Analysis of the Malicious Bots Market

Maxim Kolomeets, Andrey Chechulin
St. Petersburg Federal Research Center of the Russian Academy of Sciences
Saint-Petersburg, Russia
{kolomeec, chechulin}@comsec.spb.ru

Abstract—**Social media bots can pose a serious threat by manipulating public opinion. Attempts to detect bots on social networks have resulted in bots becoming more sophisticated. A wide variety of types of bots has appeared, which must be taken into account when developing methods for detecting them. In this paper, we present the classification of the types of bots, which we made after analyzing the offers from bot traders in the market. We studied 1657 offers from 7 companies for 5 social networks: VKontakte, Instagram, Telegram, YouTube, and TikTok. Based on this information and descriptions from bot-traders, we are aggregating the types of bots and their key features. We also perform price analysis for different types of bots for the Russian Internet segment. The results show that the main pricing factors are bot action and bot quality. At the same time for different social networks, they affect pricing in different ways. Also, for messengers and social networks in which recommendation algorithms take into account complex actions more strongly, there is a tendency for higher quality bots to perform more complex actions. While in other social networks, the complexity of the action and the quality of bots are not correlating. The results of this study can be useful for developers of tools for detecting bots and determining the cost of an attack.**

I. Introduction

Social networks have changed the internet and our society. As platforms for information exchange, they have brought the whole world together so much that even a distant event is perceived as something personal. According to the latest polls [1], [2], a significant part of society draws information from social networks, preferring them to television, newspapers, and other classical media. This trend is growing from year to year [1] and is not expected to reverse. Along with the popularity, the trust in social networks as a source of information is growing too. This phenomenon can be easily explained by the ”all-permeability” and ”speed of distribution” of information. Anyone with a smartphone can become a source of information at the click of a camera while disseminating information takes minutes. This is an opportunity to receive news first-hand, bypassing media companies, newspaper editors, and censors.

Social media has influenced our world and the Internet for the better by making it more transparent. But the same information dissemination mechanisms can be used to manipulate opinion, spread misinformation [3], spread rumors and conspiracy theories [4], create a fake reputation, fraud, and even suppress political competitors [5], [6]. The world has not yet developed universal mechanisms for the dissemination and identification of malicious information on social networks. Damage can be done to anyone who acts on a social network platform: social media, a third-party company, civil society, or government.

At the same time, social networks have a simple, built-in, and self-organizing defense mechanism – institutional reputation, which is based on social network metrics (views, likes, etc.). Low-trust accounts cannot effectively disseminate information. Therefore, to effectively spread misinformation, the attacker either needs to enlist the support of someone with a huge following (influencer) or use bots to simulate metrics of social networks.

That’s why bot detection on social networks is one of the most requested security functions from commercial companies and law enforcement agencies.

Existing bot detection approaches are based on machine learning [7], [8]. Machine learning models are trained on the features that are extracted from bots and real users: information from a profile; graph structures of friends; written texts; uploaded photos and videos; etc. As a result, such bot detection methods are highly dependent on the quality of the training datasets. After all, different bots can use different strategies for generating features. Therefore, for the development of high-quality bot detection models, the training dataset must include a variety of bot types.

Attempts to perform typing of bots have been made earlier. Bot typing has already been done in several papers for bot-detection [8]. For example, in paper [9] described strategies for controlling bots by software, human and hybrid approach. Bots classification by types of threats is presented in [10]. The analysis of bot prices is well presented in the report [11].

In this paper, we propose the classification of bots through the market. We have collected information on 1657 offers of bot services from 7 companies for 5 social networks. Based on this information and descriptions from bot-traders, we are aggregating the types of bots and their key features. We also perform price analysis for different types of bots.

Thus, the goal of the paper is to build a classification of bot types by investigating offers from bot-traders. This classification will be useful for understanding the diversity of bots, which can be useful for obtaining high-quality training datasets.

The paper consists of the following sections. In **Classification of bots threats** we describe the types of threats that bots can pose. In **Classification bot types** we describe the types of bots, their characteristics, and strategies for bot creation and bot management. In **Methodology of data collection, pricing analysis and implementation** we’ll explore bot pricing for 5 social networks: VKontakte, Instagram, Telegram, YouTube and TikTok. In **Discussion** we discuss the correlations of bot characteristics. In **Conclusion** we summarizing results and presenting plans for future work.

The proposed bots threats and bots types we built based on papers [8], [10], [11], and (to a greater extent) based on the analysis of the bot market, which we performed ourselves.

II. Classification of bots threats

As part of our research, we consider bots that pose security threats. Of course, not all bots are malicious. For example, bots that provide weather forecasts, generate memes, provide store services and so on are harmless.

In this paper, we only consider malicious bots. To do this, we identify a malicious bot through the types of threats.

There are many threats on social media, including password leaks, use of private data by third-party companies, compromise of personal correspondence, etc. But in this paper, we focus only on those threats that can be implemented using bots. We distinguish 3 classes of threats:

1) Fraud – deceiving social media users to get money or private information. Fraud occurs through correspondence with the user. For example, bots can collect private photos on dating services for blackmail, or the data needed to bypass the bank and mail security systems based on security questions. If such bots have AI and can automatically conduct conversations, this will cause serious damage to tens of thousands of users. Even if the success rate is low, they can fraud a large number of people simply by scaling the botnet.
2) Promotion of harmful or censored information – propaganda of information that was prohibited by social network platform (heat speech, trolling, etc.) or was prohibited by the government (terrorism, incitement to violence, etc.) Depending on the goal of the attacker it can be integrity – if the goal is to exacerbate the conflict and violate the integrity of the community or accessibility – if the goal is to drown alternative viewpoints with spam.
3) Rating manipulation – overestimating the rating to increase user confidence. For this, social network metrics are faked - the number of likes, friends, reviews, etc.

The implementation of these threats by bots requires one key quality from them - *malicious bots pretend to be real people* because it is a key component of user trust.

A person will not believe a fraudster if the account does not look like a real person. Real users will be skeptical about rumors spread by bots. And, of course, the customer will be suspicious of a store that has a lot of positive reviews from bots.

As we will show below, the similarity of a bot with a real person is the main property that the bots management is aimed at. Besides, the similarity of a bot to a real person is one of the main criteria for their pricing.

The complexity of creating bots that look like real people, as well as the difference in strategies for creating and managing them, creates many types of bots. We propose an analysis of the bot market, the understanding of which is necessary for people who are developing tools for detecting them.

III. Classification of bots types

To classify bots by type, we analyzed a variety of sites that trade bots. Bot traders provide 2 options – buy an account and manage the bot yourself, or rent an account (buy bot activity) and the bot trader will perform the necessary actions.

We analyzed offers from 7 bot trader companies that provide a bot rental service and 1 forum where bots are sold. The companies were selected from the Russian-speaking segment of the Internet, as we believe that this market looks more saturated. We analyzed **rental** offers on 5 platforms: VKontakte, Instagram, Telegram, YouTube, and TikTok. We analyze account **sales** only for one platform: Vkontakte (because there is not enough sales data on other platforms compared to the number of rental offers). A total of 1,657 rental offers and 45 sales offers were studied. We also bought 9 offers to analyze bot metrics. More information about the dataset is available on its page [12].

We propose several classification systems that will describe the whole variety of commercial offers.

A. Characteristics of malicious bots

Each bot trader defines the bot classes differently over multiple parameters.

Bot stores introduced their parameter systems, many of which differed terminologically. For example, one store had a quality scale with terms such as: start, premium+, ultima, etc; and another store: low, high, medium; and the third store: standard, good, best. Some stores determined the speed of bots' actions in quantitative form, other stores - in qualitative, and third stores did not write about speed.

But the bot traders published detailed instructions on their sites on what these or those characteristics of bots mean. We have aggregated all of these instructions together to develop a common terminology system.

For buying and renting account parameters are:

1) Activity. Do the real owner (if applicable) of this account still use it? If yes, then the real owner can quickly notice the suspicious activity. Thus can happen if accounts with legal activity were compromised, but the attacker was unable to change the password.
2) Registration date. When the account was registered? Older accounts are more valuable and are less likely to be blocked than newer ones. Also, people's trust in new accounts is lower as they are relatively easy to register.
3) Phone number. What is the phone number the account binds to? If the account is not tied to the phone number, then the bot is often forced to enter a captcha (what can be a problem for an attacker if the bot is controlled by a program).
4) Location. What is country/region the account tied to and what the country/region of the person which it imitates

to be belong to? Bots imitating people from one location may seem suspicious to real users from another one.

5) Owner. Is it the real person (e.g. if the account was stolen) or a virtual phone number generated by the program? Also the important parameter is the number of owners – how many people can buy and use this account at the same time. An account can be obtained by hacking or fraud through the:
   - mail service (if the attacker gained access to mail and requests to restore access to the social network);
   - malware on PC or mobile phone;
   - spoofing through unsecured public networks (metro, hotels, etc.);
   - brute force password attack on social networks or mail service;
   - fraud, which involves the usage of social engineering through correspondence with the user.

For renting account bot traders also provide the next parameters:

1) Quality – an integral ranking of bot that expresses how much a bot looks like a human. Usually expressed as:
   a) ”Low” – the user can easily recognize the bot. Usually, the profile is empty, with no photos, few friends. It also includes active users who may notice that they have been hacked and the account is being used.
   b) ”Middle” – it is difficult for the user to recognize the bot. Usually the profile not empty, some photos, the average number of friends.
   c) ”High” – bot cannot be distinguished by profile analysis. Usually, these are accounts of real people who have lost or shared access to them (due to hacking or sale). But the bot can be easily recognized by its characteristics that change due to unnatural activity (illogical messages or reposts, unusual distribution of friends, etc.).
   d) ”Live” – accounts of real people (hacked and those who act for money). Unnatural activity is the only way to recognize a bot of this type.
2) Type of action – what action the bot needs to perform. We divided the types of activity according to the degree of attracting attention:
   - leaving no public digital footprints – e.g. views;
   - leaving public digital footprints that cannot be seen by visiting the bot page – e.g. likes;
   - leaving public digital footprints that can be seen by visiting the bot page – e.g. friends;
   - leaving a digital footprint of direct user interaction, difficult to implement in automatic mode – e.g. comment;
3) Speed of action – how quickly bots can take the required action. For example, how quickly can 100 bots write a comment. Usually measured in the number of activities per day. A spike in activity can trigger social media protection algorithms.

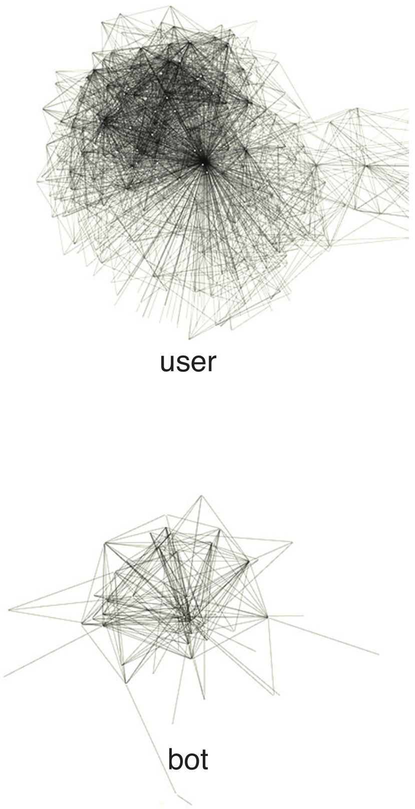

Fig. 1. The structure of friends is a small world for a real user, and the bot simulating a similar small world to disguise itself

B. Strategies for management and creation

Different bot stores provide different management strategies. Bots can be controller by:

1) Software – the bot actions perform automatically by some algorithms. For low, middle, and high quality bots. Usually for actions that can be implemented in automatic mode.
2) Operator – the bot is manually controlled by the operator. For high and live quality bots. Usually for actions that cannot be implemented in automatic mode.
3) Exchange platform – the bot is controlled by a real account owner who agrees to perform some actions for money. For high quality bots. Usually for actions that cannot be implemented in automatic mode.
4) Troll Fabric – SMM agencies employing professionals. The services of such companies are not public – therefore we did not find them. But we believe that they should be included in the list, as they are responsible for many attacks according to a lot of evidence.

Of course, to know exactly the characteristics of the account is possible only after its purchase. Nothing is stopping the bot trader from deceiving you, since this market is not entirely legal. Besides, different bot traders understand quality differently. But most of the parameters describe various aspects of the bot's similarity to a real person – quality.

By investigating bots and comparing them to real people on social media, we've identified the main ways bots try to disguise themselves as real people:

1) Use privacy settings. An attacker can fill in just a few fields (profile photo, name, and surname) and hide the rest with privacy settings. Since many users prefer to hide pages on social networks, this will not raise suspicion. This technique is used by a wide variety of bots - from low to high quality. According to our observations, live bots use privacy settings much less often.
2) Use account of a real person. An attacker can use a real person's account by hacking it or buying/renting it. Bot have live quality if a person is an inactive and low quality if active.
3) Generate profile. A difficult task that can include 3 techniques:
    - An attacker can try to generate profile fields. To do this, an attacker can fill an account with photos from another user who has this data open and randomly generate numeric and string parameters.
    - Attacker can generate photos and text content using neural networks. This approach allows the bot to pass the duplicate check (when we are looking for another account with the same photos). A neural network for writing text allows attackers to automate bots that work in chats. Depending on the filling of the account can vary from the middle to live quality.
    - Attacker can generate friendslist graph structure. Real users add people they already know to their friends, forming a small world. The likelihood that a real person will add an unfamiliar account is small. Therefore, it is difficult for a bot to form a list of friends from real users where everyone is connected. He can add random users - then they will be less likely to form at least some connected graph, or try to form the small-world structure of the friendslist from other bots (see Fig 1).

IV. Methodology of Data Collection, Pricing Analysis and Implementation

We carried out a pricing analysis and checked some correlations of parameters. The purpose of this analysis is to see how price, quality, and type of bot action correlate for various social networks. The information about the prices and parameters of the commercial offer will be sufficient for valid conclusions because the bot market obeys the same laws of the regular market, supply, and demand.

To do analysis, we have parsed HTML-pages with bots rental offers from 7 companies. In each rental offer, we determined:

1) the lot size – bot activity is sold in batches, for example, 1, 100, 1000, etc.;

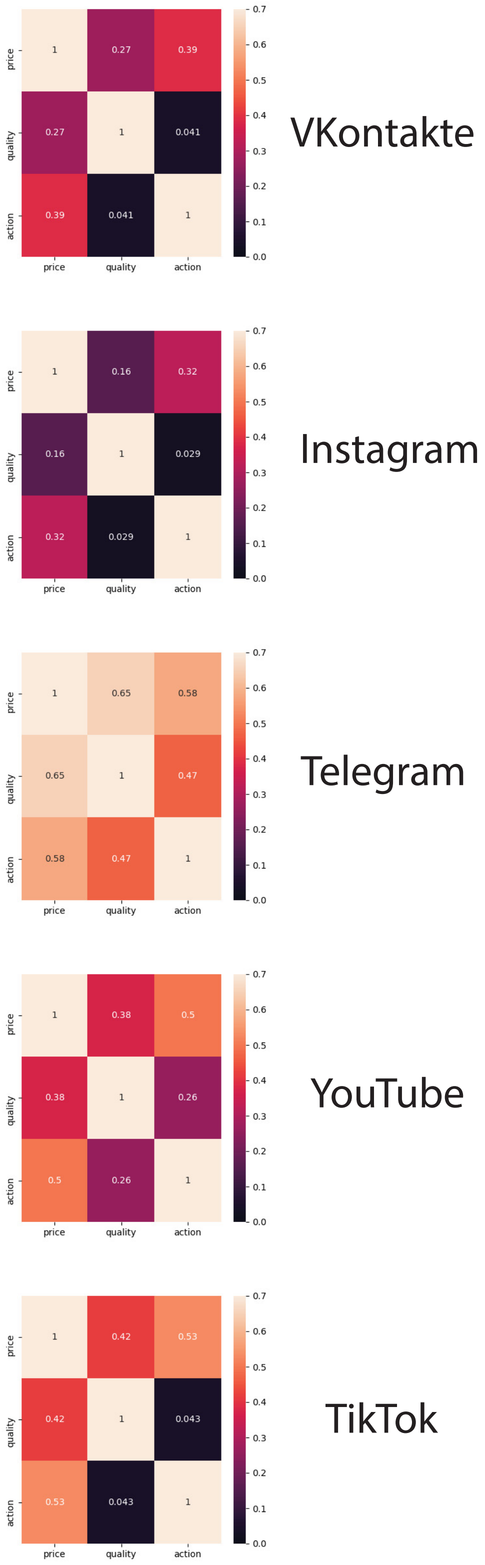

Fig. 2. Correlation between bot's quality, action type and price for different social networks

2) cost per unit – in cases where the price was indicated for a lot, we calculated the price for one bot;
3) social network – VKontakte, Instagram, Telegram, YouTube, or TikTok.
4) action – view (viewing post, photo, video, etc.), like, poll (cheat votes in a poll), repost, participate (subscribe to channel, group, etc.), friend, alerts (massive alerts for blocking content by a social network), comment.
5) quality — Low, Middle, High, and Live.

To mark up the dataset by action and quality, we looked for keywords in the description of the offer. For example, to include an offer in the low quality class, we looked for the words: ”low”, ”no avatars”, ”no guarantee”, ”slow”, ”possible activity”, etc. We did the same for the rest of the quality and action classes.

As the result we built 3 charts:

1) Figure 3 shows the bubble chart of bot pricing over quality and actions for different social networks. The size of the bubble indicates the price.
2) Figure 4 shows the scatter plot of bot pricing over actions for different social networks.
3) Figure 5 shows the scatter plot of bot pricing over quality for different social networks.

We also perform some correlation analyses.

To do this, we converted qualitative types to quantitative for actions (see table I) and quality (see table II). The conversion logic is based on the classifications that were presented before: actions that leave a more visible digital footprint have bigger values, and the quality increases linearly from low to live.

For each group of offers (the same social network, bot trader, quality, and action), we calculated the median price value. This is necessary because the same bot store usually sells services in lots. Thus, these are the same set of bots, and the price difference is due to the discount for buying a large lot.

The results of the correlation between these groups of offers are shown in Figure 2. We scaled the color scale from 0 to 0.7 (maximum correlation value excluding diagonal) for better perception of results.

Correlation shows how social networks’ features affect bot trading and bot diversity.

V. Discussion

As expected, for all social networks the price of bots depends on the quality and actions, but this dependence is not the same for different social networks.

Comments and alerts, as the most complex and attention-grabbing to the bot’s profile, have the highest price tag (Fig. 3 and Fig. 4). Views are the least expensive because they do not leave digital traces and are easily automated. This confirms the validity of the proposed classification.

For all social networks (except for Instagram), there is a dynamics of price growth depending on quality (Fig. 5). These dynamics are also noticeable in the correlation results. It can be seen that the dependence of quality on price is different for social networks. We attribute this to the effectiveness of algorithms and measures to combat bots. The more efficient the algorithms on a social network, the more valuable the difference between low and high quality bots becomes.

TABLE I. Qualitative scores to quantitative for bot’s action

action	quantitative score	action’s type (qualitative score)
comment alert	4	leaving public footprints which difficult to implement in automatic mode
friend participate repost	3	leaving public footprints that cannot be seen by visiting the bot page
poll like	2	leaving public footprints that can be seen by visiting the bot page
view	1	leaving no public footprints

TABLE II. Qualitative scores to quantitative for bot’s quality

quality (qualitative score)	quality (quantitive score)	description
Live	4	accounts of real people
High	3	the bot cannot be distinguished by profile
Middle	2	it is difficult for the user to recognize the bot
Low	1	the user can easily recognize the bot

There is also a noticeable correlation for Telegram and YouTube that better bots are used for more complex actions. For all other social networks, it is almost zero.

For Telegram, this is explained by the fact that Telegram is a messenger, where the main function is participating in chats, discussion, and comments. Therefore, Telegram has a clear demand for human-controlled bots that can write complex text.

For YouTube, this can be explained by changes in the promotion algorithms. YouTube has significantly increased the role of comment activity to promote videos with its recommendation systems. Thus, the demand for human-controlled bots that can write complex text has also increased.

TikTok and Instagram also have a function for writing comments. But in TikTok and Instagram, comments are meant to express emotions, not discussion. Thus, bots can leave emojis or some phrases from the dictionary of sentiments, which low and mid quality bots can also do.

This analysis allows one to better understand which bots are widespread in which networks, and speculate about possible features. This can be taken into account for the development of bot detection tools. For example, to detect bots on YouTube, it must be taken into account that comments are likely to be written by human-controlled bots. At the same time, on Instagram or TikTok it will be a more mixed group of bots.

VI. Conclusion

In this paper, we present the classification of the types of bots, which we made after analyzing the offers from bot traders in the market.

We have presented the parameters that the bot traders indicate and which affect bot pricing. We have presented a classification by type of action and by quality. At the same time, market analysis showed that the price of bots depends on the complexity of the action performed by the bot and the quality (similarity of the bot to a real person). But for some social networks, this dependence may be stronger than for others.

We also demonstrated that on some social networks, better quality bots perform more complex actions. While in others there is no such correlation.

This study makes it possible to obtain better datasets for training machine learning models that are used to detect malicious bots. To do this, training datasets must contain all the variety of bots, as well as their characteristics.

We plan to continue our research and consider what specific features (which are already used to train models) are most useful for detecting bots of various classes.

The dataset collected and marked up for this paper is available via the link [12].

Acknowledgment

This research was supported by the Russian Science Foundation under grant number 18-71-10094 in SPC RAS.

References

[1] Levada-Center, “Channels of information,” 2017. [Online]. Available: https://www.levada.ru/en/2018/10/12/channels-of-information/

[2] A. M. Elisa Shearer, “News use across social media platforms in 2020,” 2021. [Online]. Available: https://www.journalism.org/2021/01/12/news-use-across-social-media-platforms-in-2020

[3] C. Shao, G. L. Ciampaglia, O. Varol, A. Flammini, and F. Menczer, “The spread of fake news by social bots,” *arXiv preprint arXiv:1707.07592*, vol. 96, p. 104, 2017.

[4] E. Ferrara, “# covid-19 on twitter: Bots, conspiracies, and social media activism,” *arXiv preprint arXiv:2004.09531*, 2020.

[5] F. Pierri, A. Artoni, and S. Ceri, “Investigating italian disinformation spreading on twitter in the context of 2019 european elections,” *PloS one*, vol. 15, no. 1, p. e0227821, 2020.

[6] R. Faris, H. Roberts, B. Etling, N. Bourassa, E. Zuckerman, and Y. Benkler, “Partisanship, propaganda, and disinformation: Online media and the 2016 us presidential election,” *Berkman Klein Center Research Publication*, vol. 6, 2017.

[7] C. A. Davis, O. Varol, E. Ferrara, A. Flammini, and F. Menczer, “Botornot: A system to evaluate social bots,” in *Proceedings of the 25th international conference companion on world wide web*, 2016, pp. 273–274.

[8] M. Orabi, D. Mouheb, Z. Al Aghbari, and I. Kamel, “Detection of bots in social media: a systematic review,” *Information Processing & Management*, vol. 57, no. 4, p. 102250, 2020.

[9] C. Grimme, M. Preuss, L. Adam, and H. Trautmann, “Social bots: Human-like by means of human control?” *Big data*, vol. 5, no. 4, pp. 279–293, 2017.

[10] B. Oberer, A. Erkollar, and A. Stein, “Social bots–act like a human, think like a bot,” in *Digitalisierung und Kommunikation*. Springer, 2019, pp. 311–327.

[11] S. Bay *et al.*, “The black market for social media manipulation,” *NATO StratCom COE*, 2018.

[12] M. Kolomeets, “Security datasets: Bot market,” 2021. [Online]. Available: https://github.com/guardeec/datasets

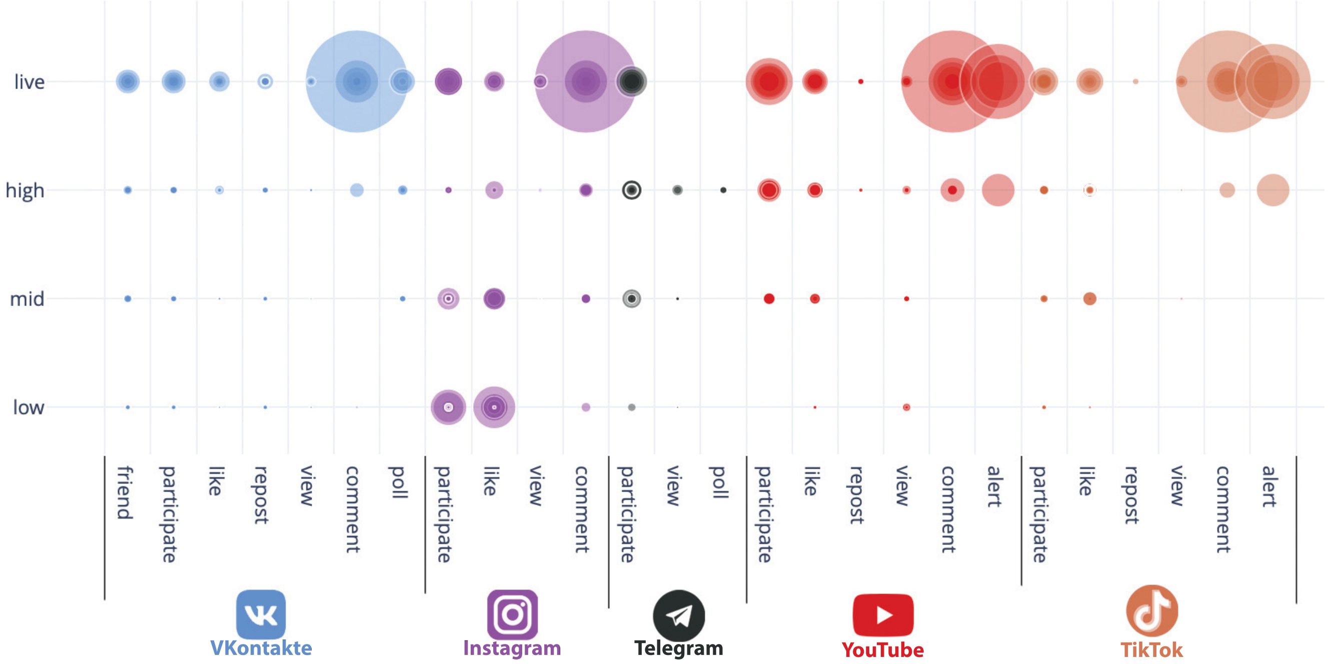

Fig. 3. Offers for renting bots with a certain quality and a certain action. Price expressed as bubble size.

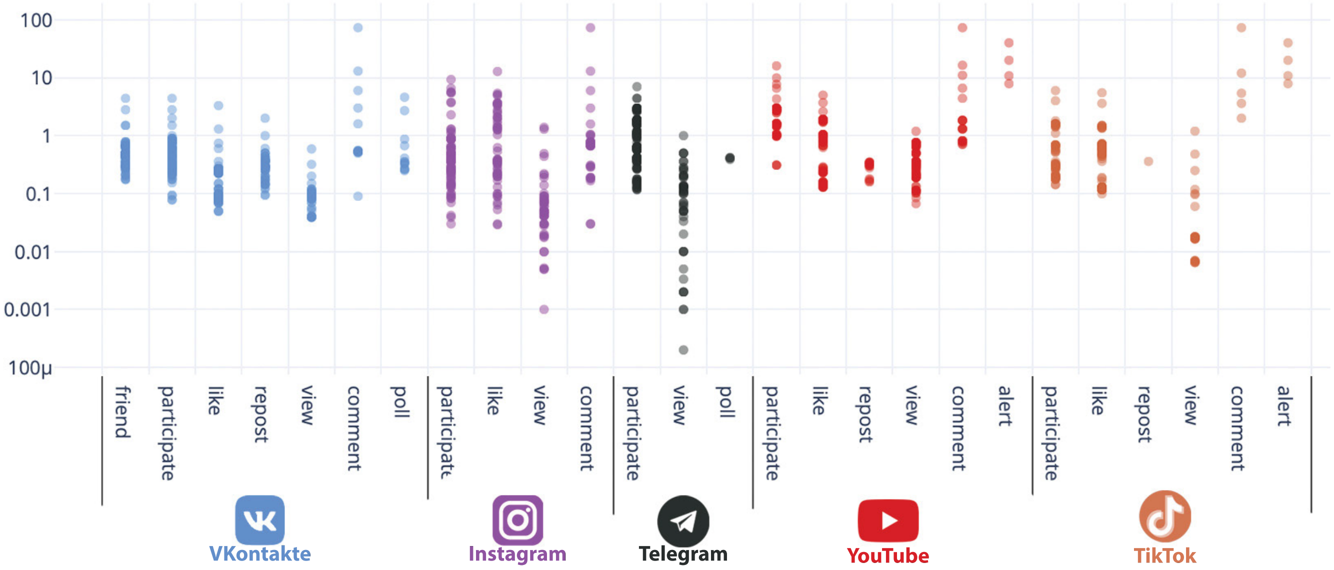

Fig. 4. Dependence of the action of bots on the price in rubles

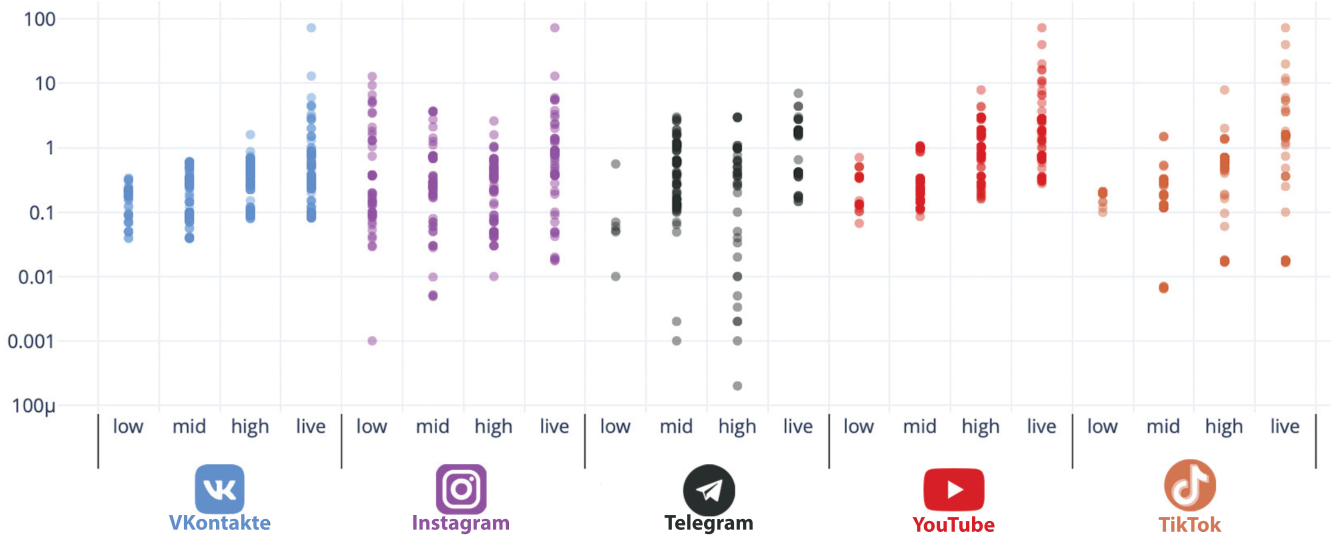

Fig. 5. Dependence of the quality of bots on the price in rubles