstall": false,
    "cell": {
        "mnc": X,
        "mcc": XXX
    },
    "operator": "XXXXXXXXXXX",
    "network": "MOBILE",
    "timepassedsincelastlaunch": "XXXXX",
    "af_v2": "XXXXXXXXXXXXXXXXXXXXX",
    "uid": "XXXXXXXXXXXXXXXXXXXXX,
    "installDate": "XXXXXXXXXXXXXXXX",
    "app_version_code": "3346",
    "firstLaunchDate": "XXXXXXXXXXXXXXXX",
    "last_boot_time": ##########,
    "deviceData": {
        "sensors": [{
                "sT": 1,
                "sVS": [0.4#####, -2.1#####, 9.3#####],
                "sV": "BOSCH",
                "sVE": [0.4#####, -2.1#####, 9.4#####],
                "sN": "BMI160 Accelerometer"
            }, {
                "sT": 4,
                "sVS": [0.0#########, -0.0#########, 0.0#########],
                "sV": "BOSCH",
                "sVE": [-0.0#########, 0.0#########, -0.0#########],
                "sN": "BMI160 Gyroscope"
            }, {
                "sT": 2,
                "sVS": [-9#.######, -3#.######, -1#.######],
                "sV": "akm",
                "sVE": [-9#.######, -3#.######, -1##.#####],
                "sN": "AK0991X Magnetometer"
            }
        ],
    },
    {"advertiserId": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",}
    "advertiserIdEnabled": "true",
}
```

Figure 26: Decrypted payload from the example packet transmission from the Hot or Not app to AppsFlyer (`launches.appsflyer.com`). We have redacted possibly identifying information and removed lines from the transmission for simplicity. We have also removed precision from the precise sensor data that was transmitted: the three-dimentional accelerometer, gyroscope, and magnetometer had their precise values transmitted. We have highlighted the transmission of the AAID in red.

We have heavily redacted information from the decrypted data. Some of this includes precise timestamps, such as when the app was installed and when the phone was last turned on. It also includes precise readings from the phone's accelerometer, gyroscope, and magnetometer, which we have modified to remove a couple digits of precision. Given the infrequency with which this data was observed being transmitted during the testing period, we presume that this sensor data is being used for click fraud detection (i.e., to infer, when ads are clicked, whether the phone is being held by a human being versus manipulated by software), rather than as a biometric for user identification (which would almost certainly require streaming the data, rather than the single discrete readings observed during the testing period).

Table 12 lists the 167 apps that communicated with AppsFlyer's domains during the testing period, many of which we observed using this obfuscation technique.

Table 12: Apps that transmitted user information to AppsFlyer during the testing period.

App	Category
"Calm - Meditate, Sleep, Relax" (com.calm.android; 10,000,000 installs), developed by Calm.com, Inc.	Health
"Walking & Running Pedometer for Health & Weight" (cc.pacer.androidapp; 10,000,000 installs), developed by Pacer Health	Health
"AllTrails: Hiking, Running & Mountain Bike Trails" (com.alltrails.alltrails; 5,000,000 installs), developed by AllTrails, LLC	Health
"Runkeeper - GPS Track Run Walk" (com.fitnesskeeper.runkeeper.pro; 10,000,000 installs), developed by ASICS Digital, Inc.	Health
"Waking Up: A Meditation Course" (org.wakingup.android; 500,000 installs), developed by Waking Up LLC	Health
"Pill Reminder & Medication Tracker - Medisafe" (com.medisafe.android.client; 1,000,000 installs), developed by Medisafe® □□	Health
"Pregnancy & Baby Tracker" (com.wte.view; 1,000,000 installs), developed by What to Expect	Health
"Sleepa: Relaxing sounds, Sleep" (net.relaxio.sleepo; 1,000,000 installs), developed by Sound Sleep - Relaxing Sounds and White Noise	Health
"Sleep Sounds" (net.metapps.sleepsounds; 5,000,000 installs), developed by Sound Sleep - Relaxing Sounds and White Noise	Health
"Calorie Counter by Lose It! for Diet & Weight Loss" (com.fitnow.loseit; 10,000,000 installs), developed by FitNow, Inc.	Health
"Carb Manager: Keto Diet Tracker & Macros Counter" (com.wombatapps.carbmanager; 1,000,000 installs), developed by Wombat Apps LLC	Health
"Freeletics Training Coach –Bodyweight & Mindset" (com.freeletics.lite; 10,000,000 installs), developed by Freeletics	Health
"BetterMe: Home Workouts & Diet" (com.gen.workoutme; 10,000,000 installs), developed by BetterMe Limited	Health
"Flo Period tracker, Ovulation & Pregnancy tracker" (org.iggymedia.periodtracker; 50,000,000 installs), developed by Flo Health, Inc.	Health
"Plant Nanny² - Your Adorable Water Reminder" (com.fourdesire.plantnanny2; 1,000,000 installs), developed by Fourdesire	Health
"Minecraft" (com.mojang.minecraftpe; 10,000,000 installs), developed by Mojang	Kids
"Monopoly - Board game classic about real-estate!" (com.marmalade.monopoly; 100,000 installs), developed by Marmalade Game Studio	Kids

(Table Continues)

Table 12 (Continued)

App	Category
"Galaxy Attack: Alien Shooter (Premium)" (com.alien.shooter.galaxy.attack.premium; 100,000 installs), developed by ONESOFT	Kids
"RollerCoaster Tycoon® Classic" (com.atari.mobile.rctclassic; 50,000 installs), developed by Atari, Inc.	Kids
"My Little Princess : Castle" (mylittleprincess.castle; 100,000 installs), developed by My Town Games Ltd	Kids
"Tinder" (com.tinder; 100,000,000 installs), developed by Tinder	Other
"Bumble - Dating, Friends & Business" (com.bumble.app; 10,000,000 installs), developed by Bumble Holding Limited	Other
"MX Player" (com.mxtech.videoplayer.ad; 500,000,000 installs), developed by MX Media & Entertainment (formerly J2 Interactive)	Other
"Roblox" (com.roblox.client; 100,000,000 installs), developed by Roblox Corporation	Other
"Grindr - Gay chat" (com.grindrapp.android; 10,000,000 installs), developed by Grindr LLC	Other
"Fishdom" (com.playrix.fishdomdd.gplay; 100,000,000 installs), developed by Playrix	Other
"Alarm Clock Xtreme: Alarm, Reminders, Timer (Free)" (com.alarmclock.xtreme.free; 50,000,000 installs), developed by AVG Labs	Other
"Wattpad - Read & Write Stories" (wp.wattpad; 100,000,000 installs), developed by Wattpad.com	Other
"Alarm Clock with Missions & Loud Ringtones -Alarmy" (droom.sleepIfUCan; 10,000,000 installs), developed by Alarm Clock Alarmy	Other
"Zoosk: Date, Connect & Find Your Best Match" (com.zoosk.zoosk; 10,000,000 installs), developed by Zoosk Inc.	Other
"Parallel Space - Multiple accounts & Two face" (com.lbe.parallel.intl; 100,000,000 installs), developed by LBE Tech	Other
"My Talking Tom 2" (com.outfit7.mytalkingtom2; 100,000,000 installs), developed by Outfit7 Limited	Other
"Investing.com: Stocks, Finance, Markets & News" (com.fusionmedia.investing; 10,000,000 installs), developed by INVESTING.com	Other
"Audiomack: Download New Music Offline Free" (com.audiomack; 10,000,000 installs), developed by Audiomack	Other
"Amino: Communities and Chats" (com.narvii.amino.master; 10,000,000 installs), developed by Amino Apps	Other
"Dragon City" (es.socialpoint.DragonCity; 100,000,000 installs), developed by Socialpoint	Other
"Caesars Casino: Free Slots Games" (com.playtika.caesarscasino; 10,000,000 installs), developed by Playtika	Other
"Email App for Any Mail" (park.outlook.sign.in.client; 5,000,000 installs), developed by Craigpark Limited	Other
"Board Kings™ " (com.jellybtn.boardkings; 10,000,000 installs), developed by Jelly Button Games	Other
"BuzzVideo: Watch something great" (com.ss.android.article.topbuzzvideo.en; 10,000,000 installs), developed by TopBuzz	Other
"My Telstra" (com.telstra.mobile.android.mytelstra; 5,000,000 installs), developed by Telstra Corporation Ltd.	Other
"Reddit" (com.reddit.frontpage; 10,000,000 installs), developed by reddit Inc.	Other
"Pinterest" (com.pinterest; 100,000,000 installs), developed by Pinterest	Other
"Stocard - Rewards Cards Wallet" (de.stocard.stocard; 10,000,000 installs), developed by Stocard GmbH	Other
"AVG AntiVirus 2020 for Android Security Free" (com.antivirus; 100,000,000 installs), developed by AVG Mobile	Other
"Plenty of Fish Free Dating App" (com.pof.android; 50,000,000 installs), developed by Plentyoffish Media ULC	Other
"Avast Antivirus –Scan & Remove Virus, Cleaner" (com.avast.android.mobilesecurity; 100,000,000 installs), developed by Avast Software	Other
"Catch: Online Shopping" (au.com.catchoftheday.android; 1,000,000 installs), developed by Catch.com.au Pty Ltd	Other

(Table Continues)

Table 12 (Continued)

App	Category
"Slack" (com.Slack; 10,000,000 installs), developed by Slack Technologies Inc.	Other
"Lightning Link Casino: Free Vegas Slots! 10M Bonus" (com.productmadness.lightninglink; 1,000,000 installs), developed by Product Madness	Other
"imo free video calls and chat" (com.imo.android.imoim; 500,000,000 installs), developed by imo.im	Other
"Slots: Heart of Vegas™ –Free Slot Casino Games" (com.productmadness.hovmobile; 10,000,000 installs), developed by Product Madness	Other
"TuneIn Radio: Live Sports, News, Music & Podcasts" (tunein.player; 100,000,000 installs), developed by TuneIn Inc	Other
"LastPass Password Manager" (com.lastpass.lpandroid; 5,000,000 installs), developed by LogMeIn, Inc.	Other
"Cashman Casino: Vegas Slot Machines! 2M Free!" (com.productmadness.cashmancasino; 5,000,000 installs), developed by Product Madness	Other
"Wordscapes" (com.peoplefun.wordcross; 10,000,000 installs), developed by PeopleFun	Other
"Opera browser with free VPN" (com.opera.browser; 100,000,000 installs), developed by Opera	Other
"Badoo —Dating App to Chat, Date & Meet New People" (com.badoo.mobile; 100,000,000 installs), developed by Badoo	Other
"Imgur: Find funny GIFs, memes & watch viral videos" (com.imgur.mobile; 10,000,000 installs), developed by Imgur	Other
"rif is fun for Reddit" (com.andrewshu.android.reddit; 5,000,000 installs), developed by TalkLittle	Other
"Homescapes" (com.playrix.homescapes; 100,000,000 installs), developed by Playrix	Other
"News Republic - Breaking and Trending News" (com.mobilesrepublic.appy; 50,000,000 installs), developed by News Republic	Other
"9GAG: Funny gifs, pics, fresh memes & viral videos" (com.ninegag.android.app; 10,000,000 installs), developed by 9GAG	Other
"Moovit: Timing & Navigation for all Transit Types" (com.tranzmate; 50,000,000 installs), developed by Moovit	Other
"Bigo Live - Live Stream, Live Video & Live Chat" (sg.bigo.live; 100,000,000 installs), developed by BIGO TECHNOLOGY PTE. LTD.	Other
"Mobile Security: VPN Proxy & Anti Theft Safe WiFi" (com.wsandroid.suite; 50,000,000 installs), developed by McAfee LLC	Other
"Grammarly Keyboard —Type with confidence" (com.grammarly.android.keyboard; 10,000,000 installs), developed by Grammarly, Inc.	Other
"Slotomania™ Slots Casino: Slot Machine Games" (air.com.playtika.slotomania; 50,000,000 installs), developed by Playtika	Other
"OkCupid - Best Online Dating App for Great Dates" (com.okcupid.okcupid; 10,000,000 installs), developed by okcupid.com	Other
"Yubo: Make New Friends - Meet & Chat Livestream" (co.yellw.yellowapp; 5,000,000 installs), developed by Twelve APP	Other
"Double Win Casino Slots - Free Vegas Casino Games" (com.huge.slots.casino.vegas.android.avid...; 1,000,000 installs), developed by Free Royal Slot Casino	Other
"Safe Security - Antivirus, Booster, Phone Cleaner" (com.qihoo.security; 100,000,000 installs), developed by Safe Security Develop	Other
"VPNhub Best Free Unlimited VPN - Secure WiFi Proxy" (com.appatomic.vpnhub; 10,000,000 installs), developed by AppAtomic Limited	Other
"Privacy Messenger - Private SMS messages, Call app" (com.melonsapp.privacymessenger; 1,000,000 installs), developed by Melons Messenger Inc.	Other
"Opera Mini - fast web browser" (com.opera.mini.native; 100,000,000 installs), developed by Opera	Other
"House of Fun™ : Free Slots & Casino Games" (com.pacificinteractive.HouseOfFun; 10,000,000 installs), developed by PLAYTIKA UK - HOUSE OF FUN LIMITED	Other

(Table Continues)

Table 12 (Continued)

App	Category
"MISTPLAY: Gift Cards & Rewards For Playing Games" (com.mistplay.mistplay; 5,000,000 installs), developed by MISTPLAY	Other
"Phone Guardian Mobile Security & VPN Protection" (com.distimo.phoneguardian; 1,000,000 installs), developed by App Annie Basics	Other
"Cash Storm Casino - Online Vegas Slots Games" (com.cashstorm.slots; 1,000,000 installs), developed by TRIWIN	Other
"Messenger" (messenger.social.chat.apps; 10,000,000 installs), developed by Text Free & Free Call & SMS & MMS & Messenger Team	Other
"myMail –Email for Hotmail, Gmail and Outlook Mail" (com.my.mail; 10,000,000 installs), developed by My.com B.V.	Other
"King James Bible (KJV) - Free Bible Verses + Audio" (kjv.bible.kingjamesbible; 10,000,000 installs), developed by iDailybread.org	Other
"Coffee Meets Bagel Free Dating App" (com.coffeemeetsbagel; 1,000,000 installs), developed by Coffee Meets Bagel	Other
"Podcast App: Free & Offline Podcasts by Player FM" (fm.player; 5,000,000 installs), developed by Player FM Podcasts	Other
"Property Finder" (ae.propertyfinder.propertyfinder; 100,000 installs), developed by Property Finder	Other
"Superb Casino - HD Free Slots Games" (com.uphill.slot.classic; 1,000,000 installs), developed by SuperB Casino	Other
"CallApp: Caller ID, Call Blocker & Call Recorder" (com.callapp.contacts; 50,000,000 installs), developed by CallApp Caller ID, Manage & Customize your calls	Other
"DoubleU Casino - Free Slots" (com.doubleugames.DoubleUCasino; 10,000,000 installs), developed by DoubleUGames	Other
"Function - Easy Email Inbox & Productivity Tools" (com.myhomescreen.email; 1,000,000 installs), developed by Yobi Mobi	Other
"Solitaire - Grand Harvest - Tripeaks" (net.supertreat.solitaire; 10,000,000 installs), developed by Supertreat	Other
"Bingo Blitz™ - Bingo Games" (air.com.buffalo_studios.newflashbingo; 10,000,000 installs), developed by Playtika Santa Monica	Other
"Translate All - Speech Text Camera Translator" (com.speech.text.translate; 10,000,000 installs), developed by Translator Lab	Other
"HelloTalk —Chat, Speak & Learn Foreign Languages" (com.hellotalk; 5,000,000 installs), developed by HelloTalk Learn Languages App	Other
"Houseparty" (com.herzick.houseparty; 10,000,000 installs), developed by Life on Air	Other
"Tagged - Meet, Chat & Dating" (com.taggedapp; 10,000,000 installs), developed by Ifwe Inc.	Other
"Klondike Adventures" (com.vizorapps.klondike; 10,000,000 installs), developed by VIZOR APPS LTD.	Other
"Translate it - Speech and Picture Translate" (com.language.speech.picture.translate; 1,000,000 installs), developed by Foto Translate	Other
"Hot or Not - Find someone right now" (com.hotornot.app; 10,000,000 installs), developed by OR NOT LIMITED	Other
"GO Launcher - 3D parallax Themes & HD Wallpapers" (com.gau.go.launcherex; 100,000,000 installs), developed by GOMO Live	Other
"imo beta free calls and text" (com.imo.android.imoimbeta; 100,000,000 installs), developed by imo.im	Other
"theCHIVE" (com.thechive; 5,000,000 installs), developed by Chive Media Group LLC	Other
"IG Trading: Spread Betting, CFDs, Forex & Stocks" (com.iggroup.android.cfd; 500,000 installs), developed by IG Group	Other
"Likee - Formerly LIKE Video" (video.like; 500,000,000 installs), developed by BIGO TECHNOLOGY PTE. LTD.	Other

(Table Continues)

Table 12 (Continued)

App	Category
"Connect for Hotmail & Outlook: Mail and Calendar" (com.connectivityapps.hotmail; 5,000,000 installs), developed by Connectivity Apps	Other
"TopBuzz News: Breaking, Local, Entertaining & FREE" (com.ss.android.article.master; 10,000,000 installs), developed by TopBuzz	Other
"theScore: Live Sports Scores, News, Stats & Videos" (com.fivemobile.thescore; 10,000,000 installs), developed by theScore, Inc.	Other
"News Home - Full Screen News Widget and Launcher" (com.myhomescreen.news; 1,000,000 installs), developed by Yobi Mobi	Other
"IMVU - Game with 3D Avatars, Chat and Real Friends" (com.imvu.mobilecordova; 10,000,000 installs), developed by IMVU, Inc.	Other
"Bigfoot - FREE in-game assistant for mobile player" (us.ozteam.bigfoot; 1,000,000 installs), developed by Oz Interactive	Other
"Bible Coloring - Paint by Number, Free Bible Games" (holy.bible.biblegame.bibleverse.color.by...; 1,000,000 installs), developed by iDailybread.org	Other
"Universal Email App" (park.hotm.email.app; 1,000,000 installs), developed by Craigpark Limited	Other
"Simeji Japanese keyboard+Emoji" (com.adamrocker.android.input.simeji; 10,000,000 installs), developed by バイドゥ 株式□社	Other
"Stylish –Customize Your Navbar & Weather Widget" (com.stylish.stylebar; 100,000 installs), developed by Stylish for Android	Other
"Lucky Time - Win Your Lucky Day & Real Money" (playgame.realmoney.free.scratchers.win.l...; 500,000 installs), developed by Luckytime App Team	Other
"Paint by Number - Pixel Art, Free Coloring Book" (sandbox.pixel.number.coloring.book.page....; 10,000,000 installs), developed by Beetles Games Studio	Other
"My Talking Tom Friends" (com.outfit7.mytalkingtomfriends; 1,000,000 installs), developed by Outfit7 Limited	Other
"hi5 - meet, chat & flirt" (com.hi5.app; 10,000,000 installs), developed by Ifwe Inc.	Other
"Flash Keyboard Emoji" (com.dotc.latin.ime.tap; 10,000,000 installs), developed by Flashkeyboard Team	Other
"Virus Cleaner-Antivirus, Phone Clean, Boost Master" (virus.cleaner.antivirus.phone.security.b...; 1,000,000 installs), developed by Super Security Studio	Other
"DIY color keyboard" (com.diy.keyboard; 1,000,000 installs), developed by Paredes BLACKGOAT	Other
"Slot Machines –Slots of Immortality™ Free Pokies" (com.bi.slots.immortality; 100,000 installs), developed by Bad Ibis Games Ltd	Other
"BaBe+ - Berita Indonesia" (com.ss.android.article.master.id; 5,000,000 installs), developed by Mainspring	Other
"Slot Bonanza - Free casino slot machine game 777" (com.infiapps.slotbonanza; 1,000,000 installs), developed by Joyvoo LTD	Other
"Gaydorado" (com.starg.rainbow; 500,000 installs), developed by CocoBear	Other
"Lucky Time - Win Rewards Every Day" (com.luckyapp.winner; 10,000,000 installs), developed by Lucky Lucky Team	Other
"TOP SEED Tennis: Sports Management Simulation Game" (com.gaminho.topseedtennis; 1,000,000 installs), developed by Gaminho	Other
"Fine Booster - Powerful Android Optimize Tool" (com.fine.booster.carytool; 500,000 installs), developed by For World Peace	Other
"Hindi News:Live India News, Live TV, Newspaper App" (com.nbt.reader; 5,000,000 installs), developed by Times Internet Limited	Other
"FanPlus - All About the Kpop World for Fans" (com.photocard.allstar; 100,000 installs), developed by Team Fan	Other
"World Poker Tour - PlayWPT Free Texas Holdem Poker" (com.playwpt.mobile.poker; 100,000 installs), developed by CaptivePlay	Other

(Table Continues)

Table 12 (Continued)

App	Category
"Sudoku. Logic Puzzle" (com.forsbit.sudoku; 10,000 installs), developed by Forsbit LLC	Other
"Jewel Blast Dragon - Match 3 Puzzle" (com.go7game.jewelclassic; 100,000 installs), developed by Go7Game	Other
"Jelly Drops - Free Puzzle Games" (com.cookapps.playgrounds.ff.jellypopmani...; 100,000 installs), developed by CookApps	Other
"Gay guys chat & dating app - GayFriendly.dating" (gayfriendly.gay.dating.app; 100,000 installs), developed by DABLTECH LTD	Other
"Casino Slots: Vegas Fever" (casino.slots.vegasfever; 100,000 installs), developed by AGS Interactive	Other
"CMN News" (ws.coverme.cmn; 10,000 installs), developed by CoverMe Secure Messenger & Vault, Inc.	Other
"Football Management Ultra 2020 - Manager Game" (com.trophymanager.ultra; 1,000,000 installs), developed by Trophy Games - Football Manager Game Makers	Other
"□仙-中□第一仙□手游" (com.pwrd.zxintscn; 100,000 installs), developed by Perfect Game Speed	Other
"News Suite by Sony" (com.sony.nfx.app.sfrc; 50,000,000 installs), developed by Sony Network Communications Inc.	Other
"Webnovel" (com.qidian.Int.reader; 10,000,000 installs), developed by Cloudary	Other
"KeepClean - Cleaner & Faster" (com.appsinnova.android.keepclean; 10,000,000 installs), developed by APPS INNOVA	Other
"TextU - Private SMS Messenger, Call app" (com.textu.sms.privacy.messenger; 100,000 installs), developed by Melons Chat Group	Other
"Mobile Security & Antivirus" (com.trendmicro.tmmspersonal; 1,000,000 installs), developed by Trend Micro	Other
"AccuWeather: Weather forecast news & live radar" (com.accuweather.android; 50,000,000 installs), developed by AccuWeather	Other
"Tycoon Casino™: Free Vegas Jackpot Slots" (com.tw.tycoon.casino; 5,000,000 installs), developed by Triwin Games	Other
"Gold Fortune Casino™ - Free Vegas Slots" (triwin.casino.slots.fortune.gold; 1,000,000 installs), developed by TRIWIN	Other
"News by The Times of India Newspaper - Latest News" (com.toi.reader.activities; 10,000,000 installs), developed by Times Internet Limited	Other
"Feeld: Dating & Chat For Couples & Singles" (co.feeld; 1,000,000 installs), developed by Feeld Ltd.	Other
"iFunny –fresh memes, gifs and videos" (mobi.ifunny; 10,000,000 installs), developed by iFunny Inc.	Other
"Sharpen Blade" (com.zplay.blade; 10,000,000 installs), developed by ZPLAY Games	Other
"Super 3D Wallpapers - Super realistic 3D effects" (com.super.wallpapers.seat; 100,000 installs), developed by Seat Wallpapers Labs	Other
"Geek Cleaner - Easy & Smart Cleaner" (com.geek.cleaner.francis.cony; 100,000 installs), developed by Francis Team	Other
"European War 6: 1804" (com.easytech.android.ew6; 1,000,000 installs), developed by EasyTech	Other
"Wood Block Puzzle - Free Classic Block Puzzle Game" (puzzle.blockpuzzle.cube.relax; 10,000,000 installs), developed by Beetles Games Studio	Other
"UC Browser- Free & Fast Video Downloader, News App" (com.UCMobile.intl; 500,000,000 installs), developed by UCWeb Singapore Pte. Ltd.	Other
"Paint By Number - Free Coloring Book & Puzzle Game" (paint.by.number.pixel.art.coloring.drawi...; 50,000,000 installs), developed by Better Life - Color and Draw	Other
"Solitaire" (com.tripledot.solitaire; 1,000,000 installs), developed by Tripledot Studios Limited	Other
"Deliveroo: Takeaway food" (com.deliveroo.orderapp; 10,000,000 installs), developed by Deliveroo	Other
"PicsArt Photo Editor: Pic, Video & Collage Maker" (com.picsart.studio; 500,000,000 installs), developed by PicsArt	Other

(Table Continues)

Table 12 (Continued)

App	Category
"NordVPN –fast VPN app for privacy & security" (com.nordvpn.android; 10,000,000 installs), developed by NordVPN apps	Other
"Tiles Hop: EDM Rush!" (com.amanotes.beathopper; 100,000,000 installs), developed by AMANOTES	Other
"Magic Tiles 3" (com.youmusic.magictiles; 100,000,000 installs), developed by AMANOTES	Other
"Paper.io 2" (io.voodoo.paper2; 100,000,000 installs), developed by VOODOO	Other
"Fortnite" (com.epicgames.fortnite; 5,000,000 installs), developed by Epic Games, Inc	Other
"Idle Miner Tycoon: Mine & Money Clicker Management" (com.fluffyfairygames.idleminertycoon; 50,000,000 installs), developed by Kolibri Games	Other
"Word Stacks" (com.peoplefun.wordstacks; 10,000,000 installs), developed by PeopleFun	Other
"CodyCross: Crossword Puzzles" (com.fanatee.cody; 50,000,000 installs), developed by Fanatee, Inc.	Other

A.3 InMobi

InMobi is a mobile advertising company. They encrypt their traffic using AES with a random key generated by the app using a secure source of randomness. They hardcode a public RSA key that they use to encrypt the AES key that they use in the payload. They send both the RSA-encrypted AES key and the AES-encrypted payload alongside each other.

Figure 27 shows an example transmission. The data itself is encoded in base64,[86] but when decoded, it is encrypted binary data. Our tools were able to automatically decrypt this data and a resulting example transmission is shown in Figure 28. We have truncated the encrypted data and redacted the decrypted data.

```
POST /config-server/v1/config/secure.cfg HTTP/1.1
User-Agent: Mozilla/5.0 ....
Content-Length: 920
Content-Type: application/x-www-form-urlencoded
Host: config.inmobi.com
Connection: Keep-Alive
Accept-Encoding: gzip

sm=QAAAAAAAAACQP-CVOTMi6-HKOD7ZhyN3JpQU-wO...&sn=1
```

Figure 27: Example truncated packet transmission from the Podcast App: Free & Offline Podcasts by Player FM app to InMobi (`config.inmobi.com`). The payload is truncated.

```
[missing 16 bytes]ND-JTATB-20191025&
im-accid=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX&
u-id-map={"GPID":"XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"}&
d-localization=en_AU&
tz=36000000&
d-language=en&
d-nettype-raw=1&
p=[{"n":"root","t":0}]&
u-appbid=fm.player&
u-id-adt=0&
d-media-volume=32&
u-appsecure=0&
d-model-name=AOSP+on+sargo&
consentObject={"gdpr_consent_available":true,"gdpr":"0"}&
d-brand-name=Android&d
-manufacturer-name=Google&
u-appdnm=Player+FM&
u-appver=4.12.0.239&
ts=XXXXXXXXXXXX
```

Figure 28: Decrypted payload from the example packet transmission from "Podcast App: Free & Offline Podcasts by Player FM" to InMobi (`launches.appsflyer.com`). We have redacted identifiable information. We have highlighted the AAID in red.

---

[86]https://en.wikipedia.org/wiki/Base64

Table 13 lists the 37 apps that communicated with InMobi's domains during the testing period, many of which we observed using this obfuscation technique.

Table 13: Apps that transmitted user information to inMobi during the testing period.

App	Category
"Sleep Sounds" (net.metapps.sleepsounds; 5,000,000 installs), developed by Sound Sleep - Relaxing Sounds and White Noise	Health
"SKOUT - Meet, Chat, Go Live" (com.skout.android; 50,000,000 installs), developed by Skout Inc.	Other
"Wattpad - Read & Write Stories" (wp.wattpad; 100,000,000 installs), developed by Wattpad.com	Other
"Daily Mail Online" (com.dailymail.online; 5,000,000 installs), developed by Daily Mail Online	Other
"Spider Solitaire" (com.mobilityware.spider; 10,000,000 installs), developed by MobilityWare	Other
"My Talking Tom 2" (com.outfit7.mytalkingtom2; 100,000,000 installs), developed by Outfit7 Limited	Other
"Make it perfect" (com.game.perfection; 1,000,000 installs), developed by VOODOO	Other
"Weatherzone" (au.com.weatherzone.android.weatherzonefr...; 1,000,000 installs), developed by Weatherzone	Other
"TuneIn Radio: Live Sports, News, Music & Podcasts" (tunein.player; 100,000,000 installs), developed by TuneIn Inc	Other
"Words With Friends 2 –Free Word Games & Puzzles" (com.zynga.words3; 10,000,000 installs), developed by Zynga	Other
"Wordscapes" (com.peoplefun.wordcross; 10,000,000 installs), developed by PeopleFun	Other
"Imgur: Find funny GIFs, memes & watch viral videos" (com.imgur.mobile; 10,000,000 installs), developed by Imgur	Other
"Solitaire" (com.mobilityware.solitaire; 100,000,000 installs), developed by MobilityWare	Other
"Cricbuzz - Live Cricket Scores & News" (com.cricbuzz.android; 100,000,000 installs), developed by Cricbuzz.com	Other
"Muslim Pro - Ramadan 2020" (com.bitsmedia.android.muslimpro; 50,000,000 installs), developed by Muslim Pro Limited	Other
"MeetMe: Chat & Meet New People" (com.myyearbook.m; 50,000,000 installs), developed by MeetMe.com	Other
"Slap Kings" (mobi.gameguru.slapkings; 50,000,000 installs), developed by Lion Studios	Other
"FreeCell Solitaire" (com.mobilityware.freecell; 10,000,000 installs), developed by MobilityWare	Other
"theCHIVE" (com.thechive; 5,000,000 installs), developed by Chive Media Group LLC	Other
"Powerful Cleaner (Boost&Clean)" (com.powerful.cleaner; 10,000,000 installs), developed by Powerful cleaner dev	Other
"Lucky Time - Win Your Lucky Day & Real Money" (playgame.realmoney.free.scratchers.win.l...; 500,000 installs), developed by Luckytime App Team	Other
"My Talking Tom Friends" (com.outfit7.mytalkingtomfriends; 1,000,000 installs), developed by Outfit7 Limited	Other
"Happy Wheels" (com.fancyforce.happywheels; 5,000,000 installs), developed by James Bonacci	Other
"WordBit 英語 (自動學習) -繁體" (net.wordbit.entw; 500,000 installs), developed by WordBit	Other
"Sikh World" (com.khushwant.sikhworld; 1,000,000 installs), developed by Khushwant Singh	Other
"Lucky Time - Win Rewards Every Day" (com.luckyapp.winner; 10,000,000 installs), developed by Lucky Lucky Team	Other
"날로영어회화 (단어조합으로문장을만드는트레이닝)" (com.joyquiz.enko; 50,000 installs), developed by None	Other
"Gay guys chat & dating app - GayFriendly.dating" (gayfriendly.gay.dating.app; 100,000 installs), developed by DABLTECH LTD	Other
"Words With Friends –Word Puzzle" (com.zynga.wwf2.free; 10,000,000 installs), developed by Zynga	Other

(Table Continues)

Table 13 (Continued)

App	Category
"Mimi 4chan Reader" (com.emogoth.android.phone.mimi; 1,000,000 installs), developed by Mimi Reader	Other
"iFunny –fresh memes, gifs and videos" (mobi.ifunny; 10,000,000 installs), developed by iFunny Inc.	Other
"WordBit Tiếng Anh" (net.wordbit.envn; 1,000,000 installs), developed by WordBit	Other
"Solitaire" (com.tripledot.solitaire; 1,000,000 installs), developed by Tripledot Studios Limited	Other
"PicsArt Photo Editor: Pic, Video & Collage Maker" (com.picsart.studio; 500,000,000 installs), developed by PicsArt	Other
"Johnny Trigger" (com.time.trigger; 50,000,000 installs), developed by SayGames	Other
"Brain Test: Tricky Puzzles" (com.unicostudio.braintest; 50,000,000 installs), developed by Unico Studio	Other
"Word Stacks" (com.peoplefun.wordstacks; 10,000,000 installs), developed by PeopleFun	Other

A.4 Supersonic / ironSource

Supersonic is a mobile monetization platform that has merged with ironSource. They encrypt their data using 256-bit AES in CBC mode. They use both a fixed key and a fixed initialization vector (IV). The key is the binary string generated by the ASCII representation of `C38FB23A402222A0C17D34A92F971D1F` and the IV is 128 bits of zero.

Figure 29 shows an example transmission. The data itself is encoded in base64, a standard encoding, but when decoded, it is encrypted binary data. Our tools are able to decrypt this data and the resulting transmission is shown in Figure 30. We have truncated the encrypted data and redacted the decrypted data.

```
GET /sdk/v6.10.1?request=hQGt9/zrQgwt08o2NyG... HTTP/1.1
User-Agent: Dalvik/2.1.0 ...
Host: init.supersonicads.com
Connection: Keep-Alive
Accept-Encoding: gzip
```

Figure 29: Example (truncated and redacted) packet transmission from the Galaxy Attack: Alien Shooter (Premium) to SuperSonic Ads (`init.supersonicads.com`). The payload has been truncated to protect identifiable information.

```
platform=android&
applicationKey=85125d9d&
applicationUserId=XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX&
sdkVersion=6.10.1&
pluginType=Unity&
pluginVersion=6.10.1&
plugin_fw_v=2017.4.33f1&
advId=XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX&
appVer=24.6&
osVer=28&
devMake=Google&
devModel=AOSP+on+sargo&
connType=wifi
```

Figure 30: Decrypted redacted payload from the example packet transmission from Galaxy Attack: Alien Shooter (Premium) to SuperSonic Ads (`init.supersonicads.com`). We have highlighted transmissions of the AAID in red. Interestingly, this app is the premium version of the app that charges users to download. The corresponding free version has more than one hundred million installations.

Table 14 lists the 36 apps that communicated with Supersonic's (and now ironSource's) ads domains during the testing period, many of which we observed using this obfuscation technique.

Table 14: Apps that transmitted user information to Supersonic (ironSource) during the testing period.

App	Category
"Sleepa: Relaxing sounds, Sleep" (net.relaxio.sleepo; 1,000,000 installs), developed by Sound Sleep - Relaxing Sounds and White Noise	Health
"Sleep Sounds" (net.metapps.sleepsounds; 5,000,000 installs), developed by Sound Sleep - Relaxing Sounds and White Noise	Health
"Be Closer" (com.becloser; 10,000,000 installs), developed by Agromart Dev	Kids
"Galaxy Attack: Alien Shooter (Premium)" (com.alien.shooter.galaxy.attack.premium; 100,000 installs), developed by ONESOFT	Kids
"Fishdom" (com.playrix.fishdomdd.gplay; 100,000,000 installs), developed by Playrix	Other
"Spider Solitaire" (com.mobilityware.spider; 10,000,000 installs), developed by MobilityWare	Other
"My Talking Tom 2" (com.outfit7.mytalkingtom2; 100,000,000 installs), developed by Outfit7 Limited	Other
"Lightning Link Casino: Free Vegas Slots! 10M Bonus" (com.productmadness.lightninglink; 1,000,000 installs), developed by Product Madness	Other
"Slots: Heart of Vegas™ –Free Slot Casino Games" (com.productmadness.hovmobile; 10,000,000 installs), developed by Product Madness	Other
"Cashman Casino: Vegas Slot Machines! 2M Free!" (com.productmadness.cashmancasino; 5,000,000 installs), developed by Product Madness	Other
"Archero" (com.habby.archero; 10,000,000 installs), developed by Habby	Other
"Solitaire" (com.mobilityware.solitaire; 100,000,000 installs), developed by MobilityWare	Other
"Tellonym: Honest Q&A" (de.tellonym.app; 10,000,000 installs), developed by Callosum Software	Other
"FreeCell Solitaire" (com.mobilityware.freecell; 10,000,000 installs), developed by MobilityWare	Other
"Idle Army Base" (com.neonplay.casualidlearmybase; 5,000,000 installs), developed by Neon Play	Other
"Lucky Time - Win Your Lucky Day & Real Money" (playgame.realmoney.free.scratchers.win.l...; 500,000 installs), developed by Luckytime App Team	Other
"My Talking Tom Friends" (com.outfit7.mytalkingtomfriends; 1,000,000 installs), developed by Outfit7 Limited	Other
"Happy Wheels" (com.fancyforce.happywheels; 5,000,000 installs), developed by James Bonacci	Other
"Slot Machines –Slots of Immortality™ Free Pokies" (com.bi.slots.immortality; 100,000 installs), developed by Bad Ibis Games Ltd	Other
"Lucky Time - Win Rewards Every Day" (com.luckyapp.winner; 10,000,000 installs), developed by Lucky Lucky Team	Other
"TOP SEED Tennis: Sports Management Simulation Game" (com.gaminho.topseedtennis; 1,000,000 installs), developed by Gaminho	Other
"Cash Hunter Casino –Free Vegas Slot Machine" (vegas.slots.cash.hunter.free.bonus.casin...; 10,000 installs), developed by Seven Slots Tech - Free Jackpot Slots Casino	Other
"Spotline" (com.famspotline; 1,000,000 installs), developed by Sociability Apps	Other
"Football Management Ultra 2020 - Manager Game" (com.trophymanager.ultra; 1,000,000 installs), developed by Trophy Games - Football Manager Game Makers	Other
"My Home - Design Dreams" (com.spacegame.homedesign; 50,000,000 installs), developed by Zentertain	Other
"Parkour Race - Freerun Game" (com.parkourrace.game; 10,000,000 installs), developed by Madbox	Other

(Table Continues)

Table 14 (Continued)

App	Category
"Gold Fortune Casino™ - Free Vegas Slots" (triwin.casino.slots.fortune.gold; 1,000,000 installs), developed by TRIWIN	Other
"Sharpen Blade" (com.zplay.blade; 10,000,000 installs), developed by ZPLAY Games	Other
"Solitaire" (com.tripledot.solitaire; 1,000,000 installs), developed by Tripledot Studios Limited	Other
"Tiles Hop: EDM Rush!" (com.amanotes.beathopper; 100,000,000 installs), developed by AMANOTES	Other
"Magic Tiles 3" (com.youmusic.magictiles; 100,000,000 installs), developed by AMANOTES	Other
"Johnny Trigger" (com.time.trigger; 50,000,000 installs), developed by SayGames	Other
"Idle Miner Tycoon: Mine & Money Clicker Management" (com.fluffyfairygames.idleminertycoon; 50,000,000 installs), developed by Kolibri Games	Other
"Brain Test: Tricky Puzzles" (com.unicostudio.braintest; 50,000,000 installs), developed by Unico Studio	Other
"Brain Out –Can you pass it?" (com.mind.quiz.brain.out; 100,000,000 installs), developed by Focus apps	Other
"CodyCross: Crossword Puzzles" (com.fanatee.cody; 50,000,000 installs), developed by Fanatee, Inc.	Other