2013R01333/AMT/AAH/LKB/CG

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon.
	:	
v.	:	Crim. No. 23- 470 (CPO)
	:	
MAKSIM SILNIKAU,	:	Count 1
a/k/a "Maksym Silnikov,"	:	(Conspiracy to Commit Wire Fraud)
a/k/a "Maksim Silnikov,"	:	18 U.S.C. §§ 1349, 3559(g)(1)
a/k/a "Maxsim Andreyevich Silnikov,"	:	
a/k/a "Maksym Mykolaiets,"	:	Count 2
ANDREI TARASOV, and	:	(Conspiracy to Commit Computer
VOLODYMYR KADARIYA,	:	Fraud and Abuse)
a/k/a "Volodymyr Kadaria,"	:	18 U.S.C. §§ 371, 3559(g)(1)
a/k/a "Vladimir Kadaria"	:	
	:	Counts 3-4
	:	(Wire Fraud)
	:	18 U.S.C. § 1343
	:	18 U.S.C. § 2
	:	
	:	FILED UNDER SEAL

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges:

Count 1
(Conspiracy to Commit Wire Fraud)

Introduction

1. From at least in or about October 2013 through in or about March 2022, the defendants set forth below, together with others, devised and executed an international wire fraud and computer hacking scheme to use malicious online advertising campaigns—so called "malvertising"—and other means to deliver various types of malicious software ("malware"), scareware, and other scams to millions of

unsuspecting victim Internet users in the United States and elsewhere. The malvertising campaigns were designed to appear legitimate, but often redirected victim Internet users who viewed or accessed the advertisements to malicious sites and servers that sought to defraud the users or delivered malware to the users' devices. The defendants and their co-conspirators, through the above-described scheme, caused unsuspecting Internet users to be forcibly redirected to malicious content on millions of occasions.

2. The defendants and their co-conspirators profited from the dissemination of malware and malicious advertisements through several means, including by selling to other cybercriminals the access they fraudulently obtained to the following: (i) victim Internet users—so-called Internet "traffic"; (ii) compromised victim devices—so-called "loads" or "bots"; and (iii) information that was stolen from victims and recorded in "logs," such as banking information and login credentials, to enable further efforts to defraud the victim Internet users or deliver additional malware to their devices.

Relevant Individuals and Entities

3. At all times relevant to this Indictment:

a. Defendant MAKSIM SILNIKAU, a/k/a "Maksym Silnikov," a/k/a "Maksim Silnikov," a/k/a "Maxsim Andreyevich Silnikov," and a/k/a "Maksym Mykolaiets" ("SILNIKAU"), was a malicious advertiser and lead malware distributor who resided outside of the United States, including in Ukraine. SILNIKAU played a leading role in orchestrating the co-conspirators' widespread distribution of malware

and malvertisements, and efforts to profit from that activity. SILNIKAU used online accounts associated with particular monikers known to the Grand Jury.

b. Defendant ANDREI TARASOV ("TARASOV") was a malicious advertiser and malware distributor who resided outside of the United States, including in Ukraine. TARASOV furthered the scheme's distribution of malware and malvertisements through numerous means, including by developing and providing computer code to obscure the malicious nature of the advertisements and facilitate their widespread distribution. TARASOV used online accounts associated with particular monikers known to the Grand Jury.

c. Defendant VOLODYMYR KADARIYA, a/k/a "Volodymyr Kadaria," and a/k/a "Vladimir Kadaria" ("KADARIYA"), was a malicious advertiser and malware distributor who resided outside of the United States, including in Ukraine. KADARIYA facilitated the distribution of malware and malvertisements by co-conspirators through numerous means, including by directing the actions of co-conspirators and managing computer infrastructure involved in the dissemination of malware. KADARIYA used online accounts associated with particular monikers known to the Grand Jury.

d. Co-Conspirator Oleksii Ivanov, a/k/a "Oleksii Petrovich Ivanov," and a/k/a "Alex Ivanov" ("Ivanov") was a malicious advertiser and malware distributor who resided outside of the United States, including in Ukraine, and conspired with the charged defendants. Ivanov used online accounts associated with particular monikers and online personas known to the Grand Jury.

