

Approved: *Thomas G. A. Brown*
THOMAS G. A. BROWN/NICOLE W. FRIEDLANDER
Assistant United States Attorneys

Before: THE HONORABLE RONALD L. ELLIS
United States Magistrate Judge
Southern District of New York

----- x
SEALED COMPLAINT
UNITED STATES OF AMERICA :
 :
- v. - : Violations of 18 U.S.C.
 : §§ 1030(a)(2) and
 : (a)(4), 1030(b), 1030
NIKITA VLADIMIROVICH KUZMIN, : (c)(2)(B)(i)-(iii) and
 : (c)(3),
 : 1029(a)(5), 1029(b)(1)
Defendant. : and (b)(2), 1349, and 2
 :
 : COUNTY OF OFFENSE:
 : NEW YORK

----- x
SOUTHERN DISTRICT OF NEW YORK, ss.:

M. KATHRYN SCOTT, being duly sworn, deposes and says that she is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE

(Computer Intrusion Obtaining Information)

1. From at least in or about March 2007, through in or about November 2010, in the Southern District of New York and elsewhere, NIKITA VLADIMIROVICH KUZMIN, the defendant, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, intentionally accessed and attempted to access a computer without authorization, and thereby obtained and attempted to obtain information contained in a financial record of a financial institution, and of a card issuer as defined in 15 U.S.C. § 1602(n), and from a protected computer, the value of which exceeded \$5,000, to wit, using the computer virus known and described as the "Gozi Virus," KUZMIN accessed and attempted to access without authorization computers owned by private

individuals and businesses, and thereby obtained and attempted to obtain the bank account information of such individuals and businesses, which information was used fraudulently to withdraw millions of dollars from such individuals' and businesses' bank accounts.

(Title 18, United States Code,
Sections 1030(a)(2), 1030(b), 1030(c)(2)(B)(i)-(iii), and 2.)

COUNT TWO

(Computer Intrusion Furthering Fraud)

2. From at least in or about March 2007, up to and including in or about November 2010, in the Southern District of New York and elsewhere, NIKITA VLADIMIROVICH KUZMIN, the defendant, knowingly and with intent to defraud, accessed and attempted to access a protected computer without authorization, and by means of such conduct furthered the intended fraud and obtained something of value exceeding \$5,000, to wit, using the computer virus known and described as the "Gozi Virus," KUZMIN accessed and attempted to access without authorization computers owned by private individuals and businesses, and thereby obtained and attempted to obtain the bank account information of such individuals and businesses, which information was used fraudulently to withdraw millions of dollars from such individuals' and businesses' bank accounts.

(Title 18, United States Code,
Sections 1030(a)(4), 1030(b), 1030(c)(3)(A), and 2).

COUNT THREE

(Conspiracy to Commit Bank Fraud)

3. From at least in or about March 2007, up to and including in or about November 2010, in the Southern District of New York and elsewhere, NIKITA VLADIMIROVICH KUZMIN, the defendant, and others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit an offense against the United States, to wit, to violate Title 18, United States Code, Section 1344.

4. It was a part and an object of the conspiracy that NIKITA VLADIMIROVICH KUZMIN, the defendant, and others known and unknown, unlawfully, willfully, and knowingly would and did execute and attempt to execute a scheme and artifice to defraud a

financial institution, the deposits of which were insured by the Federal Deposit Insurance Corporation, and to obtain monies, funds, credits, assets, securities, and other property owned by and under the custody and control of that financial institution by means of false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344.

Overt Acts

5. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about October 30, 2009, NIKITA VLADIMIROVICH KUZMIN, the defendant, sent an instant message communication to a co-conspirator about bank accounts.

b. On or about January 9, 2010, KUZMIN offered to provide a co-conspirator with access to the Gozi Virus.

c. On or about August 13, 2010, \$8,710 was transferred out of the bank account of a victim in Bronx, New York ("Victim-1") without Victim-1's consent after Victim-1's bank account information was stolen from a computer infected with the Gozi Virus.

(Title 18, United States Code, Sections 1349 and 2).

COUNT FOUR

(Conspiracy to Commit Access Device Fraud)

6. From in or about March 2007, up to and including in or about November 2010, in the Southern District of New York and elsewhere, NIKITA VLADIMIROVICH KUZMIN, the defendant, and others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit an offense against the United States, to wit, to violate Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3), and 1029(a)(5).

7. It was a part and an object of the conspiracy that NIKITA VLADIMIROVICH KUZMIN, the defendant, and others known and unknown, unlawfully, willfully and knowingly, and with intent to defraud, in an offense affecting interstate and foreign commerce, would and did traffic in and use one and more unauthorized access

devices during a one-year period, and by such conduct would and did obtain a thing of value aggregating \$1,000 and more during that period, in violation of Title 18, United States Code, Section 1029(a)(2).

8. It was further a part and an object of the conspiracy that NIKITA VLADIMIROVICH KUZMIN, the defendant, and others known and unknown, unlawfully, willfully and knowingly, and with intent to defraud, in an offense affecting interstate and foreign commerce, would and did possess fifteen and more devices which were counterfeit and unauthorized access devices, in violation of Title 18, United States Code, Section 1029(a)(3).

9. It was further a part and an object of the conspiracy that NIKITA VLADIMIROVICH KUZMIN, the defendant, and others known and unknown, unlawfully, willfully and knowingly, and with intent to defraud, in an offense affecting interstate and foreign commerce, would and did effect transactions, with one and more access devices issued to another person and persons, to receive payment and another thing of value during a one-year period the aggregate value of which was equal to or greater than \$1,000, in violation of Title 18, United States Code, Section 1029(a)(5).

Overt Acts

10. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about October 5, 2009, NIKITA VLADIMIROVICH KUZMIN, the defendant, sent an instant message communication to a co-conspirator about stolen bank account information.

b. On or about October 30, 2009, KUZMIN sent an instant message communication to a co-conspirator about bank accounts.

c. On or about January 9, 2010, KUZMIN offered to provide a co-conspirator with access to the Gozi Virus.

d. On or about August 13, 2010, \$8,710 was transferred out of the bank account of Victim-1, of Bronx, New York, without Victim-1's consent after Victim-1's bank account information was stolen from a computer infected with the Gozi Virus.

(Title 18, United States Code, Section 1029(b)(2)).

COUNT FIVE

(Access Device Fraud)

11. From at least in or about March 2007, up to and including in or about November 2010, in the Southern District of New York and elsewhere, NIKITA VLADIMIROVICH KUZMIN, the defendant, unlawfully, willfully, and knowingly, and with intent to defraud, in an offense affecting interstate and foreign commerce, did effect and attempt to effect transactions, with one and more access devices issued to another person and persons, to receive payment and another thing of value during a one-year period the aggregate value of which was equal to or greater than \$1,000, to wit, KUZMIN provided a computer virus known and described as the "Gozi Virus" to others for the purpose of stealing the bank account information of individuals and businesses, which information was used fraudulently to withdraw monies from such individuals' and businesses' bank accounts in amounts totaling more than \$1,000 within a one-year period, without authorization from the account holders.

(Title 18, United States Code, Sections 1029(a)(5),
1029(b)(1), and 2.)

The bases for my knowledge and the foregoing charges are, in part, as follows:

12. I am a Special Agent with the FBI. I am currently assigned to the Computer Intrusion Squad of the New York Division of the FBI, and have received training in computer technology, computer fraud, intellectual property crimes, and white collar crimes. Prior to joining the FBI, I worked for approximately five years as an electrical engineer in the private sector designing computer hardware and software. I am familiar with the facts and circumstances set forth below from my personal participation in the investigation, including my examination of reports and records, interviews I have conducted, and conversations with other law enforcement officers and other individuals. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, unless noted otherwise.

TECHNICAL BACKGROUND

13. Based on my training and experience, I am aware of the following:

a. **Internet Service Provider ("ISP").** An ISP is a commercial service that provides Internet connections for its subscribers. In addition to providing access to the Internet via telephone or other telecommunications lines, ISPs may also provide Internet e-mail accounts and other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with them. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, and other information.

b. **IP address.** The Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods. Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

c. **Instant messaging.** Instant messaging (IM) is a collection of technologies that create the possibility of real-time text-based communication between two or more participants via the Internet. Instant messaging allows for the immediate transmission of communications, including immediate receipt of acknowledgment or reply.

d. **Jabber.** Jabber is another name for the Extensible Messaging and Presence Protocol (XMPP), an Internet protocol (or set of rules) that allows for near-real-time instant messaging and presence information. Jabber is an open system where anyone who has a domain name and a suitable Internet connection can run their own Jabber server and talk to users on other Jabber servers.

e. **Server.** A server is a centralized computer that provides services for other computers connected to it via a network or the Internet. The computers that use the server's services are sometimes called "clients." When a user accesses email, Internet web pages, or accesses files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network or Internet. Notably, server computers

can be physically located in any location; for example, it is not uncommon for a network's server to be located hundreds (or even thousands) of miles away from the client computers. In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a "Web server." Similarly, a server that only stores and processes e-mail is known as a "mail server."

f. **Trojan.** A trojan is malicious software, or malware, that appears to perform a desirable function for the user prior to run or install but instead facilitates the unauthorized access of the user's computer system. The Gozi Virus is a trojan.

g. **Bot.** A bot is a computer that has been compromised by malicious software for use in completing malicious and/or illegal tasks via remote direction. Most users that have a computer acting as a bot are not aware that their computers have been compromised. "Compromised computer" is synonymous with bot, and either may be used based on context. A larger number of bots, called a bot network or botnet, are typically controlled by one computer called a command and control server. The owner of the command and control server can direct the botnet to, among other things, send spam, operate as proxies (blindly forwarding Internet data), or participate in other cybercrime.

h. **Malware.** Short for "malicious software," malware is computer software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of hostile or intrusive program code. Computer viruses and spyware are types of malware.

SUMMARY OF THE INVESTIGATION

14. For approximately the past six months, the FBI, in conjunction with law enforcement authorities and private sector information security experts throughout the United States and Europe, has been investigating an international identity theft ring that is engaged in a scheme to defraud individuals and businesses in the United States and abroad using the "Gozi Virus," a malicious computer program. The Gozi Virus is designed to steal personal bank account information from computers on a vast scale, while remaining virtually undetectable in the computers it infects. As set forth more fully below, NIKITA VLADIMIROVICH KUZMIN, the defendant, who is based primarily in Russia, is a key member of this identity theft ring.

15. As set forth more fully below, NIKITA VLADIMIROVICH KUZMIN, the defendant, and his co-conspirators created and used the Gozi Virus to obtain account access information (such as account numbers, usernames, and passwords) for the bank accounts of individuals and businesses (the "Victim Accounts"), and to steal money from the Victim Accounts. In the past, the co-conspirators used the Gozi Virus primarily to target accounts at European banks. Recently, however, they have begun using the Gozi Virus to attack U.S. bank accounts, including, at a minimum, dozens of bank accounts at Bank-1, a large financial institution which is headquartered in New York, New York. Bank-1 provides a broad range of banking and non-banking financial services and products both within and outside of the United States. Bank-1's deposits are insured by the Federal Deposit Insurance Corporation.

16. Since its inception, the Gozi Virus has infected, at a minimum, tens of thousands of computers around the world and approximately 25,000 United States IP addresses, and has caused, at the least, tens of millions of dollars in losses.

BACKGROUND ON THE GOZI VIRUS

17. Based on my participation in this investigation, I know that among the ways that the Gozi Virus infects a victim's computer is when the victim receives and clicks on an apparently-benign .pdf document (i.e., a document in the widely used .pdf format, a format which is easily shared among different computer operating systems). Upon clicking on the .pdf document, the Gozi Virus is secretly downloaded onto the victim's computer, where it is generally undetectable by anti-virus software. Once downloaded, the Gozi Virus collects data from the infected computer in order to capture the victim's bank account user name, password, and other vital security information. The stolen bank account data is then used fraudulently to transfer funds out of the Victim Accounts and, ultimately, into the possession of NIKITA VLADIMIROVICH KUZMIN, the defendant, and his co-conspirators.

18. As set forth below, based on my experience, participation in this investigation, review of documents prepared by, and conversations with, law enforcement agents and private sector information security experts, I know that there is a particular command-and-control server for computers infected with the Gozi Virus ("Domain Name-2").

THE INVESTIGATION

I. The Identification of the User of Alias-1 as the Promoter of the Gozi Virus

19. I have spoken with and reviewed a report prepared by an information security expert ("Information Security Expert-1") who is generally credited with identifying the Gozi Virus in or about March 2007. Based on my review of the report and my conversations with the Information Security Expert, I have learned, in substance and in part, the following:

a. Information Security Expert-1 initially identified the Gozi Virus when he analyzed a computer infected with a previously unidentified computer virus. His analysis revealed that this virus, which he subsequently named "Gozi," was configured to capture usernames and passwords from the infected computer and send that data to a particular IP address (the "IP Address").

b. Information Security Expert-1 subsequently accessed a publicly available index of the directories on the server associated with the IP Address. In one such directory, which was also publicly available, Information Security Expert-1 found a login page for subscribers to a service that provides access to stolen information obtained by the Gozi Virus. This login page identified the service as the "Alias-1¹ Service." Thus, Information Security Expert-1 determined that the same server both received the usernames and passwords stolen by the Gozi Virus, and also, through the Alias-1 Service, enabled others to gain access to such stolen information.

c. I have reviewed instant messages, or "chats," obtained pursuant to a series of search warrants for a particular Jabber server which were issued by United States Magistrate Judges in the District of Nebraska in the course of a related cybercriminal investigation (the "Nebraska Search Warrant Chats").² These chats, which took place in Russian and of which I have reviewed preliminary translations, involved an individual using an email address of "Alias-1@[Domain Name-1].com" (the "Alias-1 Email Address"). Based on my training and experience,

¹ "Alias-1" is a distinctive series of numbers which are also believed to be used as a nickname by NIKITA VLADIMIROVICH KUZMIN, the defendant, as described below.

² The search warrants were issued in September 2009, December 2009, March 2010, and May 2010, respectively.

and my conversations with the Information Security Expert and other FBI cybercrime agents, I know that cybercriminals are highly protective of their online aliases (of which they often have several), which serve as their brand names and identities, and are unlikely to allow others to assume those aliases. Thus, based on the use of Alias-1 in both the name of the Alias-1 Service and the Alias-1 Email Address, as well as the contents of the chats involving the Alias-1 Email Address, which are set forth below, I believe that the person using the Alias-1 Email Address is the same person offering the Alias-1 Service discussed above.

d. The following are preliminary English translations of excerpts of certain pertinent Nebraska Search Warrant chats³ involving the Alias-1 Email Address and email addresses of certain co-conspirators ("CC-2," "CC-3," and "CC-4"), among others, and my preliminary interpretation, in brackets, of some of the terms used in the chats, which is based on my training, experience, and the information developed in the investigation. In sum, these chats show the user of the Alias-1 Email Address offering the Alias-1 Service, and discussing the distribution and sale to co-conspirators of bank account information from victims around the world:

October 5, 2009

<u>Time</u>	<u>Author</u>	<u>Message</u>
10:57:20:63 PM	CC-2	I used to get downloads [meaning stolen bank account information] from you long time ago
10:57:24:95 PM	CC-2	quality was good [meaning the account information was valid]
10:57:37:76 PM	CC-2	it was 2-3 years ago)
10:57:48:47 PM	CC-2	my own supplies [meaning sources of account information] are exhausted now
10:58:35 PM	CC-2	so I'm thinking maybe we can find an acceptable solution for you as well as for me

³ All chats set forth in this Complaint (a) are relevant excerpts of longer chats; (b) originally occurred in Russian; and (c) are preliminary translations which I have reviewed.

11:00:28 PM Alias-1 what country? [asking which country CC-2 would like stolen account information from]

11:00:34:13 PM CC-2 es [meaning Spain]

11:01:00:13 PM Alias-1 I'll ask partners.

11:01:05:99 PM CC-2 I'm also interested in other countries

11:01:07:75 PM CC-2 uk us [meaning, the bank account information of victims in the United Kingdom and United States]

11:01:18:46 PM CC-2 when can you give me an answer?

11:01:29:17 PM Alias-1 tomorrow

11:02:41:74 PM CC-2 okay

October 29, 2009

<u>Time</u>	<u>Author</u>	<u>Message</u>
11:09:26:65 PM	CC-3	hey it's me
11:09:32:08 PM	CC-3	what do you mean send with yours
11:09:39:50 PM	CC-3	is it so difficult shit to ask which exploit [meaning computer code used to take advantage of vulnerabilities on a victim computer to install malware]?
11:15:32:30 PM	Alias-1	Fragus [meaning the name of the "exploit" or code]
11:15:44:25 PM	CC-3	I see I have fragus too
11:30:02:68 PM	Alias-1	give me your crypter [meaning the code used to encrypt malware]
11:30:14:53 PM	CC-3	562420782

October 30, 2009

<u>Time</u>	<u>Author</u>	<u>Message</u>
02:31:25:90 AM	Alias-1	ha ha, I uploaded one bot for my spain [meaning a botnet targeting Spain] and already entered everything
03:20:35:23 AM	CC-3	is acc [meaning bank account] alive?
03:21:17:46 AM	Alias-1	let me look
03:22:06:30 AM	Alias-1	uh-huh
03:22:53:08 AM	CC-3	how much [meaning how much money] is on the acc ?
03:22:59:64 AM	CC-3	and which acc pers or corp [meaning personal or corporate account]?
03:23:24:71 AM	Alias-1	pers 2k
03:23:30:02 AM	Alias-1	I only did pers for your
03:23:50:35 AM	CC-3	f[*]cking great
03:23:51:59 AM	CC-3	what about bbvanetoffice [possibly referring to a website related to BBVA Bank in Spain]?
03:23:59:57 AM	CC-3	it's a fact
03:23:59:29 AM	CC-3	we talked about two banks
03:24:03:93 AM	CC-3	and also
03:24:06:35 AM	CC-3	15 coord is not good enough
03:24:14:94 AM	CC-3	you can only hit 3 accs out of 10 [meaning information for only three accounts out of every ten accounts would normally be valid]

January 9, 2010

<u>Time</u>	<u>Author</u>	<u>Message</u>
09:46:52:27 PM	CC-4	hi
09:54:11:18 PM	Alias-1	hi
09:54:46:99 PM	CC-4	what do we decide about exploit [meaning computer code used to take advantage of vulnerabilities in a computer to install malware]
09:56:04:71 PM	Alias-1	Remind me the conditions, how many downloads what countries do I have
10:01:13:33 PM	CC-4	I'm downloading it es pt fi [meaning account information for accounts in Italy, Spain, Portugal and Finland], mine - es and it [meaning Spain and Italy], you'll have 1k downloads a day [meaning 1 kilobyte worth of bank account information]
	* * *	
10:45:30:86 PM	CC-4	pt and fi [meaning account information for accounts in Portugal and Finland] will start going now
10:56:33:35 PM	Alias-1	and is this total volume for pt and fi? Or you can increase it for \$?
11:07:33:32 PM	CC-4	it just probably didn't warm up yet
11:07:38:52 PM	CC-4	but it can be increased
11:45:27:36 PM	Alias-1	good
11:45:59:93 PM	CC-4	do you have loader [meaning an application for loading malware onto a victim computer]?
11:47:43:03 PM	Alias-1	nah

11:47:48:53 PM Alias-1 but response is good even without it

11:47:55:33 PM Alias-1 90% of my troy [meaning trojan virus] response is from this exploit

11:48:14:96 PM CC-4 I don't have it

11:48:53:08 PM Alias-1 but what do you download there in general?

11:49:11:99 PM CC-4 zeus [meaning the Zeus Virus, a notorious trojan virus similar in effect to the Gozi Virus]

11:51:27:28 PM CC-4 how much pt and fi [meaning Portugal and Finland] accumulated there?

11:53:26:24 PM Alias-1 Portugal
Finland 76
Korea, Republic of 9

11:53:44:50 PM Alias-1 why do you need zeus, take my trojan [meaning the Gozi Virus]. Mine is much cooler, it doesn't get burned by proactives [meaning a certain type of anti-virus detection method] and works with win7 and vista [meaning the Windows 7 and Vista operating systems]

11:54:13:25 PM CC-4 what about fakes are they going to work with zeus?

11:54:29:85 PM Alias-1 fakes are exactly that redirect to another page?

11:54:41:58 PM CC-4 yes

11:54:59:71 PM Alias-1 yes, there is this function

11:55:42:68 PM CC-4 how much your trojan will cost me?
[meaning, how much do you charge
for access to the Gozi Virus (i.e.,
the access provided through the
Alias-1 Service)?]

11:56:33:00 PM Alias-1 2k a month including hosting and
support [meaning \$2000 a month,
which includes certain technical
assistance with the Alias-1
Service]

11:56:37:33 PM Alias-1 so you'll just have to upload

11:56:43:22 PM Alias-1 I have the most convenient admin

11:56:47:09 PM Alias-1 and bots [meaning botnets] sharing

11:56:55:38 PM Alias-1 you can give it [meaning access to
the botnet] to different people,
checker and co-workers

February 23, 2010

<u>Time</u>	<u>Author</u>	<u>Message</u>
12:28:22:32 AM	Alias-1	it's up to you I have .exe [meaning a type of program known as an "executable"] which gives at least 200-300 bucks from 1k of downloads for US UK CA AU NZ [meaning, it will provide returns of \$200 - \$300 in stolen proceeds for every 1000 sets of stolen information from victims in the United States, United Kingdom, Canada, Australia, and New Zealand]
12:28:39:68 AM	Alias-1	now I need CH, PT and DE [meaning Switzerland, Portugal and Germany] countries.
12:28:43:81 AM	Alias-1	switzerland portugal and germany

* * *

12:38:50:58 AM Alias-1

what do you say about US UK CA AU NZ? You can sell these downloads to someone (for example there are buyers for UK), and also work on my partner's program.

20. In the course of this investigation, I have also reviewed instant messages obtained pursuant to a search warrant issued by a United States Magistrate Judge for the Southern District of New York for a second Jabber server. Stored on that server were Russian-language "chats" involving the Alias-1 Email Address (the "SDNY Search Warrant Chats"), including the following:

<u>Date/Time</u>	<u>Author</u>	<u>Message</u>
9/29/2010 03:14:37 AM	Alias-1	my bot [meaning botnet] - https://[Domain Name-2].com. . .

Based on my experience, participation in this investigation, review of documents prepared by, and conversations with, law enforcement agents and private sector information security experts, I know that "[Domain Name-2]," which the user of the Alias-1 Email Address identified as "my bot," is the command-and-control server for the Gozi Virus. In particular, private sector information security experts have analyzed computers infected with the Gozi Virus and have learned, based on that analysis, that Domain Name-2 serves as the command-and-control server for the Gozi Virus.

II. The Identification of NIKITA VLADIMIROVICH KUZMIN, the Defendant, as the User of Alias-1

21. I have reviewed certain SDNY Search Warrant Chats involving an individual using a particular alias ("Alias-2") and an email address of Alias-2@[Domain Name-1] (the "Alias-2 Email Address"). In sum, as set forth below, based on the content of those and other SDNY Search Warrant Chats, as well as other information obtained in this investigation, other law enforcement agents and I have determined that the user of Alias-1 and Alias-2 is the same individual, and that such individual is NIKITA VLADIMIROVICH KUZMIN, the defendant.

A. The Identification of the User of Alias-1 and Alias-2 as the Same Person

22. I have reviewed a report prepared by an information security expert who obtained copies of chats from the server on which the SDNY Search Warrant Chats were located, including chats that occurred after the execution of the SDNY Search Warrant (the "Information Security Expert-2 Report"). Based on my review of the SDNY Search Warrant Chats and the Information Security Expert-2 Report, I know that the user of the Alias-1 Email Address and the user of the Alias-2 Email Address are the same person because, among other things, such users:

a. Share the same Jabber server, which I know, based upon reviewing records provided by the owner of such server, is privately rented and controlled. This Jabber server is associated with Domain Name-1.

b. Have described being physically ill in chats sent at approximately the same time, as reflected in the following SDNY Search Warrant Chats sent on September 7, 2010:

<u>Time</u>	<u>Author</u>	<u>Message</u>
04:46:34 PM	Alias-1	well I took a shit load of immunostimulators
04:46:36 PM	Alias-1	and the hell's over
04:46:46 PM	Alias-1	I've been treating myself for 2-3 days
07:40:11 PM	Alias-2	well let's meet up and talk about it. I'm just a little sick right now.
07:40:49 PM	Alias-2	yeah I'll be feeling better by Saturday

c. Have described being physically present in Switzerland in chats sent on the same day, as reflected in the following English translations of particular SDNY Search Warrant Chats:

<u>Date</u>	<u>Author</u>	<u>Message</u>
June 25, 2010	Alias-1	I am in switzerland
June 25, 2010	Alias-2	there was such a tragedy here in CH [meaning Switzerland] - they did not manage to win Honduras and pass through [referring to the World Cup match between Switzerland and Honduras]

d. Have described traveling by "6," which I believe, based on my participation in this investigation, my review of publicly available information, and my review of reports prepared by others, means a BMW 6-series convertible:

July 30, 2010

<u>Time</u>	<u>Author</u>	<u>Message</u>
05:39:58 PM	Alias-1	im driving around europe in cabri [meaning, a cabriolet convertible]
	* * *	
05:47:25 PM	CC-5	on that cabri that you bought for yours?
05:48:56 PM	Alias-	I didn't buy her a cabri
05:48:59 PM	Alias-1	I have my own :)
05:51:19 PM	CC-5	which one?)()
05:51:26 PM	CC-5	you used to have audi)
05:56:58 PM	Alias-1	audi was in the winter
05:57:00 PM	Alias-1	six cabri in the summer

July 13, 2010

<u>Time</u>	<u>Author</u>	<u>Message</u>
05:33:18 PM	Alias-2	by the way we want to ship the six there
05:38:45 PM	Individual-1	cliker just wrote that nobody fucking needs it there
05:38:50 PM	Individual-1	he asked to tell you
05:39:21 PM	Alias-2	how are we supposed to get around? There're a lot of people

e. Have described, in chats sent in or about November 2010, in sum and substance, obtaining an opportunity, through long-planned efforts on his part, for his girlfriend to pose in the Russian version of Playboy Magazine, which opportunity he planned shortly to present to his girlfriend as a gift.

B. The Identification of NIKITA VLADIMIROVICH KUZMIN as the User of Alias-2

23. As set forth more fully below, I have reviewed the SDNY Search Warrant Chats, certain publicly available information, and reports prepared by other law enforcement agents. Based on that review, I believe that the user of Alias-2 is NIKITA VLADIMIROVICH KUZMIN, the defendant. Because, as set forth in the preceding section, the user of Alias-2 and Alias-1 is the same person, I therefore believe that KUZMIN is the user of Alias-1 and the Alias-1 Email Address, and thus the promoter of the Alias-1 Service and the Gozi Virus.

24. The following is an SDNY Search Warrant Chat that took place on July 13, 2010 between the user of the Alias-2 Email Address and another individual ("Individual-1"). In sum and substance, my preliminary interpretation, which is based on a plain reading and my participation in this investigation, is that in this chat, the user of Alias-2 provides his bank account number to Individual-1 so that Individual-1 can electronically transfer money to that account (the "Alias-2 Bank Account"); Individual-1 subsequently provides confirmation that he has transferred money into the Alias-2 Bank Account; and such confirmation is in the form of a copy of an electronic funds transfer notification stating, among other things, that the owner of the Alias-2 Bank Account is "Kuzmin Nikita Vladimirovich" (i.e., NIKITA VLADIMIROVICH KUZMIN, the defendant):

<u>Time</u>	<u>Author</u>	<u>Message</u>
03:06:43 PM	Alias-2	if you have a little cash on alfa can you send it to me through online
03:07:05 PM	Individual-1	yes, I have
03:07:08 PM	Individual-1	give me the number
03:07:14 PM	Alias-2	XXXXXXXXXXXX1160 account
03:10:31 PM	Individual-1	ruble account?
03:11:26 PM	Alias-2	yes
03:11:37 PM	Alias-2	by law you can't transfer bucks to other people beside your close relatives
03:13:01 PM	Individual-1	4k was sent
03:13:19 PM	Individual-1	Your transfer was accepted. Do you pay for your purchases online? Now it is more secure with Virtual card! Get the Virtual card at online bank "Alfa-Click" right now! From the account: Current account -XXXXXXXXXXXX8069. Recipient name: Kuzmin Nikita Vladimirovich Recipient's account number: XXXXXXXXXXXX1160. Reason for transfer: Debt repayment. Payment amount: 4 000.00 RUB Reference: 37815565. Date of transfer: 13.07.2010 14:10:46

25. From the sources set forth below, I have learned the following information showing that Alias-2 and NIKITA VLADIMIROVICH KUZMIN, the defendant, have been in Thailand within the past week:

a. From reviewing the Information Security Expert-2 Report, I know, among other things:

- i. On November 19, 2010, Alias-2 sent an instant message communication providing, "i think i will go to thai and then i will go to somewhere else and get lost"; and
- ii. On November 22, 2010, Alias-2 sent an instant message communication providing, "in Bangkok."

b. As set forth more fully below, I know from reviewing records of the Bureau of Immigration and Customs Enforcement ("ICE") that NIKITA VLADIMIROVICH KUZMIN, the defendant, recently arrived in the United States via a series of flights that originated on November 27, 2010 in Bangkok, Thailand.

26. In an SDNY Search Warrant Chat sent by the Alias-2 Email Address on or about August 30, 2010, the Alias-2 Email Address indicated, in sum and substance, that he could be contacted, among other ways, at the email address "nikita@youdo.ru." Based on my participation in this investigation and a review of publicly available information, I know that "youdo.ru" is Russian social networking website ("YouDo").

27. From reviewing the YouDo website (including English translations of Russian text on YouDo) and reports prepared by other law enforcement agents, I know that on his personal page on YouDo ("YouDo Profile Page"), an individual who is identified as "Nikita":

a. has, among other things, posted pictures of himself, one of which is attached to this Complaint as Exhibit A; and

b. is identified as being user "1" (i.e., the first participant) on YouDo.

28. From reviewing the SDNY Search Warrant Chats, I know that the user of the Alias-2 Email Address is also identified by the name "Nikita" and has a significant affiliation with YouDo. In particular, the following is an excerpt of an SDNY Search Warrant Chat that was received by the Alias-2 Email Address on or about August 18, 2010: "Hi Nikita! Congratulations! youdo was sold! Why didn't you tell me? We have to celebrate this! ;)."⁴

⁴ In addition, as set forth above in paragraph 26, on August 30, 2010, the user of the Alias-2 Email Address sent a chat stating, in sum and substance, that he could be contacted at "nikita@youdo.ru."

29. From reviewing publicly available databases (including English translations of Russian text appearing on such databases) and reports prepared by other law enforcement agents, I know that a search of publicly available databases shows that in a particular internet forum, an individual identifying himself as "Nikita Kuzmin" (i.e., NIKITA VLADIMIROVICH KUZMIN, the defendant) posted an answer to a question regarding YouDo.

30. From reviewing the YouDo Profile Page (including English translations of Russian text appearing on that page), publicly available databases and information, and reports prepared by other law enforcement agents, I know that:

a. The YouDo Profile Page lists various "friends" of the user of that page, including a woman identified by name and photograph ("Woman-1").

b. Woman-1 is the daughter of a Russian musician, Father-1, who also has a son, Nikita Kuzmin, i.e., NIKITA VLADIMIROVICH KUZMIN, the defendant.

31. From speaking with, and reviewing reports prepared by, other law enforcement agents, I know that on his personal profile page on the Russian social networking site www.odnolassniki.ru (the "Odnolassniki Profile Page"), an individual identifying himself as "Nikita Kuzmin," i.e., NIKITA VLADIMIROVICH KUZMIN, the defendant, posted, among other things, a photograph of himself that is identical to the photograph posted on the YouDo Profile Page which is attached as Exhibit A.

32. As set forth above in paragraph 22(d), the user of both the Alias-1 Email Address and the Alias-2 Email Address referred to driving a "6," i.e., a BMW 6-series convertible. From reviewing the Odnolassniki Profile Page, I know that the Odnolassniki Profile Page contains a photograph of NIKITA VLADIMIROVICH KUZMIN, the defendant, and a woman in front of a car which appears, based on my review of publicly available information, to be a BMW 6-series convertible.

NIKITA VLADIMIROVICH KUZMIN'S RECENT TRAVEL

33. Based on my review of United States Department of State visa records and ICE border crossing records, I know the following:

a. On or about June 26, 2009, the United States

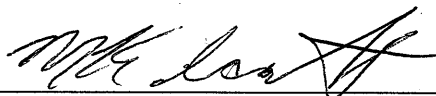
issued NIKITA VLADIMIROVICH KUZMIN, the defendant, a B1/B2 class visa to visit the United States on a temporary basis. In his application for that visa, KUZMIN presented a passport in his name issued by the Russian Federation. KUZMIN's U.S. visa expires on June 25, 2011.

b. On or about November 27, 2010, KUZMIN entered the United States through San Francisco, and provided information to border crossing agents which stated, in sum and substance, that KUZMIN would be staying at a particular hotel in the San Francisco area. KUZMIN's flight originated in Bangkok, Thailand on November 27, 2010.

34. Attached to this Complaint as Exhibit B is the passport photograph of NIKITA VLADIMIROVICH KUZMIN, the defendant, which I obtained from ICE, and which matches the photograph of "Nikita" which is posted on the YouDo Profile Page and attached as Exhibit A.

35. I have reviewed documents provided by Bank-1, including a list of Bank-1 Accounts that were compromised by computers infected with the Gozi Virus. That list includes the account of Victim-1, who according to the Bank-1 records, is located in Bronx, New York.

WHEREFORE, deponent prays that an arrest warrant be issued for the above-named defendant, and that he be imprisoned or bailed, as the case may be.



M. KATHRYN SCOTT
Special Agent
Federal Bureau of Investigation

Sworn to before me this
29th day of November, 2010.



HON. RONALD L. ELLIS
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK