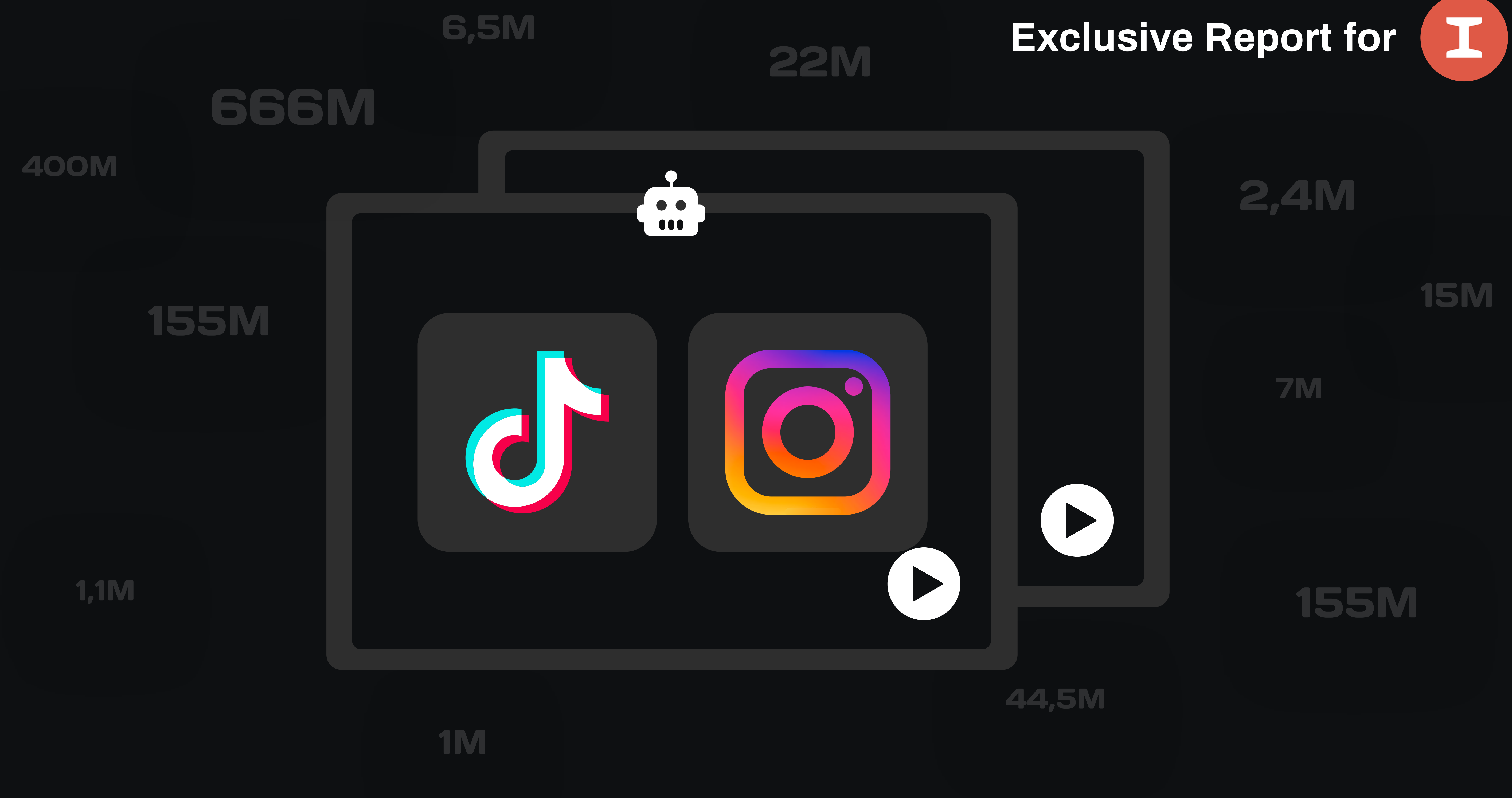
Exclusive Report for



Spambots, fake video views

and other issues on

TikTok & Instagram

Authors:

Andrea Stroppa
Bernardo Parrella
Danny di Stefano

DESIGN
Radek Skrzypczak

Rome, New York 12 June 2020

1.
INTRODUCTION

TikTok's popularity is skyrocketing particularly among teenagers. The latest stats cannot lie: 800 million users worldwide, 1.5 billion downloads[1]. As detailed in our October 2019 study published by the Washington Post[2], Tiktok is becoming a global force and it is now a strong Instagram competitor.

During the coronavirus lockdown, downloads of TikTok saw a sharp increase particularly in India[3], while its US unique visitors jumped up nearly 50% since January[4].

Overall Tiktok topped a new record with 315 million downloads (on App Store and Google Play combined) for the first 2020 quarter[5]. According to The Guardian, people confined in their homes are choosing TikTok to broadcast their own creative productions[6].

In the meantime, the company is trying to improve its reputation after receiving some inquiry requests from the American government, in addition to several inquisitive media reports – such as the one on the Washington Post with our substantial contribution[7].

[1] https://www.oberlo.com/blog/tiktok-statistics

[2] https://ghostdata.io/report/Instagram_TikTok_GD.pdf

[3] "India's lockdown is making life hard for its most popular apps", Manish Singh, Techcrunch, April 14 2020 https://techcrunch.com/2020/04/13/popular-apps-download-and-revenue-take-a-hit-in-india-as-people-stay-home

[4] "US Consumers Are Flocking to TikTok", Debra Ah Williamson, eMarketer, April 27 2020 https://www.emarketer.com/content/us-consumers-are-flocking-to-tiktok

[5] "Q1 2020", Sensor Town, March 2020 https://go.sensortower.com/rs/351-RWH-315/images/Sensor-Tower-Q1-2020-Data-Digest.pdf

[6] " How coronavirus helped TikTok find its voice ", Sirin Kale, The Guardian, April 26 2020 https://www.theguardian.com/technology/2020/apr/26/how-coronavirus-helped-tiktok-find-its-voice

[7] "Inside TikTok: A culture clash where U.S. views about censorship often were overridden by the Chinese bosses ", Drew Harwell, Tony Romm, The Washington Post, November 5 2019 https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/

TikTok now provides a transparency report on requests from governments to remove contents and/or accounts. A step that came with its own problems[8], while waiting for a promised full-fledge Transparency Center . Also available are some much needed parental control options[10], while now users can donate to non-profit and charity organizations directly within the app[11].

Since popular creators are paid to promote certain hashtags, TikTok is attracting a broad range of users while trying to navigate "uncharted" ad markets – as explained in a recent Bloomberg story[12]. TikTok exponential growth in early 2020 also gave way to controversial tools and options, such as spam bots and fake engagement trends, often promoted by unscrupulous or dubious sources.

In the meantime, Instagram continues its consolidation in the shopping online[13] sector, while at the same time expanding its user features with new stickers and improving the integration of AR filters[14]. This greater customizability and a newly announced revenue share program for its creators[15] will surely expand its user base, thus further affirming Instagram as a true Facebook's jewel.

Given this on-going battle for stardom in today's social media platforms, it is important for the public at large to better understand limits and benefits of such rapidly evolving environments. That's the main goal of our independent research projects, mostly focused on Instagram since 2016.

[8] "TikTok's First Transparency Report Doesn't Tell the Full Story", Louise Matsakis, Wired, January 3 2020 https://www.wired.com/story/tiktok-first-transparency-report/

[9] "TikTok to launch Transparency Center for moderation and data practices", Vanessa Pappas, Tiktok, 3 March 2020 https://newsroom.tiktok.com/en-us/tiktok-to-launch-transparency-center-for-moderation-and-data-practices

[10] "Q1 2020", Sensor Town, March 2020 https://go.sensortower.com/rs/351-RWH-315/images/Sensor-Tower-Q1-2020-Data-Digest.pdf

[11] "TikTok to launch parental controls globally, disable direct messaging for users under 16", Sarah Perez, Techcrunch, April 16 2020 https://techcrunch.com/2020/04/16/tiktok-to-launch-parental-controls-globally-disable-direct-messaging-for-users-under-16/

[12] "TikTok Marketers Chase Billions of Views in Uncharted Terrain", Sarah Frier, Kurt Wagner, Bloomberg, 27 February 2020 https://www.bloomberg.com/news/articles/2020-02-27/tiktok-marketers-chase-billions-of-views-in-uncharted-terrain

[13] "Introducing Facebook Shops: Helping Small Businesses Sell Online", Facebook https://about.fb.com/news/2020/05/introducing-facebook-shops/

[14] "Instagram's AR filters are getting more dynamic", Lucas Matney, Techcrunch, May 27 2020 https://techcrunch.com/2020/05/27/instagrams-ar-filters-are-getting-more-dynamic/

[15] "Instagram will share revenue with creators for the first time through ads in IGTV", Ashley Carman, The Verge, May 27 2020 https://www.theverge.com/2020/5/27/21271009/instagram-ads-igtv-live-badges-test-update-creators

Therefore our studies covered controversial and less known aspects of Instagram activities, including bot proliferation, counterfeit goods, terrorism, propaganda and misinformation. Our reports were published on mainstream media outlets, such as The New York Times, Washington Post, Wall Street Journal, The Information, Reuters, Associated Press.

It is only natural that now our attention is re-focusing on issues specific to TikTok in the context of its upscaling competition with Instagram.

2.