e. Co-Conspirator A was a malware coder who used particular online monikers known to the Grand Jury.

f. Company A was a company headquartered in New York that provided online advertising technology services. Company A's primary computer servers were located in Hudson County, New Jersey.

g. The Media Trust ("TMT") was a company headquartered in Virginia that provided online security services, including to combat malvertising.

h. Confiant Inc. ("Confiant") was a company headquartered in New York that provided online security services, including to combat malvertising.

Background on Relevant Online Advertising and Hacking Terms

i. An "Internet browser" was a software application that allowed an Internet user to view and interact with information on the Internet through a range of electronic devices, such as desktops, laptops, tablets, and smartphones. Browser "plug-ins" and "extensions" were additional pieces of software that a user could install to add functionalities to an Internet browser, such as to handle Internet content that an Internet browser was not designed to process.

j. In online advertising, the term "publisher" referred to a website owner, such as a news, entertainment, or sports website, who displayed web banner and other graphical advertisements ("ads") online on behalf of paying advertisers. Such ads often contained images, text, or multimedia. A single ad displayed to a single user on a single occasion was called an "impression."

k. When an Internet user opened a website with an Internet browser, a complex series of transactions determined which ad was displayed to a user in each available advertising space on the webpage. These transactions typically occurred nearly instantaneously and were largely invisible to the Internet user. The term "advertising technology" or "ad tech" refers to the technological tools and services that connected publishers selling advertising spaces to individuals or entities who sought to buy those advertising spaces ("advertisers"). These sales were often negotiated by other advertising companies ("brokers") and the sold ads were delivered by other companies ("ad servers"). Further, a number of other companies provided various online security services designed to help their clients combat malvertising. Collectively, all of the companies involved in this process are referred to herein as "advertising companies."

l. "Malware" referred to software programs designed to disrupt the intended operation of a computer or other device, gather sensitive information, gain access to the computer or other device, and take other unwanted actions.

m. An "exploit kit" was a class of malware that cybercriminals used to attack or "exploit" vulnerabilities in victim computer systems to gain unauthorized access to victim computer systems and then deliver additional malware to the victim system or perform other malicious activities.

n. A "locker" was a type of malware that cybercriminals used to impair a victim's access to or use of a computer system, program, or data and, often,

demand payment in order for the victim to regain access to the affected system, program, or data.

o. "Scareware" referred to messaging displayed to victim computer systems falsely claiming to have identified a virus or other issue with a victim Internet user's device, and then attempting to deceive the victim into buying or downloading dangerous software, providing remote access to the device, or disclosing personal identifying or financial information.

p. Online "scams" referred to messaging displayed to victim computer systems falsely claiming that the victim user had won a prize or initiating another scheme designed to induce the individual to provide remote access to the device or to disclose personal identifying or financial information.

q. "Malicious advertisements" or "malvertisements" were online advertisements that contained malicious computer code that forcibly redirected a victim's Internet browser to computers from which online scams, scareware, or malware were delivered or downloaded.

r. A "botnet" referred to a network of Internet-connected devices infected with malware that caused them to operate under common control.

s. A "counter-antivirus service" or "CAV service" provided information that malicious actors could use to determine whether computer viruses and other malware they created or obtained would be detected by antivirus software. While legitimate scanning services shared data about uploaded files with the antivirus community and notified users that they would do so, CAV services would

not share the results of the files they scanned with the antivirus community and made it possible for malicious actors to modify their malware to evade detection.

t. "Internet Protocol" or "IP" addresses were unique numeric addresses assigned to every Internet connection. Every device connected to the Internet was assigned an IP address in order to send and receive communications with other devices or services available on the Internet.

u. A "domain name" or "domain" was a simple, easy-to-remember way to identify computers, servers, and networks, using a series of characters (e.g., letters, numbers, or other characters such as www.google.com) that corresponded with a particular IP address.

The Conspiracy

4. The allegations contained in paragraphs 1 through 3 of this Count are realleged and incorporated here.

5. From in or about October 2013 through in or about March 2022, in the District of New Jersey and elsewhere, and in an offense begun outside the jurisdiction of any particular State or district of the United States, the defendants,

MAKSIM SILNIKAU,
a/k/a "Maksym Silnikov,"
a/k/a "Maksim Silnikov,"
a/k/a "Maxsim Andreyevich Silnikov,"
a/k/a "Maksym Mykolaiets,"
ANDREI TARASOV, and
VOLODYMYR KADARIYA,
a/k/a "Volodymyr Kadaria,"
a/k/a "Vladimir Kadaria,"

did knowingly and intentionally conspire and agree with each other and others to devise a scheme and artifice to defraud victim Internet users, publishers, and ad tech companies, including Company A, TMT, and Confiant, 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 defraud, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

Goal of the Conspiracy

6. It was the goal of the conspiracy for SILNIKAU, TARASOV, KADARIYA, and others to enrich themselves by: (i) distributing malvertisements under fictitious entities and online personas for the purposes of defrauding victim Internet users and disseminating malware, scareware, and scams to the users' devices to facilitate the further victimization of the Internet users; and (ii) selling the access they fraudulently obtained to victim Internet "traffic," compromised victim devices, and "logs" of sensitive victim information, to facilitate further efforts by cybercriminals to defraud the victims or deliver additional malware, scareware, and scams to their devices.

Manner and Means of the Conspiracy

7. It was part of the conspiracy that:

a. SILNIKAU, TARASOV, KADARIYA, and others, including Ivanov, developed and distributed malware and other malicious code and content

designed to gain and exploit unauthorized access to victim computer systems and to elicit personal identifying and financial information from victims, often without any user action or consent. One strain of malware that SILNIKAU and others took a leading role in disseminating was an exploit named the Angler Exploit Kit ("AEK"), which targeted web-based vulnerabilities in Internet browsers and associated plug-ins. The co-conspirators caused the dissemination of malware, scareware, and scams to victim computer systems through malvertising and the sale of access to malware and other malicious code and tools. Some of the co-conspirators' malware, such as AEK, could then be used by cybercriminals as vehicles for delivering additional malware onto a victim electronic device. For example:

i. On or about February 11, 2016, SILNIKAU sent an online chat message to TARASOV in which he shared administrative access to one or more computers associated with the operation of an exploit kit.

ii. On or about March 24, 2016, SILNIKAU sent online chat messages to a user of a predominantly Russian-language cybercrime forum ("Forum-1") to offer for sale a license to a "bundle" that included domains, servers, and other computer code needed to support malvertising.

iii. On or about July 27, 2016, SILNIKAU sent an online chat message to an associate through the direct messaging feature of another predominantly Russian-language cybercrime forum ("Forum-2") in which he sought an "affiliate" for a locker he controlled.

iv. On or about June 5, 2017, and June 6, 2017, SILNIKAU and TARASOV exchanged online chat messages in which they discussed a plan to develop a locker for locking the Internet browsers of victims who viewed their malvertisements.

b. SILNIKAU, TARASOV, KADARIYA, and others, including Ivanov, created and used dozens of online personas and fictitious entities to pose as legitimate advertising companies, in order to trick other advertising companies into delivering their malvertising campaigns. Examples of these entities included Veldex LTD, TwerkMedia, Broker Ltd., Deepreach Media, Face2Trade, Smart Media, and Polus Media.

c. SILNIKAU, TARASOV, KADARIYA, and others, including Ivanov, knowingly used fictitious and fraudulent aliases to falsely register domains, and knowingly used those domains to host malware, host malicious advertisements, and further malvertising-related activities, all in the course of committing the offenses charged in Counts 1 and 2, in violation of 18 U.S.C. § 3559(g)(1). Examples of domain names that were registered with false names and addresses to further the scheme included:

Registration Date (On or about)	Domain	False Alias
March 19, 2015	Mediavvads.uk	Dmitrij Zaleskis
August 14, 2015	3lf4vlxegj1luy6kbs.com	Dmitrij Zaleskis
March 6, 2019	easywaypixel.com	Allen Freemont
March 26, 2019	strlooks.com	Larry Revere

April 25, 2019	4bi.us	Aels Linden

d. SILNIKAU, TARASOV, KADARIYA, and others, including Ivanov, deceived, or caused to be deceived, advertising companies, including Company A, into facilitating the publication of malvertisements. Examples of the co-conspirators' fraudulent advertising campaigns include:

i. On or about April 24, 2014, Ivanov, using the alias "Dmitrij Zaleskis," caused malvertisements to be electronically transmitted through servers of Company A in the District of New Jersey and delivered to victim Internet users.

ii. Between on or about June 24, 2014, and July 15, 2014, Ivanov, using the alias "Dmitrij Zaleskis" and the entity "Veldex Ltd.," caused malvertisements to be electronically transmitted through servers of Company A in the District of New Jersey and delivered to victim Internet users.

iii. Between in or about February 2019 and in or about June 2019, one or more co-conspirators, using the aliases "Rahul Gill" and "David Haimovich," and the entity "Face2Trade" caused malvertisements to be electronically delivered to the servers of U.S.-based ad tech and online security companies in an attempt to deliver scareware to victim Internet users via the domain windowsappcenter.secures-updatesr.pw.

iv. On or about October 16, 2019, one or more co-conspirators, using the entity "Smart Media," caused a malvertisement to be electronically delivered to a computer in Kansas City, Missouri being operated by an individual known to the Grand Jury ("Person A") via the domain bigstartrade.com.

v. Between in or about May 2020 and in or about July 2020, one or more co-conspirators, using the entity "Smart Media," caused malvertisements to be electronically delivered to the servers of U.S.-based ad tech and online security companies, including Company A, in an attempt to deliver malicious content to victim Internet users via advertising campaigns associated with the domains beams.co.jp and lightinthebox.com.

e. SILNIKAU, TARASOV, KADARIYA, and others developed, used, and shared traffic direction systems, also known as traffic distribution systems, (collectively, "TDSes") that managed the online content that would be delivered to Internet users. The TDSes used by the co-conspirators often employed sophisticated technologies and computer code developed by TARASOV and others to limit the deployment of their malvertisements to victim Internet devices that were deemed susceptible to compromise or exploitation. These constraints on the distribution of malvertisements reduced the likelihood that co-conspirators' advertising campaigns would be quickly detected and blocked by online security companies and other ad tech companies. Internet users who were not deemed as susceptible to compromise or exploitation would be delivered non-malicious advertising content. The co-conspirators often discussed their development and use of TDSes in online chats, including:

i. In or about January 2016, TARASOV and KADARIYA exchanged online chat messages in which TARASOV agreed to a build a TDS for KADARIYA for $2500 and provided guidance on how to operate the TDS.

ii. On or about July 4, 2016, TARASOV and KADARIYA exchanged online chat messages in which they discussed TARASOV's development of traffic redirection code that could support the operation of KADARIYA's TDS.

iii. Between on or about February 8, 2017, and on or about February 20, 2017, TARASOV and Co-Conspirator A exchanged online chat messages in which they discussed troubleshooting technical issues associated with their TDS and traffic redirection code, and instructions that the "boss" had provided.

iv. On or about April 11, 2017, TARASOV sent online chat messages to an associate in which he explained that monikers of SILNIKAU and another co-conspirator used the TDS of a moniker associated with KADARIYA.

v. On or about June 17 and 18, 2018, SILNIKAU sent online chat messages to TARASOV about their TDS.

f. SILNIKAU, TARASOV, KADARIYA, and others, including Ivanov, developed sophisticated technologies and computer code to refine their malvertisements, malware, TDSes, and other infrastructure to conceal the malicious nature of their ads and limit the deployment of their malvertisements to victim Internet devices that were deemed susceptible to compromise or exploitation. These strategies included using CAV services to test malware and developing and deploying a range of computer code that helped the co-conspirators hide malicious computer code within the co-conspirators' malvertisements or domains to which the victim users were directed. The co-conspirators also attempted to refine their techniques by

seeking information about how U.S.-based advertising servers, brokers, and security firms identified their advertisements as malicious. For example:

i. On or about February 11, 2016, SILNIKAU and TARASOV exchanged online chat messages in which they discussed cloaking malvertisements.

ii. Between in or about May 2016 and in or about July 2016, SILNIKAU, KADARIYA or other co-conspirators used accounts with a particular CAV service to run hundreds of thousands of scans of their files.

iii. Between on or about January 23, 2017, and on or about January 24, 2017, TARASOV separately exchanged online chat messages with Co-Conspirator A and SILNIKAU concerning TMTs effectiveness at identifying their malvertisements. As part of the chats, SILNIKAU directed TARASOV to start corresponding with TMT.

iv. On or about July 4, 2017, SILNIKAU sent online chat messages to TARASOV indicating that a co-conspirator's code had failed to prevent a list of domains from being blocked as malicious for forced redirection.

v. On or about August 15 and on or about August 16, 2017, TARASOV and Co-Conspirator A exchanged online chat messages in which they attempted to determine why the co-conspirators' malvertisements associated with the entity Face2Trade were getting banned.

vi. On or about October 16, 2017, TARASOV sent online chat messages to Co-Conspirator A requesting access to a server involved in the co-conspirators' malvertising activity for the purposes of troubleshooting a coding issue.

vii. Between in or about July 2017 and in or about September 2018, Ivanov and other co-conspirators used fake personas associated with the entity "TwerkMedia" to correspond with TMT about their methodology for flagging malvertisements. The co-conspirators also used TMT's malware scanning service to test if their malvertisements could be detected by TMT.

viii. On or about June 5, 2018, SILNIKAU and TARASOV exchanged online chat messages in which they discussed how they could improve the code used by their malvertisements to evade detection by Company A.

ix. In or about January 2019 and in or about July 2019, TARASOV used malicious advertisements to send computer code to Confiant's computers designed to extract details about how Confiant screened advertisements for malicious content.

g. After advertising companies detected their malvertisements, SILNIKAU, TARASOV, KADARIYA, and others, including Ivanov, often made or caused others to make false and misleading statements in an effort to avoid suspension of their campaigns or advertising accounts. When such efforts failed, the co-conspirators often either switched advertisers or submitted future ad campaigns to the same companies under different online personas and entities. For example:

i. On or about August 10, 2018, KADARIYA and Ivanov exchanged voice messages in which they discussed how to respond to advertising platforms that were refusing their advertisements on suspicion of "malware."

ii. On or about September 24, 2018, a co-conspirator using the alias "Hugo Rossi" from the entity Smart Media agreed his client would "remove pieces of code from the [ad] tag that can cause suspicion," but then sought a "detailed explanation" about what exactly needed to be fixed.

iii. On or about March 4, 2020, a co-conspirator using the alias "Amelia Jenkin" explained to a Cyprus-based advertising company that a flagged malvertisement was uploaded in a "terrible mistake" and asked that the company "forget this confusion."

h. SILNIKAU, TARASOV, KADARIYA, and others, including Ivanov, shared online accounts, fictitious or fraudulent personas, domains, computer infrastructure, and tools.

i. SILNIKAU, KADARIYA, and others attempted to further profit from their malvertising campaigns by selling to other affiliates the access they fraudulently obtained to (i) victim Internet users—so-called Internet "traffic"; (ii) compromised victim devices—so-called "loads" or "bots"; and (iii) information that was stolen from victims and recorded in "logs," such as banking information and login credentials. SILNIKAU, KADARIYA, and others knew and intended to aid and abet the affiliates' further exploitation of Internet users through scareware and delivery of additional malware. For example:

i. On or about February 28, 2014, SILNIKAU posted a message on Forum-1 offering to sell "loads" in the United States and elsewhere.

ii. On or about June 6, 2014, SILNIKAU posted a message on Forum-1 offering to sell U.S. "traffic."

iii. On or about July 28, 2014, KADARIYA posted a message on Forum-2 offering to sell access to "loads," including in the U.S., that could be used as part of a bank botnet.

iv. In or about September 2015, SILNIKAU used a direct messaging feature of Forum-2 to offer bank "logs" to another Forum-2 user.

v. On or about January 22, 2020, SILNIKAU used the direct messaging feature of Forum-2 to offer "logs" to a buyer who sought "Usa logs."

j. SILNIKAU, TARASOV, KADARIYA, and others supported the conspiracy's effort to sell illicit material to other cybercriminals by vouching for each other on cybercrime forums, including on Forum-2.

All in violation of Title 18, United States Code, Sections 1349 and 3559(g)(1).

Count 2
(Conspiracy to Commit Computer Fraud and Abuse)

1. The allegations contained in paragraphs 1 through 3 and 7 of Count 1 of this Indictment are realleged and incorporated here.

2. From in or about October 2013 through in or about May 2022, in the District of New Jersey and elsewhere, and in an offense begun outside the jurisdiction of any particular State or district of the United States, the defendants,

MAKSIM SILNIKAU,
a/k/a "Maksym Silnikov,"
a/k/a "Maksim Silnikov,"
a/k/a "Maxsim Andreyevich Silnikov,"
a/k/a "Maksym Mykolaiets,"
ANDREI TARASOV, and
VOLODYMYR KADARIYA,
a/k/a "Volodymyr Kadaria,"
a/k/a "Vladimir Kadaria,"

did knowingly and intentionally conspire and agree with each other and others to commit and aid and abet offenses against the United States, that is:

a. to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss to persons during a one-year period from the co-conspirators' course of conduct affecting protected computers aggregating at least $5,000 in value, and cause damage affecting 10 or more protected computers during a one-year period, contrary to Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B); and

b. to intentionally access a protected computer without authorization, and thereby obtain information from a protected computer for

purposes of private financial gain, and in furtherance of any criminal and tortious act in violation of the laws of the United States, contrary to Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B).

Goal of the Conspiracy

3. It was the goal of the conspiracy for SILNIKAU, TARASOV, KADARIYA, and others to enrich themselves through computer hacking by (i) delivering malware and aiding and abetting the distribution of malware to victim Internet devices through malvertising and other means, and (ii) using malware to steal sensitive victim information, such as banking information and login credentials, to enable further efforts to defraud victim Internet users.

Manner and Means of the Conspiracy

4. To carry out the conspiracy and effect its illegal objects, SILNIKAU, TARASOV, KADARIYA, and others, including Ivanov, engaged in a number of manner and means, including those described in Paragraph 7 of Count 1 of this Indictment.

Overt Acts in Furtherance of the Conspiracy

5. The acts specified in paragraph 7, subparagraphs a-c, d.i-ii, e.i-ii, f.ii, g.i, and i.i-v of Count 1 of this Indictment were also committed in furtherance of the conspiracy alleged in this Count and are realleged and incorporated here.

6. Additionally, on or about August 14, 2015, a co-conspirator registered the domain 3lf4vlxegj1luy6kbs.com, which was registered using the alias "Dmitrij

Zaleskis" and was thereafter used to infect thousands of victim devices with malware in a one-year period, including the computer of G.S. of Ogdensburg, New Jersey.

All in violation of Title 18, United States Code, Sections 371 and 3559(g)(1).

Counts 3-4
(Wire Fraud)

7. The allegations contained in paragraphs 1 through 3 and 7 of Count 1 of this Indictment are realleged and incorporated here.

8. On or about the dates set forth below, in the District of New Jersey and elsewhere, and in an offense begun outside the jurisdiction of any particular State or district of the United States, the defendants,

MAKSIM SILNIKAU,
a/k/a "Maksym Silnikov,"
a/k/a "Maksim Silnikov,"
a/k/a "Maxsim Andreyevich Silnikov,"
a/k/a "Maksym Mykolaiets,"
ANDREI TARASOV, and
VOLODYMYR KADARIYA,
a/k/a "Volodymyr Kadaria,"
a/k/a "Vladimir Kadaria,"

did knowingly and intentionally devise a scheme and artifice to defraud victim Internet users and advertising companies, including Company A, 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 defraud, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce to New Jersey, certain writings, signs, signals, and sounds, namely the specified advertisements described below, each constituting a separate Count of this Indictment:

Count	Approximate Date (On or About)	Description
3	May 20, 2020, through June 11, 2020	A malicious advertisement that "Smart Media" caused to be electronically transmitted to the servers of Company A, in connection with a malvertising campaign associated with the domain beams.co.jp.
4	June 15, 2020, through July 15, 2020	A malicious advertisement that "Smart Media" caused to be electronically transmitted to the servers of Company A, in connection with a malvertising campaign associated with the domain lightinthebox.com.

In violation of Title 18, United States Code, Section 1343 and Section 2.

FORFEITURE ALLEGATION AS TO COUNTS 1, 3, AND 4

1. As a result of committing the offenses charged in Counts 1, 3, and 4 of this Indictment, the defendants,

MAKSIM SILNIKAU,
a/k/a "Maksym Silnikov,"
a/k/a "Maksim Silnikov,"
a/k/a "Maxsim Andreyevich Silnikov,"
a/k/a "Maksym Mykolaiets,"
ANDREI TARASOV, and
VOLODYMYR KADARIYA,
a/k/a "Volodymyr Kadaria,"
a/k/a "Vladimir Kadaria,"

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of the said offenses, and all property traceable thereto.

FORFEITURE ALLEGATION AS TO COUNT 2

2. As a result of committing the offense charged in Count 2 of this Indictment, the defendants,

MAKSIM SILNIKAU,
a/k/a "Maksym Silnikov,"
a/k/a "Maksim Silnikov,"
a/k/a "Maxsim Andreyevich Silnikov,"
a/k/a "Maksym Mykolaiets,"
ANDREI TARASOV, and
VOLODYMYR KADARIYA,
a/k/a "Volodymyr Kadaria,"
a/k/a "Vladimir Kadaria,"

shall forfeit to the United States:

a. pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of the offense charged in Count 2 of this Indictment; and

b. pursuant to Title 18, United States Code, Section 1030(i), all right, title, and interest in any personal property that was used or intended to be used to commit or to facilitate the commission of the offense charged in Count 2 of this Indictment.

SUBSTITUTE ASSETS PROVISION
(Applicable to All Forfeiture Allegations)

If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty.

the United States shall be entitled, pursuant to Title 21, United States Code, Section 853(p) (as incorporated by Title 28, United States Code, Section 2461(c), Title 18, United States Code, Section 1030(i), and Title 18, United States Code, Section 982(b)), to forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.

A TRUE BILL,

[redacted]

Foreperson

Philip R. Sellinger

PHILIP R. SELLINGER
UNITED STATES ATTORNEY

CASE NUMBER: _____

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

MAKSIM SILNIKAU,
a/k/a "Maksym Silnikov," a/k/a "Maksim Silnikov,"
a/k/a "Maxsim Andreyevich Silnikov," a/k/a "Maksym Mykolaiets,"
ANDREI TARASOV, and
VOLODYMYR KADARIYA,
a/k/a "Volodymyr Kadaria," a/k/a "Vladimir Kadaria"

INDICTMENT FOR

18 U.S.C. §§ 1349, 3559(g)(1), 371, 1343, 2

A True Bill,

[redacted]

Foreperson

PHILIP R. SELLINGER
UNITED STATES ATTORNEY

ANDREW M. TROMBLY
ASSISTANT U.S. ATTORNEY

LOUISA K. BECKER, CHRISTEN GALLAGHER, AND AARASH A. HAGHIGHAT
TRIAL ATTORNEYS, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION