secure D

Powered by upstream

THE INVISIBLE DIGITAL THREAT

Hijacked devices, depleted data, unwanted charges
& stolen personal info affecting billions of mobile users

MOBILE AD FRAUD
2019 REPORT

Contents

Executive Summary

Mobile ad fraud affects billions of people across the world. The adverse effects from this criminal enterprise are felt by consumers, mobile operators, advertisers and even app publishers. And yet, it is usually not at the top of many people's list of digital threats and can often go undetected. It is an invisible epidemic.

This report exposes the workings of mobile ad fraud and its connection to malware and shares real-world statistics to provide an accurate picture of the current state of the threat.

Focus is placed on Android that is by far the most dominant mobile operating system (OS) globally with Android devices accounting to around 75-85% of all smartphone sales worldwide[1]. At the same time, it is the most vulnerable OS due to its open nature, making it a favorite playground for fraudsters. This is especially true in emerging markets where inexperienced consumers are going online for the first time via their smartphones, which are primarily low-end Android devices. Add in the fact that people in these regions are predominantly unbanked and therefore use their mobile airtime as currency to purchase goods and services online, and you have the perfect opportunity for malware and digital criminals to siphon funds from unsuspecting users.

The report further explains how malicious mobile apps operate, their major forms and the state of malware in numbers, as captured by Secure-D, Upstream's full-stack anti-fraud platform.

It also profiles five of the top offenders in 2019 and examines in detail five key emerging markets, including Brazil and South Africa while juxtaposing insights from the United Kingdom and the United States.

Main highlights include the following 2019 statistics which are based on proprietary data from markets where Secure-D is used by mobile operators to protect all their customers simultaneously at the mobile network level:

98,000
malicious Android apps have been identified

32
out of 100 most malicious Android apps are available on Google Play

23 million
malware infected Android devices in Brazil

99%
of mobile transaction attempts in Egypt are fraudulent

As Secure-D has been deployed by 31 mobile operators across 20 countries, covering nearly 700 million consumers, this represents one of the largest and most detailed set of data regarding mobile ad fraud and mobile malware available.

[1] Statista & Statcounter

Mobile Ad Fraud A multi-billion dollar criminal enterprise

What is mobile ad fraud?

Mobile ad fraud is any attempt to exploit mobile advertising technology to defraud advertisers, publishers, consumers or ecosystem partners, such as mobile operators. The big-picture objective of this tactic is to steal from advertising budgets, though it can take multiple forms.

The malware connection

At first glance, the connection between mobile ad fraud and mobile malware may not be apparent. However, they are closely tied to one another.

We know malware to be causing primarily mischief and disruption, however today it is almost entirely about money. Without the motivation of making money, the instances of mobile infection would likely be a tiny proportion of what it is now.

Why is it happening?

Follow the money. With mobile advertising spending on the rise, so is fraud. This “business” is extremely profitable for criminals who use mobile ad fraud to make money quickly and relatively easily with little fear of being caught or punished. It is a low-risk, high-return venture.

How big is the problem?

Losses from online, mobile and in-app advertising reached $42 billion in 2019 and are expected to reach $100 billion by 2023[2].

[2] Juniper Research

Who suffers from mobile ad fraud?

Mobile ad fraud is not a victimless crime, nor are advertisers the only losers. There are many victims in this multi-billion dollar criminal activity, including:

End-users

In many cases, mobile ad fraud is enabled through malware being installed on a consumer's mobile device. Once the malware hijacks the phone, it works silently in the background, repeatedly visiting pages, viewing ads and even "clicking" on them, all without the user's knowledge or consent. As a result, the infected phone may display various negative "symptoms" such as overheating and excessive battery consumption, data depletion and unwanted charges to airtime for premium unwanted subscriptions. This is particularly damaging to mobile users in emerging markets where the cost of data is significantly higher. For example, while an average worker in Germany only needs to work 30 minutes to afford 1GB of data, it would take a minimum-wage worker in Brazil six hours. In these regions, prepaid airtime is the norm and the main way of paying for digital services. This type of transaction does not require credit or debit card details, meaning funds can be siphoned from consumers' prepaid airtime accounts without their knowledge. To understand the scale of the problem, 4Shared, just one of the 98,000 malicious apps that Upstream detected in 2019, would have cost consumers $150 million in fraudulent charges had it not been blocked by Secure-D.

Mobile operators

When mobile devices are infected with malware, consumers, who experience its effects, such as unwanted charges and data depletion, tend to blame the mobile operator. In the example of one African mobile operator, the problem became so acute that its call centers and social media channels were overloaded with complaints from confused, angry customers. Even though malware-infected devices are not mobile operators' fault, they very quickly become their problem, impacting both their reputation and bottom line.

Advertisers

Ad fraud wastes media budgets on fake impressions and clicks that will never translate into sales or revenue. Mobile fraudsters trick advertisers into thinking ads are generating loads of impressions and engagement – while generating zero conversions. When spending decisions are made on mistaken assumptions and falsified metrics the overall effectiveness of marketing strategies is undermined and the impact on the broader mobile media economy can be profoundly damaging.

App publishers

Sometimes, legitimate app developers are as much a victim of such scams as device users. Malware can hijack an app without the developer's knowledge, generating fraudulent revenue on their back through bogus ad clicks "silently" in the background. Unfortunately, when an app is publicly outed as being malicious, it can damage the developer's reputation, regardless of who's to blame.

Which regions are affected the most?

No territory escapes mobile ad fraud. However, emerging markets display special characteristics that leave consumers particularly vulnerable.

Android is the dominant mobile operating system (OS) in these regions and also the OS of choice for fraudsters.

Data depletion, one of the side effects of malware, hits users' wallets in a big way as the cost of data is relatively higher compared to developed markets. For example, in Africa, 1GB for prepaid subscribers costs the equivalent of 16h of work at minimum wage.

The majority of consumers are new internet users, therefore, they are less aware of the dangers that exist and less able to protect themselves from them.

Most people are unbanked, and prepaid mobile subscribers use their airtime balance to pay for digital services, leaving them financially exposed to malware that subscribes them to premium services without their knowledge.

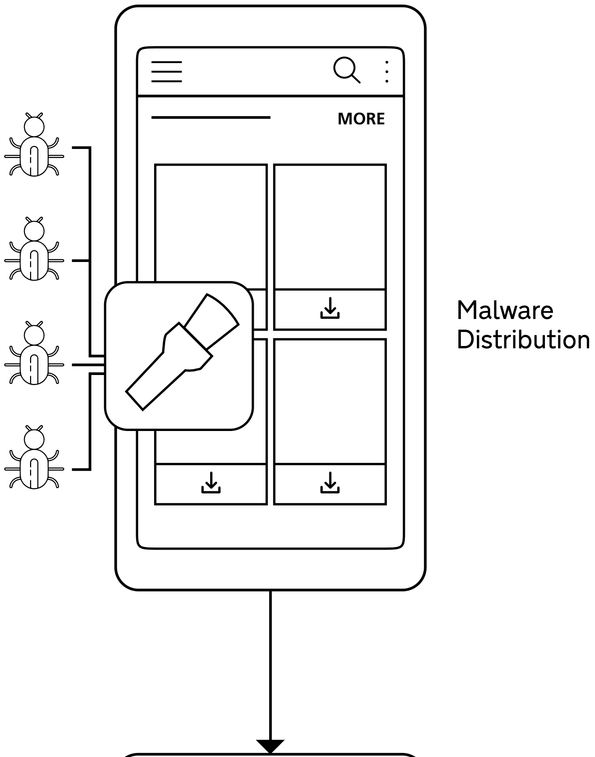
How malicious apps operate

The lifecycle of malware designed for mobile ad fraud generally progresses across four stages:

Stage 1

Distribution

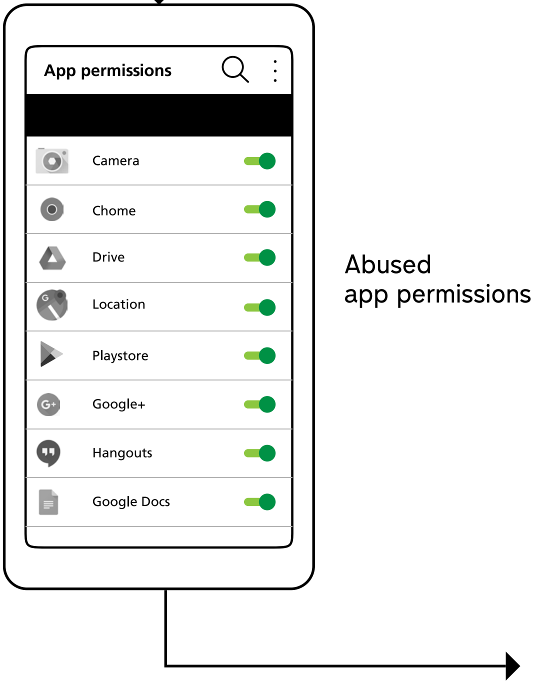
Fraudsters trick the user into intentionally downloading and installing an infected app. The easiest way to do this is to create what looks, feels and runs like a legitimate app. For example, a weather app may do exactly what it claims and at the same time run malicious activity that remains undetected in the background. The distribution mechanism could be an app storefront such as Google Play or a third-party Android store, such as Uptodown or Softonic – or even an ad. There is also evidence of cybercriminals targeting the tools that developers use to create apps, such as a Software Development Kit (SDK) that allows their malicious code to become integrated into multiple, otherwise legitimate, third-party apps



Stage 2

Permissions

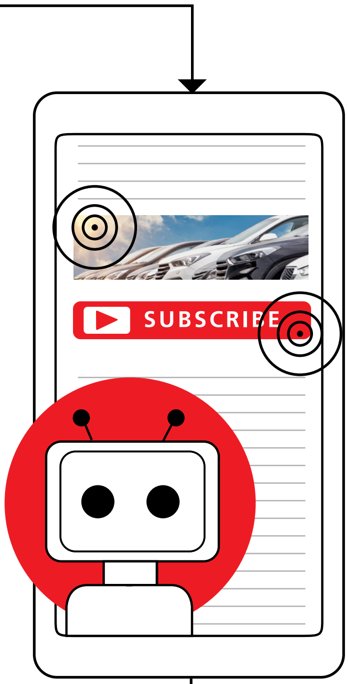
The Android operating system (OS) aims to protect its users through permissions-based access. The idea is that users can approve what permissions an app is allowed, preventing unauthorized access to their resources or data. It's a great idea in theory, but in practice, users don't always pay full attention to the permissions they give an app. Malware creators take advantage of this weakness to gain greater control over the device.