SHORT DESCRIPTION OF TIKTOK (EX MUSICAL.LY) TECHNICAL FUNCTIONALITIES

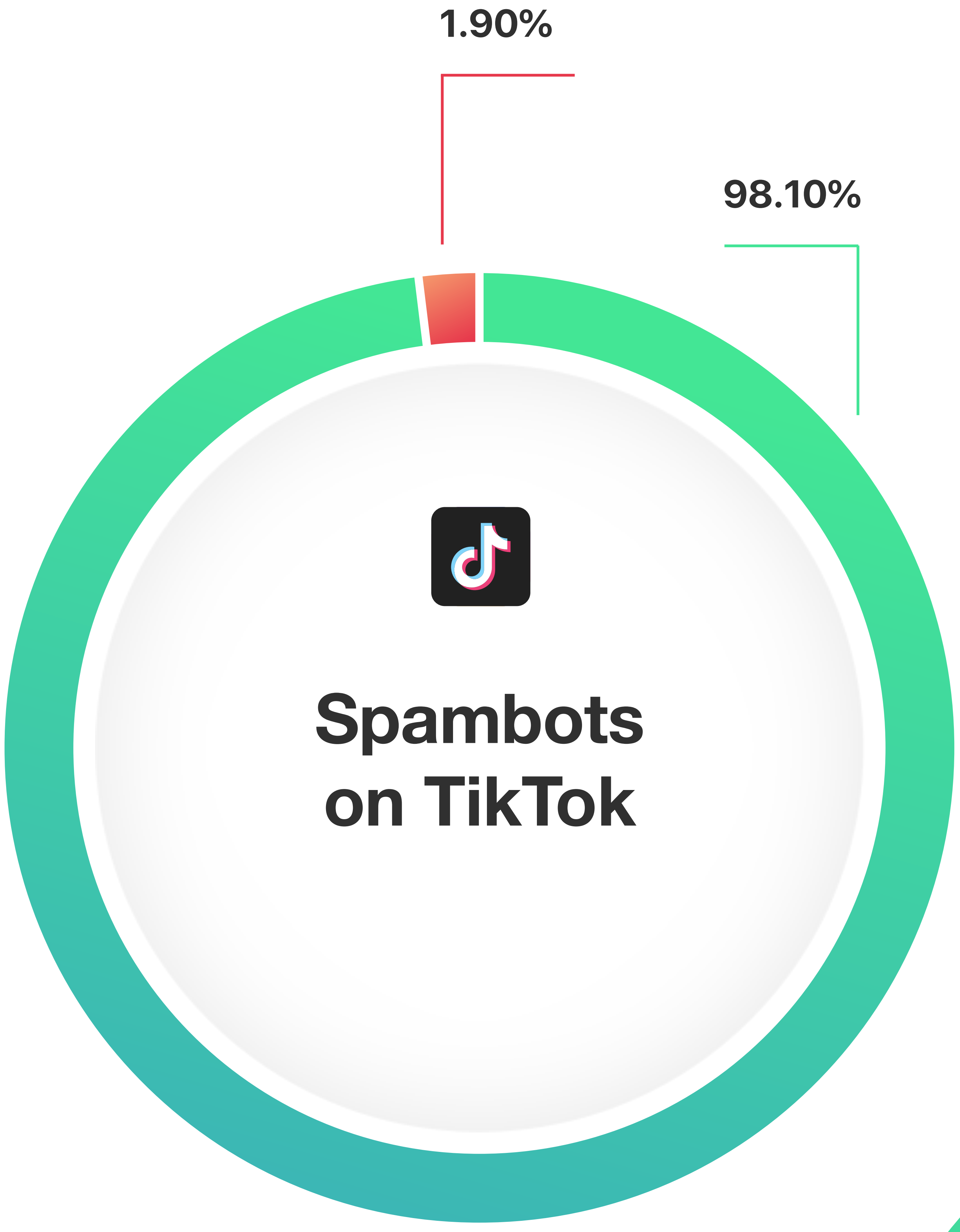
In mid-2018, TikTok aroused the interest of several IT security experts who, according to very few public sources knowledgeable with this sensitive matter, a complete reverse engineering of the app in order to understand its underline operative structure.

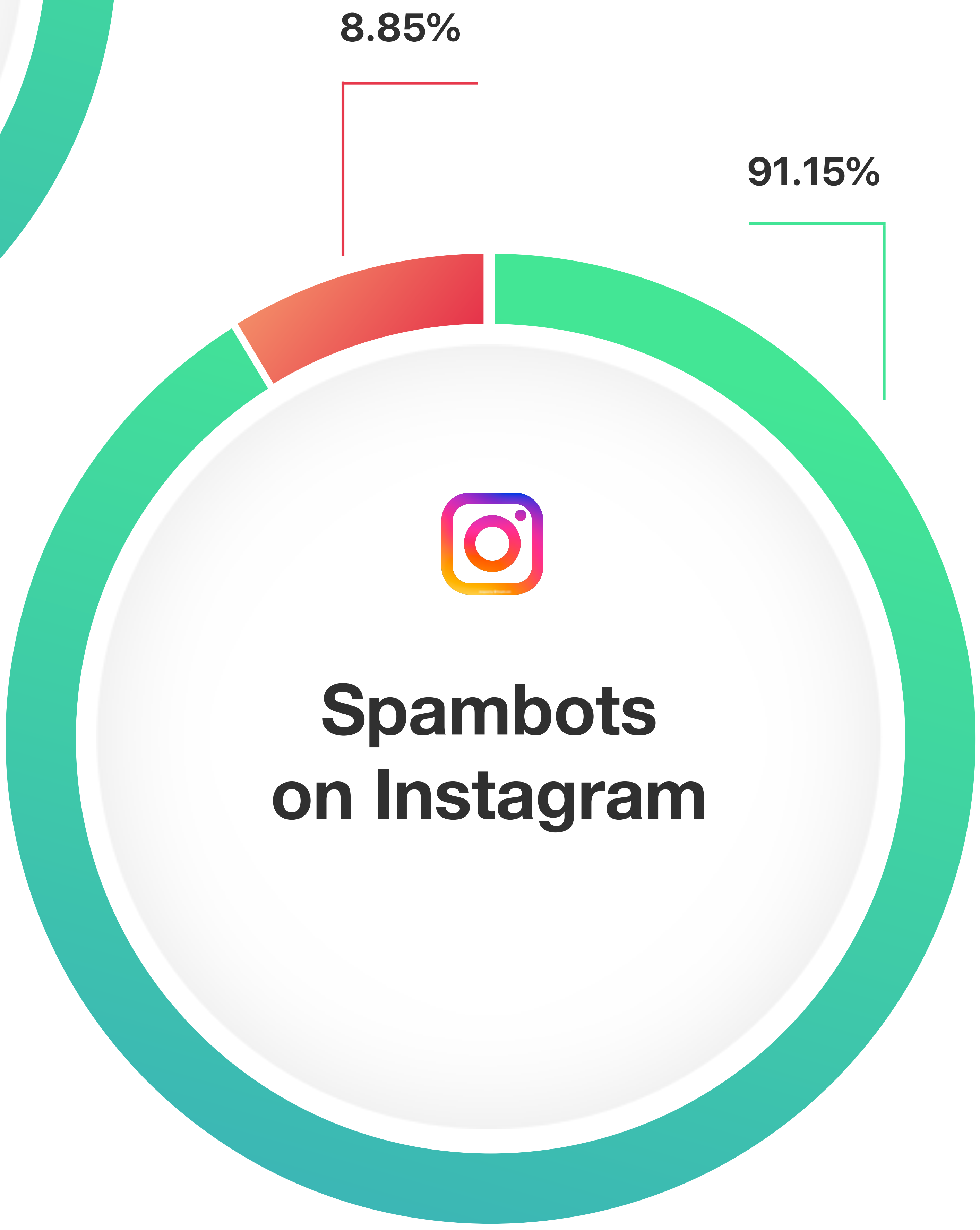
In August 2018 the mobile app known as Musical.ly officially became TikTok. Unlike Instagram that applies a standard encryption system, TikTok decided right away to step up its own technical safeguard and focused on a proprietary encryption system.

A little known curiosity is that TikTok programmers liked to insert in their code names related to Greek mythology, such as X-kronos e X-Gorgon. While X-kronos is a simple timestamp, X-gorgon is a more important token hiding information about a user's device and is used to validate a request validity.

Since 2018 TikTok has worked hard to constantly updated its app in order to prevent, at least for now, a widespread presence of spam-bots or fake accounts, thus avoiding a typical problem affecting Instagram.

Indeed, today most spambots developers on Tiktok could not produce software to easily create these botnets and/or accounts able to perform actions such as following a profile or automatically uploading a video. Usually these developers take advantage of Android device emulators to extract the token and perform certain actions, given their inability to completely reverse-engineer the app.





Spambot presence on TikTok and Instagram (2019)

3.

A BRIEF COMPARISON OF INSTAGRAM AND TIKTOK TECHNICAL FEATURES

Over the years Instagram has developed several artificial intelligence options in order to intercept spambots and block them. Several account verification options are also in place, such as cell phone text verification codes or IP validation, along with a limit on accounts registered from a single device.

Obviously enough, the purpose of these feature is to intercept in advance or to verify later on those activities that look as non-human behaviors. On the other hand, malicious actors try instead to create software able to mimic human behavior and thus to become invisible to those detection and verification features.

Instagram started to check on user IPs, particularly by searching for IPs that are part of a same subnetworks or IPs already known to be public or shared proxies. To avoid such detection, initially spambot creators started using dedicated Proxies (IPV4 / IPV6), then moving from datacenter proxies to residential proxies up to the latest 4G proxies. Instagram also provides checks about user devices and other parameters for the connecting network, including the autonomous system number, (ASN). However, using device emulators and/or the so-called "Private APIs" enable people to bypass these Instagram security checks.

Apparently TikTok applies fewer technical restrictions and a lower threshold for spambot creation and management. However, at a technological level there are still no cheap and scalable public solutions to activate a botnet.

As mentioned earlier, it’s probable that soon TikTok will also suffer from the same problems affecting Instagram, as soon as some kind of scalable and inexpensive system will allow developers to create functional and profitable botnets capable of mimicking human behavior.

