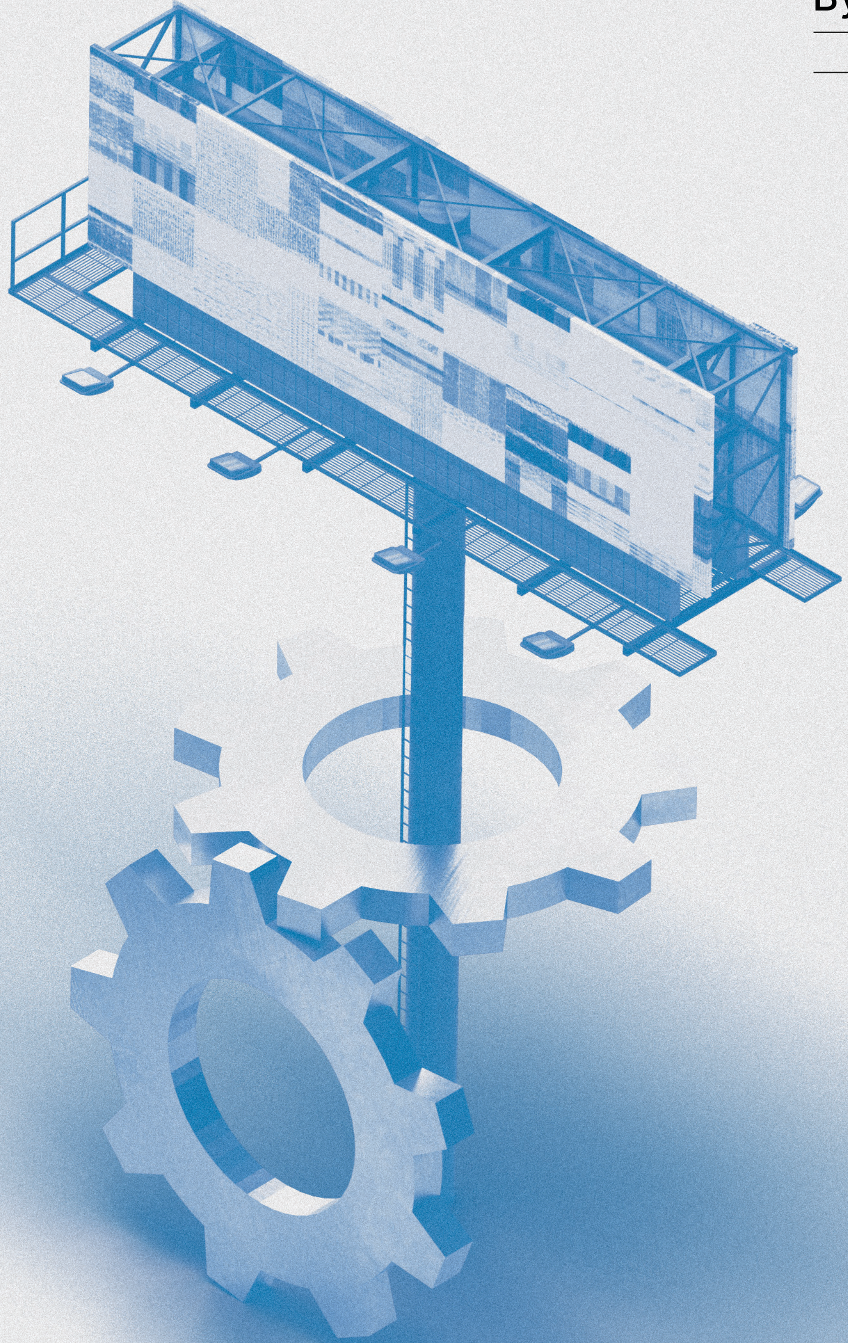
CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

November 14, 2023



Improving Automation and Accessibility Drive $100 Billion in Projected Ad Fraud Losses

Executive Summary

Automation enables cybercrime, and ad fraud is no exception. Ad fraud occurs when fraudsters artificially inflate the metrics used to measure ad performance for personal or financial gain. The advancement and growing accessibility of easy-to-use bot software and other automation solutions reduce the technical requirements necessary to conduct ad fraud. This dynamic lowers the barrier to entry for ad fraudsters, thereby raising the threat that ad fraud poses as well as its impact on various parties. Ad fraud directly impacts advertisers and publishers, whose advertising budgets ("ad spend") and ad revenue are respectively parasitized by fraudsters: according to Statista, losses from ad fraud are projected to reach $100 billion by the end of 2023. Ad fraud also damages the credibility of the ecosystem, raising the risk of brand impairment for ad tech companies and other intermediaries that enable programmatic advertising. More broadly, ad fraud's appeal and accessibility likely facilitate a convergence of threats, including for money-laundering, and fraudsters also exploit automated online advertising to facilitate card fraud-funded malvertising attacks.

To reduce the threat posed by ad fraud, stakeholders throughout the ecosystem should implement automated solutions to detect and prevent invalid traffic (IVT), ensure advertisers have access to the information they require to identify inefficiencies in ad spend, and employ threat intelligence to better understand and mitigate the ad fraud threat. Looking forward, the impact of ad fraud is likely to increase as a function of the size of the online advertising market as a whole, and artificial intelligence (AI) will likely play a larger role in both conducting and preventing ad fraud. Given these considerations, organizations that act as online advertisers or ad publishers should consider online advertising a holistic marketing, data-based, and cybersecurity effort and allocate their resources accordingly.

Key Findings

- Automation lowers barriers to entry for fraudsters, expanding the pool of threat actors who can conduct online fraud and other cybercrime at scale.
- Ad fraud must be conducted at scale — and by extension, using automation — to be profitable.
- Advancing automation capabilities and improved collaboration have lowered the technical barriers that fraudsters must overcome to conduct ad fraud and improved fraudsters' ability to avoid detection.
- Because ad fraud and the programmatic ad ecosystem are both highly scalable, improving automation likely contributes to the substantial impacts of ad fraud, which grow each year.

Background

Automation allows fraudsters and other cybercriminals to conduct their illegal activity more effectively, specifically by allowing them to increase the scale and speed of their operations. Similarly, automation solutions that are accessible — particularly in terms of resource and skill requirements necessary to operate them — lower barriers to entry for fraudsters and other cybercriminals. These automation solutions typically take the form of bots, which are essentially scripts capable of performing repetitive tasks.

Previously, Recorded Future has frequently analyzed fraudsters' use of bots and the risk posed by accessible automation solutions for fraud, including in the following reports:

- **On March 4, 2021, we reported on Magecart actors' use of Telegram bots to exfiltrate stolen payment card data.** After a Magecart e-skimmer stole victim card data from an infected e-commerce website, the e-skimmer script transmitted the stolen card data to a Telegram bot application programming interface (API) under the Magecart actor's control. Telegram bots provide Magecart actors with easily configurable attack infrastructure on a legitimate resource, which complicates the detection, remediation, and attribution of e-skimmer infections.
- **On April 1, 2021, we reported on fraudsters' use of Telegram bot shops to purvey stolen payment card data.** Bot shops on Telegram automate the sale and validation of stolen card data, and unlike dark web carding shops and marketplaces, fraudsters do not require specialized software to access them. Ultimately, Telegram bot shops allow card data vendors to reach a wider pool of buyers than is possible on the dark web.
- **On June 29, 2022, we reported on fraudsters' use of bots to steal one-time passwords (OTPs) and simplify their fraud schemes.** OTP bypass bots combine time-tested social engineering and vishing techniques with automation and easy-to-use interfaces, dramatically reducing the effort needed to steal victims' OTPs for online fraud and other cybercrime activity. As a result, these bots increase the scale of attacks that threat actors can conduct within a short period of time and expand the pool of threat actors who can conduct these attacks.

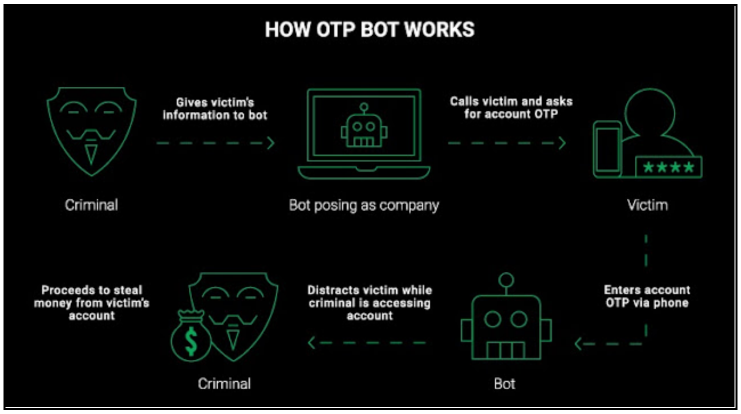

HOW OTP BOT WORKS
Gives victim's information to bot
Calls victim and asks for account OTP
Criminal
Bot posing as company
****
Victim
Proceeds to steal money from victim's account
$
Distracts victim while criminal is accessing account
Enters account OTP via phone
Criminal
Bot

Figure 1: *This workflow demonstrates how an OTP bypass bot can automatically facilitate a "man-in-the-middle" attack to steal victims OTPs, ultimately allowing threat actors to easily scale up their attacks (Source: GitHub)*

Threat Analysis

Fraudsters are also reliant on automation to conduct ad fraud in the programmatic advertising market. Programmatic advertising is a highly automated form of online advertising that relies on software and algorithms to determine what ads will be shown to which audiences and at what price. The underlying architecture of the programmatic advertising market is simple: advertisers place bids for ad space, and publishers sell their ad space to the highest bidder. Within this ecosystem, various entities — including advertising technology ("ad tech") companies, ad exchanges, advertising agencies, and marketing networks — act as intermediaries, enabling the delivery of ads to publishers' websites moments after users open a web page.

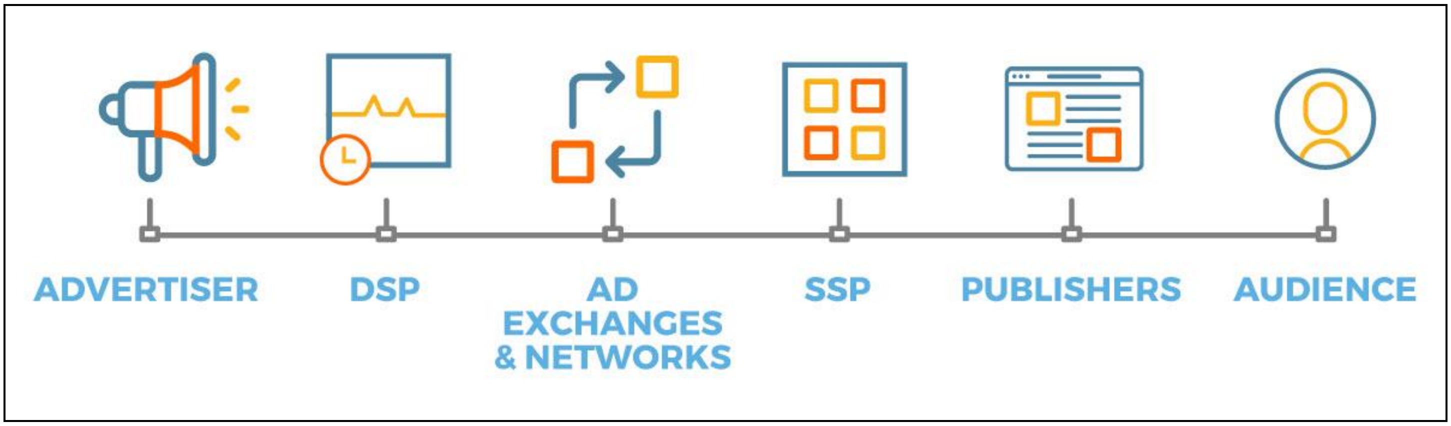


Figure 2: *The programmatic ad market is a sophisticated ecosystem that allows advertisers to deliver targeted ads to audiences on publishers' websites and applications. Demand-side platforms (DSPs) and supply-side platforms (SSPs) are ad tech companies that help enable the market to function in real time. (Source: Publir)*

Ad Fraud Requires Scale to Be Effective; Bots Provide a Solution

Ad fraud comprises various tactics, techniques, and procedures (TTPs) that are aimed at "gaming" the metrics used to measure the performance of an advertising campaign, such as the number of clicks or views that an ad receives. In a perfect world, these metrics only reflect actions performed by living, breathing users with actual (or potential) interest in the advertisement's offering. In reality, however, fraudsters use various techniques to inflate these metrics and receive higher payments for ads that are never actually delivered to target audiences.

To earn meaningful income from ad fraud, fraudsters must conduct it at scale. For example, SEO Chatter lists average revenue for Google AdSense as ranging from $0.0008 to $0.020 per view or $0.20 to $15.00 per click. Similarly, WordStream's Google Ads advertising benchmarks price the average Google Ads cost-per-click (CPC) at $4.22 and cost-per-lead (CPL) at $53.52, respectively. According to SEO Chatter, publishers — and by extension, fraudsters — can receive up to 68% of this revenue. However, given the effort necessary to make bogus clicks, views, and leads appear legitimate to ad verification systems, fraudster's returns on ad fraud at this scale would likely be a pittance.

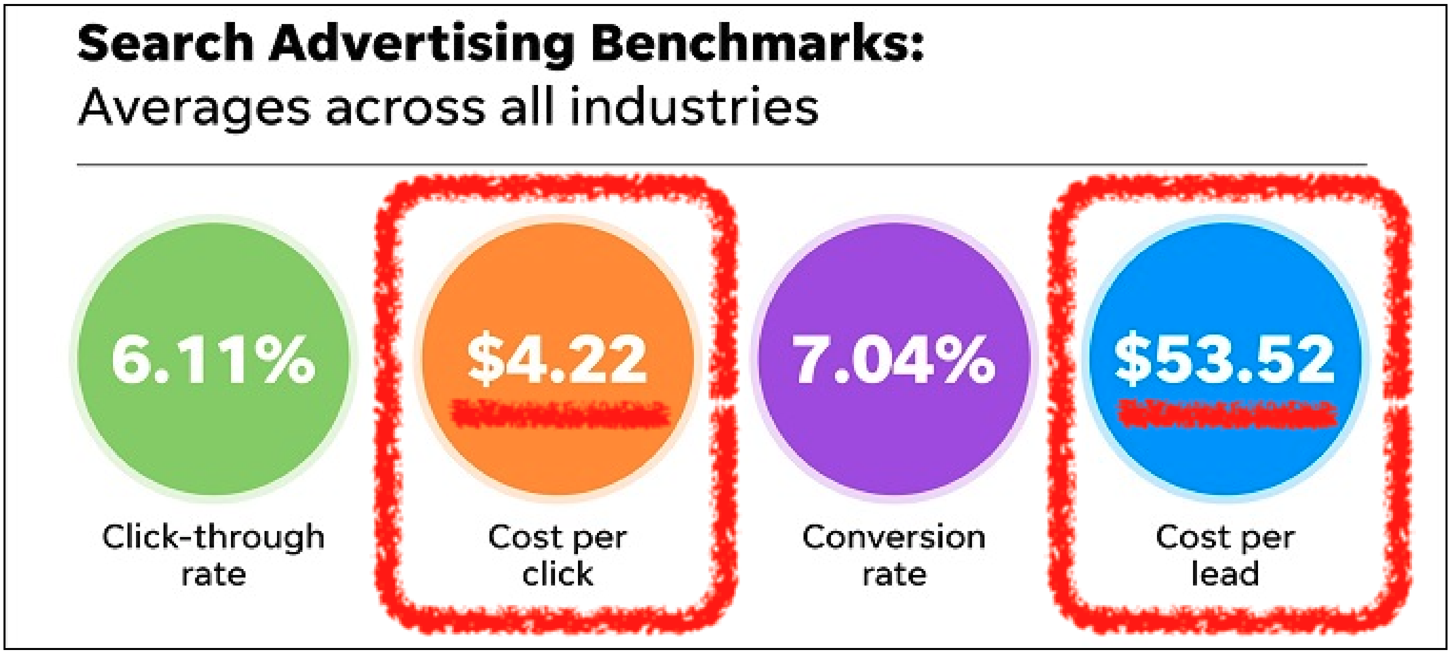


Figure 3: *At their most basic level, advertisers' fees are relatively low, which means fraudsters must conduct ad fraud at scale for it to be profitable (Source: WordStream)*

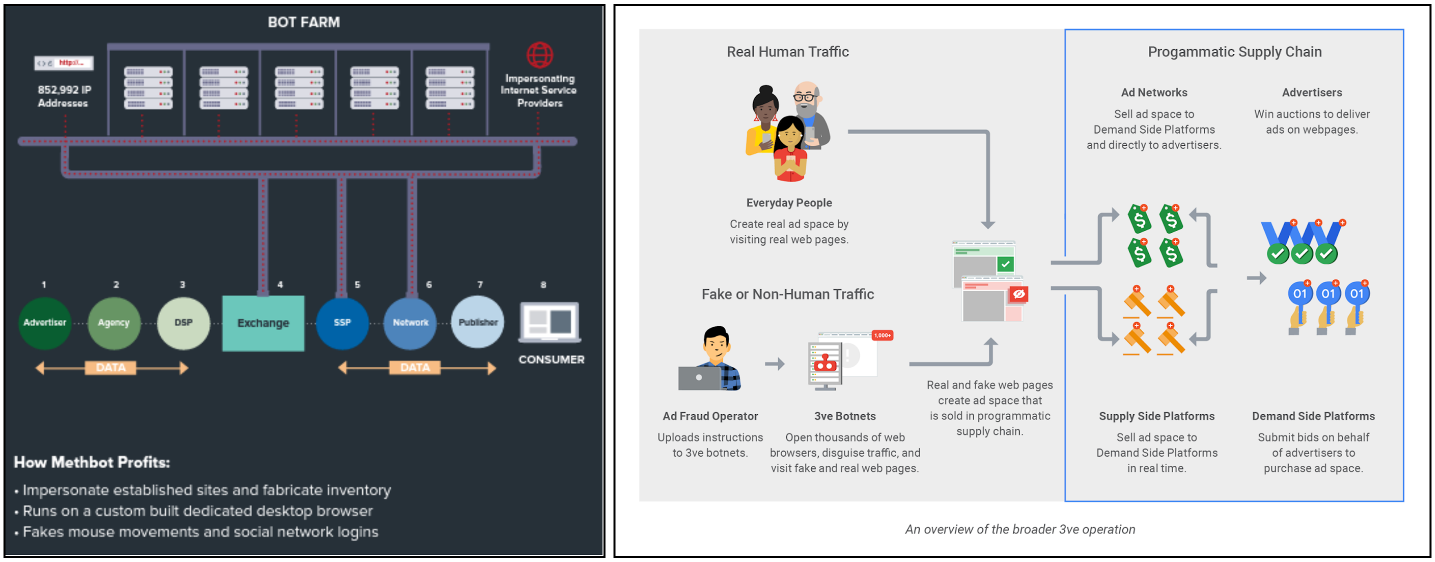
This dynamic means that fraudsters require automation to effectively conduct ad fraud. Malicious bots used to conduct ad fraud or other forms of cybercrime are broadly organized into **botnets** and **bot farms.**

- **Botnets** are networks of devices infected with malware. After users unknowingly download the malware, their devices join a larger network of infected devices controlled by a threat actor.
- **Bot farms** are collections of bots that may be physically centralized: for example, on servers rented from a data center or homemade "phone farms" operated by threat actors.

2 historical bot-based ad fraud schemes dismantled by authorities in 2018 — **Methbot** and **3ve** — illustrate just how effective automation-enabled ad fraud can be:

- **Methbot was a data center-based ad fraud scheme that used a bot farm instead of a botnet.** This large-scale ad fraud operation used bots on servers rented from data centers to simulate ad views. Methbot's operators designed their bot farm to mimic human browsing behavior in order to deceive ad verification systems. The fraudsters obfuscated the servers' IP addresses using proxy servers and employed a sophisticated network of fake websites to publish ads.
- **3ve was a combination of 3 botnet and bot farm-based ad fraud schemes that obtained control over 1.7 million IP addresses using various malware variants.** For one of their schemes, 3ve's operators infected thousands of devices with malware, then used the infected devices to engage in ad fraud by simulating human activity and manipulating ad campaign performance.

According to press releases from the Justice Department's Eastern District of New York in 2018 and 2019, Methbot's operators earned $7 million between September 2014 and December 2016, and 3ve's operators earned $29 million between December 2015 and October 2018.



How Methbot Profits:

- Impersonate established sites and fabricate inventory
- Runs on a custom built dedicated desktop browser
- Fakes mouse movements and social network logins

Create real ad space by visiting real web pages.

Uploads instructions to 3ve botnets.

Open thousands of web browsers, disguise traffic, and visit fake and real web pages.

Real and fake web pages create ad space that is sold in programmatic supply chain.

Sell ad space to Demand Side Platforms and directly to advertisers.

Win auctions to deliver ads on webpages.

Sell ad space to Demand Side Platforms in real time.

Submit bids on behalf of advertisers to purchase ad space.

An overview of the broader 3ve operation

Figures 4 and 5: *Despite differences in execution, Methbot and 3ve were both sophisticated ad fraud operations that relied on the establishment and maintenance of formidable bot infrastructure capable of imitating human activity (Source: HUMAN; Google, HUMAN)*

Improving Automation Solutions Democratize Ad Fraud, Expanding the Threat

While fraudsters have traditionally depended on automation to conduct ad fraud at scale, continual improvements in the effectiveness and accessibility of automation offerings are now widening the pool of actors who can conduct ad fraud. This dynamic likely allows low-level fraudsters with little experience or technical expertise to leverage ad fraud en masse to earn modest sums. While the scale of this activity might be minor for a single fraudster, the collective impact is a vastly expanded threat to advertisers and publishers. For example, in 2019, VICE reported on Americans' use of "phone farms" to earn from $50 to $2,000 per month via ad fraud. Similarly, various open sources indicate that ordinary users routinely access information on similar TTPs to generate income.

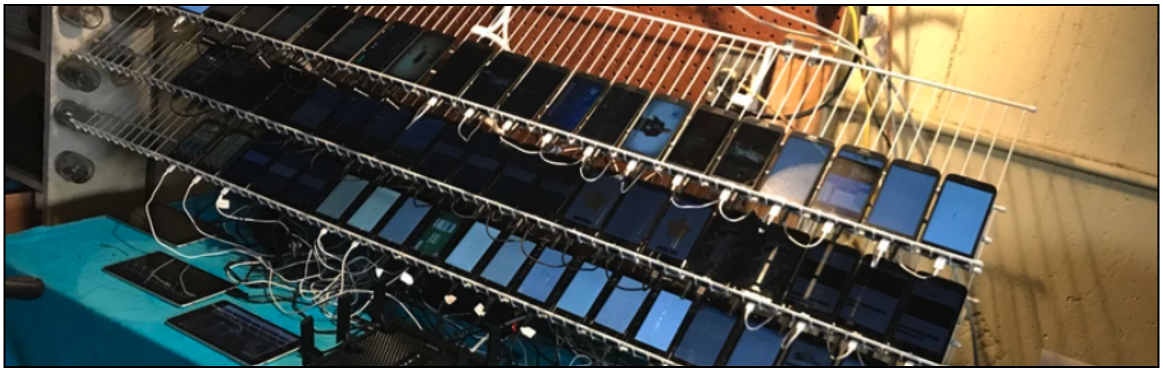


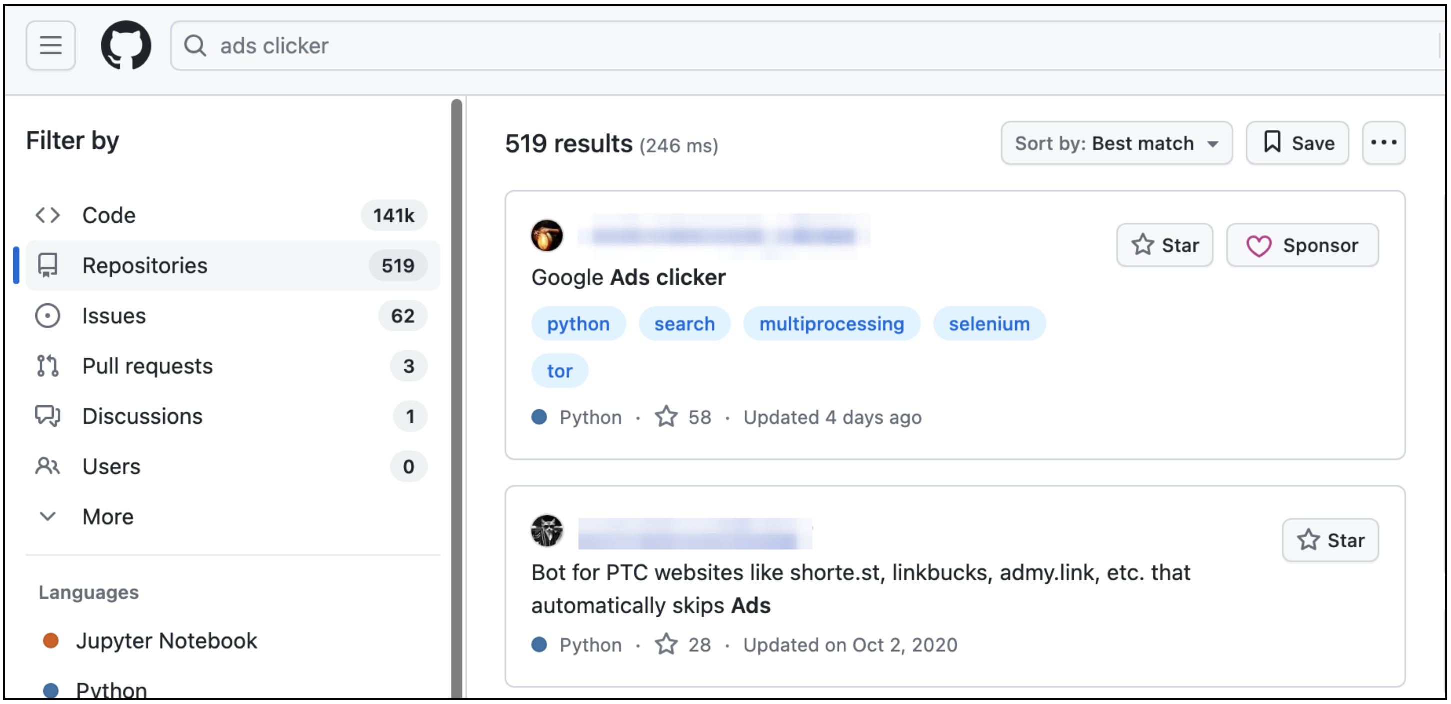
Figure 6: *An image of a phone farm used to conduct ad fraud (Source: VICE)*

During our investigation, we identified a number of dark web and cybercrime-focused clearnet sources where fraudsters discuss which ad fraud tools and TTPs are effective, advertise their own offerings among their peers, and request or provide guidance regarding ad fraud tools and TTPs.

Open Sources Offer "Ready-to-Go" Solutions That Facilitate Automation and Evade Detection

Open sources offer fraudsters access to user-friendly bot software with "out-of-the-box" functionality. Code repositories like GitHub offer ready-made scripts and codes that fraudsters can use to swiftly operationalize bot farms to conduct ad fraud at scale. One example is Selenium, a programming project supporting browser automation, which allows fraudsters to create scripts that automatically click on banner ads and website links. By altering its IP address and user-agent data via proxy servers, the software also allows fraudsters to alter their device's geodata and other indicators that fraud prevention systems use to detect fraud.

As of this writing, a keyword search for "ads clicker" allowed us to surface approximately 500 code repositories that may facilitate the use of bots for fraudsters who lack experience or technical expertise.



ads clicker

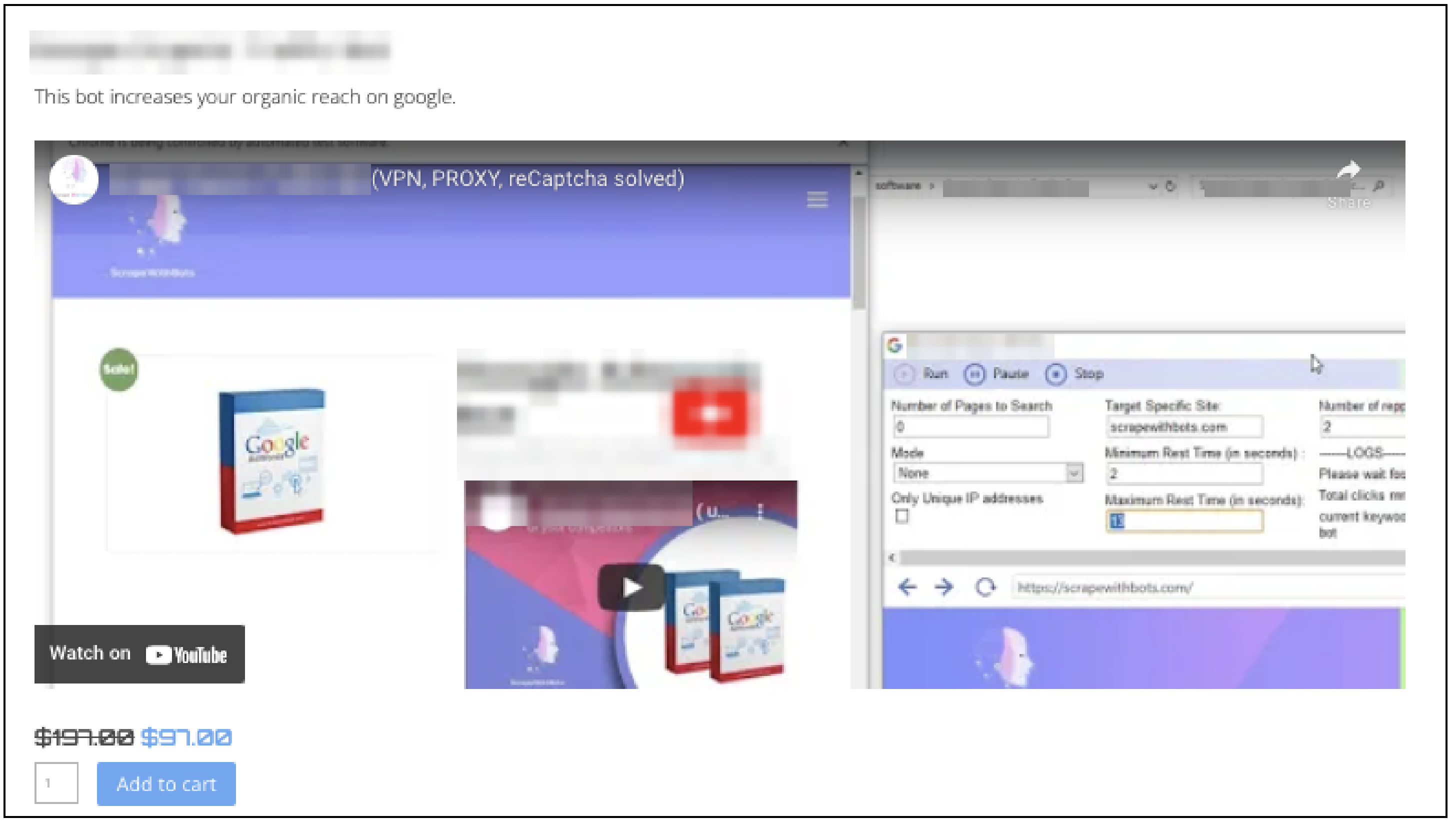
519 results (246 ms)

Google Ads clicker

Bot for PTC websites like shorte.st, linkbucks, admy.link, etc. that automatically skips Ads

Figure 7: *Using a keyword search, we surfaced approximately 500 projects on GitHub that may facilitate the use of bots for "small-time" fraudsters (Source: GitHub)*

Another paid solution offered by a bot provider website enables fraudsters to feed organic web traffic to their websites in order to conduct ad fraud or malvertising attacks. One bot automatically searches for keywords associated with a targeted site, and then clicks on the site to increase its prominence in Google search results. As a result, when real users search for the keywords, the targeted site will appear higher in their search results, increasing the likelihood that they will click on the resource and be exposed to its paid ads, which may also contain malvertising payloads. To evade detection, the bot is equipped with various countermeasures, including virtual private network (VPN) functionality and unique browser fingerprints.



This bot increases your organic reach on google.

(VPN, PROXY, reCaptcha solved)

Number of Pages to Search: 0
Target Specific Site: scrapewithbots.com
Mode: None
Minimum Rest Time (in seconds) : 2
Only Unique IP addresses: □
Maximum Rest Time (in seconds): 13

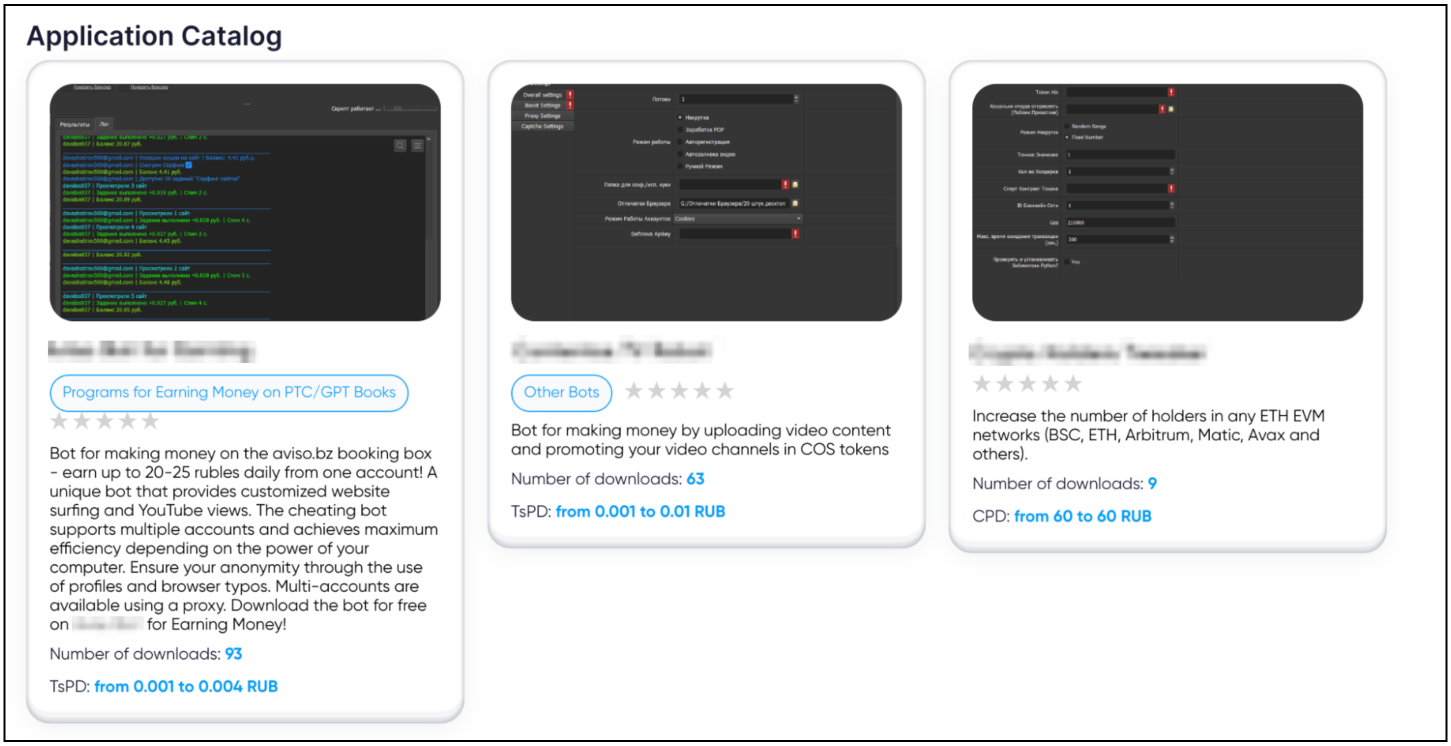
------LOGS------
Please wait fo
Total clicks m
current keywo
bot

https://scrapewithbots.com/

~~$197.00~~ $97.00

Figure 8: *One paid bot solution increases organic traffic to a website by artificially increasing its prominence in Google search results (Source: Bot provider website)*

On underground forums, fraudsters also actively promote bot solutions that can be used to conduct ad fraud. For example, a threat actor on a Russian-language underground forum shared various bot software products, which were available for download via another bot provider website. The threat actor advised their peers to use the bots to complete paid assignments on an online service that offers advertising traffic-as-a-service. The threat actor also recommended a fast CAPTCHA-solving service for use with the bots and advised that their peers use a reliable virtual private server (VPS) and operate multiple fraudulent user accounts with different cryptocurrency wallets and email addresses. By operating 10 to 15 fraudulent accounts, the threat actor claimed that users could earn from 500 to 600 rubles per day — or around $5.16 to $6.19 USD as of this writing.



Application Catalog

[redacted]

Programs for Earning Money on PTC/GPT Books

★★★★★

Bot for making money on the aviso.bz booking box - earn up to 20-25 rubles daily from one account! A unique bot that provides customized website surfing and YouTube views. The cheating bot supports multiple accounts and achieves maximum efficiency depending on the power of your computer. Ensure your anonymity through the use of profiles and browser typos. Multi-accounts are available using a proxy. Download the bot for free on [redacted] for Earning Money!

Number of downloads: 93

TsPD: from 0.001 to 0.004 RUB

[redacted]

Other Bots ★★★★★

Bot for making money by uploading video content and promoting your video channels in COS tokens

Number of downloads: 63

TsPD: from 0.001 to 0.01 RUB

[redacted]

★★★★★

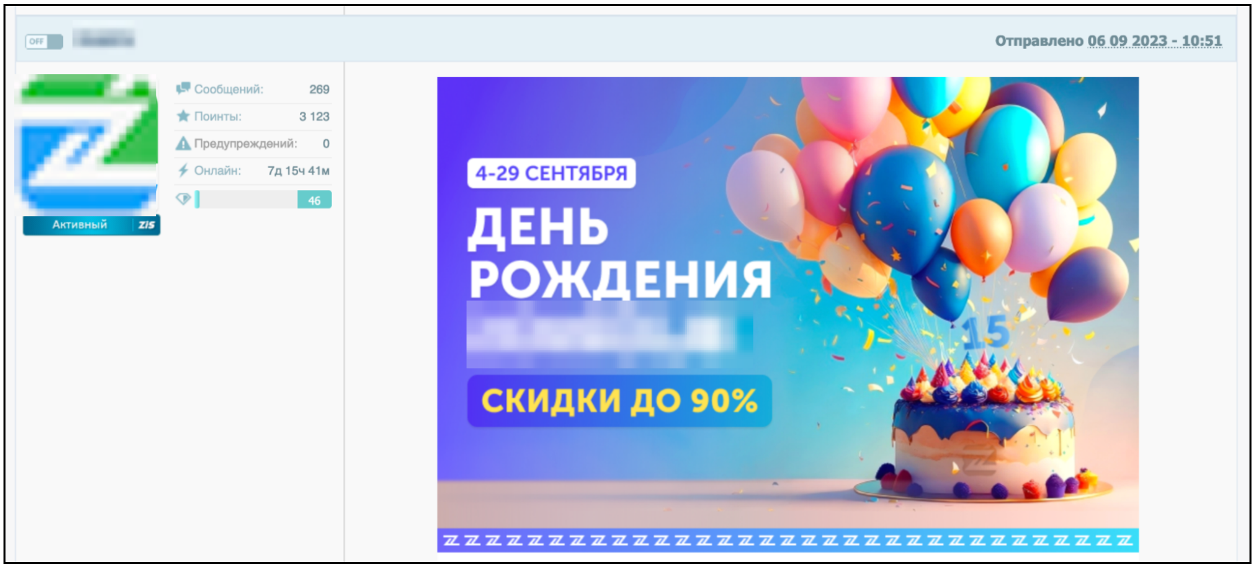
Increase the number of holders in any ETH EVM networks (BSC, ETH, Arbitrum, Matic, Avax and others).

Number of downloads: 9

CPD: from 60 to 60 RUB

Figure 9: *On an underground forum, a threat actor shared a link to downloadable bot software that could be used to conduct ad fraud (image text machine-translated from Russian) (Source: Bot provider website)*

Another threat actor on the same forum promoted additional bot software that facilitates ad fraud. These included software products from a well-known bot provider. These products also offer "out-of-the-box" functionality.



OFF [redacted]

Отправлено 06 09 2023 - 10:51

Активный

Сообщений: 269

Поинты: 3 123

Предупреждений: 0

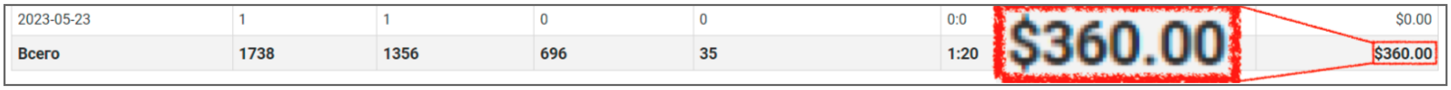
Онлайн: 7д 15ч 41м

46

Figure 10: *Other offerings for automation-based tools are not uncommon on certain web forums (Translation from Russian: "September 4-29, [redacted] Birthday, Discounts up to 90%") (Source: Underground forum)*

Various Sources Provide Fraudsters with "Safe Space" to Discuss, Learn Ad Fraud TTPs

The well-known bot provider's forum includes ad fraud-related guides and discussions that facilitate information sharing among fraudsters engaged in ad fraud. For example, a user on the forum offered detailed guidance to conduct ad fraud on YouTube. At the end of their walk-through, the user boasted of their own earnings: $360 after a month of conducting ad fraud for approximately an hour each day. While these earnings are modest, the collective impact of similar activity is likely to be substantial. (We discuss these impacts in the section "The Impacts of Ad Fraud Are Substantial and Growing Each Year".)

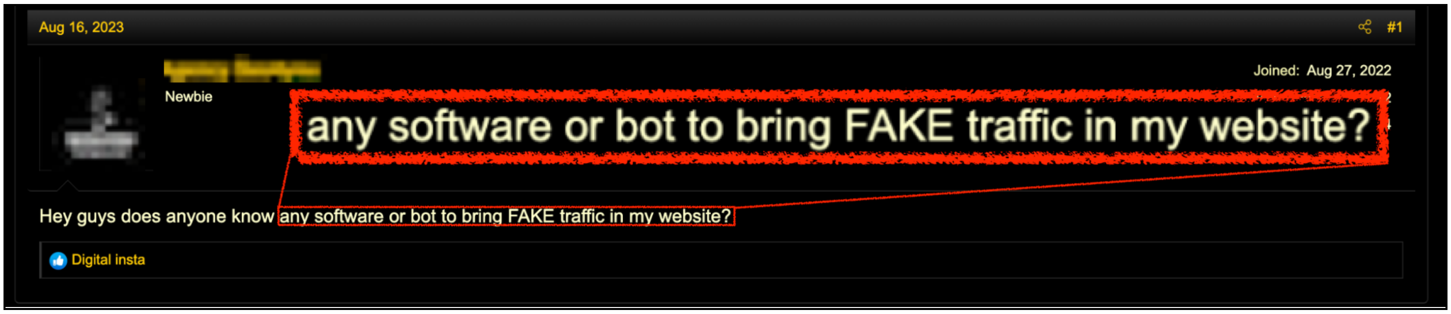


2023-05-23	1	1	0	0	0:0	$0.00
Bcero	1738	1356	696	35	1:20	$360.00

Figure 11: *Although individual earnings from ad fraud are modest, the collective impact of similar activity is likely substantial (Source: Bot provider website forum)*

Fraudsters on underground forums provide tailored ad fraud guidance in response to requests from less experienced peers. For example, on August 16, 2023, a threat actor on an underground forum requested software that could help drive fake traffic to their website. In reply, another threat actor suggested an ad traffic bot. A linked thread claimed that the bot was capable of the following:

- Simultaneous operation of multiple browsers
- Concealing the user's IP address through proxy servers
- Support for various protocols, including HTTP, SOCKS4, SOCKS5, and X-FORWARD
- Scheduling projects for future execution
- Enabling the setting of referrers to make traffic appear to originate from specific websites
- Allowing the creation or use of scripts for more natural and intricate interactions
- Emulating over 400 different devices.



Aug 16, 2023

#1

[redacted]

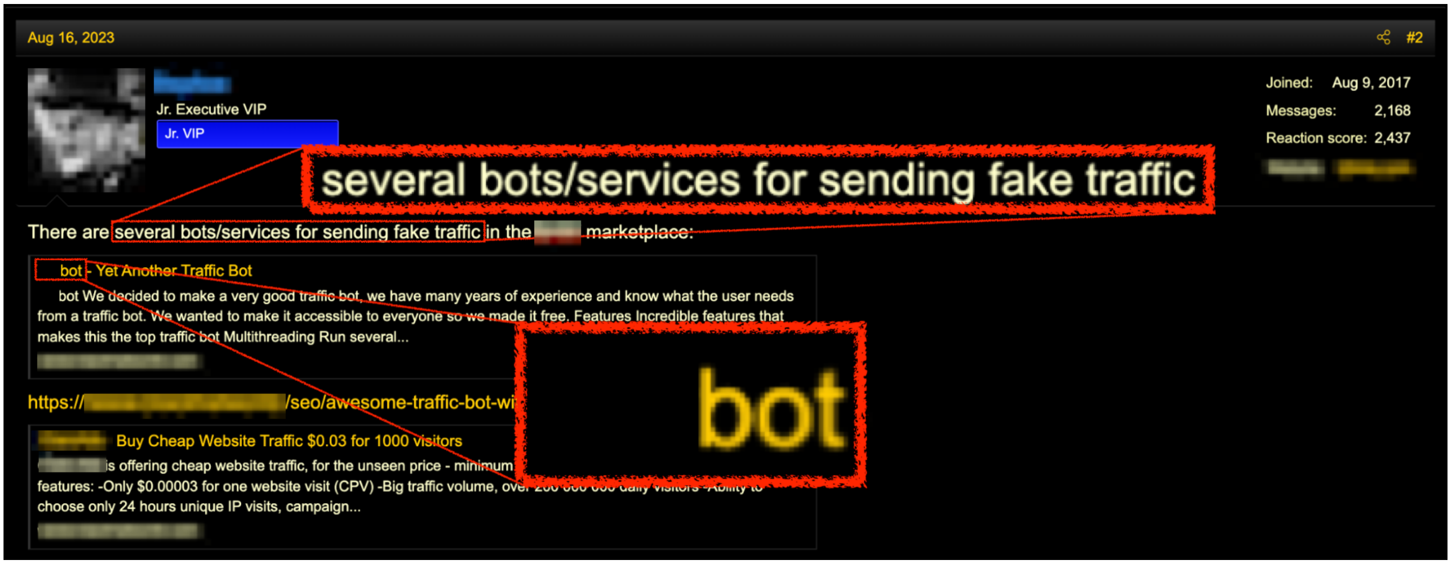
Newbie

Joined: Aug 27, 2022

Hey guys does anyone know any software or bot to bring FAKE traffic in my website?

Digital insta

Figure 12: *A threat actor requests guidance for driving fake traffic to their website (Source: Underground forum)*



Aug 16, 2023 #2

[redacted]
Jr. Executive VIP
Jr. VIP

Joined: Aug 9, 2017
Messages: 2,168
Reaction score: 2,437
[redacted]

several bots/services for sending fake traffic

There are several bots/services for sending fake traffic in the [redacted] marketplace:

bot - Yet Another Traffic Bot
bot We decided to make a very good traffic bot, we have many years of experience and know what the user needs from a traffic bot. We wanted to make it accessible to everyone so we made it free. Features Incredible features that makes this the top traffic bot Multithreading Run several...
[redacted]

https://[redacted]/seo/awesome-traffic-bot-wi

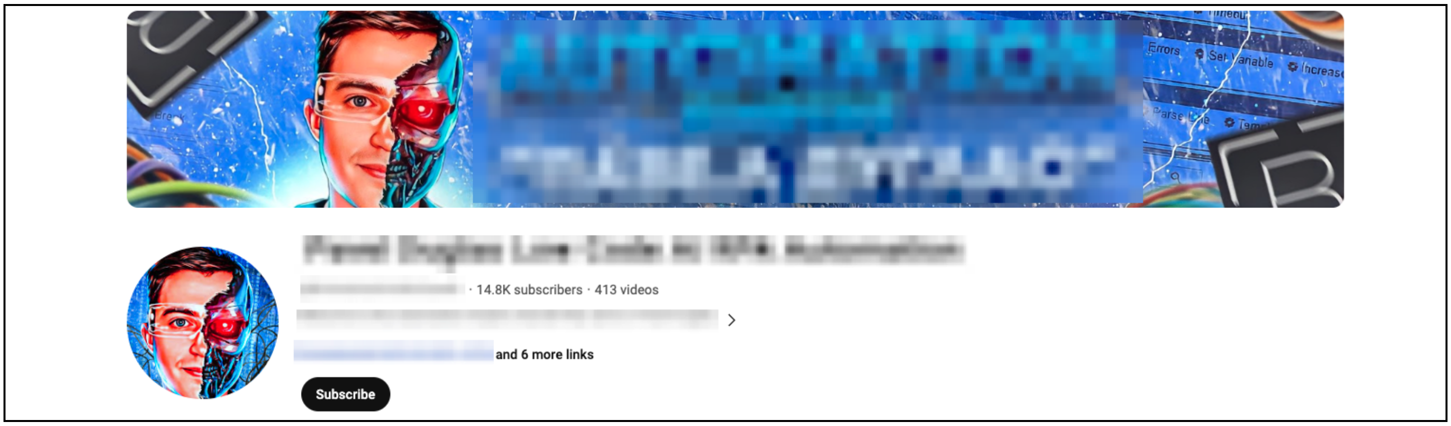
bot

[redacted] Buy Cheap Website Traffic $0.03 for 1000 visitors
[redacted] is offering cheap website traffic, for the unseen price - minimum features: -Only $0.00003 for one website visit (CPV) -Big traffic volume, over 200 000 000 daily visitors -Ability to choose only 24 hours unique IP visits, campaign...
[redacted]

Figure 13: *In response to a request for guidance (Figure 12), another threat actor recommended a specific bot with advanced capabilities that could be used for ad fraud (Source: Underground forum)*

Certain YouTube channels make information on ad fraud readily available for fraudsters, increasing the accessibility of ad fraud as a whole. For example, one YouTube channel claims in its description that viewers can "find everything [they] need to know about creating bots to automate a wide variety of processes, from business tasks to making money." A video on the channel promotes a bot for another traffic-as-a-service website that offers paid advertising traffic for YouTube ads.

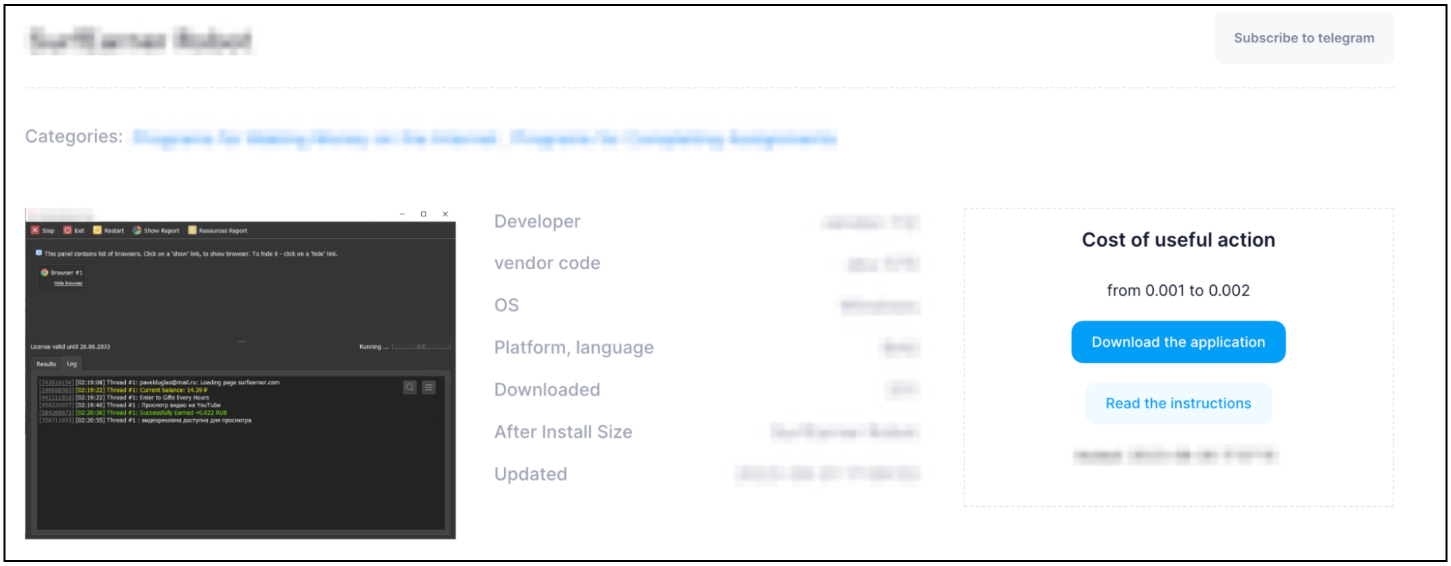
As of this writing, the channel has published 413 videos and garnered over 14,000 subscribers, demonstrating that the wider public has ample access to information on ad fraud.



[redacted]
[redacted] · 14.8K subscribers · 413 videos
[redacted]
[redacted] and 6 more links

Figure 14: *Certain YouTube channels disseminate information regarding tools that can be used for ad fraud (Source: YouTube)*

Notably, the bot promoted by the YouTube channel was also available for download via the bot provider website linked by another threat actor in this report (Figure 9), indicating that ad fraudsters broadly make use of the same tools.



[redacted]

Subscribe to telegram

Categories: [redacted]

Stop Exit Restart Show Report Resources Report

This panel contains list of browsers. Click on a 'show' link, to show browser. To hide it - click on a 'hide' link.

Browser #1
Hide browser

License valid until 26.06.2033

Running ...

Results Log

```
[742919154] [02:19:08] Thread #1: pavelduglas@mail.ru: Loading page surfearner.com
[196088593] [02:19:22] Thread #1: Current balance: 14.39 ₽
[441311810] [02:19:22] Thread #1: Enter to Gifts Every Hours
[858220657] [02:19:40] Thread #1 : Просмотр видео на YouTube
[584268673] [02:20:36] Thread #1: Successfully Earned +0.022 RUB
[358711653] [02:20:55] Thread #1 : видеореклама доступна для просмотра
```

Developer	[redacted]
vendor code	[redacted]
OS	[redacted]
Platform, language	[redacted]
Downloaded	[redacted]
After Install Size	[redacted]
Updated	[redacted]

Cost of useful action

from 0.001 to 0.002

Download the application

Read the instructions

[redacted]

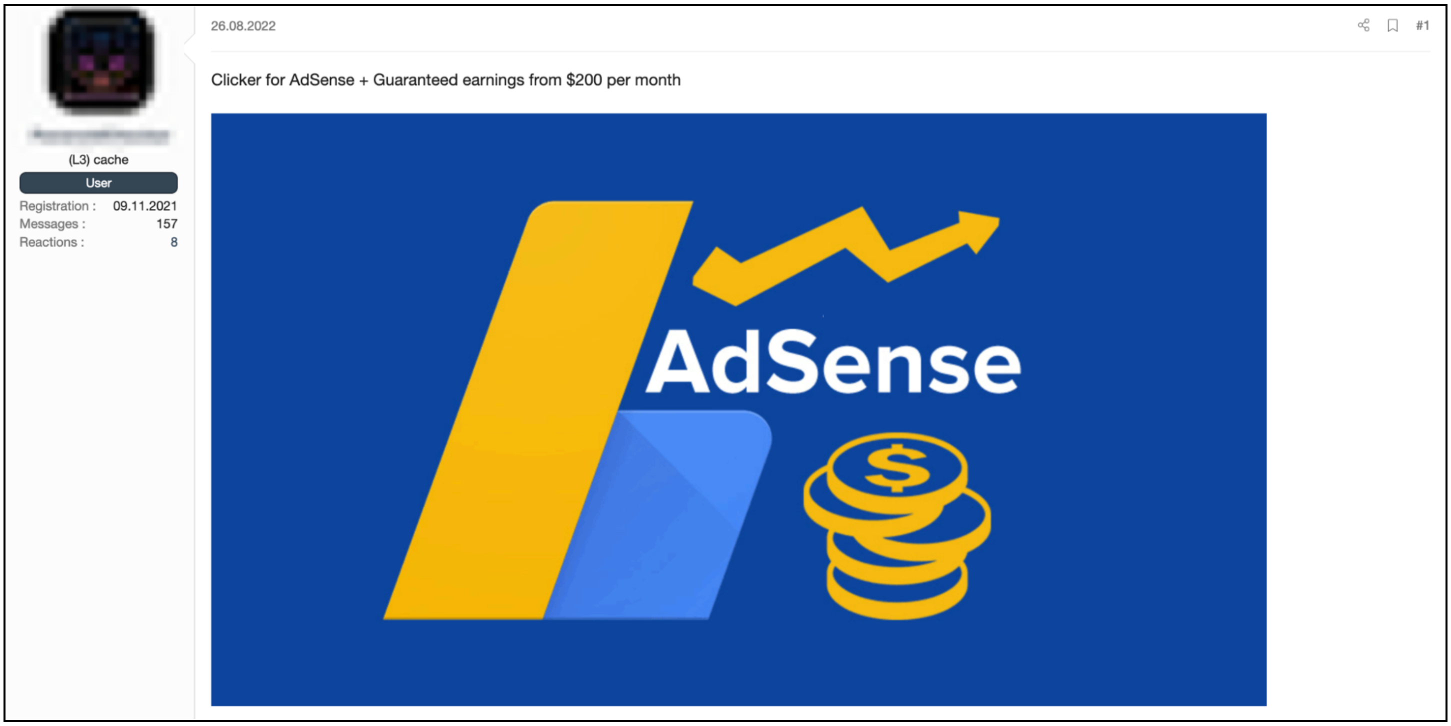
Figure 15: *The bot promoted by the YouTube channel was available for download via a link in a post on an underground forum, demonstrating that ad fraudsters generally use the same tools (image text machine-translated from Russian) (Source: Bot provider website)*

Sophisticated Actors Discuss and Promote Sophisticated Automation Offerings on Dark Web Forums

No review of current ad fraud bot offerings would be complete without mentioning dark web sources, which more advanced threat actors actively use to promote tools for ad fraud. For example, on August 26, 2022, a threat actor on a top-tier dark web forum promoted an automated tool designed to facilitate ad fraud via Google AdSense. According to the post, the tool has a graphical interface, requires a remote server, and is capable of the following:

- Performing automated clicks on AdSense ads
- Simulating human behavior by changing attributes for each visit and performing natural actions to avoid detection by Google's ad verification
- Using various methods to access sites that host AdSense ads, including direct visits, search engine referrals, and website referrals
- Using features like keyword filtering and flexible proxy settings

The threat actor listed the software's price at $500, which included the software, instructions, setup assistance, and support.



[redacted]

(L3) cache

User

Registration : 09.11.2021

Messages : 157

Reactions : 8

26.08.2022

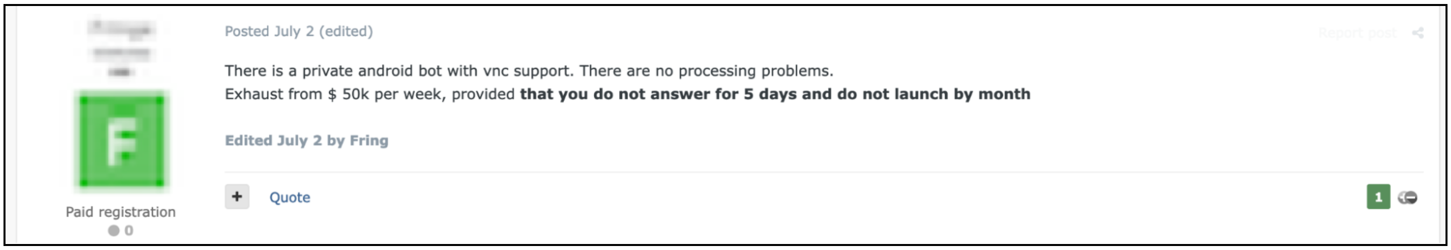
#1

Clicker for AdSense + Guaranteed earnings from $200 per month

__Figure 16:__ A threat actor promoted an automated tool for ad fraud (image text machine-translated from Russian) (Source: Top-tier dark web forum)

In a response to the post, another threat actor discussed an alternative use of the bot, demonstrating threat actors' adaptability. This threat actor pointed out that if AdSense detects and prevents fraud conducted with the bot, threat actors may be able to use this to their advantage by engaging with competitors' ads to flag them for ad fraud and/or drain their advertising budgets. In doing so, threat actors would be able to eliminate competitors' ads.

Threat actors and groups with the resources to conduct ad fraud at a larger scale likely maintain a greater presence on dark web forums, as indicated by a post on another top-tier dark web forum. On July 2, 2023, a threat actor requested partners who could supply fraudulent ad traffic to their Android-based botnet. According to the threat actor, the botnet can generate ad traffic worth more than $50,000 per week and was equipped with virtual network computing (VNC), which facilitates remote access to control victims' infected computers.



[redacted]

Paid registration

● 0

Posted July 2 (edited)

Report post

There is a private android bot with vnc support. There are no processing problems.
Exhaust from $ 50k per week, provided **that you do not answer for 5 days and do not launch by month**

Edited July 2 by Fring

__Figure 17:__ An offer to supply $50,000 worth of fake ad traffic each week indicates dark web actors engaged in ad fraud likely operate at a higher scale than many of their peers (image text machine-translated from Russian) (Source: Top-tier dark web forum)

Additionally, the actors on dark web forums are likely familiar with more advanced ad fraud applications than those who frequent other sources. On February 18, 2022, a threat actor on a top-tier dark web forum offered to pay $1,000 to a specialist with programming experience who could provide bespoke bot "clicker" software that they could customize for specific tasks, likely to support ad fraud. The threat actor stated that purchasing bot traffic was unsuitable for their purposes and requested advice from other users who had experience with clickers.

Functions desired by the threat actor for the requested clicker included the following:

- The ability to work through various profiles on an anonymous browser.
- The ability to work through proxy servers to conceal their IP address or bypass access restrictions.
- Multithreading functionality to perform multiple tasks simultaneously.
- The ability to record and edit action scripts, as well as customize them to avoid detection by web application firewalls (WAF).
- Support for "farm" cookies from various sites that can be used to disguise bot activity as human activity

The Impacts of Ad Fraud Are Substantial and Growing Each Year

Ultimately, improving automation offerings and their increasing accessibility are driving more losses from ad fraud each year. Part of this is a function of the sheer size of the programmatic ad industry, as both programmatic advertising and ad fraud are equally scalable. According to eMarketer, digital ad spend is slated to surpass $600 billion by the end of 2023. Meanwhile, according to an analysis by Lunio, 5.5% of total online ad spend is wasted as a result of IVT or other factors that are indicative of ad fraud. Taken together, these estimates suggest aggregate losses from ad fraud may reach $33 billion for 2023 alone. Statista forecasts even higher losses of $100 billion for 2023. By comparison, Chainalysis estimates that ransomware actors earned $2 billion in value from victims between 2020 and 2022.

Importantly, it is worth noting that not all wasted ad spend is attributable to bot-based ad fraud. According to the Association of National Advertisers (ANA), the programmatic ad ecosystem is rife with inefficiencies, contributing to 23% in wasted ad spend. Unaligned incentives across the programmatic advertising ecosystem create opportunities for advertising agencies to employ dubious marketing techniques to increase their revenue. As an illustrative example, Uber sued multiple ad agencies and networks in 2017 and 2019 for misrepresenting ad effectiveness and purchasing nonexistent, nonviewable, or fraudulent advertising. Meanwhile, the same misaligned incentives that encourage ad agencies to "game" the system also discourage ad tech companies from implementing meaningful changes that would help prevent ad fraud, as these parties earn the same commissions from ad sales regardless of whether or not advertisers' budgets are well spent or wasted from fraud and mismanagement.

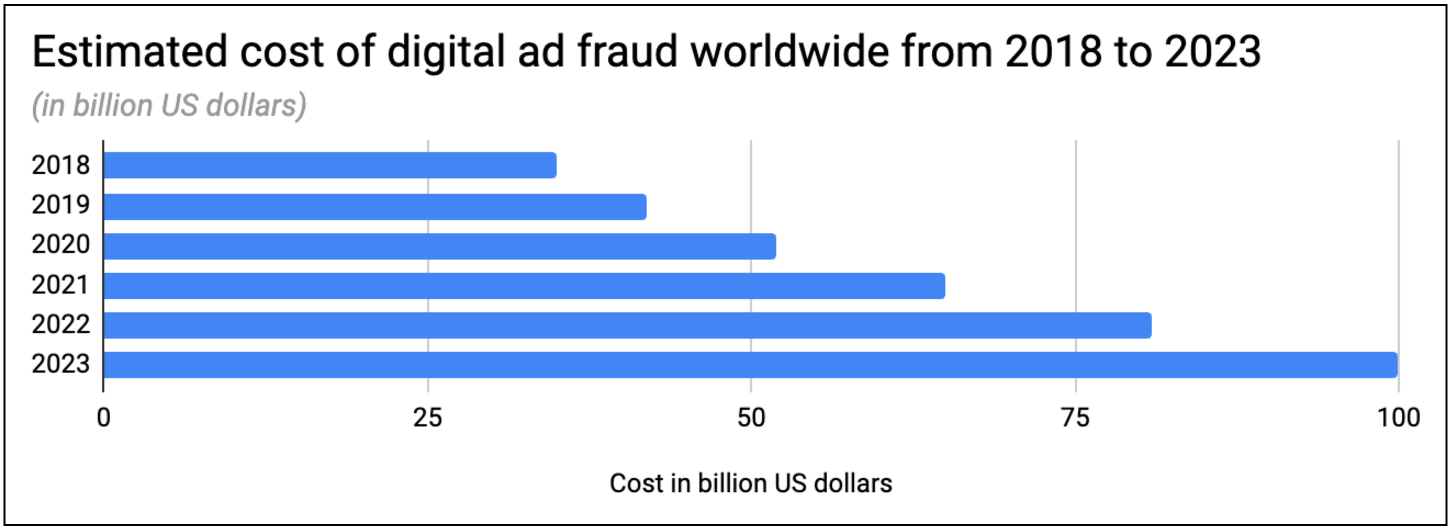


Figure 18: *Ad fraud losses are predicted to reach $100 billion in 2023, up from $81 billion in 2022 and $35 billion in 2018 (Source: Statista)*

Ad Ecosystem Likely Developing into "Connective Tissue" for Converging Physical, Online Threats

The automation-enabled accessibility of ad fraud likely facilitates a convergence of threats. For example, in early September 2023, Svenska Dagbladet and other news outlets reported that Swedish gangs behind an increase in bombings and shootings had begun to use streaming manipulation to launder money from drug deals, robberies, fraud, and contract killings. Streaming manipulation is an ad fraud-adjacent technique that involves the use of fake streams or views on streaming platforms — predictably enabled by automation solutions similar to those described in this report — to generate income. Previously, Dr. Augustine Fou, a cybersecurity and ad fraud researcher, predicted a similar use of "vertically integrated" ad fraud operations to launder dark money in a social media blog article in April 2020.

In addition to its fraud-focused money-laundering applications, fraudsters have seized upon the programmatic advertising market to conduct combined payment fraud and malvertising cybercrime schemes. By using compromised or fraudulently registered online advertising accounts, fraudsters can monetize linked payment methods — including payment cards or bank accounts — to purchase ad inventory. In turn, the fraudsters sell this ad inventory to third-party threat actors, who then use the purchased ads to deliver malvertising attacks that distribute phishing pages, scam pages, and stealer malware to victims. These malvertising attacks expose victims to the risk of compromise of payment card data, personally identifiable information (PII), or account credentials that can be successively monetized using the same tactics, indirectly creating a "vicious cycle".

Mitigations

- Implement technical solutions capable of detecting and filtering out IVT, which is indicative of bot activity. Various providers offer effective services and tools to screen out fraudulent bot activity from legitimate clicks or views.
- Seek and promote "information symmetry" to better understand the effectiveness of your ad spend and/or authenticity of your traffic. According to an ANA report, the inability to widely access data leads to inefficiency and waste in the programmatic advertising ecosystem.
- Identify and address inefficiencies in ad spend by prioritizing advertising effectiveness over low cost. If possible, work with credible demand-side (for advertisers) or supply-side (for publishers) marketing networks. Cost-per-action (CPA) networks, for example, often guarantee premium traffic from vetted publishers.
- For publishers, use ads.txt and sellers.json to increase transparency for advertisers and help combat ad fraud.
- Employ threat intelligence to better understand — and by extension, mitigate — the threat that ad fraud poses to your organization. Ad fraud exposes different risks to advertisers, publishers, and ad tech companies, but all stakeholders in the advertising ecosystem can mitigate the threat more effectively by understanding the tools and TTPs used by fraudsters.

Outlook

Programmatic advertising and ad fraud are both largely dependent on automation. As a result, the impact of ad fraud will likely continue to grow each year as a function of the size of the programmatic advertising market as a whole. Besides wasted ad spend, other consequences of ad fraud include skewed performance metrics, inaccurate audience targeting, and spam or fake lead submissions, all of which distort advertising analytics and deceive advertisers into believing their ad campaigns are more effective than they are. Advertisers and publishers sustain the direct brunt of these impacts, but they also damage the credibility of the entire programmatic advertising ecosystem, presenting a risk of brand impairment for ad tech companies and other advertising intermediaries.

Because the improving effectiveness of fraud-enabling automation solutions is largely rooted in their capacity to avoid detection, advertising stakeholders' ability to leverage AI solutions in coming years to detect and prevent IVT and ad fraud will likely moderate the threat posed by ad fraud. As indicated in our report, the tools and TTPs used to conduct ad fraud are accessible and scalable, and they will likely become more so as large language model AI technology continues to develop. Therefore, the sophistication and accessibility of these tools and TTPs combined with fraudsters' perennial adaptability mean that stakeholders must adopt proactive strategies that incorporate AI technology to safeguard their advertising campaigns and ensure the integrity of their marketing efforts — especially since fraudsters will almost certainly seek to use the same tools against them.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture