

RMT:SK/AFM/MTK
F.#2016R02228

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
-----X

UNITED STATES OF AMERICA

TO BE FILED UNDER SEAL

- against -

ALEXANDER ZHUKOV,
BORIS TIMOKHIN,
MIKHAIL ANDREEV,
DENIS AVDEEV AND
DMITRY NOVIKOV,

COMPLAINT AND
AFFIDAVIT IN
SUPPORT OF
APPLICATION FOR
ARREST WARRANTS

(18 U.S.C. § 1349)

Defendants.

Case No. 18-MJ-696

-----X

EASTERN DISTRICT OF NEW YORK, SS:

EVELINA ASLANYAN, being duly sworn, deposes and states that she is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such.

In or about and between September 2014 and December 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants ALEXANDER ZHUKOV, BORIS TIMOKHIN, MIKHAIL ANDREEV, DENIS AVDEEV and DMITRY NOVIKOV, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud online advertising companies and businesses, and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: electronic

communications to computers and servers in the United States and elsewhere, emails and other online communications, and monetary transfers, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Section 1349)

The source of your deponent's information and the grounds for her belief are as follows:¹

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since March 2012. I have been involved in the investigation of numerous cases involving cybercrime, financial fraud and money laundering, during the course of which I have conducted physical surveillance, interviewed witnesses, executed court-authorized search warrants and used other investigative techniques to secure relevant information. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from:
(a) my personal participation in the investigation; (b) my review of the investigative file; and
(c) reports made to me by witnesses and other law enforcement officers involved in the investigation.

¹ Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

3. The FBI is conducting an investigation into online advertising fraud by certain individuals and businesses. The government's investigation has uncovered evidence that the defendants ALEXANDER ZHUKOV, BORIS TIMOKHIN, MIKHAIL ANDREEV, DENIS AVDEEV and DMITRY NOVIKOV executed an online advertising fraud scheme that victimized individuals and businesses in the United States and elsewhere. Specifically, the evidence obtained in the investigation shows that the defendants used computers that they controlled to create the illusion that a real human internet user was viewing an advertisement on a real internet webpage -- when, in fact, a computer was loading the advertisement on a counterfeit webpage via an automated program -- in order to fraudulently obtain a share of the resulting advertising revenue.

Background Regarding Online Advertising

4. Based on my knowledge, training and experience, and consultation with experts in online advertising, website owners (or "publishers") commonly use entities called supply-side platforms (or "SSPs") to find bidders for the advertising space on their websites. Businesses (or "brands") and their advertising companies commonly use entities called demand-side platforms (or "DSPs") to bid for advertising space on websites that real human internet users are browsing. These auctions are conducted by the SSPs, and take place in a span of milliseconds while a user is launching a webpage. This ecosystem functions to facilitate the brands' ability to advertise their goods and services online, and the publishers' ability to earn revenue for providing content online. The brands typically pay for advertising on a lump-sum basis, and website owners typically receive payment for the amount of internet traffic that is directed to the brands' advertisements, on a per-click or per-impression basis.

5. DSPs typically have direct relationships with advertising companies, but SSPs are not always in direct communication with publishers. Instead, the SSP and the publisher may be connected through a chain of intermediaries, known as advertising networks. This chain, which may be several entities deep, stretches toward the brand in one direction (the “demand side”) and toward the publisher in the other direction (the “supply side”). An advertising network’s partner typically supplies the advertising network with a snippet of code, known as an “ad tag,” that it wishes to have placed on publishers’ websites. The advertising network then agrees to ensure that the ad tag is placed in particular advertising slots on publisher’s webpages, either by negotiating with publishers directly or by contracting with other intermediaries.

6. Each time a user browses to a webpage that contains an ad tag, the user’s computer activates the ad tag. A signal (the “ad call”) is then sent to one or more SSPs putting the designated ad slot out for immediate bid by potential advertisers. The signal includes the IP address of the computer loading the tag, the URL of the page on which the tag was encountered, and some information regarding the intermediaries responsible for placing the tag.

7. When the bidder wins an advertising opportunity and the advertisement is served to the relevant advertising slot, a process is triggered that ultimately results in a payment moving from the demand side of the chain to the various intermediaries responsible for placing the ad tag on the webpage.

Online Advertising Fraud

8. Based on my knowledge, training and experience, and consultation with experts in cybercrime and online advertising fraud, “advertising fraud” is generally a type of cybercrime in which malicious actors fraudulently obtain money from online advertising companies and businesses. In the subtype of advertising fraud known as an “impression” fraud scheme, internet advertisers are made to believe that advertisements they purchase are viewed by real human internet users (an occurrence known as an “impression”), when in fact the advertisements are automatically loaded onto computers controlled by the malicious actors and are not viewed by real human internet users. In the subtype of advertising fraud known as a “click” fraud scheme, internet advertisers are made to believe that advertisements they purchase are clicked on by real human internet users, when in fact the advertisements are automatically activated by computers controlled by the malicious actors and are not clicked on by real human internet users.

9. In conjunction with fake impressions and fake clicks, malicious actors carrying out an impression fraud or click fraud commonly send out falsified data to fraudulently represent to SSPs that advertisements are being viewed or clicked on by real human internet users, ultimately resulting in the issuance of payments by advertisers. The malicious actors have business arrangements in place that allow them to claim a portion of those payments. The process of falsifying data to indicate that an advertisement is being viewed or clicked on by a real human internet user in the context of a particular website is known as “domain spoofing,” or, more simply, “spoofing.”

The Defendants' Scheme

10. By way of an overview, and as further described below, the defendants carried out their scheme by operating a purported advertising network called Mediamethane. Mediamethane had business arrangements with other advertising networks that enabled it to receive payment in return for placing ad tags with publishers on behalf of those advertising networks. Rather than place these ad tags on real publishers' websites, however, Mediamethane maintained a network of computers located at a commercial server farm in Dallas, Texas. The defendants wrote computer code that caused these computers to simulate the internet activity of human internet users. At the defendants' instruction, the computers purported to load webpages belonging to well-known publishers, including publishers in the Eastern District of New York. The computers then sent signals to SSPs indicating that real human internet users were loading the webpages, and soliciting bids on the opportunity to show advertisements to those purported users. In response, DSPs bid on those opportunities. The winning DSPs made payments to SSPs (using money provided by brands) in return for the purported impressions, and the SSPs transferred those payments to advertising networks to be passed along the chain of intermediaries described above. Mediamethane stood at the end of this chain, claiming payment for the purported impressions.

11. In order to disguise the true nature of these automated internet browsers, the defendants created fraudulent entries in a global register that made it appear that the computers belonged to real internet users, rather than being located in a server facility. The defendants also programmed their computers to automatically engage in

activity (such as mouse movements and scrolling) that would create the impression of control by individual human users.

12. As set forth below, ZHUKOV was Mediamethane's CEO.

TIMOKHIN functioned as ZHUKOV's partner and the company's chief technical officer.

ANDREEV, AVDEEV and NOVIKOV provided technical and logistical support for the charged scheme.

The Scheme is Publicly Revealed

13. On or about December 20, 2016, researchers at a private cybersecurity firm based in New York, New York published a white paper titled "The Methbot Operation," revealing the operation of an online advertising fraud scheme. In the white paper, the cybersecurity firm revealed the IP addresses of computers used to carry out the fraud (the "Malicious IPs"). The cybersecurity firm identified the Malicious IPs based on its monitoring of network traffic related to advertisement impressions on behalf of various advertising clients. It explained that, based on its observations, computers associated with the Malicious IPs transmitted false data to create the impression that a real human internet user was viewing an advertisement on a real internet webpage, when in fact a computer that was not controlled by an individual human was loading the advertisement on a counterfeit webpage. It further explained that the Malicious IPs were associated with false registration data in publicly available IP registration databases. Law enforcement agents reviewed a sample of the cybersecurity firm's traffic data and confirmed that it was associated with anomalous activity.

14. In or about July 2017, a major U.S. technology company that provides, among other things, advertising services for individuals and businesses informed law

enforcement agents that it had corroborated the cybersecurity firm's observations.

Specifically, the technology company also monitors traffic data associated with advertisement impressions on behalf of various advertising clients, and noted that the Malicious IPs were associated with fraudulent traffic and bore a common signature.

15. Records obtained from the cybersecurity firm revealed more than 5,000 domains associated with online publishers that the malicious actors had counterfeited, including the domains of thousands of businesses in the United States and multiple businesses in the Eastern District of New York. Records obtained from the technology company revealed that the technology company had reimbursed its clients more than seven million dollars, collectively, for advertising fees that resulted from advertisements that had been fraudulently loaded by computers and not actually viewed by real human internet users. These clients included hundreds of businesses in the United States, including at least one business with offices in the Eastern District of New York.

Identification of the Malicious Actors

16. Records obtained from a company that archives IP registration data revealed that many of the Malicious IPs purported to be registered to one or another of six major U.S. internet service providers, including at least one provider with offices in the Eastern District of New York. However, information obtained from the six internet service providers revealed that none of the Malicious IPs registered in their respective names was actually in their possession, custody or control.

17. Law enforcement agents investigated the publicly available registration data for the Malicious IPs and discovered information linking the Malicious IPs to ZHUKOV, TIMOKHIN, ANDREEV and AVDEEV as set forth below.

18. More than 1,400 Malicious IPs were registered to an email address identified herein as the "Registration Email Account." Law enforcement agents identified another email address described herein as "Andreev Email Account 1." Records obtained from the service provider for Andreev Email Account 1 revealed that Andreev Email Account 1 was registered to "Mikhaeil Andreev" and listed a nickname that was a portion of the account name for the Registration Email Account.

19. Records obtained from the service provider for the Registration Email Account further revealed that the account sent frequent emails at regular intervals to an email address identified herein as "Zhukov Email Account 1." In turn, records obtained from the service provider for Zhukov Email Account 1 revealed that Zhukov Email Account 1 was registered to "Alexander Zhukov." Law enforcement agents identified another email address identified herein as "Zhukov Email Account 2." Records obtained from the service provider for Zhukov Email Account 2 revealed that Zhukov Email Account 2 was registered to "Alexander Z" and listed Zhukov Email Account 1 as a recovery email.

20. Records obtained from the service provider for the Registration Email Account also revealed that the account sent frequent emails at regular intervals to an email address identified herein as "Timokhin Email Account 1." Records obtained from the service provider for Timokhin Email Account 1 revealed that Timokhin Email Account 1 was registered to "Boris Timokhin" and listed as a recovery email an email address identified herein as "Timokhin Email Account 2." Records obtained from the service provider for Timokhin Email Account 2 revealed that Timokhin Email Account 2 was registered to a name in Cyrillic characters which transliterates to "Boris Timokhin," and listed a recovery email account of tim-boris@yandex.ru.

21. Records obtained from the service provider for the Registration Email Account also revealed that the account sent frequent emails at regular intervals to an email address identified herein as "Avdeev Email Account 1."

22. On March 10, 2017, the Honorable Ramon E. Reyes, Jr., United States Magistrate Judge for the Eastern District of New York, issued a search warrant for the Registration Email Account, Zhukov Email Account 1, Timokhin Email Account 1 and Avdeev Email Account 1, among others. On June 23, 2017, the Honorable Lois Bloom, United States Magistrate Judge for the Eastern District of New York, issued a search warrant for Andreev Email Account 1, Zhukov Email Account 2 and Timokhin Email Account 2, among others.

23. During the execution of the search warrants, law enforcement agents observed email communications and other records that appear to confirm that: MIKHAIL ANDREEV used Andreev Email Account 1; ALEXANDER ZHUKOV used Zhukov Email Account 1 and Zhukov Email Account 2; BORIS TIMOKHIN used Timokhin Email Account 1 and Timokhin Email Account 2; and DENIS AVDEEV used Avdeev Email Account 1. For example, the email accounts contained personal identity documents, contracts, invoices and emails in the users' true names. In addition, the email communications and other records also revealed that ZHUKOV used a third email address, identified herein as "Zhukov Email Account 3." For example, the user of Zhukov Email Account 3 sent emails (to TIMOKHIN and others) signed "Aleksandr Zhukov," and the user

of Zhukov Email Account 1 sent ANDREEV an email that stated, in part, "Misha: Here is my email [Zhukov Email Account 3]."²

24. ZHUKOV sent emails in which he identified himself as the CEO of a purported advertising network called Mediamethane. Law enforcement agents reviewed communications indicating that both ZHUKOV and TIMOKHIN used email accounts with the domain mediamethane.com. The registrant of ZHUKOV's account at mediamethane.com listed Zhukov Email Account 2 as a recovery email address.

The Defendants Obtain and Fraudulently Register IP Addresses

25. In reviewing the returns from the search warrants, law enforcement agents observed invoices and communications from a server provider in Dallas, Texas reflecting that, beginning in mid-2015, ZHUKOV and TIMOKHIN rented hundreds of servers from the server provider.

26. Relatedly, law enforcement agents observed records and communications reflecting that ZHUKOV and his co-conspirators rented hundreds of thousands of IP addresses from various IP address leasing companies and then registered those IP addresses with false information. For example, on April 25, 2016, ZHUKOV communicated to TIMOKHIN that he had leased more than 131,000 IP addresses and registered them in one of the names on the list (which name mimicked the name of a major U.S. internet service provider). Thereafter, on October 15, 2015, ZHUKOV communicated with an employee of the Dallas-based server provider about assigning 35,000 IP addresses to newly rented servers. And on May 13, 2016, AVDEEV communicated with an employee of

² Excerpts and summaries of online communications and documents may be drawn from draft and summary translations from Russian to English that are subject to revision.

an IP leasing company and instructed the employee to make certain changes to the location and usage information associated with the leased IP addresses. Specifically, AVDEEV directed that the IP leasing company change the "Usage type" for the leased IP addresses from "commercial" or "datacenter" to "ISP" (internet service provider); ascribe a more diverse set of cities and states to the leased IP addresses; and reduce the number of leased IP addresses associated with certain small cities (AVDEEV commented that "200,000 IP in the city [of] Wilmington with a population [of] 71,525 [is] overly [sic]").

27. Based on my knowledge, training and experience, the foregoing measures were intended to disguise the rented servers to make them appear as if they were legitimate computers from various locations across the United States and elsewhere, rather than a set of servers located in a single datacenter, in order to create the illusion that real human internet users were at the controls of the computers.

28. Law enforcement agents searched Timokhin Email Account 1 for each of the Malicious IPs and found that approximately 15,500 of the Malicious IPs appeared in sent or received emails therein.

29. Law enforcement agents also observed a note related to IP address registration in the cloud storage account associated with Zhukov Email Account 1. In the note, which is dated September 18, 2015, ZHUKOV listed numerous false corporate names that mimicked the names of various major U.S. internet service providers. The list included the false names associated with many of the Malicious IPs in publicly available IP registration data (supra ¶ 16).

The Defendants Communicate Regarding Software Design

30. During their review of the returns from search warrants on Zhukov Email Account 1 and Timokhin Email Account 1, law enforcement agents observed a series of communications between and among ZHUKOV, TIMOKHIN, ANDREEV, AVDEEV and NOVIKOV using a specific online collaboration tool designed for software project management (the "Collaboration Software") that allows messages to be posted within a secure shared space. The Collaboration Software caused each message to be automatically emailed to Zhukov Email Account 1 and Timokhin Email Account 1 from a separate email account. The communications included discussions related to the development of software code that would direct servers to simulate human beings viewing online advertisements. For example, on October 25, 2014, ANDREEV circulated programming code designed to ensure that signals coming from the computers had the correct "browser" parameters." Based on my knowledge, training and experience, ANDREEV's use of quotation marks around the word "browser" indicates that the conspirators custom-designed an automatic web browser so that it could mimic signals sent by typical internet browsers that a real human would operate. Later that same day, ANDREEV posted a message stating that he had implemented the code and speculated that it was "possible to click ten times per hour."

31. On October 31, 2014, ANDREEV posted a message using the collaboration software that stated, "Dmitry Novikov, write in detail how it should be proceeding? 'This many clicks per hour' or 'This many clicks per day.'" On December 28, 2014, ZHUKOV posted a message complaining that the computers were clicking too rapidly, stating: "Mikhail Andreev set . . . 10 clicks per day per IP. However, within an hour it already downloaded 300 clicks. It has to be a bug. It should be about 50-60 clicks per hour total."

32. On October 28, 2014, NOVIKOV posted a message using the collaboration software titled, "Make mouse move and scroll more meaningful." In the message, NOVIKOV directed TIMOKHIN to carry out "research about how to make 'mouse moves and scroll more realistic/meaningful.'" Similarly, on June 25, 2015, ZHUKOV sent a "to-do" list to TIMOKHIN directing him to address a "lack of mouse move." Based on my knowledge, training and experience, the foregoing messages reveal an effort to remotely induce mouse movements in computers in order to create the illusion that real human internet users were at the controls of the computers for the purpose of misleading security software deployed by advertisers and SSPs.

33. In ZHUKOV's June 25, 2015 to-do list, ZHUKOV also instructed TIMOKHIN "to add authorization for Facebook [] users. There is Google, twitter too; [but] no FB (There should be approximately 40% of them.)" Based on my knowledge, training and experience, the foregoing comment reveals an effort to make computers appear to be signed into Facebook in order to further create the illusion that real human internet users were at the controls of the computers.

34. Other messages posted by the conspirators using the Collaboration Software dealt specifically with nonhuman viewing of video advertisements. For example, on October 28, 2014, NOVIKOV posted a message titled "Emulating 'video watch,'" in which he cautioned, "The videos need to be clicked on and watched for 60-90 seconds." Based on my knowledge, training and experience, the foregoing message reveals an effort to ensure that a sufficient portion of each advertisement was watched to ensure payment by advertisers. On December 1, 2014, ANDREEV circulated programming code designed to cause computers to automatically play and pause an online video player and wrote,

“Basically this is how it is possible to generate the events.” Based on my knowledge, training and experience, the foregoing message reveals efforts to start and stop a video, rather than playing it all the way through or not at all, in order to further create the illusion that real human internet users were at the controls of the computers.

35. The conspirators explicitly discussed their efforts to evade security software deployed by advertisers and SSPs to detect nonhuman browsing. Such software is typically sold and operated by third-party cybersecurity vendors. For example, in a note dated August 4, 2015, found within the cloud storage account associated with Zhukov Email Account 1, ZHUKOV referred to two specific U.S. cybersecurity firms and wrote that he intended to “check [] out [their] filter for the possibility of fucking them over a la,” followed by the name of a third firm. Based on my knowledge, training and experience, the note indicates that ZHUKOV was making efforts to understand and evade cybersecurity firms’ detection software (or “filters”).

36. Similarly, on October 12, 2016, ZHUKOV directed TIMOKHIN to “turn[] off the block” on a certain cybersecurity firm. Based on my knowledge, training and experience, the foregoing message reveals that the conspirators had programmed their system not to load advertisements that deployed fraud detection software supplied by the referenced firm. Finally, on October 16, 2016, after discovering that his online advertising impressions did not register as fraudulent with a certain cybersecurity firm, ZHUKOV wrote a celebratory email to TIMOKHIN stating that their scheme “[was] magnificent.”

37. The defendants made a selling point of Mediamethane’s ability to provide advertising traffic that did not trigger fraud detection software and registered as coming from United States computers. For example, on December 10, 2016, ZHUKOV

sent an email to a potential business partner in which he offered “100% USA traffic” that could pass through “filters” from various U.S. cybersecurity firms that monitor internet traffic for fraudulent activity and amounted to “20-50 millions [sic] impressions daily.”

The Defendants’ “Git” and Control Panel are Discovered

38. On September 5, 2017, law enforcement agents downloaded, from a publicly accessible file-sharing service, a file whose location had been posted online by an internet commenter who claimed that it was the “git” for the defendants’ scheme. Based on my knowledge, training and experience, and consultation with a computer scientist, a “git,” also known as a version-control repository, is a storehouse of data that captures the process of revising a piece of software code and stores important information about the contributions of various collaborators, their comments on the software code, and different versions that each component of the code has been through.

39. The file contained programming code that causes computers to operate an automated browser, click on online advertisements a randomly determined number of times, scroll and move the mouse, control and monitor video playback, and falsely appear to be signed into Facebook. The git contained numerous references to TIMOKHIN, identified with Timokhin Email Account 1, and ANDREEV, identified with Andreev Email Account 1, as authors of various sections of the code. The git also contained references to files hosted at a domain associated with the IP address 176.58.122.237. A search of publicly available databases revealed that the IP address 176.58.122.237 was associated with a server hosted at a server provider based in Galloway, New Jersey. Records obtained from that provider revealed that the server associated with the IP address 176.58.122.237 was registered to BORIS TIMOKHIN.

40. In the course of executing the search warrants described above, law enforcement agents also observed records and communications reflecting that the conspirators monitored the activity of the computers within their control using an online control panel located at a specific domain (the “Control Panel Domain”). For example, in a message posted using the Collaboration Software on October 25, 2014, ANDREEV stated that the defendants’ software “clicks and periodically sends the statistics to [the Control Panel Domain].” Records obtained from the domain registration company for the Control Panel Domain revealed that the Control Panel Domain was registered to “Aleksander Zhukov,” with a registration email of Zhukov Email Account 2. In or about and between May 2015 and December 2016, an email account associated with the Control Panel Domain sent regular emails to TIMOKHIN, ZHUKOV and AVDEEV reporting on server performance. The cloud storage account associated with Zhukov Email Account 1 also contained screenshots of the online control panel located at the Control Panel Domain.

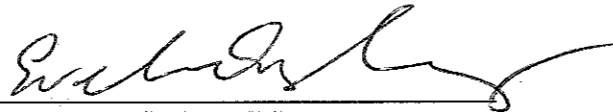
41. The email reports and screenshots reveal that, in 2016, the conspirators were monitoring the performance of thousands of computers, tracking millions of online advertising impressions, and recording thousands of dollars per hour in revenue. For example, the screenshots reveal that during a 24-hour period between October 14, 2016 and October 15, 2016, the conspirators recorded \$56,253 in revenue.

ANDREEV Admits Association with the Defendants’ Scheme

42. In communications with associates, days after the publication of the white paper on the defendants’ scheme (*supra* ¶ 13), ANDREEV acknowledged his association with the scheme. ANDREEV speculated that he was “being investigated by the

FBI,” admitted to writing code for the scheme “[a]t the initial stage,” and explained that “[t]he companies that get fooled consider it fraud.”

WHEREFORE, your deponent respectfully requests that arrest warrants be issued for the defendants ALEXANDER ZHUKOV, BORIS TIMOKHIN, MIKHAIL ANDREEV, DENIS AVDEEV and DMITRY NOVIKOV, so that they be dealt with according to law.


EVELINA ASLANYAN
Special Agent, Federal Bureau of Investigation

Sworn to before me this
31st day of July



THE HONORABLE
UNITED STATES DISTRICT JUDGE
EASTERN DISTRICT OF NEW YORK