4.
FAKE ACCOUNT FEATURES AND MARKET POTENTIAL

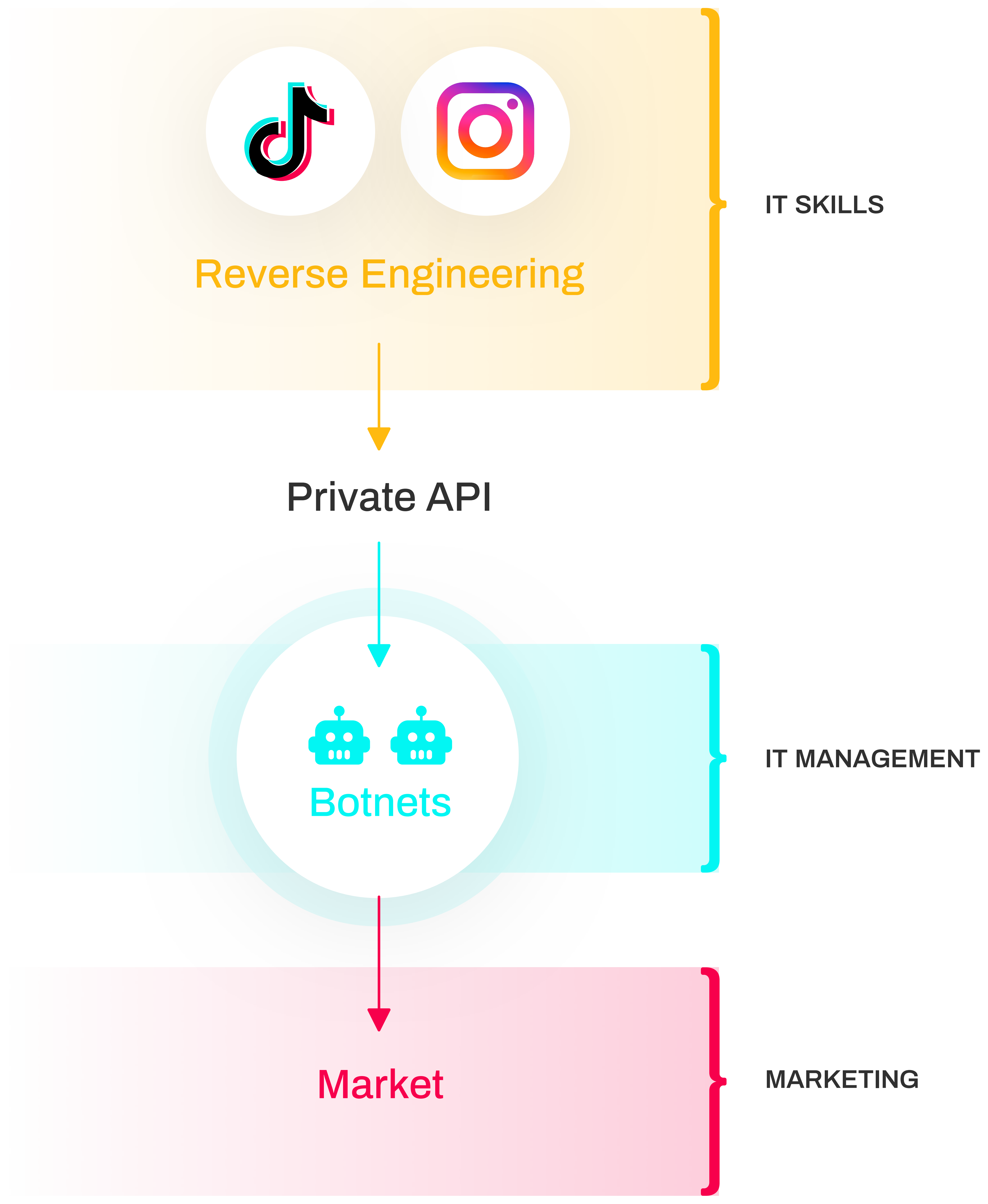
On Instagram the raw features (email, virtual phone numbers, proxies) necessary to activate fake accounts require a higher cost than what is needed on Tiktok. However, the technology to manage botnets on Instagram has a sustainable cost and it is publicly available, while on TikTok it is difficult to find and has higher management costs (server calculation capacity).

It is worth repeating that TikTok does not apply a strong level of email or cell phone verification in case of suspicious activities; it relies heavily on simple captcha features easily circumvented with anti-captcha programs[16].

On the other hand, Instagram provides several security checks (on devices, connection system and account behavior) that are activated when its automatic system detects suspicious non-human behavior (spam activities, suspicious or blacklisted IP).

[16] https://anti-captcha.com/mainpage

The market for these services is usually headed by reverse engineering experts quite familiar with Instagram and Tiktok app. Experienced developers can also create Private APIs to perform such operations as creating user accounts. Then the IT management team takes care of daily activities for multiple accounts (botnets). Finally the marketing people are in charge of promoting and selling these services.

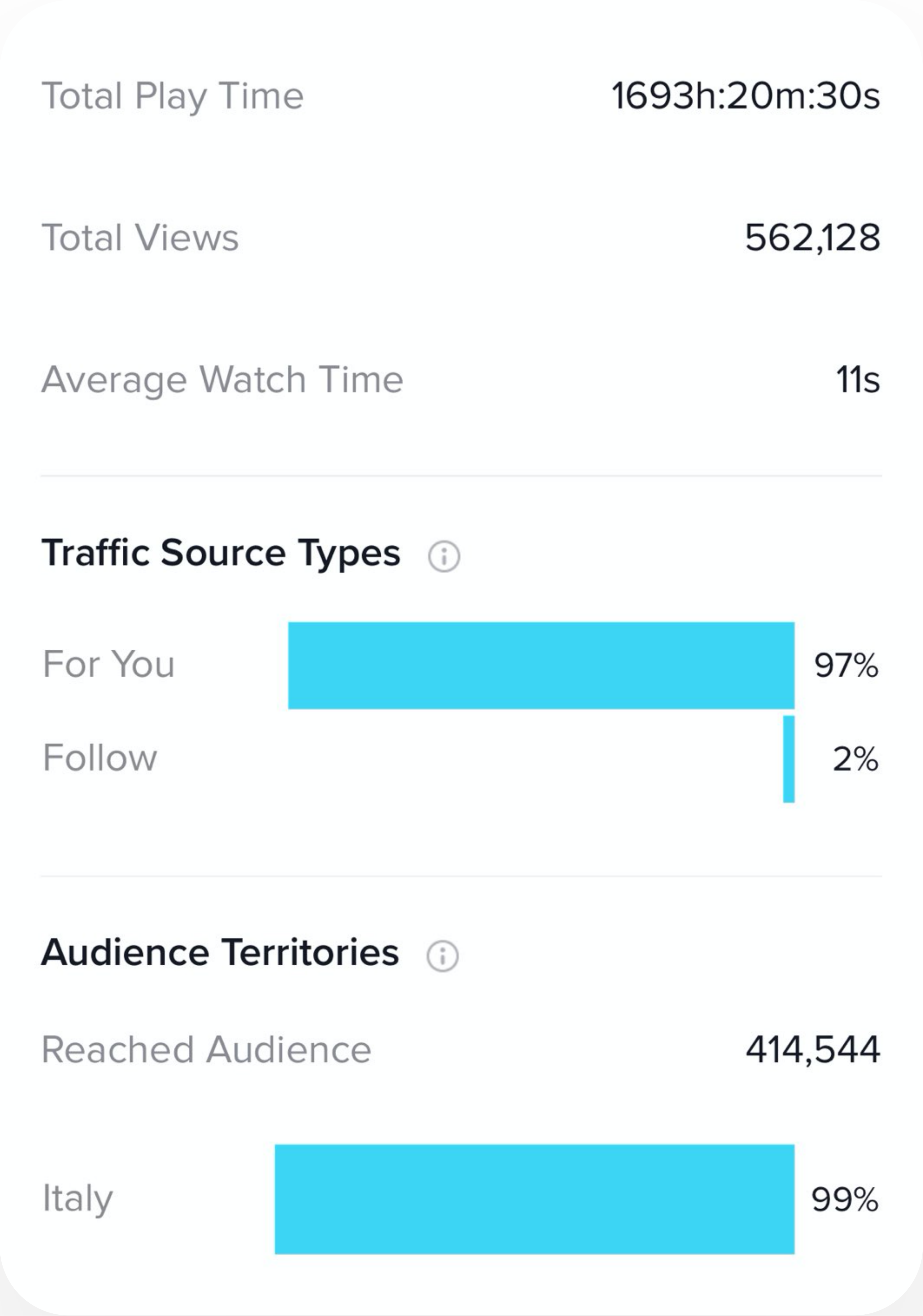


Obviously, not everybody dealing with reverse engineering or Private APIs have malicious and/or commercial goals in mind. There are countless examples of both practices for academic, well-accepted purposes for the tech community at large (research and reporting on bugs, vulnerabilities, etc.).

5.
MANAGING VIDEO VIEWS ON TIKTOK

Although not publicly known, TikTok views are counted differently from other social networks. The number and percentage of views shown are not from unique visitors, but just generic views. This means that a same user can watch a video 50 times and the counter will still grow to 50. Currently it seems there is no total or temporal limitation on how many views a user can generate on his/her video.

The analytics system of each TikTok profile, which can only be activated through an automatic procedure pointing to the "Pro Account", provides also other metrics relating to a certain video.



Total Play Time	1693h:20m:30s
Total Views	562,128
Average Watch Time	11s

Traffic Source Types

For You	97%
Follow	2%

Audience Territories

Reached Audience	414,544
Italy	99%

6.
MANAGING VIDEO VIEWS ON INSTAGRAM

In comparison to TikTok, Instagram is much more transparent and view counting is spelled out:
“A video's view count doesn't include video loops, and a view is counted when a video is watched for 3 seconds or more.
Keep in mind that view counts will only show up on videos that were uploaded after November 19, 2015.”[17]

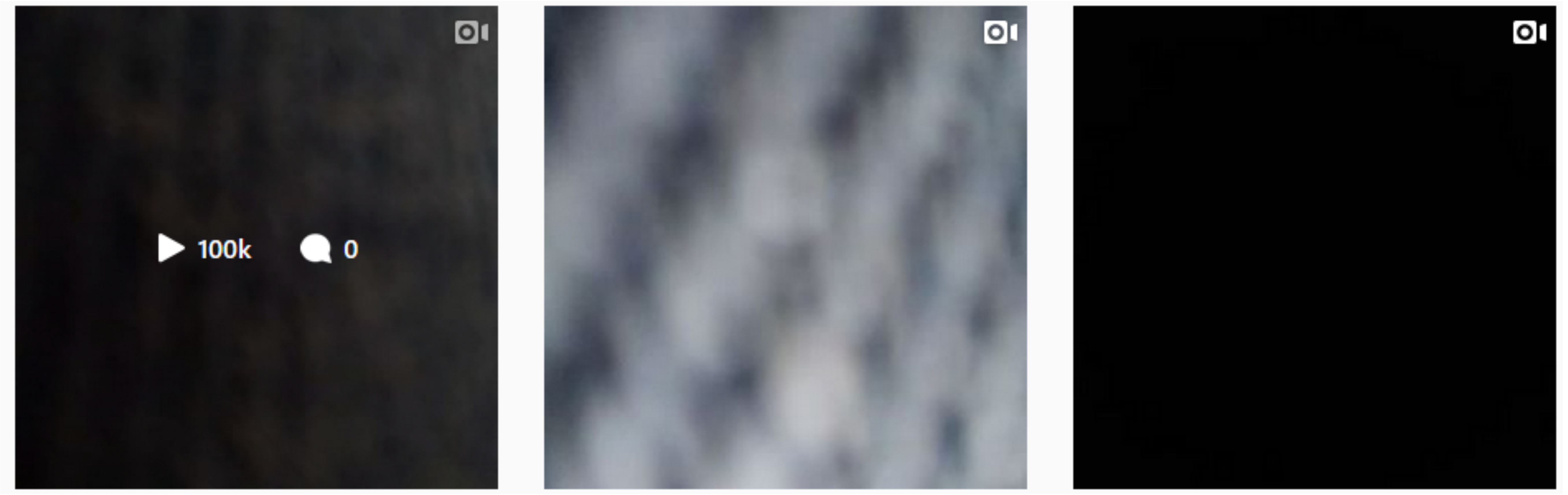
[17] https://help.instagram.com/551909181643223

7.

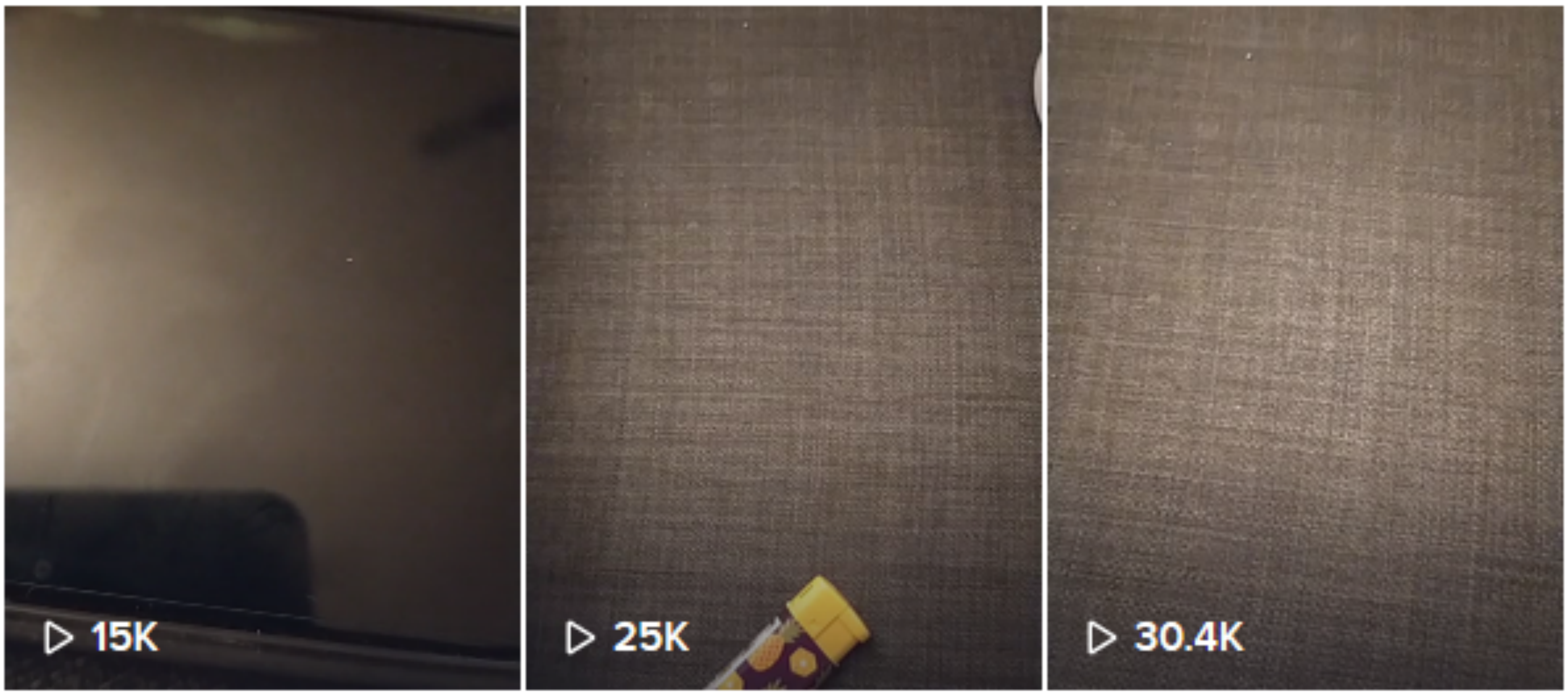
OUR TEST DRIVE

We decide to set up three different tests for each platform. We uploaded three videos on both TikTok and Instagram with no hashtag. The accounts used have zero followers.

Here are our videos uploaded on Instagram:



The following are our videos uploaded on TikTok:



8.

BASIC RESULTS AND TECHNICAL DIFFERENCES

Both on Instagram and on Tiktok, we used a third party managed software to generate the following view stats for each of the test videos. These view counts are therefore "fake".

	Instagram	TikTok
Video1	3555	30400
Video2	20045	25000
Video3	100085	15000

After uploading our videos, we waited for 7 days in order to monitor the ability of Instagram and TikTok detection systems to locate and remove those fake view counts. Both detection systems have failed to detect the views generated by the software.

9.
BOT VIDEO VIEWS ON INSTAGRAM VS TIKTOK

In addition to public data (i.e., the counters of public profiles), we also monitored the happens in the app analytics – the only tools available to users to properly understand their account performance.

The following chart shows that in both apps bots can generate video views, which are still visible from the outside after 7 days. This is also true for the analytics data.

We can therefore say that both TikTok and Instagram apps not only fail to recognize those fake views, but they even count them in their stat data.

A major difference is that, while Tiktok analytics cannot provide complete data on all metrics, on Instagram those bots are able to mimic human behavior and all metrics data are available – as summarized here below.

Metric	TikTok	Metric	Instagram
Total Play Time	N	Total Views	Y
Total Views	Y	Reach	Y
Avg Watch Time	N	Profile Visits	Y
Traffic Source Type	N		
Audience Territories	N		

10.

A "SAFE" AND PROFITABLE BUSINESS ON INSTAGRAM

As a matter of fact, the business of selling fake views is very safe and effective, unlike selling fake followers or interactions (likes, comments, shares). This mostly due to unimpressive detection systems, particularly on Instagram. It seems that for years Instagram has been busy blocking web and mobile apps deploying the "follow-unfollow"[18] technique that generates interactions to quickly grow an Instagram account. On the hand, just watching videos in other profiles is certainly a passive use much more difficult to differentiate when run by a legitimate user or instead by a fake bot.

This also appears to be a safe business. It is true that Instagram checks and temporary blocks those accounts following too many people in a short period of time (a somewhat suspicious behavior). But apparently there are no relevant limitations for actual users (and therefore for bots properly mimicking human behavior) that spend their time watching a lot of videos on the platform.

[18] "Instagram kills off fake followers, threatens accounts that keep using apps to get them" , Josh Constine , Techcrunch, November 19 2018, https://techcrunch.com/2018/11/19/instagram-fake-followers/https://techcrunch.com/2018/11/19/instagram-fake-followers/

11.
MARKET ESTIMATES FOR FAKE VIDEO VIEWS

According to eMarketer, Facebook earns billions of dollars annually through video advertising and promotion[19]. Being a video-only based app, TikTok is poised to profit even more in this market[20]. Therefore it is not surprising to learn that, as first reported by the Wall Street Journal and then confirmed by Facebook execs, in the last two years the social media giant has regularly inflated its video stats[21].

Our simple test exposed that both TikTok and Instagram have a serious problem with their fake views.

Also, in a March-May 2020 study of the "black market" we have identified over 80 groups or individuals that provided false view counts for TikTok and Instagram.

While on TikTok the maximum number of fake views on a single video can be reasonably set at about 10 million, we estimate that over 55 million fake views can be purchased on Instagram on a single video content. These are conservative estimates: we specifically excluded botnets of cyber-criminals and/or groups that do not publicly advertise their services about fake view counts.

While on TikTok the views are currently available only for posts and not for streaming, on Instagram fake views are sold for posts, direct streaming, the IGTV format and Stories as well.

[19] "Social Networks' Video Ad Revenues Balloon", eMarketer, https://www.emarketer.com/content/us-social-video-ad-spending-will-reach-11-69-billion-by-2020

[20] "Social Networks' Video Ad Revenues Balloon", eMarketer, https://www.emarketer.com/content/us-social-video-ad-spending-will-reach-11-69-billion-by-2020

[21] "Facebook Overestimated Key Video Metric for Two Years", Suzanne Vranica, Jack Marshall, The Wall Street Journal, September 22 2016 https://www.wsj.com/articles/facebook-overestimated-key-video-metric-for-two-years-1474586951?mod=article_inline&mod=article_inline

It is worth noticing that our 2018 research study, exclusively published by The Information, already identified up to 95 million fake bot accounts on Instagram. Even if in the past Instagram, through its owner Facebook, denounced several businesses selling "likes" and "followers"[22].

[22] "Cracking Down on the Sale of Fake Accounts, Likes and Followers", Facebook Inc, March 1 2019 https://about.fb.com/news/2019/03/sale-of-fake-accounts-likes-and-followers/

12.
CONCLUSIONS

Since 2016 the issue of fake video views has emerged in parallel with the bot market growth. According to a Bloomberg story[23], in 2019 Instagram earned more than YouTube with advertising sales.

While Instagram introduced various security features to locate and block bot accounts, there is still a lack of transparency about the quantity of bots currently active (and/or estimated) and its analytics system.

The flaws we identified are very well known in the botnet market and are detrimental to legit advertisers. There is no way for them to correctly differentiate credible video views from those due to fake bots or techniques. As described earlier, right now this "business" seems to proceed quietly under the radar: a more proactive approach by Instagram itself is clearly needed.

Instead TikTok made considerable efforts to keep its platform "clean". As a result, its fake view statistics are quite low as compared to Instagram's. The ability to mimic and falsify all video metrics data is limited to more sophisticated actors, even if undeniably an "underground" market exists for TikTok as well.

This short study seems to support our previous research on controversial aspects of top social media apps, particularly those carried on Instagram. The results show once again that these companies do not pay enough attention to data credibility and transparency, thus damaging all users and especially their advertisers. Facing an increasing market share and user behavior reliability, though, we should expect that these flaws will soon be addressed once and for all.

[19] "Instagram Brings In More Than a Quarter of Facebook Sales", Sarah Frier, Nico Grant, Bloomberg, Feb 4 2020 https://www.bloomberg.com/news/articles/2020-02-04/instagram-generates-more-than-a-quarter-of-facebook-s-sales