SCALARR

The Ultimate Guide to App-Install Fraud Types

“This report equips app marketers to make data-informed decisions while assessing the quality of acquired installs”.

scalarr.io

0

Content

1

Introduction

Scalarr is an innovative, ML-based anti-fraud solution that detects all types of mobile app-install fraud with high accuracy by applying both unsupervised and semi-supervised machine learning algorithms.

Working on fraud detection for two years already, Scalarr knows the fraud problem from within, while at the same time, only **44%** of mobile marketers realize this problem. We have clients for whom Scalarr is the first anti-fraud solution they have ever used. So we decided to create “The Definitive Guide to Mobile Fraud Types” with an aim to review all existing types of fraud in detail (both traditional types and new modified ones) and give insights on how to counter this threat.

2

Scalarr's Approach

Scalarr gives a direct evaluation of traffic with accuracy up to 97%.

Fraud patterns are constantly shifting, becoming more complicated and difficult to identify. This cannot be done without an analysis of the numerous metrics and interrelations linking them.
From all the antifraud techniques available on the market, we have chosen machine learning and big data algorithms. Our approach is based on the fact that in fraud detection, machine learning gives more accurate and complete results than manual human and rule-based analyses are able to do. For an even better analysis of traffic, we have implemented two different models of machine learning algorithms: Unsupervised Machine Learning (UML) and Semi-Supervised Machine Learning (SSML). These two algorithms are shaped differently but work perfectly together: UML is self-learning and takes a lead in the detection of new evolving fraud types, while SSML interprets and explains the UML results.
By using these two machine learning algorithms for the analysis, Scalarr gives a direct evaluation of traffic with accuracy of up to **97%**. Aslo, as we are aware that even **1%** of errors could mean a great financial cost to our clients, we are constantly working to further improve our algorithms.

3

Scalarr Fraud Findings

>$4,6 billion

Estimated app-install fraud losses in 2018.

- In 2017 app-install fraud losses were more than $3.6 billion. According to Scalarr's estimate, the financial damage caused by app-install ad fraud could reach $4.6 billion in 2018.

- Annual fraud rate will grow by 20% on average and become the biggest threat to advertising spend over the next 5 years.

- The share of fraudulent installs in mobile apps has increased by 18%, affecting 15% of all marketing-driven installs, according to Scalarr.

- By category the apps, which suffer from fraud the most, are: Mobile Games, eCommerce and Shopping, Travel, Financial, Delivery and other apps with high CPI/CPA rates.

- The most common form of attack now is modified click-spamming. Smart bots have replaced classic bots and device farms and new fraud types have emerged called "mixes" - the mixture of different types of fraud or mixture of real users and app-install fraud. In 2018, the total share of "The New Face of Mobile Fraud" has significantly increased and accounts for 60.5% of all known types of fraud.

Scalarr Fraud Findings

14% of all analysed paid installs are fraudulent

- In 2018 only 15% of all analysed apps had less than 10% fraud, and 38% had over 30% fraudulent installs.

- Mobile apps with high CPI/CPA payout, massive scale, or both is a tidbit for fraudsters in 2018 (and always was).

- A new type of fraud, called Intelligent Device Farms is one of the most inconspicuous and therefore dangerous, very common in the Social Casino category due to high CPI rates.

- Fraudsters are methodologically developing more refined schemes and methods to fake installs. The fastest mimicry occurred in 18 hours.

- Within the same trusted network, you can have campaigns with fraud rates below 3% and other ones above 95%.

- In measuring 150 million analysed installs in the 8 months of 2018, 21,5% of all fraudulent installs were from Smart Bots.

- The majority of developers don't have a specific fraud prevention strategy or policies, which are distinct from their ordinary user acquisition routine.

- Higher-revenue app developers use two or more fraud detection tools to manage mobile fraud, compared with none or just one tool used by lower-revenue app developers.

4

Classic Mobile Fraud Types

By Classic Mobile Fraud types we mean all app install fraud types, which have been attacking mobile marketers for many years. This category includes some primitive types of fraud along with more complex and hard to identify techniques.

Currently, we include five different types of fraud in this category:

1. Classic Click Spam
2. Click Injection
3. Bots
4. Device Farms
5. Incentive Traffic

4.1

Classic Click Spam

Description

In the case of click spam, fraudsters send a huge number of clicks (in different ways) aiming to deliver the last-click prior to the organic installs and ‘steal’ them.

About 100 billion apps were downloaded on both Android and iOS platforms in 2017. Additionally, by Scalarr’s estimates, 20 billion installs have passed through mobile tracking providers. In other words, non-organic installs (ads, cross-promo, paid search) were accounting for 20 billion installs in 2017. So 80% of installs in the ecosystem are organic. Generally, organic users are highly motivated to use a downloaded mobile product and this makes them a greater target for attribution fraudsters, in particular classic click spammers.

In the case of click spam, fraudsters send a huge number of clicks (in different ways) aiming to deliver the last-click prior to the organic installs and ‘steal’ them. Thus, the installs that were generated organically are assigned to the fraudster with the ‘last action’ (click / view before opening the app). Thus, the fraudster receives payment for the ‘provided’ installs.

In some cases, installs can also be “stolen” from other publishers. But in most cases, fraudsters steal organic installs from their developers.

How it works

Click spam has a variety of different subtypes that are often mistakenly isolated in certain types of fraud, such as pixel stuffing, ad stacking, cookie-stuffing, auto redirects. In fact, these subtypes are just the methods of delivering fraud. In Scalarr's terminology we use a combined term "classic click spam".

The logic of click-spam is always the same:

1."Infection" of as many mobile devices as possible by clicking on sponsored links for as many apps and games as possible. These are clicks which the users did not want to perform of their own free will;

2. Processing as many advertising tracking links as possible on every device (hundreds and thousands of mobile apps and games that currently perform a paid user acquisition campaign in a particular GEO);

3. Maintaining the relevance of tracking links within the attribution window (regularity of clicking on promotional tracking links in order to get into the target attribution window);

4. Creation of a fluent system, working on finding and sending the fraudster-caught installs to clients (almost in real-time).

All this is done to "catch" the organic installs made by these infected users and attributing it to themselves.

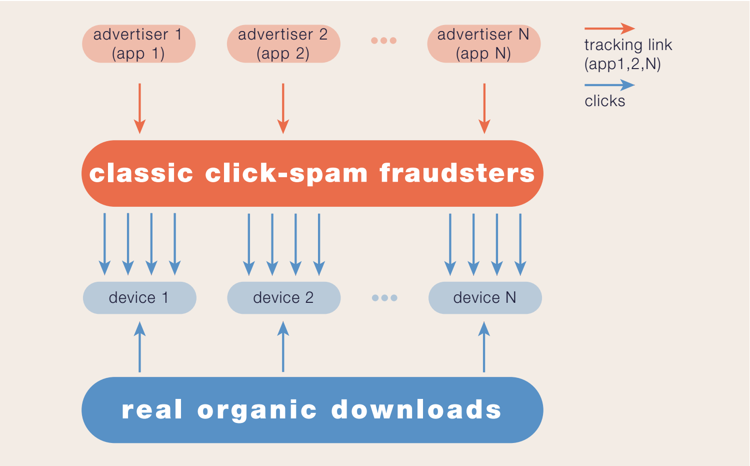
The "click-spam subtypes" may be different:

- **Auto Redirects** are one of the earliest known types of attribution fraud when a user is forcibly redirected through promotional tracking links to the page of the app store. In this way, it's difficult to proceed with a large amount of links and the user sees that he's being forwarded to the page of the app/game he aimed to download initially, although at the same time he hasn't clicked on the advertisement of this particular app/game. This method is still used by fraudsters, despite being obsolete.

- In the event of **Ad Stacking** a lot of advertisements are hidden behind the front ad so that they cannot be seen by the user. By clicking on the front banner/video the user is literally clicking on all other background ads.

- **Pixel/Click Stuffing** - is a processing of advertising links in the background when they are placed in an invisible pixel. Inside this pixel, the fraudster can process a significant amount of ad links, remaining completely unseen for the user. For example, in the mobile web it usually happens while watching a video. For in-app inventory, click-spam fraudsters can generate background clicks from already installed and infected apps (such as battery savers, different cleaners and so on).

There are also other mechanisms and ways to implement click-spam fraud. As with any other kind of mobile ad fraud, it is constantly changing in order to remain unseen for as long as possible.



Signs you are at risk

The more popular the app/game, the higher it is in the popularity charts, the more coverage for different GEOs - the more attractive it is for click-spam fraudsters. Since the most popular mobile products have a huge amount of organic installs, the chances of "successful catching" for fraudsters are higher. It is also important to note that iOS apps are more prone to the risk of classic click spam, as the number of iOS devices is less, and, therefore, the statistical probability for fraudsters to take an organic install from an iOS device is higher. Click-spam is inherently organic, so all financial indicators, post-install events, other attributes of the device and install will be absolutely real. From this side, it is impossible to identify such type of fraud.

Click-spam is inherently organic, so all financial indicators, post-install events, other attributes of the device and install - will be absolutely real.

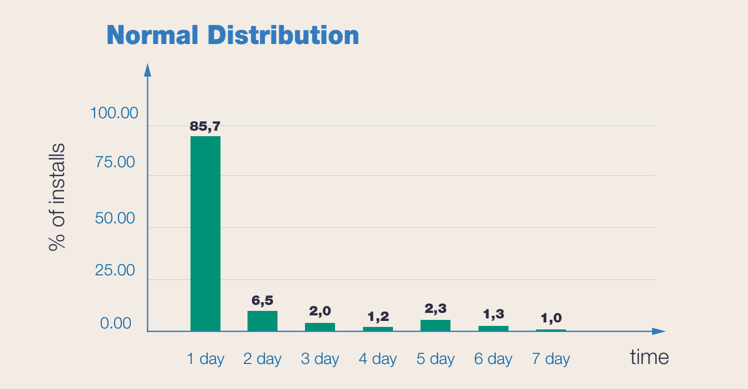
So what can indicate the possible presence of click-spam?

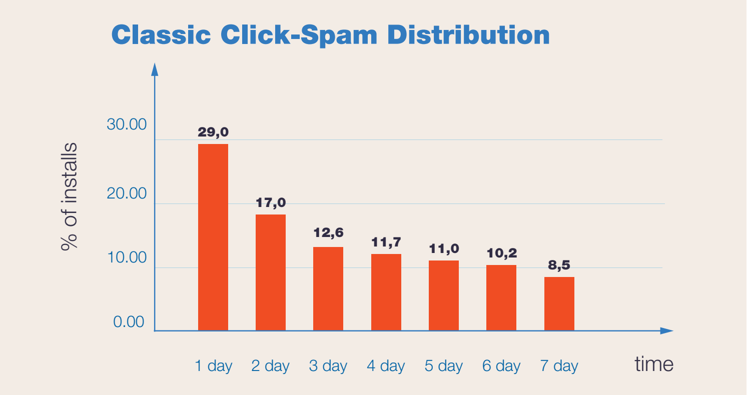
1. A large number of clicks in relation to installs (CR<0.5%).

But be careful, there may be some exceptions: some kinds of redirect traffic for mass, utility apps, casual games or small-format banners can have a similar level of CR, but it does NOT mean click-spam. Also, click-spam fraudsters actively use mix-technics (more on this in the “Mixes” chapter). In this way, CR can artificially rise to a normal level.

2. An abnormal TTI (time to install) distribution.

The fact is click-spammers can only manage clicks, but they can't influence the user when he/she downloads (organically) an app. Therefore, this type of fraudster can be uncovered by looking at the TTI distribution by days. In non-fraudulent traffic, most of the installs of the whole cohort arrive on the first day after the click. But classic click-spam has a "long tail" in the TTI distribution by days. But, as always, there are some exceptions: the absence of such a tail in the TTI distribution by days does not mean that there is no click-spam. Also, the natural distortion of TTI distribution can be affected by different attribution windows for various sources, the presence of pre-install campaigns, different proportions of attribution actions.





How to deal with Classic Click Spam

As with any other fraud type, there are many patterns and thousands of data points and features - so there is no single approach to the identification of click spam, but we recommend paying particular attention to:

1. The number of organic users coming from the app (to understand the general health of an app);

2. The TTI distribution modeling.

For achieving maximum accuracy and completeness in decision-making regarding fraud you need to take into account all data points and its multivariate relationships.

Thus, for achieving maximum accuracy and completeness in decision-making regarding fraud you need to take into account all data points and their multivariate relationships. It is important to note that fraud patterns are not rules that can be prescribed in the format "if x = y, then this is a fraud". By itself, without including other hundreds and thousands of parameters, the pattern is not sufficient for the binary identification of app install ad fraud. In addition, the manual review of such distributions for each bundle (there may be thousands of such bundles every 3-4 days) is an extremely time-consuming process, which does not result in a single "fraud/non-fraud" answer.

To fight click spam accurately and completely we recommend using Scalarr as the main anti-fraud solution.

4.2

Click injection

Description

The given type of fraud, like classic click-spam, is related to the class of “attribution fraud”. Click injection fraudsters also aim to steal organic installs and traffic from non-fraudulent publishers. Click-injection has quite a complex technological base and requires significant resources. In most cases, this type of fraud is found as part of the work of big teams, who are engaged in making real mobile apps with an embedded malware virus, through which the infection directly occurs. In order to have a significant volume of installs, fraudsters have to massively spread their app with an embedded malware virus, and it should be installed in hundreds of thousands or even millions of users’ devices.

In most cases, this type of fraud is found as part of the work of big teams, who are engaged in making real mobile apps with an embedded malware virus, through which the infection directly occurs.

For such a significant effect, they use two strategies:

1. Promotion of their own “infected” app;

2. Collusion with already existing mass apps.

Unfortunately, the second option is also very common in the mobile ecosystem. The mass apps include different casual apps, card games, utilities, battery savers, flashlights, etc., which have, at least, a million user base. Usually, their business model is based on advertising monetization, but the ad revenue is limited and often not very high. At the same time, such apps usually spend a lot of money on user acquisition at the early stages of their life cycle. Considering quite decent budget injections in the app promotion and limited earnings further along the road, a lot of developers pass on the “dark side” with the aim to earn extra money on click injection.

How it works

Click Injection can be found only on the Android platform since it uses technical features particular to Android.

This type of fraud can be found only on the Android platform since it uses technical features particular to Android. Click-injection fraudsters integrate a malware virus in the code of their fraud app. In most of the cases, such fraud apps include mass, popular and simple apps / games. Such apps may have already been installed on the user’s device and the malware virus could appear there with a regular update or the user could have installed this app with the virus already existing inside. Finally, if the user’s device is already infected with the fraudster's application, all subsequent installs can be assigned to the fraudsters. The mechanism of this form of fraud is as follows:

1. A malware virus in the app gains access to a variety of installs of the device;

2. After this, the malware virus checks whether there is a mobile app/game which is carrying paid user acquisition campaigns at the moment;

3. If the downloading app/game (organically or through the activity of a non-fraud publisher) is on this list, the fraudster can assign this install to himself;

4. While the installation process is underway, the fraudster generates a synthetic click from this device. This is can be a click from any publisher to whom the click-injection fraudster is connected and who has this app in the list of advertised offers;

5. As a result, when the app would be downloaded and opened, the tracking analytics would attribute the "organic" install directly to the fraudster.

In their basic form, both classic click spam and click-injection have one essence, but a multi-vector orientation:

- Classic click spam infects devices with links to those apps that carry out a paid user acquisition. Then, when such apps are installed - "steals them by itself";

- Click-injection infects a device with the malware virus that checks all new installs on this device. Later, after the installation of those apps that carry out a paid user acquisition, the fraudster steals these installs.

Signs you are at risk

The more popular your product and the more actively you buy traffic - the more likely the threat of click-injection for your app.

The fraud signs are very similar to classic click-spam: the more popular your product and the more actively you buy traffic - the more likely is the threat of click-injection to be carried out against your app. At the same time, the high risk group includes not only countries with high CPI, but also all other GEOs without exception.

So what indicates the possible presence of click injection?

- An abnormal time between a download click and an install;

- Fraudsters usually run their click instantly after the completed download.

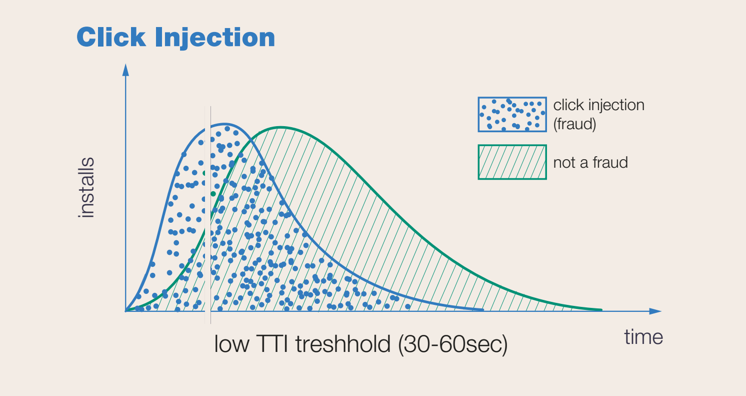
How to deal with Click Injection

Last year (2017) one of the main patterns, discussed by most antifraud solutions - the search of installs with a very short TTI (time to install). For example, a TTI up to 30 sec.

Indeed, the mechanics of click-injection assumes that the real click time shifts forward (prior to downloading the app). Accordingly, the final TTI greatly reduces.

The automatic reject of installs with a fast TTI has low accuracy since alongside possible click-injection false-positive decisions can be made, leading to rejection of non-fraudulent installs. Up to 7-10% of traffic can be rejected by mistake.

Some of the traditional fraud detection tools suggest to fight click-injection, is the automatic reject of installs with a fast TTI. But this approach has low accuracy since alongside possible click-injection the false-positive decisions can be made, leading to rejection of non-fraudulent installs: included in the “small TTI” cluster can be found genuine



examples with retargeting effect, reinstalls with old ID on a new device, influencer campaigns or simple bags in calculating of the TTI by tracking-analytics. Based on that, up to 7-10% of traffic can be rejected by mistake.

Up to 40-50% of Click Injection have the TTI with more than 30 seconds.

But more interesting is the fact that up to 40-50% of click injections have a TTI with more than 30 seconds as the user behavior model does not always assume the opening of apps/ games just after completing install. Scalarr's ML algorithms use different approaches to clusterization, thus identifying practically all occurrences of click-injection.

At the end of 2017, Google introduced a few additional time parameters that can be passed on to the tracking providers:

- The transition time to the app store (following the click);
- The installation start time;
- The time of the install's completion (but without opening).

Now, knowing these parameters, it is much easier to identify click-injection on each conversion. Nevertheless, at the time of writing not all tracking providers (tracking analytics) have implemented the transfer of these parameters. Also worth noting is that these additional tracking options from Google Play are not a panacea. Without much detail and a complex analysis, a lot of false-positive conclusions can be drawn. For example, you can make a decision about click-injection, mistakenly confusing it with multi-touch attribution effects.

In 2018, almost all click-injection fraud comes exactly in the form of Mixes (more on this in the chapter “Mixes”).

4.3

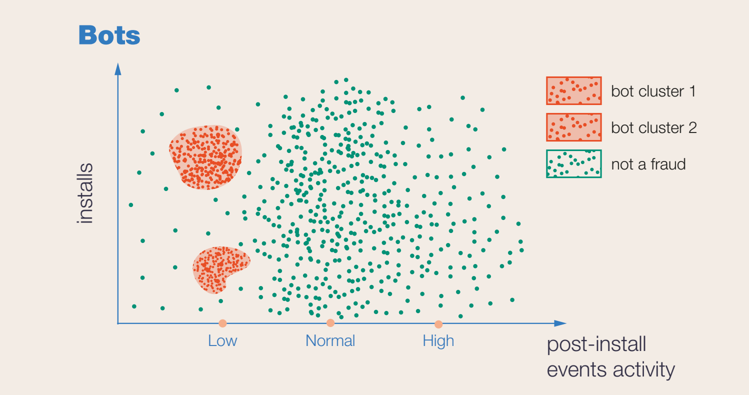
Bots

Description

Bots were one of the first types of app-install ad fraud.

By “bots”, we mean a type of fraud, when the app is not installed on the physical device but the install is “emulated” by software. In this case, the fraudster sends the information about the install, event or even transaction to tracking provider, but it is only a “virtual” install, event or transaction. That’s why bots are often called “emulators”.

This type of fraud was one of the first among app-install fraud and has undergone significant changes during the growth of the mobile ecosystem, becoming more similar to real users.



How it works

The fraudsters create a device with artificial parameters, then emulate an install from the app store or even from the memory cache that is already loaded and get paid for this emulation. By using different types of emulation software, the fraudsters create a device with artificial parameters: device name, advertiser ID, OS version etc. and make the install with it that pops up in reports of tracking analytics.

The biggest part of bots has transformed to a new type of "sophisticated bots".

In the very beginning, such type of fraud was very primitive because it emulated the install only. Later, the "retention rate era" has come with retention being the main KPI in traffic quality evaluation for advertisers. And bots have started to fake the openings in order to manipulate retention rates as well.

Nowadays, the majority of bot fraud has transformed into a new type of "sophisticated bots", which are already faking not only openings but also the post-install events and even purchases. Below are more details on this new type of fraud.

Signs you are at risk

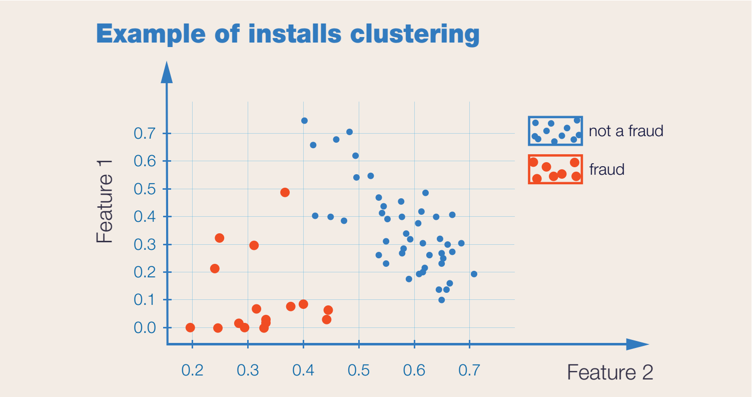
The common rule of the user acquisition market says the following: if you buy traffic for significantly lower than average market prices - it is very likely that such offers will be attractive for the most "primitive" bots. The higher your CPI bid - the more sophisticated bots are aimed at your app/game.

Any significant anomalies in post-install activity may indicate a possible bot-fraud, but not every such anomaly is an unambiguous interpretation of fraud.

How to deal with bots

The most simple bots are easy to identify. Usually, these clusters are disclosed by the absence of any post-install activity, or by the most primitive ways of faking the app openings (for overstating the retention rate). But, in practice it is not so obvious: in the case of facing advanced bots it becomes problematic to identify them with high reliability. This is because in the scripts of their behavior, there is a constant replication of real user behavior. Also, it is quite difficult for manual searches or rules-based engines to distinguish bot fraud in case of mixes with other clusters. In this instance, there are no obvious anomalies at the level of the entire analyzed cohort (for example: app-publisher - sub-publisher - sub-sub-publisher -campaign).

Simple Bots are disclosed by the absence of any post-install activity, or by the most primitive ways of faking the app openings.

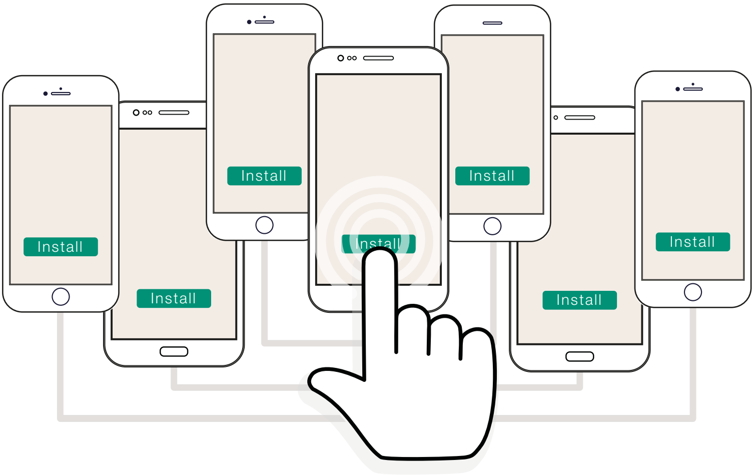

Example of installs clustering

4.4

Device Farms

Description

Device farms also belong to one of the most “ancient” types of fraud. Partially they were used for incentive campaigns, but very soon fraudsters switched their attention to non-incentive campaigns. The most popular visual description of device farms is the photo of a woman sitting in front of a large vertical board with dozens of mobile phones and manipulating with clicks.



How it works

A device farm can have up to several thousand devices.

More often, Android devices were used for such farms, due to their low price, easier "hacking" for changing advertising identifiers and a wider choice of phone models for the farm. Additionally, Android devices may be used in so-called “hybrid farms” - when fraudsters do not use a whole phone but only a phone motherboard. Such a board is much cheaper than a whole smartphone, which allows fraudsters to increase their efficiency. The rest of the actions on the device motherboard are faked with the help of emulation software. Downloads of apps into the device farm are mostly performed through the cache server to save on the pay for Internet traffic. At the same time, downloads directly from the app store are also very common. iOS device farms also exist, but in much smaller volumes: the diversity of iOS devices is smaller, the price is higher.

The first step for device farm fraudsters is to connect to different publishers for constant monitoring of all available apps/games, which are looking for paid traffic sources. Then they clarify the expected KPI for assessing traffic quality.

Most metrics and rules from anti-fraud solutions are usually open and therefore may be reverse-engineered by fraudsters. Finally, a device farm operator gets the parameters: how to download, what post-install events should take place within the next few days and when exactly each should be done. In more technically advanced device farms the work of operators is automated by “matrices”, that can project taps on the display simultaneously to a couple of devices.

Signs you are at risk

Device farms do not have a common pattern of behavior, so each fraud farm operates according to its own scripts and algorithms. But the central line of their behavior is the ambition to look like real users.

The time has passed when device farms were focused only on the volumes of fraudulent installs. With the growing awareness of market participants, the technical development of tracking providers and the growth in the protection level of antifraud services, simple app install scripts no longer work.

The device farms can fake the post-install events up to 14 and even 30 days.

The farms, just like the bots, are trying to fake the post-install events up to 14 and even 30 days. Therefore, the algorithms and concepts of the most complete and precise identification of such type of fraud should be grounded on a detailed analysis of data points in post-install events. And, at the same time, some of the most obvious and primitive device farms can be disclosed by:

1. Numerous installs from one phone model;

2. Numerous installs from several identical IP addresses.

How to deal with Device Farms

Fraudsters, including device farms, are always trying to re-work antifraud services in order to stay undetected for as long as possible. Some time ago, one of the antifraud solutions publicly introduced a new metric for bot and device farm identification: the percentage of new devices, that weren’t previously identified by this antifraud solution among other apps/games. This metric marks any cohort with 80-90% of new devices as “bots/device farms” (while 15-20% of new devices is considered as normal). And just two weeks later, online forums popular with app developers and advertisers became full of questions like “Why does my app have abnormal peaks of organic installs without any post-install activity afterward?”. Nobody knew the exact answer at that time.

But one of the versions was a reverse-engineered version of a “% of new devices” metric made by fraudsters. It was enough for them just to download some more apps organically before downloading the target app, and this fraudulent device no longer had been displayed as "new" and already had a history of app downloads. So this metric has lost its accuracy in fraud identification.

It is enough for fraudsters just to download some more apps organically before downloading the target app, and this fraudulent device no longer displays as "new".

As a conclusion from the example above, we can emphasize once more that fraud patterns are dynamic and change at a fast pace. It is still possible to identify the most obsolete and primitive device farms on the basis of many installs from one or more devices and taking in to consideration the lack of post-install activity. But all these patterns have been well-known to fraudsters for a long time already and more complex modifications require much more effort, data, and technology.

4.5

Incentive

Description

To fully describe this type of fraud, it is necessary to make a few clarifications in order to understand when the incentive is really a fraud:

- For incentive campaigns (CPE) - an incentive install is not a fraud, since in this case the advertiser is interested in this specific type of traffic;

- For non-incentive campaigns - an incentive install is the obvious sign of fraud activity.

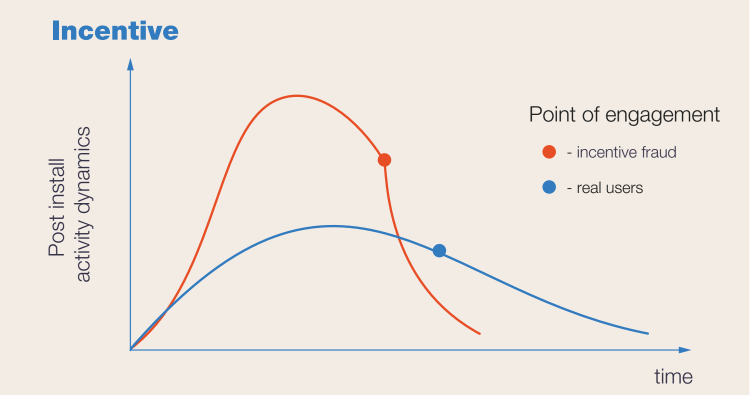
The attempts to present an incentive install as a non-incentive one were also one of the very first types of fraud. But if back then it was a very primitive incentive (only install), now knowing the mechanisms of the user's progress, fraudsters can reproduce patterns, which are very similar to real users' behavior.

In Scalarr's classification, the incentive fraud means the amount of installs that come from independent users who receive a reward in various forms for the install taking place. Device farms do not belong to incentive fraud.

How it works

The mechanics of the incentive are simple: the user (private person) is offered a reward for the download and further progress actions in the mobile app/game. Options for getting a reward may be different: receiving soft currency in another app/game (via offer wall); receiving money via a mobile phone account; receiving money via a personal bank account; other types of rewards.

After completing a specific task ("download", "registration", "reached N level", "purchase on X $", "use of the app during Y days"), the user receives a reward. But the most users will no longer interact with the advertiser’s product.



Signs you are at risk

A more primitive incentive fraud is characterized by the high leaps of CR and abnormal patterns in post-install events.

How to deal with Device Farms

The high CR and its increases are masked by "dilution" of clicks, therefore this method can work on very primitive forms of incentive fraud. Since such installs come from real decentralized devices, they do not differ in any way from real installs and cannot be identified using the "device data points" (IP, SDK, OS version, etc.). The most complete way to protect against this kind of fraud is a comprehensive analysis of post-install activity, since fraudsters can't ideally "fake" the behavior of real users in all aspects.

5

The New Face of Mobile Fraud

In contrary to Classic Mobile Fraud Types, the category reviewed below comprises the relatively new and most progressive techniques of mobile app fraudsters.

It includes **Modified Click Spam**, which is more heavily disguised than Classic Click Spam due to advanced manipulation with TTI (time to install), **Smart/Sophisticated Bots** and **Intelligent Device Farms** that can fully emulate user behavior and even make payments inside the app and suchlike. This year, we have also seen a significant growth of **“Mixes”** and so-called **Soft Fraud**, two of the most insidious types of fraud these days.

5.1

Modified Click Spam

Description

Click-spam fraudsters have quickly noticed that antifraud solutions identify them through an abnormal TTI distribution by days.

A "long tail" with the TTI of 2,3,4 days was clearly pointing at click-spammers. And they have modified their tactics to "cut off" the long tail, leaving visible one day installs only.

When click spammers receive the information or precise metrics in the form of guides or reject reports, they use them to modify the algorithm: they have started to simply "cut off" the long tail, leaving one day installs only, thereby hoping in this way to be much less visible. In Scalarr we call this new type of fraud a Modified Click Spam.

How it works

Using various techniques, modified click-spam fraudsters try to limit the TTI of their traffic to up to 1 day. It works due to:

- Self-substitution of the attribution window for up to 1 day;

- Constant update of clicks from infected users, so that the "click" remains for as long as possible with a "fresh time".

Modified click-spam can also use new ways to "infect" users. For example, through the wi-fi access points in public places. In this case, users click on the elements of the UI start page, and all subsequent organic devices automatically reach click-spammers. Thus, fraud becomes more difficult to identify.

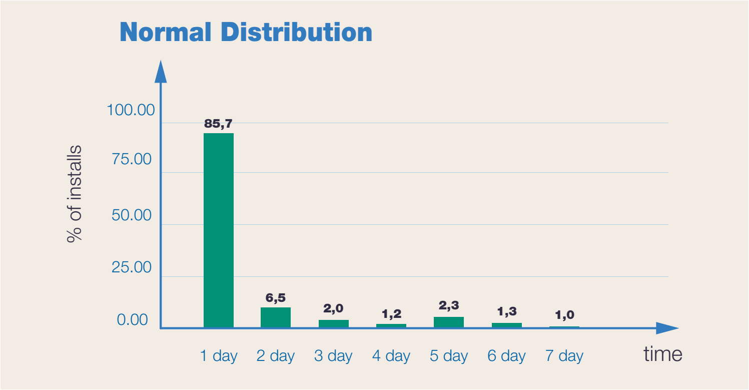
Signs you are at risk

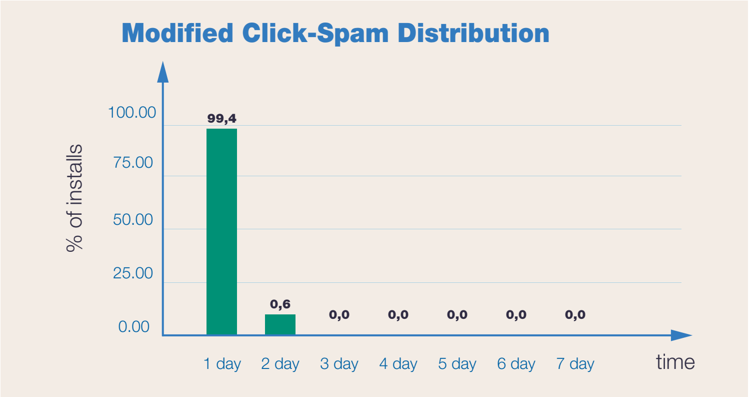
Similar to classic click-spam, Modified Click-Spam is inherently organic, so all financial indicators, post-install events, other attributes of the device and install will be absolutely real.

Signs that you may be at risk are:

1. A large number of clicks in relation to installs (CR < 0.5%);

2. An abnormal TTI (time to install) distribution.





How to deal with Modified Click-Spam

You should pay attention to the TTI distribution by the hour. For modified click-spam, the distribution will be flatter.

In addition to other methods identical for both modified and classic click-spam, you should pay attention to the TTI distribution by the hour. For modified click-spam, the distribution will be flatter. The reason is that, although click-spammers can manage the attribution window with clicks, they can't make the user download an app/game organically.

Modifications of click-spam fraud evolve simultaneously with the disclosure of rules/heuristics by anti-fraud services and with reverse-engineering of these opened rules from the fraudster's side.While modifying their algorithms consistently, the fraudsters stay invisible for the automated rules-based analysis, but ML-based antifraud solutions are capable of identifying all these changes immediately.

5.2

Smart / Sophisticated Bots

Description

Sophisticated bots can fully emulate the user behavior with high accuracy by performing all in-app activities for up to 30 days.

Compared with simple bots smart ones fully emulate user behavior by performing all post-install activities for a long time. From a human perspective they are almost like real users having a personal IP, device ID, etc. Smart bots are an advanced type of fraud and hardly detectable.

Fraudsters are much better prepared for the "attack": they find out all the post-install events and KPIs of the advertiser.

How it works

The basic mechanics are similar to classic bot fraud, but in this case, fraudsters are much better prepared for the "attack":

1. They find out all the post-install events and KPIs of the advertiser;

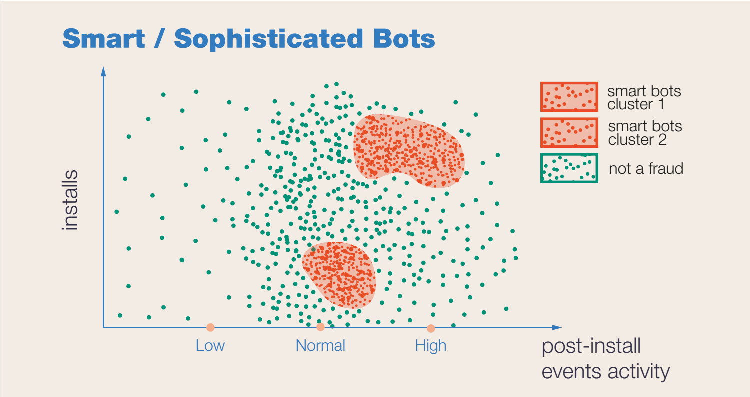
2. They configure the emulation of financial events (in some cases, it can be real payments);

3. They actualize the SDK version of the app/game from the store;

4. They make a realistic TTI for this product;

5. They divide the traffic volume into various smaller sub-publishers and emulate different GEOs.

After the first test attack, fraudsters measure the advertiser's reaction. If sophisticated bots get approved, then they begin to increase the volumes. A common strategy is that in the next stage fraudsters look for other publishers who have access to the advertiser's campaigns. After, fraudsters are reaching out to publishers with the approximate following message: "We have a high-quality traffic for this app, here are skins with our volumes. Let's work together". If the attack has not been identified, then smart bots start to scale, giving even more fake installs, which look like they are coming from real users.



Signs you are at risk

Most often sophisticated bots are almost invisible from identification by a simple "human analysis", as their fraud patterns are hidden in a large number of data-points.

It is also obvious that smart bots are aimed at user acquisition campaigns with a high CPI, since a low CPI is not profitable for them. Thus, the higher your CPI, the higher the probability of attack by smart bots.

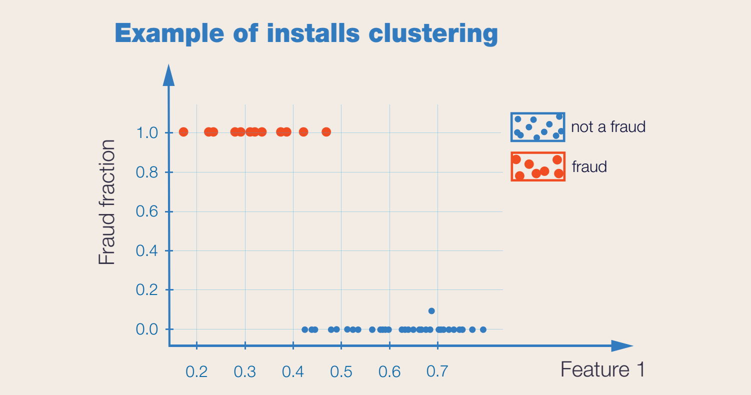
How to deal with Sophisticated Bots

Sophisticated Bots are one of the most dynamic app-install ad fraud types which use constant reverse engineering.

There are no universal recommendations for protection from sophisticated bots.

Firstly, this type of fraud is one of the most dynamic, using constant reverse engineering. Secondly, each app/game is different from the others by using different personalized custom post-install events. And finally, the fraudulent strategies and patterns are also unique and very different from each other.

The basic recommendation here is the same - detailed analysis of post-install events.



5.3

Mixed Fraud

Description

Mixed fraud is a totally new and very dangerous type of fraud, as here we can observe different types of fraud, as well as real users mixed within one sub-publisher, e.g. real users and fraudulent 'fake' installs, or real users and different types of fraud, such as attribution fraud and bots.

Mixed fraud represents different kinds of fraud mixed in one indivisible bundle.

Mixed fraud concentrates a big threat to advertisers, since almost all anti-fraud solutions and self-search for fraud include the analysis of the cohort within the undivided bundle to the maximum detail. An example of such a bundle: app - publisher - sub-publisher - sub-sub-publisher - campaign. And all the metrics, the rules for almost all anti-fraud solutions are available only at this level of detail. In the case of mixed fraud within the bundle, there are different ways it is realized:

- One type of fraudulent and non-fraudulent traffic;
- Several types of fraudulent traffic;
- Several types of fraudulent and non-fraudulent traffic.

How it works

The mixing options:

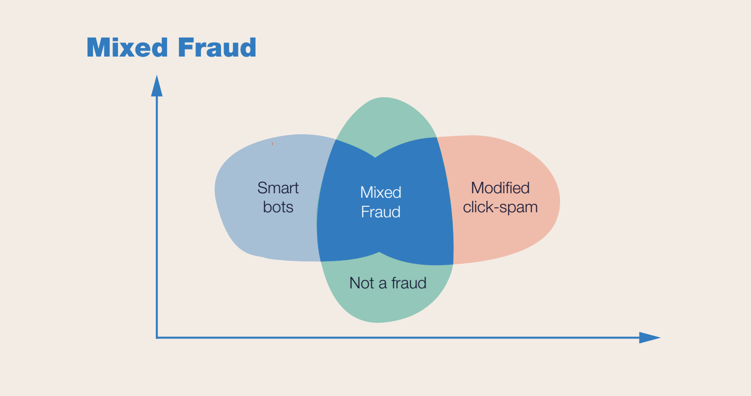
1. The conscious use of several different types of fraud to get over the known protection measures of anti-fraud services;

2. A chaotic mixture of different types of fraud in the case of connecting to the publisher with an uncontrolled number of re-brokering levels.

As a result, different types of traffic are mixed in one indivisible bundle, making common metrics and patterns inefficient in this case. Both variants of mixed fraud are extremely dangerous. In the first variant the fraudster deliberately combines different types and patterns of fraud, knowing exactly what common metric to fake. Then in the second case, mixing takes place in a random uncontrolled stream. A considerable effort is required to cluster and isolate the homogeneous fraud clusters.

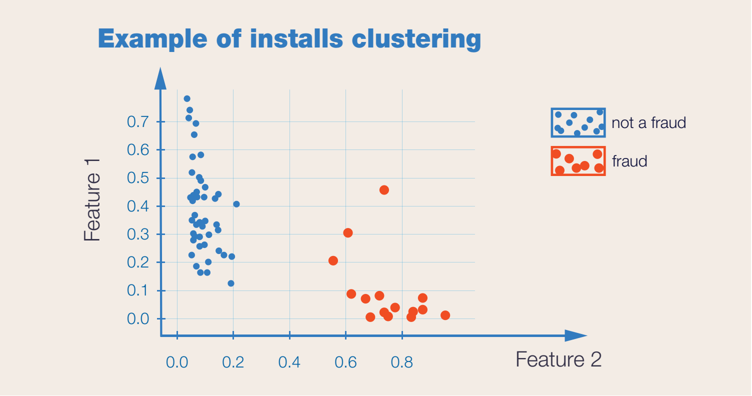
Signs you are at risk

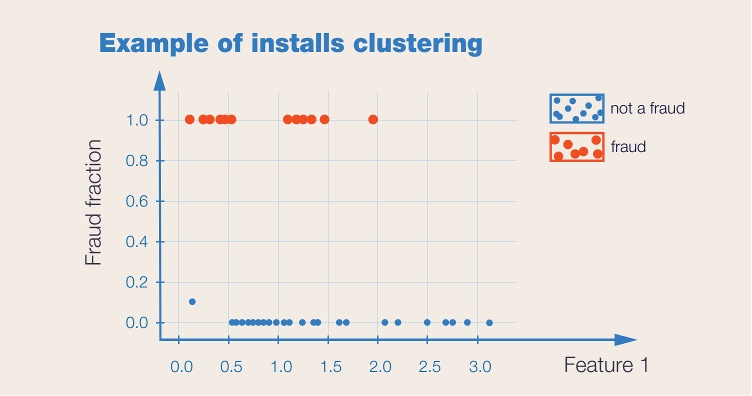
This type of fraud is hardly detectable and there are no obvious patterns that could be visually recognized. In most cases, the maximum that you can see is "the general KPI for traffic is slightly below the target". But this can't be sufficient reason to stop the cohort.



How to deal with Mixed Fraud

In the case of mixed fraud, the only effective protection measure is clustering technologies, when the ML algorithm can fully isolate the individual fraudulent clusters inside the indivisible bundle and clearly recognize the fraudulent and the non-fraudulent traffic, as well as the various types of fraud within.





5.4

Soft Fraud / Organic Stealing

Description

A fairly new kind of fraud, usually seen among the "trusted video ad networks." It comes out of publishers that are dragging a part of the advertiser's organic traffic to themselves, manipulating ways of install attribution (display/click).

How it works

Under standard conditions, there are 2 types of attribution on the market: display and click.
The standard window of attribution for them: display - 1 day, click - 7 days.
For advertising video networks, the advertiser generates two tracking links - for attribution of impressions and clicks.
The publisher intentionally attaches a click-tracking link to both impressions and clicks, thereby increasing the attribution window for impressions from one day to one week.
Then, a part of the organic installs goes to this publisher.
Thus, he reduces the average CPI of his channel and increases the chances of growing budgets in the future.

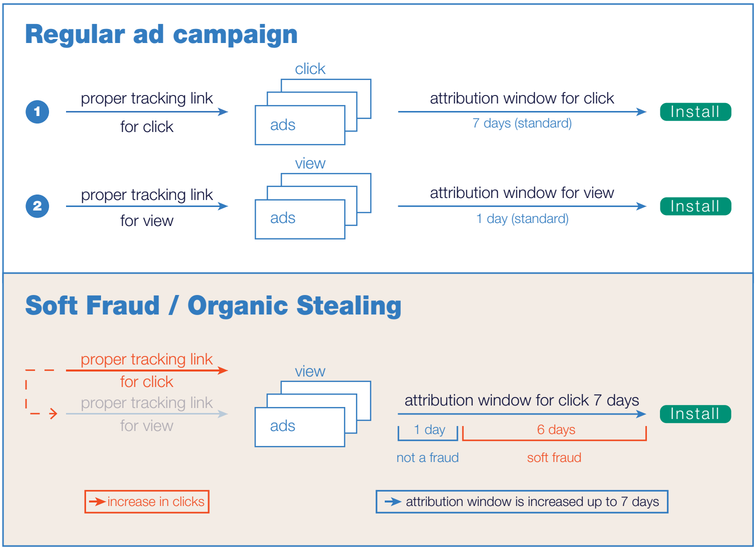
Signs you are at risk:

One of the hallmarks of soft fraud can be a sharp increase of view through attribution (VTA) that is attribution by impression. As a rule, this share is stable enough, although it can differ between traffic channels (publishers).

Fraudsters are using the link for click attribution instead of using the link for view attribution. As a result, they increase the share of VTA within provided traffic.

How to deal with Soft Fraud

One of the indicators of this type of fraud is an extremely high share of impression-attributions. At the same time, it is quite difficult to identify which ones are soft fraud, and which ones are the real impressions through attribution.

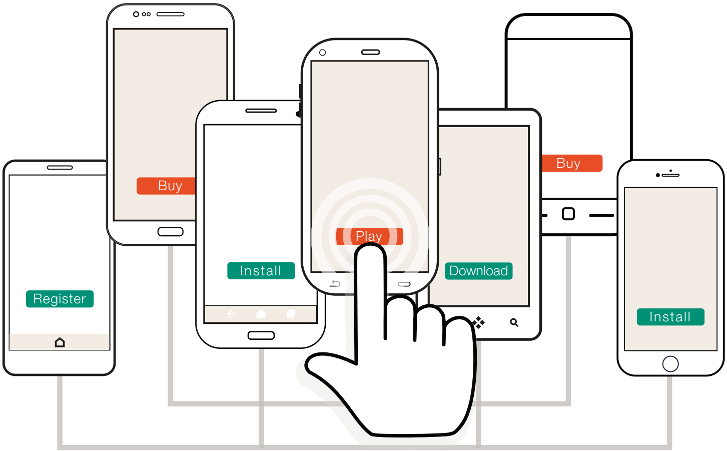


5.5

Intelligent Device Farms

Description

This type of fraud is one of the newest in the industry, and the data of an Intelligent Device Farm is significantly different from classic device farms. Fraudsters here can almost perfectly fake post-install activity, engagement, even payments. And although at the moment, it cannot be called the most widespread type by the volume of fraudulent installations, the potential risk is very large. Because Intelligent Device Farms are trying to "connect" to apps and games with the highest CPI on the market, this type of fraud very often goes undetected for a long time.

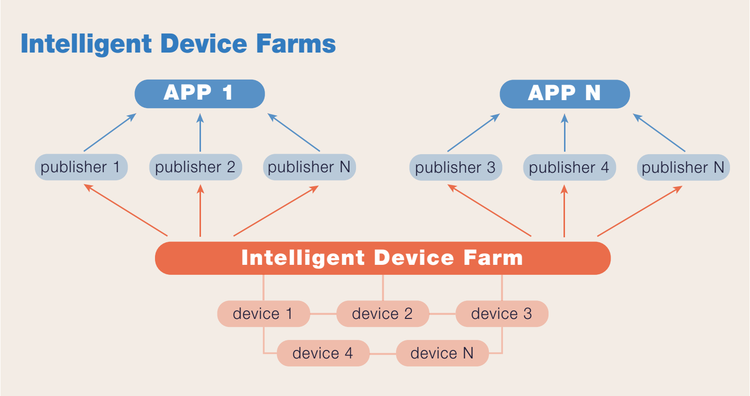


How it works

Intelligent Device Farms have a wide variety of devices and other attributes and can emulate the real user's behavior for 14 days or even more. One of its tactics is to connect simultaneously to many publishers (including conditional trusts) and split their volume into many small clusters.

Signs you are at risk

It is quite difficult to identify this type of fraud internally for the above reasons.
For full protection from Intelligent Device Farms, we highly recommend to use Scalarr as the primary anti-fraud solution.



How to deal with Intelligent Device Farms

ML algorithm uses the technology which analyzes unstructured data from all publishers together. By processing the entire stream of billions of data points, it can cluster the Intelligent Device Farms at a higher level of analysis. Only this technology makes this identification possible.

6

Final Thoughts & Recommendations

We've described 10 different types of fraud in this report. And it covers only the basics, as various fraudulent subtypes make the fraud an even more massive and omnipresent threat.

The biggest challenge mobile advertisers need to face is that the mobile app install fraud has revolutionized itself within the past year and become hardly detectable, as well as new smarter types erased.

With such a spread of app install fraud it is not possible to mark any ad network as absolutely trustworthy. However, even now, in 2018, a significant proportion of companies do not treat the fraud issue properly, which leads to losses, which they cannot even begin to imagine.

But even more problematic is that not all protective measures have the same level of efficiency. The traditional manual human analysis or rules-based engines (rules sets) no longer meet the expectations of the current market. At the moment, only the advanced technologies

By the end of 2018, app install ad fraud could cause losses of $4.6B out of the total advertising market worth $21.5B.

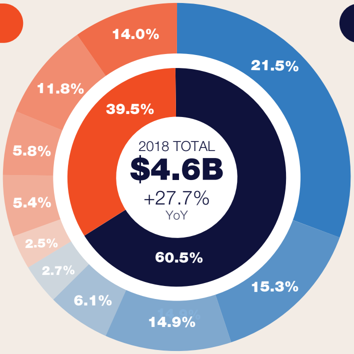
are able to analyze the hundreds of parameters simultaneously and get to the level, which is not available or understandable to humans.

And remember, the worst thing you can do is ignore the problem or do nothing about it. The effectiveness of your advertising campaigns depends on your decision. Choose wisely!

2018 GLOBAL APP-INSTALL AD FRAUD MARKET

CLASSIC MOBILE FRAUD TYPES

- Bots 14.0%
- Click Injection 11.8%
- Device Farms 5.8%
- Classic Click Spam 5.4%
- Incentive 2.5%



THE NEW FACE OF MOBILE FRAUD

- Smart Bots 21.5%
- Mixed Fraud 15.3%
- Modified Click Spam 14.9%
- Intelligent Device Farms 6.1%
- Soft Fraud 2.7%

In 2018, app install ad fraud could cause losses of **$4.6B** or **21.4%** of the total app-install ad market

SCALARR

To find out more about how you can stop mobile ad fraud, please contact us:

www.scalarr.io
hello@scalarr.io

2018
STEVIE®
BRONZE
WINNER
INTERNATIONAL
BUSINESS AWARDS