Stage 3

Getting to work

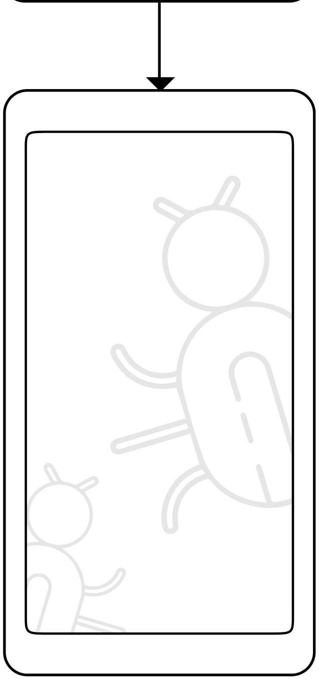
Once installed, mobile malware becomes part of a "botnet" (short for robot network) of infected devices. These botnets, networks of malware-infused devices, can now be remote-controlled at scale by a "bot-herder".
In the case of mobile ad fraud, the malicious application can visit websites, click on banner ads and simulate a real person going through a subscription process. It can even override a two-step authentication process.
The goal, in any case, is for fraudsters to claim pay-outs from advertisers for bogus traffic.



Stage 4

Staying hidden

What is especially tricky about mobile malware is that it continues to operate without raising suspicions from the user of the device. Tricks include making sure the app functions well even when malware runs in the background or ensuring that excessive battery drain doesn't occur. Some apps change their name after they have been downloaded or remain totally out of sight i.e. they cannot be found at the homepage of a device with an app icon.



A sneaky bypass

Some malware creators make their work even easier by pre-installing malware onto phones before the owner purchases it, skipping the download step altogether. One route is to take advantage of buyers in developing countries by putting malware on cheap handsets. In one example, malware has been found pre-installed on Alcatel Android devices manufactured by TCL Corporation, a Chinese tech firm known for making the Alcatel and Blackberry devices. The Weather Forecast - World Weather Accurate Radar app initiated calls to servers unrelated to the app's main function, collected users' personal information and triggered a suspicious background activity undetected by the users.

The five “villains” of mobile ad fraud

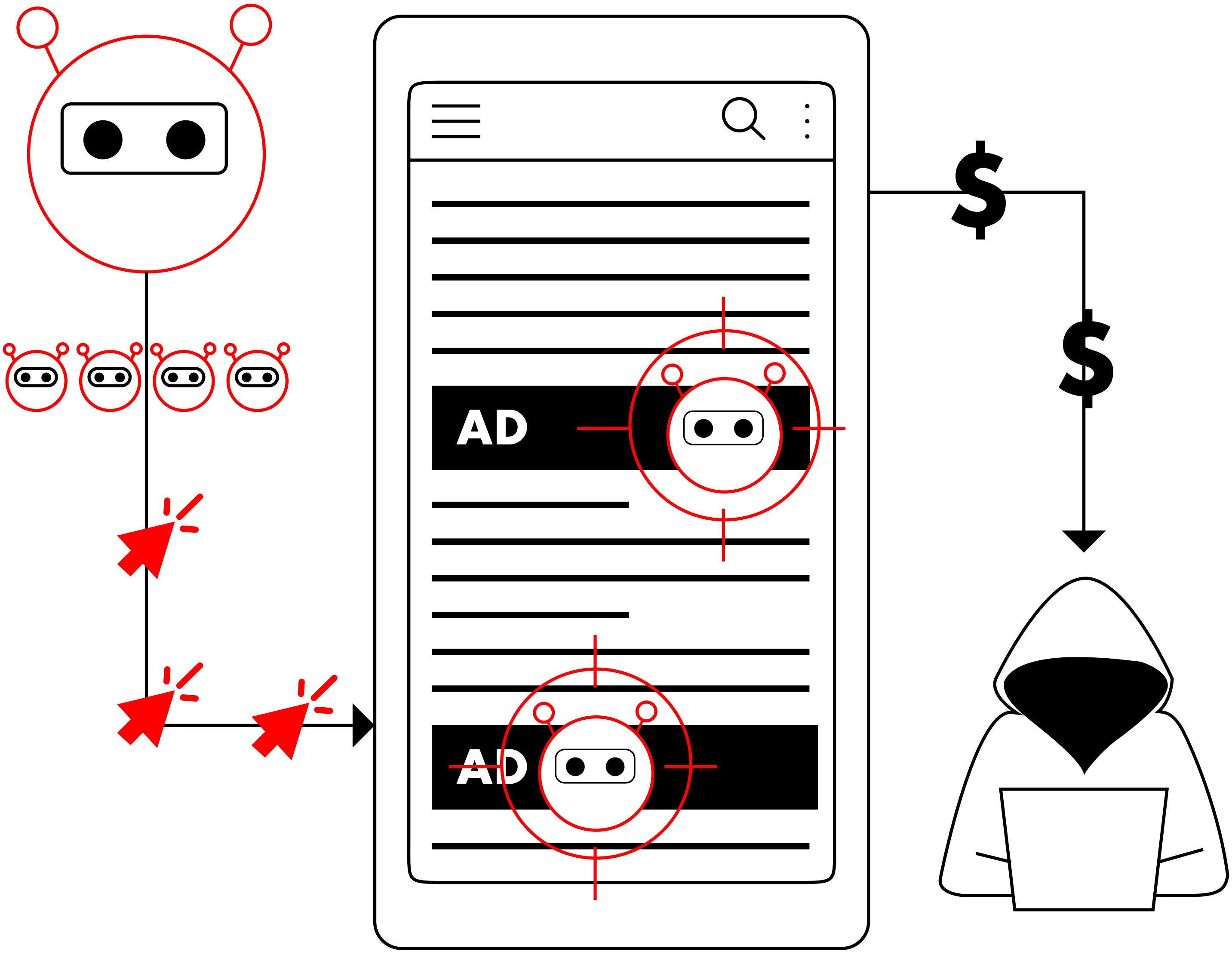
While there are many different ways for cybercriminals to commit ad fraud, they typically fall under five mobile ad fraud archetypes. Malicious apps may exhibit one or multiple of the following types of rogue behavior.

Clickbots

Click fraud uses malware-infected devices like mobile handsets to make fake visits and clicks on ads. Fraudsters use all manner of tricks to get around attempts by advertisers to spot this scam. Specially designed malware can use random delays and fake finger movements to better simulate a real human clicking an ad. Normally, advertisers are the main victims of click fraud; however, end-users also suffer the side effects of click fraud, getting falsely subscribed to premium services with high charges.

How it works

- Fraudsters pay to use a botnet, a huge collection of devices hijacked by malware.
- Fraudsters use the botnet to navigate to sites under their control and show ads from legitimate advertisers which are invisible to the user.
- Fraudsters use the botnet to create millions of fake clicks on ads without the device owners knowing.
- The ads are hosted on the fraudsters' own pages, so they collect money from legitimate advertisers.



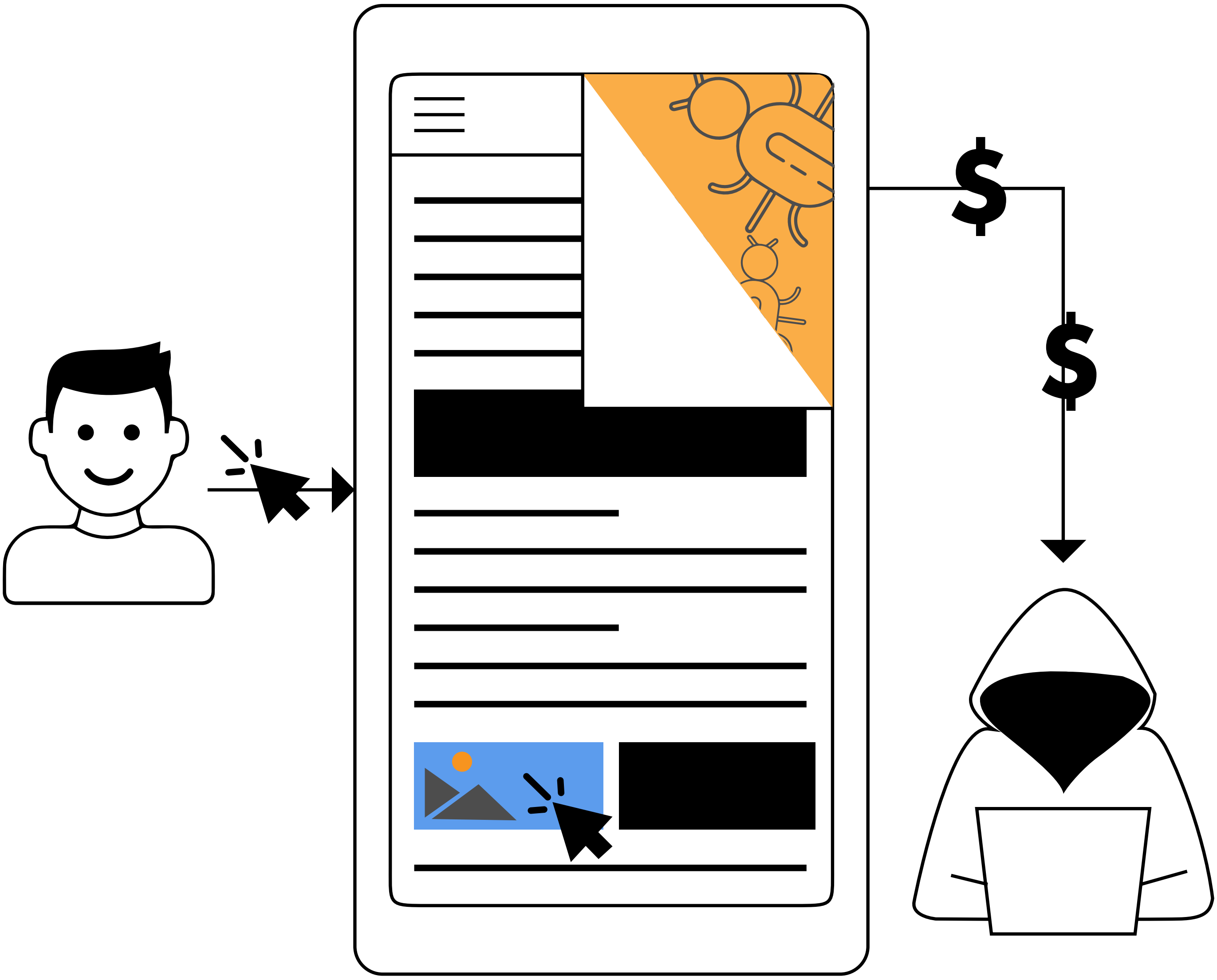
Click-Jackers

Click-jacking occurs when a user taps on a button or link that appears legitimate; in reality this is a click on a hidden or disguised ad, not visible to the user. Fraudsters have to stay one step ahead of browser and mobile operating system (OS) developers, finding new ways to hide the invisible elements so they are not blocked or revealed. They also use carefully chosen wording and imagery to entice users to click on a specific part of the page. For example, the link might appear to be a coupon for products or services, or it might provide a link for a free offer.

Fraudsters also use a range of options for taking advantage of the click, such as sending a user to an ad-laden site that claims revenue from the advertiser. Alternatively, the user may be redirected to confusing web pages that entice or trick them into a digital subscription. Another trick is to use invisible links to trigger a malware download.

How it works

- Legitimate users tap or click on what they think is part of the visible page.
- The page actually includes invisible elements, such as transparent windows that contain misleading links.
- The browser believes the user meant to click on the misleading link and performs an action.



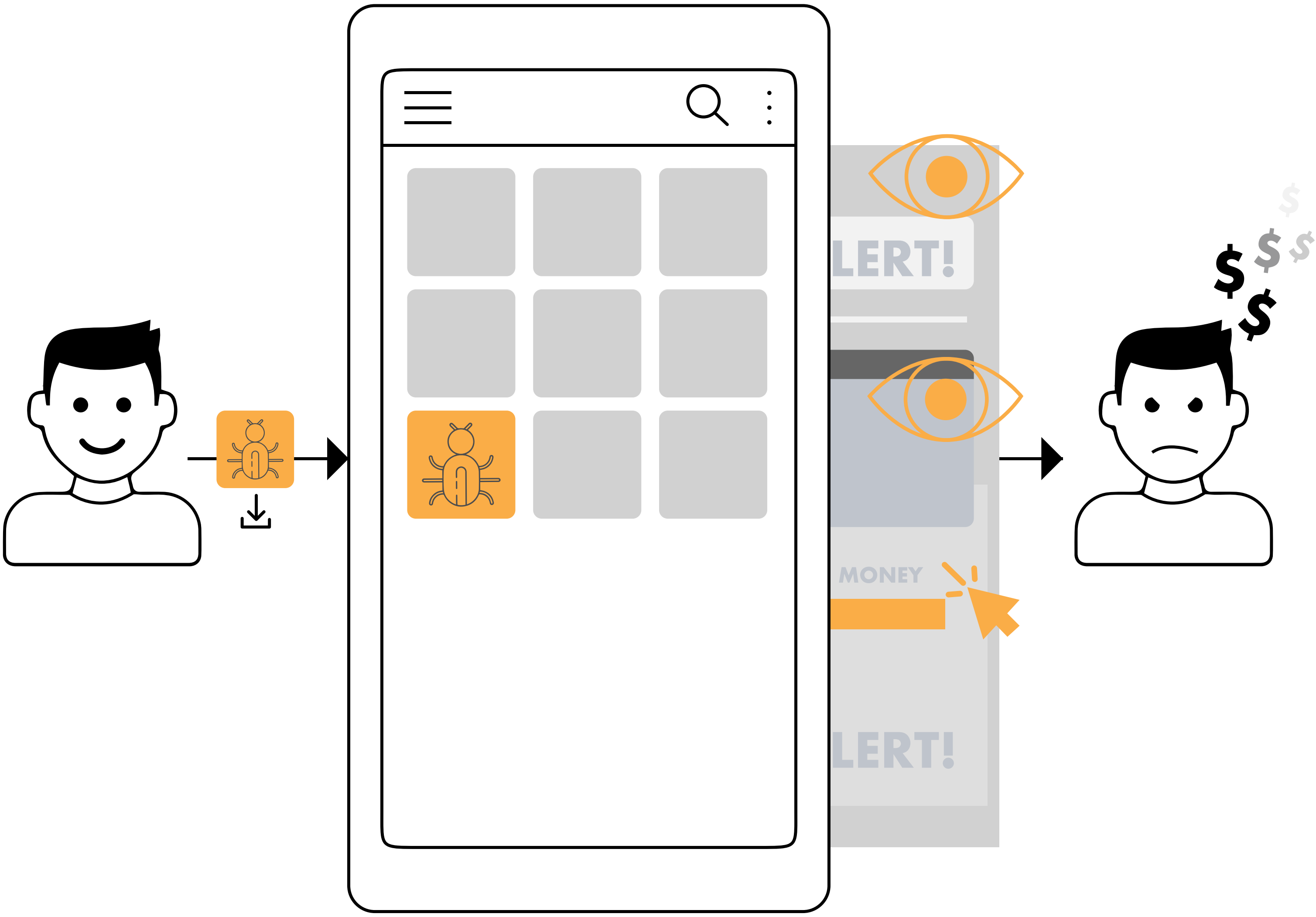
Phone-Jackers

Fraudsters use intricate techniques to get malware onto phones. This includes disguising or encrypting code in apps so that they evade security checks before going into the official Google Play Store. Another technique is using an app that looks innocent but secretly downloads and installs other apps that do damage.

When mobile device hijacking like this occurs, the malware loads ads repeatedly so fraudsters can falsely claim revenue from advertisers. Such apps often hide their activity from the users; for example, a background process might be set to begin as the phone boots up, which means there is no visible activity and the malware won't usually show up in a list of running apps.

How it works

- The user unintentionally downloads an app that contains malware.
- The malware hijacks the device and can relentlessly load ads without the user ever seeing them.
- The malicious publisher claims revenue for the ad views, while the user remains unaware unless there are data use spikes or overheating batteries.



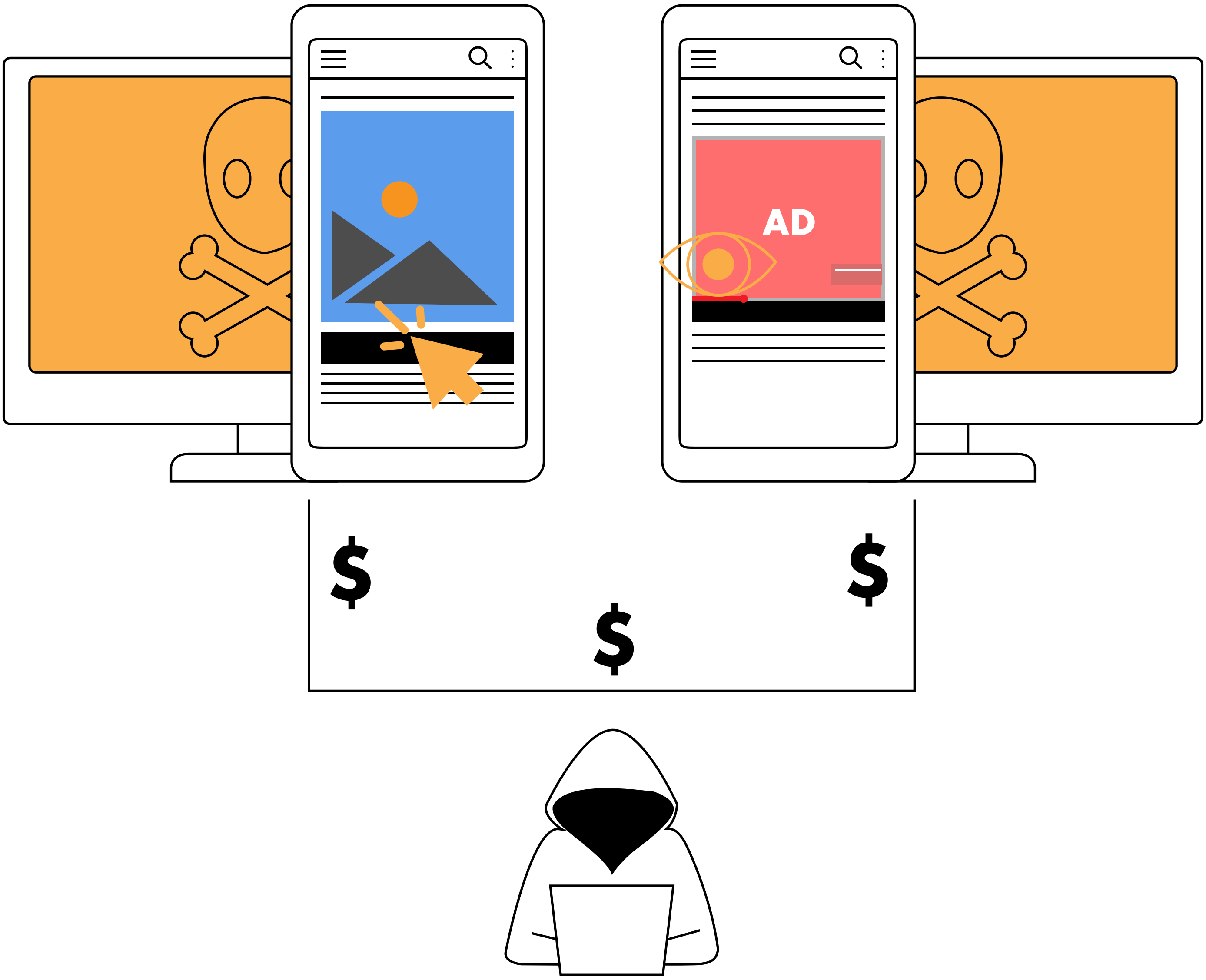
Emulators

Some ad fraudsters use server farms or non-mobile devices for ad fraud, so they can generate more bogus clicks, while still posing as a mobile device user. This requires carefully crafted techniques that disguise the true nature of the device, so the bogus ad click often poses as a specific phone or tablet model.

Mobile device emulation takes advantage of advertisers that pay premium rates to advertise on mobile devices rather than desktop computers. This is driven by research that shows mobile users spend more online per month than desktop users and are twice as likely to make big purchases over $250.

How it works

- Fraudsters use traditional desktop computers and servers to carry out bogus views and clicks.
- Emulator tools give the impression that traffic is coming from mobile devices.
- Because there's no need to hijack real mobile devices, there's no risk of being spotted by device owners. Fraudsters get paid for the events at premium ad rates.



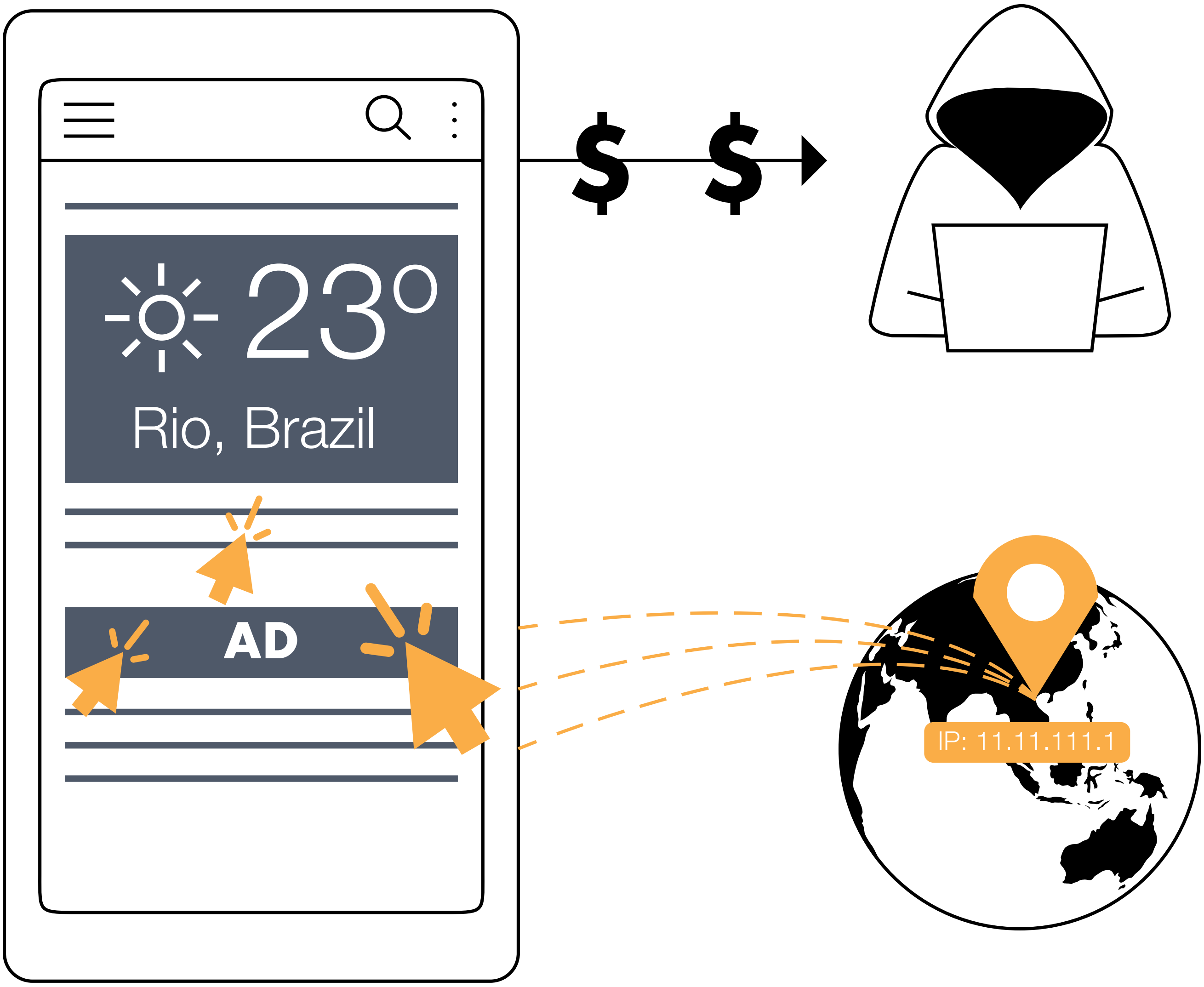
IP - Spoofers

This is a technique used to make any form of mobile ad fraud more effective. It involves using various techniques to change the reported IP address by making requests as clicks or ad impressions. Rather than the hijacked device's IP, the reported address can be far away and even in a different country. This can be used to make the user appear to be in a more lucrative market. It's also commonly done to avoid having too many fake clicks reported from the same IP address, thereby avoiding detection.

Fraudsters use complex techniques to disguise the device's identity, such as going through multiple redirections before initiating the connection to the ad server to create a complex digital trail. In other cases, fraudsters use virtual private networks (VPNs) and other similar tools to create a different IP address as the supposed source of each view or click.

How it works

- Click farms in Country A, for instance India, target a website in Country B, say Brazil, by generating bogus non-human traffic. A user's hijacked phone in Country B gets a high number of requests from the IP based in Country A.
- Fraudsters utilize users' highjacked phones in Brazil as proxies, thereby making the traffic appear to be originating from Brazilian IP addresses.
- Fraudsters get paid for the fake events, including ad clicks and views.

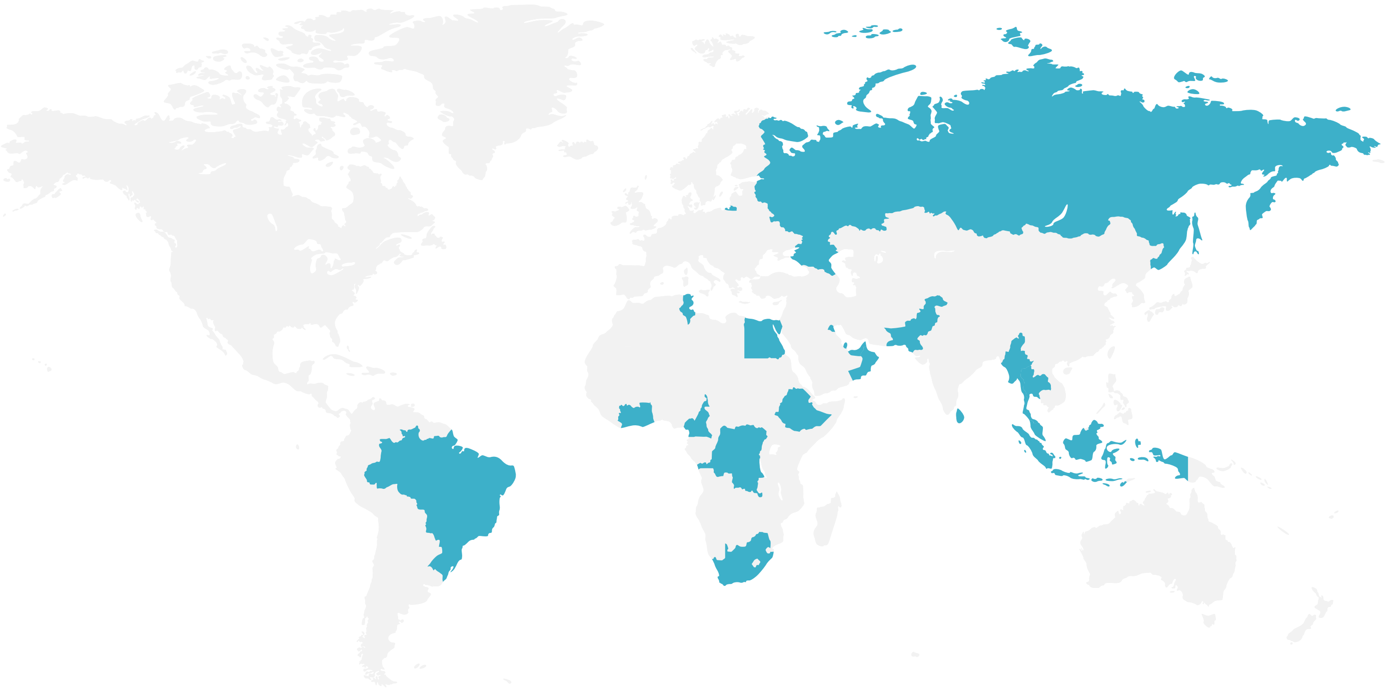


Mobile malware market statistics 2019

Upstream partners with mobile operators to protect their subscriber base through its security platform Secure-D. The insights below are taken from Secure-D's monitoring and blocking operations across 20 countries, where its mass-scale deployment in 2019 protected 700 million mobile subscribers, making the below one of the largest and most accurate data set available to discern the true scale and scope of mobile malware and ad fraud operations around the world.

This report does not estimate global figures, which will inevitably be much higher. Instead, it highlights accurate figures from those 20 countries, wherefrom the impact of mobile malware and ad fraud may be extrapolated.

Secure-D 2019 deployment

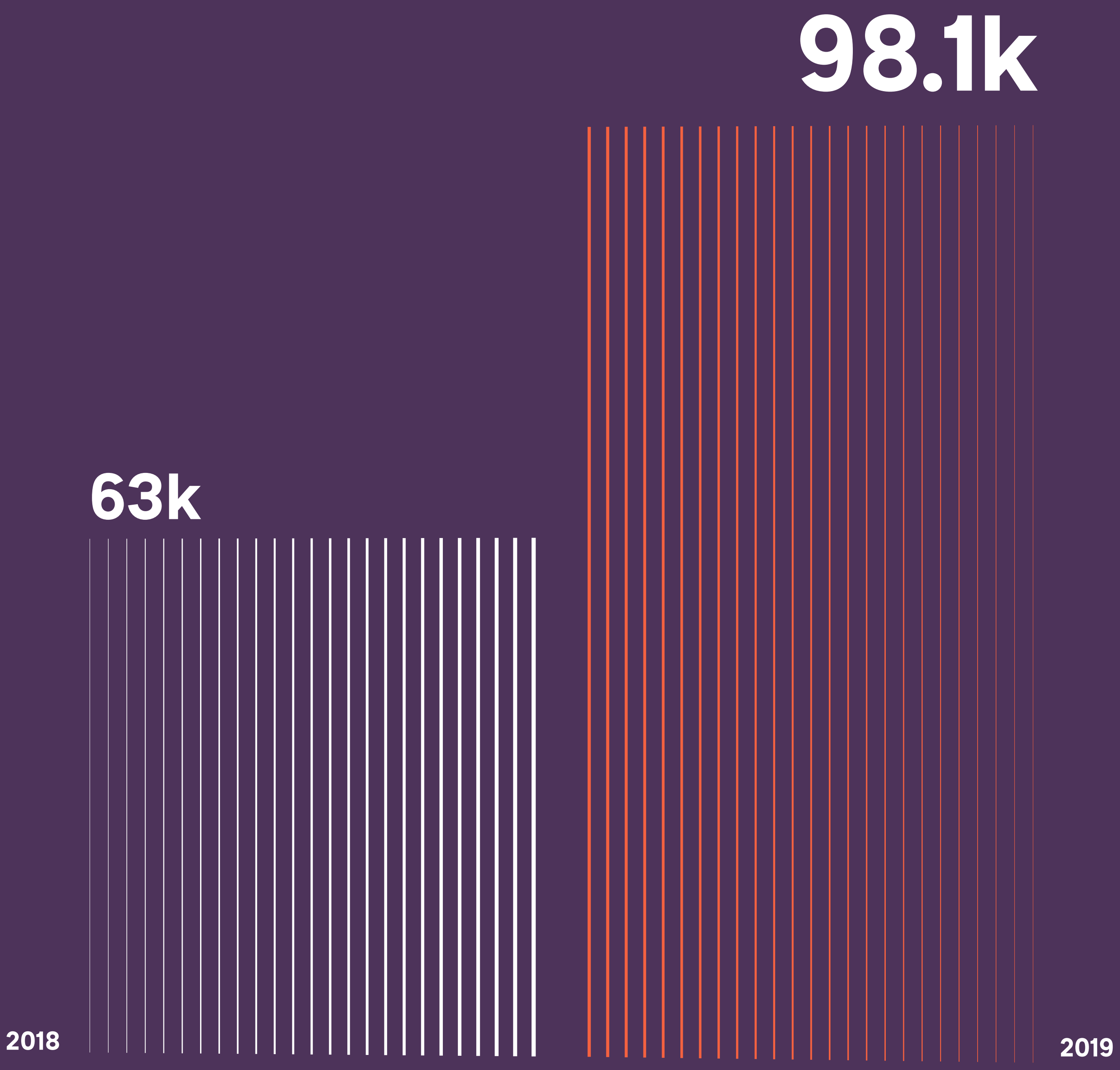


In 2019, Secure-D published the first-ever mobile malware index, which shares details of the top 1,500 Android mobile malware, based on data taken from the security platform's operations. The Secure-D Index is a free and regularly updated online resource, which is intended to help concerned smartphone users, mobile operators, cybersecurity professionals and industry observers.

Number of malicious apps

In 2019, across the 20 countries where Secure-D is deployed, it has identified nearly 98,000 malicious apps in operation, up by 55 per cent compared to 2018, when around 63,000 malicious apps were identified.

Figure 1: Number of malicious apps 2018-2019 (in thousands)



1.71B

Transactions processed

In 2019, Secure-D processed 1.71 billion mobile transactions across 20 markets and blocked 1.6 billion of them as fraudulent, a staggering 93 per cent of total transactions. This demonstrates the vast scale of mobile ad fraud operations.

43.3M

Malware infected devices

Secure-D detected over 43.31 million unique mobile devices infected by malware in 2019. The number of infected devices increased since 2018 when Secure-D identified 30 million.

$2.1B

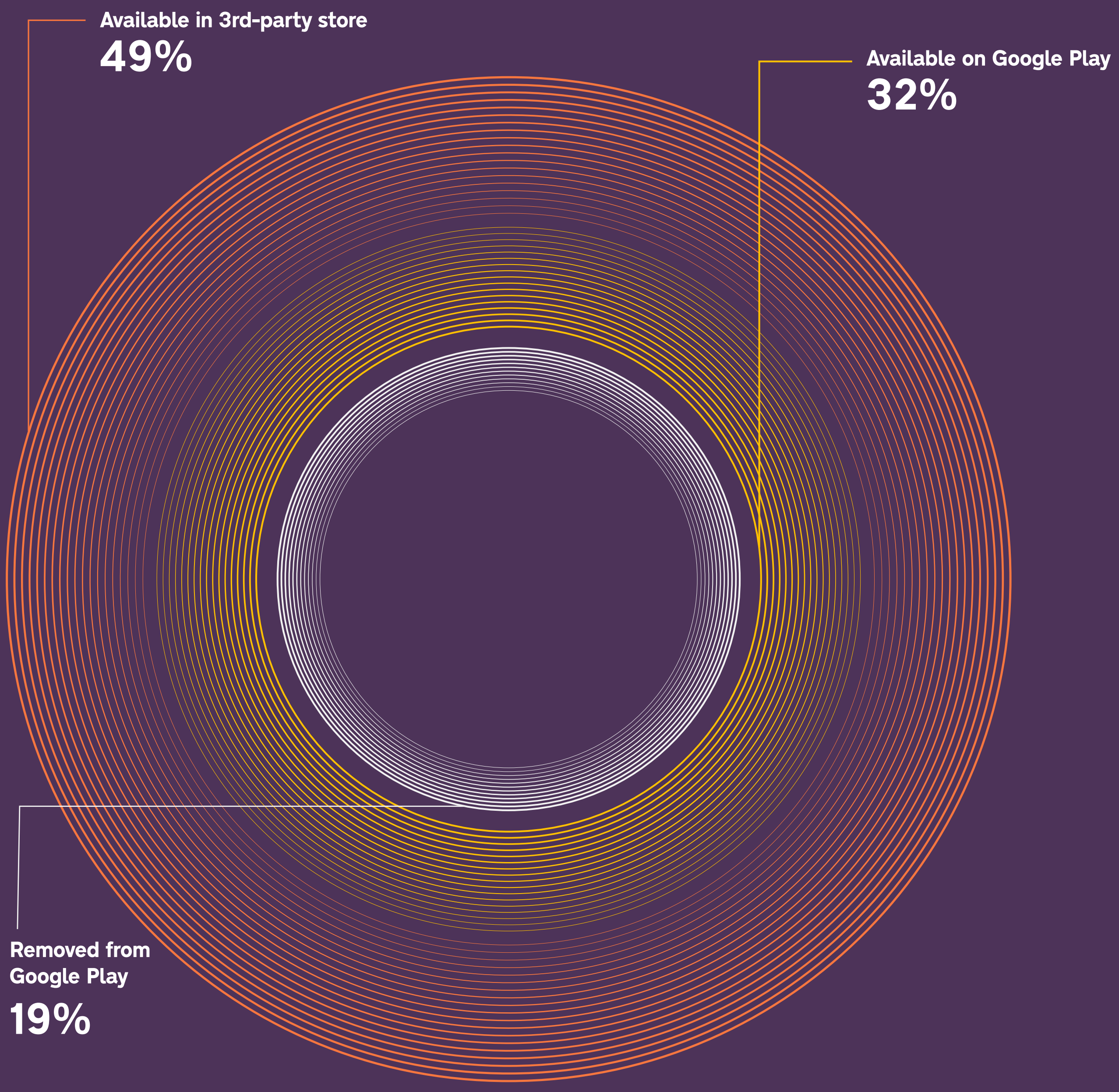
Fraudulent charges prevented

Across the 20 countries where Secure-D is deployed, Upstream's security platform blocked $2.1bn worth of fraudulent transactions in 2019.

Availability of malicious apps in Google Play Store

While it has always been a good rule-of-thumb for consumers to only download apps from Google's official storefront, Google Play, to avoid some of the worst malware-laden apps, it is by no means a guarantee of safety. Thanks to Google Play's scale and set-up, there is always a chance of rogue apps getting through its defenses. Of the top 100 most active malicious apps of 2019 that Secure-D blocked, 32 per cent of them are still currently available to download on Google Play. 19 per cent of the worst-offending apps were previously on Google Play but have since been removed. A further 49 per cent have never been available on Google Play and are only available through third-party app stores.

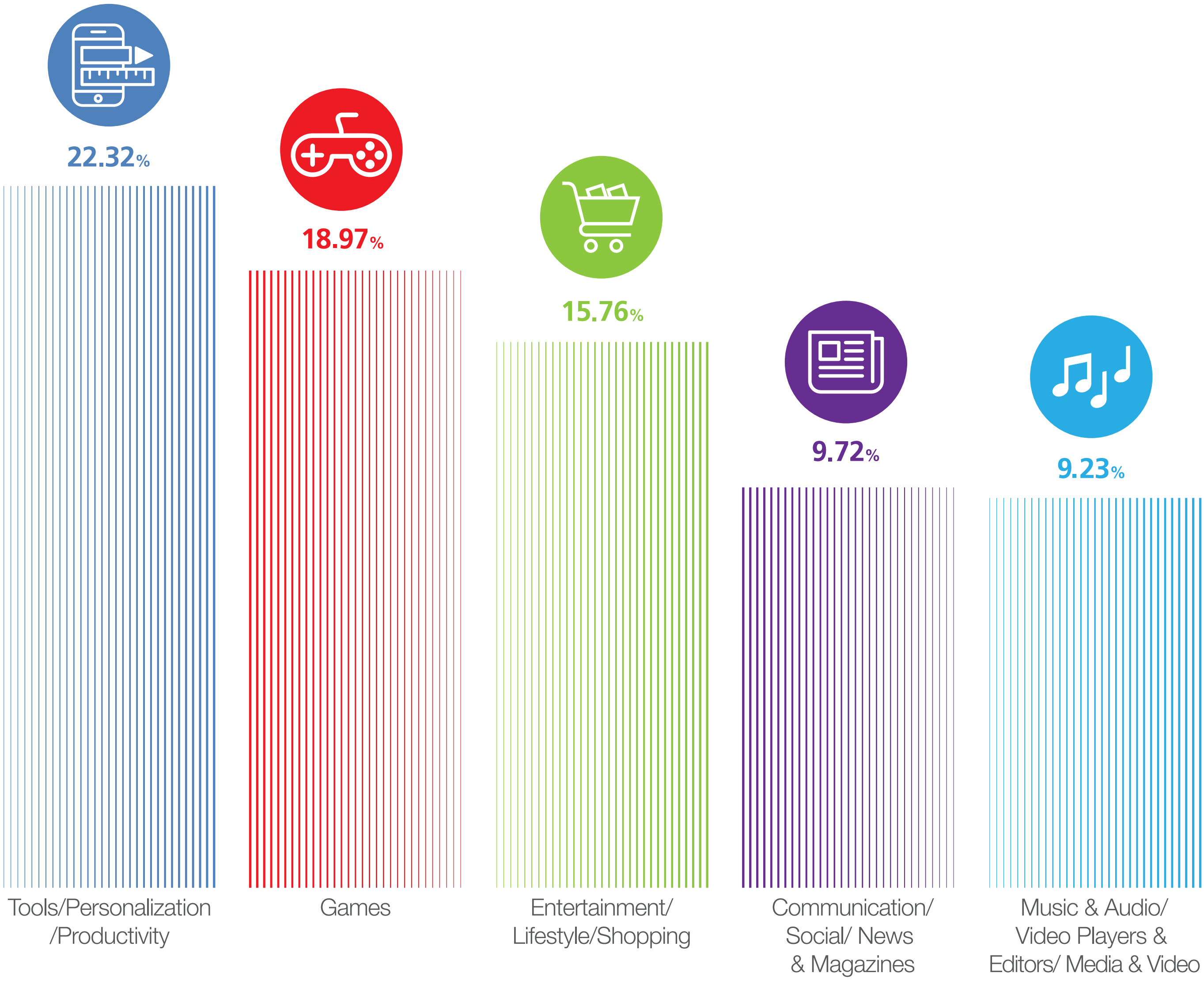
Figure 2: App store availability of the top 100 malicious apps in 2019



Top categories for malicious apps

Different categories of apps are more likely to be used by cybercriminals than others. Ironically, the categories of apps that are supposed to make a device function better and make everyday life easier for their users are often the ones that can be the most harmful. Tools/Personalization/Productivity are some with a high probability of malware. Globally, 22.32 per cent of malicious apps fall under these. The second-most popular category for fraudsters to target is Games with 18.97 per cent. These are followed by Shopping/Entertainment/Lifestyle with 15.76 per cent and Communication/Social/News & Magazines with 9.72%[3].

Figure 3: Top app categories targeted by fraudsters



[3] Note that as these categories are Google Play store specific, above percentages apply only to apps that are currently available or were previously available on Google Play.

Five of the most malicious apps of 2019

Fake smiles - The emoji keyboard that robs its users

Ai.type is a popular "emoji keyboard" app for Android devices. It collected more than 10 million downloads from Google Play and claimed more than 40 million users overall. Developed in Israel by ai.type LTD, the app allows end-users to customize the keyboard to their personal preferences. It also "learns" the user's writing style over time, anticipating commonly used words and phrases to speed up written composition. The app was available on Google Play until June 2019, when it was removed.

The app was found to be delivering millions of invisible ads and non-human clicks in 2019. While these ads are never seen by the users and do not appear on screen, genuine user data about real views, clicks and purchases are reported to ad networks. Suspicious activity originating from the app spiked in July 2019, soon after its removal from Google Play.

In 2019, Secure-D blocked more than 14 million suspicious mobile transaction requests originating from the ai.type keyboard app. If not blocked, the 14 million fraudulent transaction requests tracked by Upstream's security platform would have triggered the purchase of premium digital services, potentially costing users in 13 countries up to $18 million in unwanted premium charges. Most of the suspicious activity, which is still ongoing, took place in Egypt and Brazil.

Downloads[4]	40 million
Developer	ai.type LTD.
Availability on Google Play	Until June 2019
Suspicious transactions blocked	14 million
Publicly exposed	October 2019
Fraudulent charges prevented	$18 million
Published in	Forbes Daily Mail FOX BUSINESS

More info

Ai.type

[4] No. of downloads as reported at the time of Secure-D investigation publication

"Free" Video downloader that makes its users pay the price

Snaptube allows users to download videos and audios from popular video and music streaming sites, as well as social networking apps. It was developed by China-based Mobiuspace, a company that has secured series B financing from Chinese venture capitalists (VCs).

The app made millions of suspicious transactions without the knowledge of its users. It delivered invisible ads, generating non-human clicks and purchases, while reporting them as real views, clicks and conversions to the advertising networks that served them. These ads were hidden from users. Snaptube used a suspicious third-party SDK called Mango, which connects to external servers to commit ad fraud. The developer apparently cut ties with Mango after Snaptube's malicious behavior was exposed.

Secure-D detected and blocked more than 70 million suspicious transaction requests originating from 4.4 million unique devices in just six months. If not blocked, those 70 million transaction requests would have triggered the purchase of premium digital services, potentially costing users up to $91 million in unwanted premium charges. Most of the suspicious activity, which is still ongoing in some locations, originated from devices in Egypt, Brazil, Sri Lanka, South Africa and Malaysia.

Downloads[5]	40 million
Developer	Mobiuspace
Availability on Google Play	Third-party app stores only
Suspicious transactions blocked	70 million
Publicly exposed	October 2019
Fraudulent charges prevented	$91 million
Published in	Forbes abc7 TechCrunch CNBC INDONESIA

More info

Snaptube

[5] No. of downloads as reported at the time of Secure-D investigation publication

File-sharing app that attempted to “share” $150 million of its users’ money

4shared is a popular file sharing and storage mobile and desktop app. Available since 2011, it has received generally positive ratings from sources like PC World, Softonic and Microsoft Store. The Android app generated more than 100 million downloads and ranked 2nd in its category in Austria, 7th in Italy and 10th in Switzerland. In April 2019, the app was abruptly removed from Google Play and then replaced the following day. The new version was submitted as an entirely new app – not a version update – and maintained the original 4shared icon, albeit with a “new” ribbon.

The first version of 4shared hides suspicious background activity and delivers bogus ads to devices to generate fake views, clicks and purchases that are reported as valid to advertising networks. The ads are never seen by users and don’t actually appear on screen. 4shared is fraudulently used to fake user engagement metrics and claim revenue from online advertising networks. The app attempted to mask its identity whilst conducting suspicious activity. Instead of appearing under its own name, it assumed the names of either existing legitimate apps (i.e., com.chrome.beta – the new beta version of Google’s Chrome browser) or non-existing ones.

More than 100 million users downloaded the first version of 4shared before the new release in April; however, the earlier downloads contained the code responsible for the suspicious activity. Secure-D identified and blocked more than 114 million suspicious mobile transactions originating from 4shared.

These transactions originated from 2 million unique mobile devices across 17 countries and could have cost users up to $150 million in unwanted charges.

Downloads[6]	100 million
Developer	New IT Solutions Ltd.
Availability on Google Play	Removed April 2019 replaced the following day
Suspicious transactions blocked	114 million
Publicly exposed	July 2019
Fraudulent charges prevented	$150 million
Published in	TechCrunch msn Canaltech WIRED

More info

4shared

[6] No. of downloads as reported at the time of Secure-D investigation publication

The malicious app that downloads much more than cat videos

VidMate is a popular Android app that allows users to stream and download videos and songs from services such as Dailymotion, Vimeo and YouTube. VidMate is not available in Google Play store but can be downloaded through third-party app stores, such as Uptodown.

A hidden component within the app delivers invisible ads, generates fake clicks and purchases, installs other suspicious apps without consent and collects personal users' information. The app also started collecting personal user information, such as International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI) and IP addresses without requiring user permission, while also transferring them to servers in Singapore. VidMate used the same suspicious Mango SDK which was responsible for malicious behavior on Snaptube.

Secure-D detected and blocked more than 128 million suspicious mobile transactions initiated by VidMate. These transactions originated from 4.8 million unique mobile devices across 15 countries. If not blocked, users would have been subscribed users to premium digital services potentially costing them up to $170 million in unwanted charges.

Downloads[7]	500 million
Developer	UC Web
Availability on Google Play	Third-party app stores only
Suspicious transactions blocked	128 million
Publicly exposed	May 2019
Fraudulent charges prevented	$170 million
Published in	BuzzFeed News Daily Mail techradar

More info

VidMate

[7] No. of downloads as reported at the time of Secure-D investigation publication

Cloudy with a chance of click-fraud for rogue weather app

Com.tct.weather is a weather forecast application that has advanced malware designed to siphon data and attempt fraudulent transactions. With more than 10 million installs, the malware was found pre-installed on Alcatel Android devices manufactured by TCL Corporation and on Google Play.

The com.tct.weather application initiated calls to a server in China that were not related to the application's main function. It collected the user's device ID, email and location without gaining user consent and accessed web pages with digital ads. A second URL continuously requested by the app redirects to web pages with digital ads. The application then clicks buttons on those pages, committing click fraud. After an idle two-month period following the app's public "outing", Secure-D detected and blocked 34 million fresh suspicious transaction attempts.

Had it not been blocked, users on Alcatel Android smartphones in countries like Brazil, Malaysia and Nigeria would have been billed for unwanted services to the tune of more than $1.5 million. This activity occurred in the background and succeeded in remaining undetected by the users, making it a potent and far-reaching malware.

Downloads[8]	10 million
Developer	TCL Corporation
Availability on Google Play	Yes
Suspicious transactions blocked	27 million
Publicly exposed	January 2019
Fraudulent charges prevented	$1.5 million
Published in	WSJ BBC O GLOBO BUSINESS INSIDER

More info

Weather Forecast - World Weather Accurate Radar

[8] No. of downloads as reported at the time of Secure-D investigation publication

Top infected markets

Malware in emerging markets

Android, as previously explained, is the dominant mobile operating system (OS) globally with consumers in emerging markets opting for the low-end, cheaper available handsets. Android is also the OS of choice for fraudsters. Due to the special characteristics of these markets consumers there are more vulnerable to mobile fraud:

- Most of them go online for the first time via their mobile phones and are unaware of the dangers.
- Data depletion caused by malware has a much greater effect on them due to the high cost of mobile data.
- As most people in these regions are unbanked and use their airtime to pay for digital services they are more susceptible to malware subscribing them to premium services without their knowledge.

Below are snapshots of mobile malware and mobile ad fraud that Secure-D detected and blocked in five of the markets where the security platform is deployed.

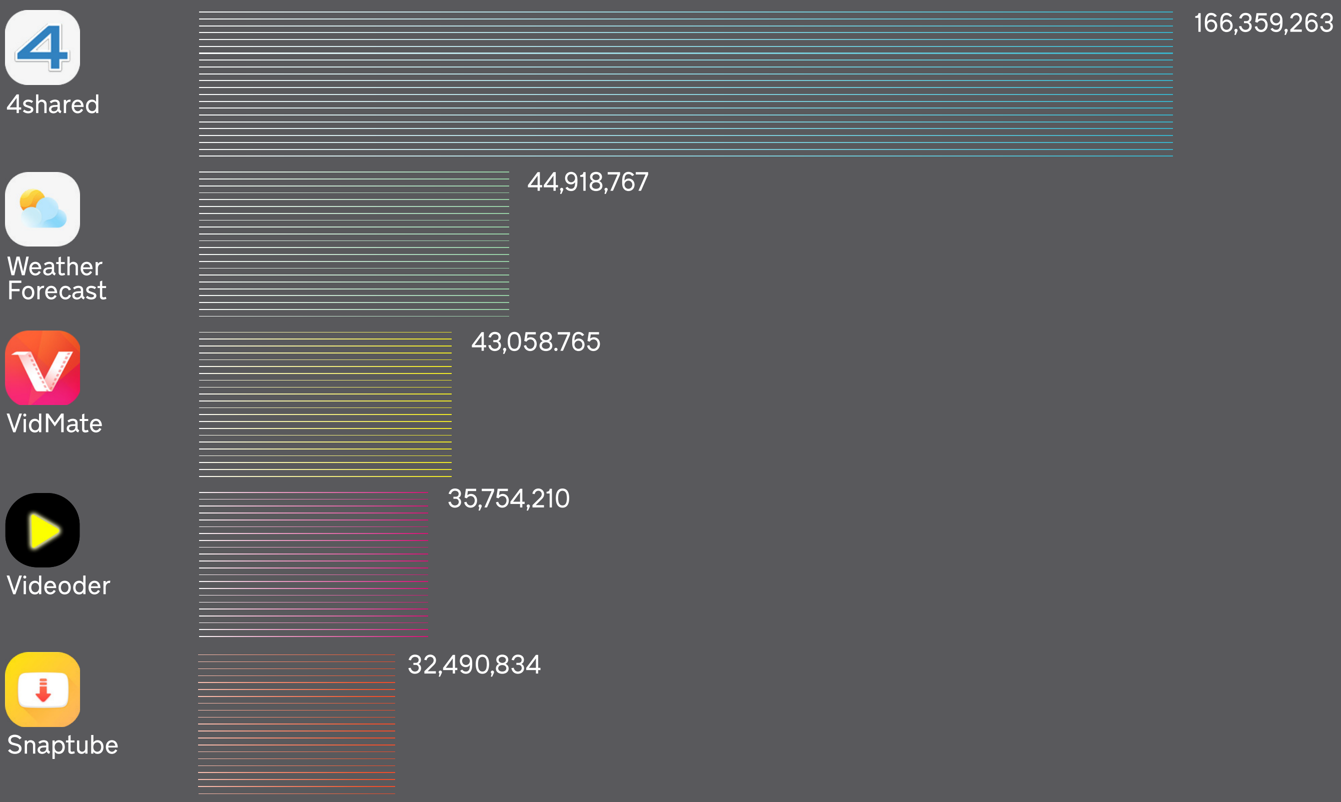
Secure-D is currently used by 31 mobile operators across 20 different countries.

Brazil

As an emerging market and an extremely large one at that, Brazil has been heavily targeted by fraudsters. Secure-D caught nearly 55,000 malicious apps in operation in Brazil with over 23 million malware-infected devices identified. However, as Secure-D is operational across two major Brazilian mobile operators, it has been able to significantly reduce the impact of mobile cybercriminals in the country. During 2019, Secure-D detected that 91 per cent of the 986 million mobile transactions in Brazil were fraudulent, and subsequently blocked them.

Malware-infected devices	23,207,542
Malicious apps blocked	54,853
Mobile transactions processed	986,478,119
Fraudulent transactions (%)	91%
Most malicious app category	Tools/Personalization/ Productivity (33.7%)

Figure 4: Top 5 malicious apps found/blocked fraudulent transactions in Brazil in 2019

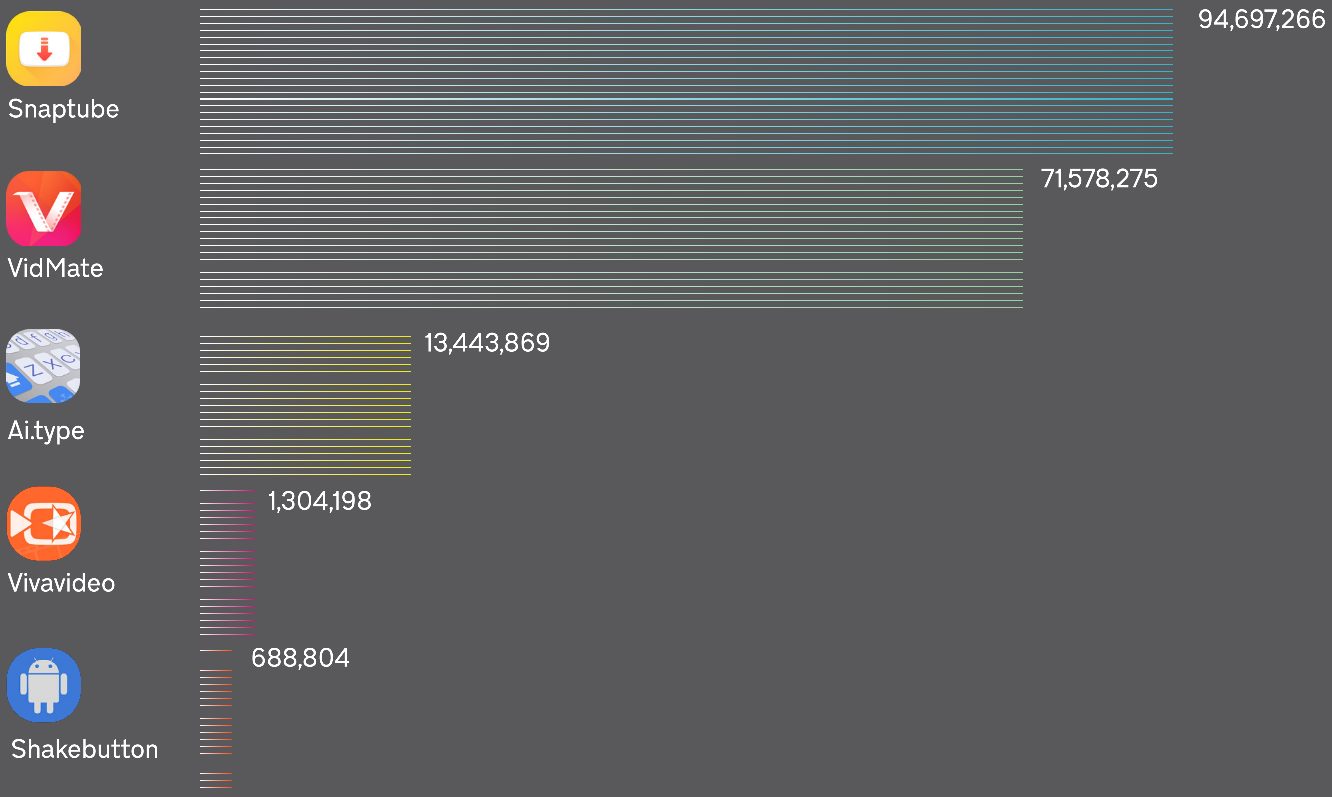


Egypt

With a population of over 100 million, Egypt is the most populous country in the Arab world and has the fourteenth largest population globally. It also has more than its fair share of mobile malware. Over three million malware-infected devices were identified in Egypt, with over 4,600 malicious apps targeting the country. In 2019, Secure-D processed and secured over 212 million transactions in the market, where a staggering 99 per cent were found to be fraudulent. The top three most prolific malicious apps in Egypt are all profiled in Section 5 of this report.

Malware-infected devices	3,229,736
Malicious apps blocked	4,663
Mobile transactions processed	212,440,510
Fraudulent transactions (%)	99%
Most malicious app category	Tools/Personalization/ Productivity (25%)

Figure 5: Top 5 malicious apps found/blocked fraudulent transactions in Egypt in 2019

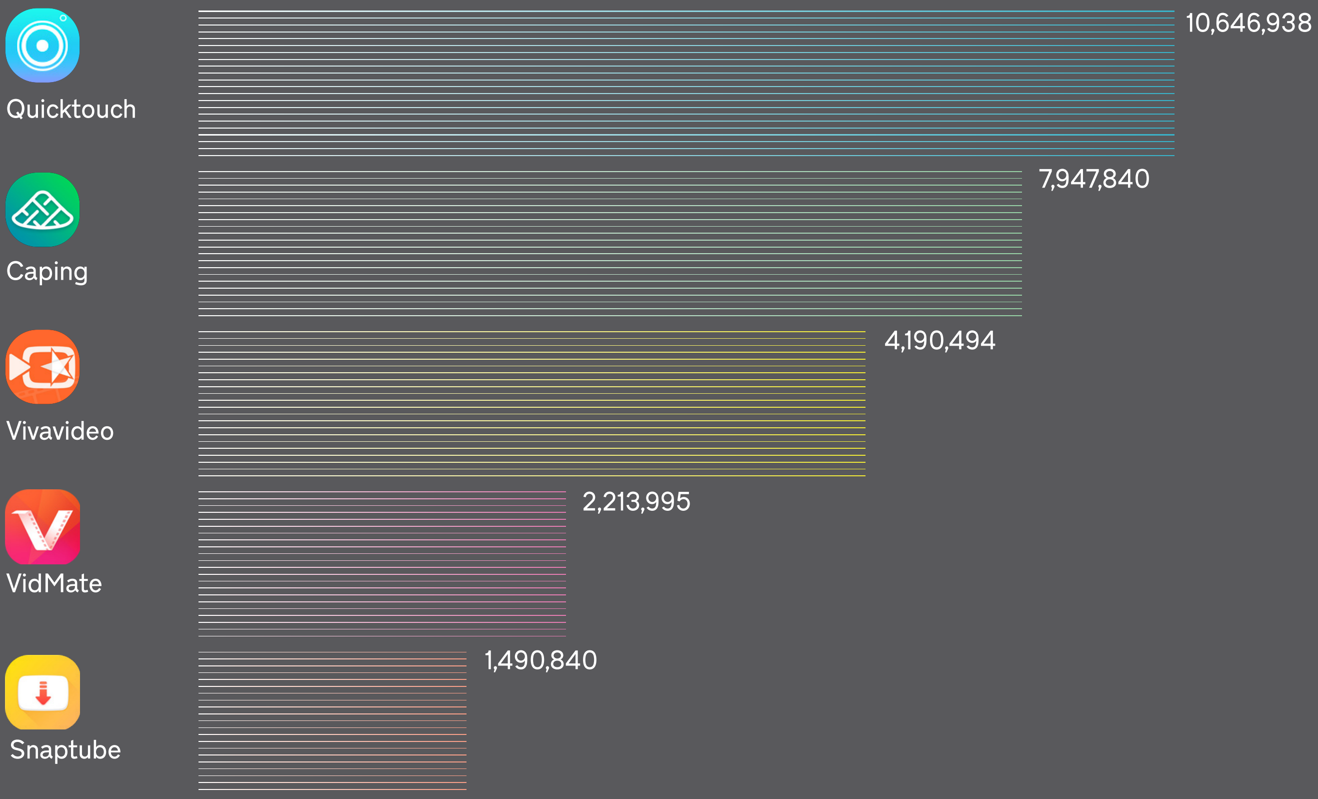


Indonesia

Indonesia has the world's fourth largest population, with over 270 million people. The country is also home to 3.7 million malware-infected devices with 17,260 malicious apps targeting end-users and advertisers in the country. In 2019, Secure-D processed 275 million mobile transactions in the country, blocking 98 per cent of them, due to their fraudulent behavior.

Malware-infected devices	3,699,203
Malicious apps blocked	17,260
Mobile transactions processed	275,319,263
Fraudulent transactions (%)	98%
Most malicious app category	Tools/Personalization/ Productivity (24.2%)

Figure 6: Top 5 malicious apps found/blocked fraudulent transactions in Indonesia in 2019

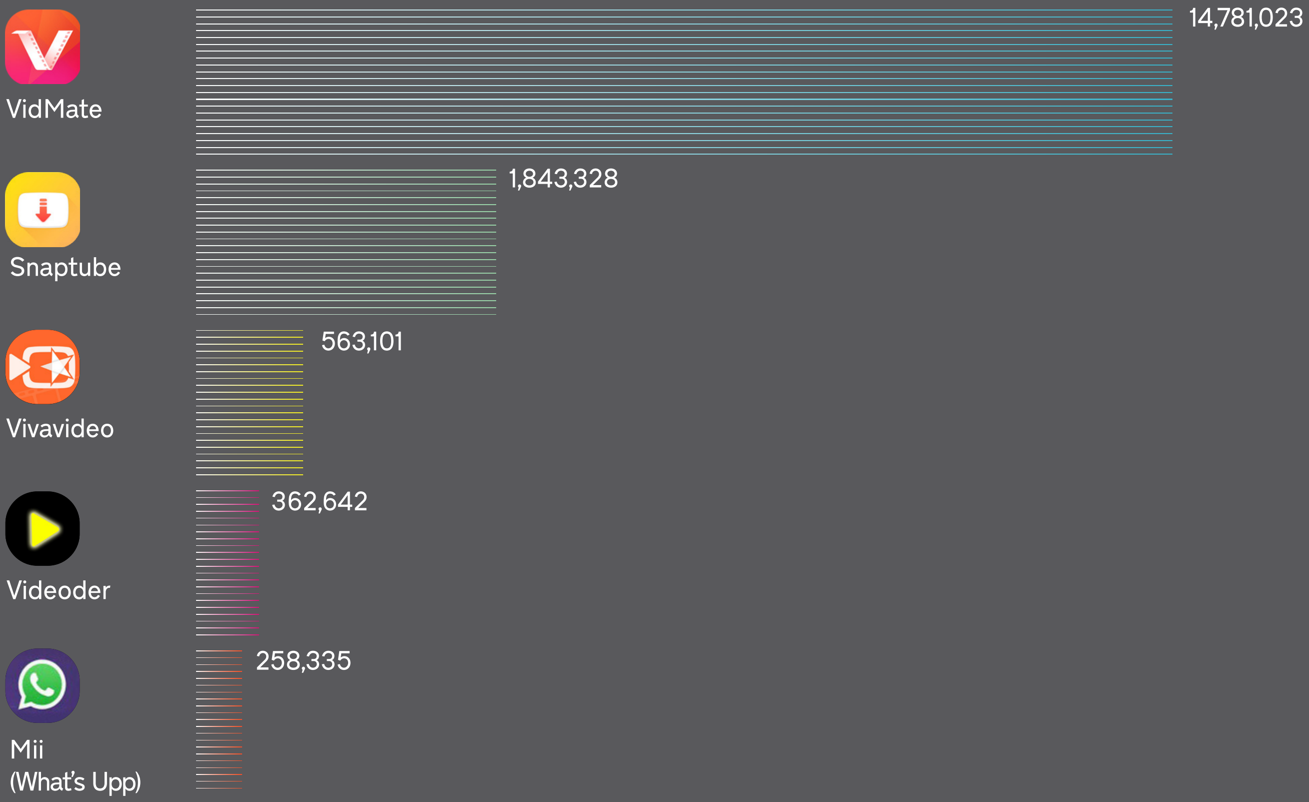


South Africa

South Africa is Africa's second-largest economy, with a population of nearly 57 million. In 2019, Secure-D safely processed nearly 50 million mobile transactions, blocking 86 per cent of them, which were fraudulent. 1.69 million malware-infected devices have been identified in the country and there are well over 18,000 malicious apps in operation. VidMate and Snaptube, both profiled in Section 5 of this report, were the two worst offenders in South Africa.

Malware-infected devices	1,694,841
Malicious apps blocked	18,127
Mobile transactions processed	50,581,005
Fraudulent transactions (%)	86%
Most malicious app category	Games (23.7%)

Figure 7: Top 5 malicious apps found/blocked fraudulent transactions in South Africa in 2019

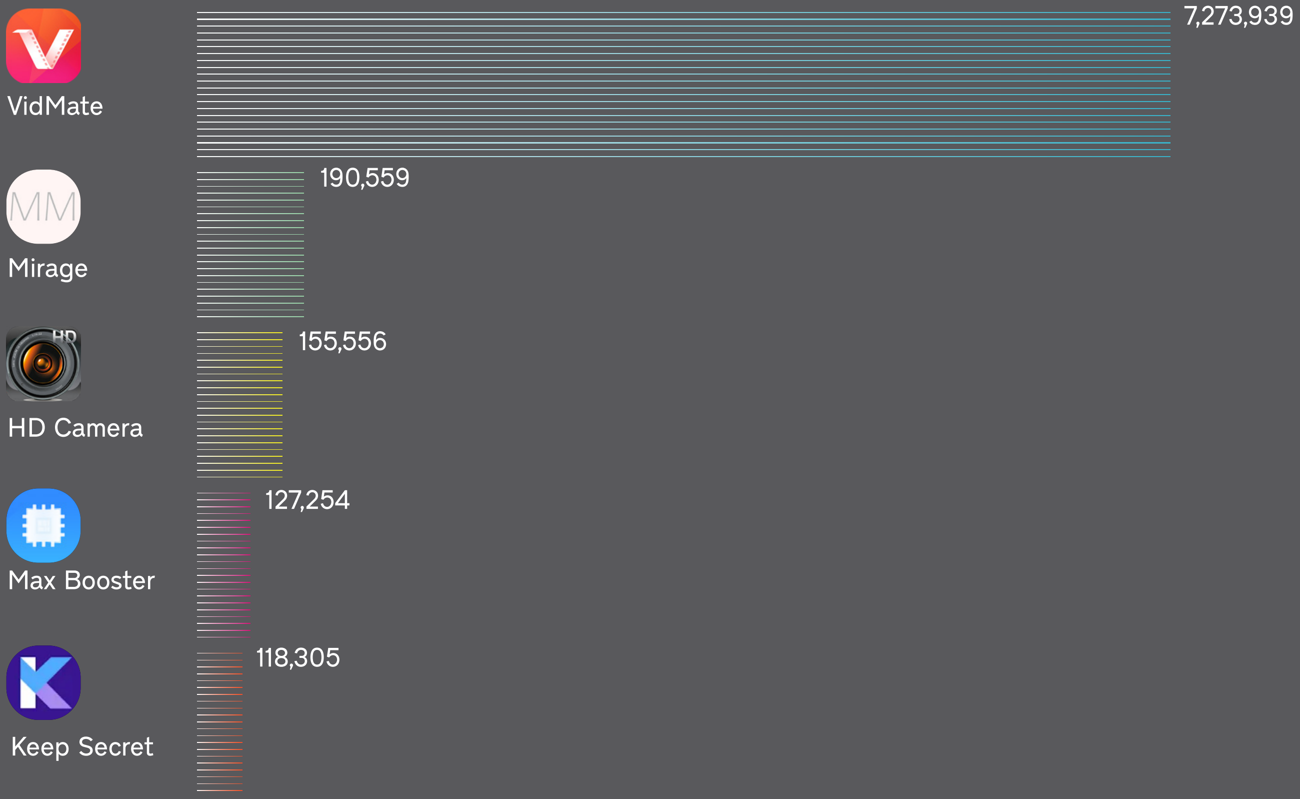


Ethiopia

Ethiopia has a population of over 100 million, combined with 1.3 million malware-infected devices. Vidmate, one of the malicious apps profiled in Section 5 of this report, dominated the fraudulent transaction requests in the country. Overall, there are 9,900 malicious apps targeting end-users and advertisers in Ethiopia. Secure-D processed 35.6 million transaction requests in Ethiopia, blocking 93 per cent of them, which were fraudulent.

Malware-infected devices	1,294,391
Malicious apps blocked	9,374
Mobile transactions processed	36,392,390
Fraudulent transactions (%)	93%
Most malicious app category	Tools/Personalization/ Productivity (26.8%)

Figure 8: Top 5 malicious apps found/blocked fraudulent transactions in Ethiopia in 2019



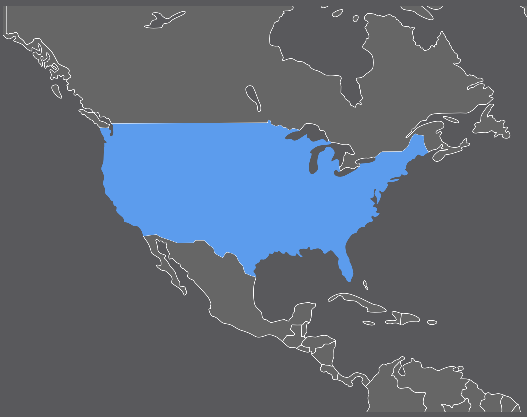
Global malware footprint

Android is by far the most dominant mobile operating system (OS) across the world and at the same time the most vulnerable due to its open-source nature. Android malware and mobile ad fraud are global problems and criminals operate internationally to siphon off the maximum amount of money from all territories. In this section, two major markets, the United Kingdom and the United States, are profiled. As Secure-D is not directly deployed within mobile operators in these two countries, Upstream is running sensor campaigns to observe the fraud level in each market.

United Kingdom

Fraudulent transactions (%) 95%

Most malicious app category Tools/ Personalization/ Productivity (36.3%)



United States

Fraudulent transactions (%) 92%

Most malicious app category Tools/ Personalization/ Productivity (40.4%)

Top 5 Malicious Apps In The United Kingdom

- Snaptube
- Ai.type
- Weather Forecast
- Vivid Caller
- Super Calculator

Top 5 Malicious Apps In The United States

- Free Messages, Video, Chat,Text for Messenger Plus
- GPS Speedometer
- Q video
- Easy Scanner
- Who Unfriended Me

Conclusion

The Android ecosystem has a critical problem with malware. According to data from Secure-D's operations in 2019 98,000 malicious apps were identified, compared to 63,000 in 2018.

Malware infected Android devices are in the millions; Secure-D identified over 43 million in 20 markets alone. 32 per cent of the top 100 most malicious Android apps as detected by Secure-D, are still available on Google Play and a 23% of suspicious apps discovered come under the "Tools and Personalization" category, meaning that Android tools meant to make a phone work better end up defrauding their users.

Demonstrating scale, in the course of only a few months in 2019, Secure-D reported on the suspicious background activity of five very popular Android apps: with a total of nearly 700 million downloads, they were or had been at some point available on Google Play. In these five cases alone, Secure-D detected and blocked 353 million suspicious mobile transactions preventing $430,5 million in fraudulent charges.

Deep diving into five emerging markets shows the extremely high percentage of fraudulent transactions nearing or, in most cases, exceeding the 90% mark. In Egypt, the problem is so critical that 99 per cent of mobile transactions were found to be fraudulent. As Secure-D has been deployed by 31 mobile operators across 20 countries, covering 700 million consumers, this represents one of the largest and most detailed set of data regarding mobile ad fraud and mobile malware available.

Mobile ad fraud and its partner-in-crime, mobile malware, are funneling billions away from businesses and consumers. Everyone loses from this activity. While advertisers are the most obvious targets of mobile ad fraud, the mobile user is arguably getting hit the worst. The many millions of users with malware-infected Android devices are having their mobile experience destroyed with fraudulent sign-ups to digital services, prepaid credit being stolen, reduced battery life, over-heating devices and more. Inevitably, mobile operators are then left to pick up the pieces, dealing with confused and angry subscribers that wrongly identify their operator as the problem.

55% increase in malicious apps blocked in 2019 compared to last year

43 million malware infected devices identified across 20 markets in 2019 alone

32 out of 100 most malicious Android apps are still available in Google Play Store

[9] 4shared, a popular file-sharing app, Vidmate, a video downloader, Weather Forecast a preinstalled app on Alcatel devices, Snaptube, another video and audio app, and ai.type, an on-screen keyboard app.

What Android users can do to protect themselves

Mobile ad fraud is growing in frequency and sophistication. To avoid falling victim to mobile ad fraud, Android users should regularly check their phones to see if they have a suspicious app installed. If so, they should uninstall it immediately and review any recent mobile airtime charges for possible fraud. In most cases, only installing Android apps from Google Play is a good rule of thumb – but even apps from legitimate sources can be compromised. Before making an installation, users should check the app's reviews, developer details and list of requested permissions, making sure that they all relate to the app's stated purpose.

Considering that fraudsters operate at scale and can simultaneously target millions, tens of millions or even hundreds of millions of devices in one hit, the means to stop them in their tracks need to likewise operate at scale. As no entity in the mobile ecosystem remains unaffected, the solution to eliminate the problem of mobile malware and mobile ad fraud requires a concerted approach, where all actors of the ecosystem work together.

Increased mobile security urgently needs to rise up in the industry's priority list, a need underlined by the growing sophistication of disguised malware calling for continuous technological innovation. A crucial part of the fight against mobile ad fraud and malware is awareness, which not only mobile users but, surprisingly, a large part of the industry lacks. To this end, information security experts have a key role to play by steadily and openly sharing their proprietary findings on mobile ad fraud and malware with the whole community in order to raise awareness and increase preparedness.

In short, Google, handset manufacturers, mobile operators, content providers and aggregators, app developers, advertisers, ad networks and anti-fraud technology providers need to recognize the scale of the problem and act to tackle it head-on.

No one in the mobile ecosystem remains unaffected from mobile malware

Increased mobile security needs to rise up in the industry's priority list

About Secure-D

Upstream's security platform Secure-D combines machine learning algorithms with payment processing workflows to protect app publishers, mobile operators and their subscribers against online transaction fraud and data depletion, caused by all types of malware and other online threats. In 2019 alone, Secure-D processed over 1.7 billion mobile transactions, detected and blocked nearly 98,000 malicious apps across 20 countries.

secure D

www.secure-d.io

About Upstream

Upstream is a leading mobile technology company providing 1.2 billion people in developing countries with affordable and secure access to digital services on their mobile devices. Integrated with over 60 mobile operators, across more than 45 high growth markets, Upstream leverages their unique assets to boost their digital revenues and speed up their growth.

upstream

info@upstreamsystems.com
www.upstreamsystems.com