UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA

v.

OLEG Y. NIKOLAENKO (dob: 7/17/1987)

CRIMINAL COMPLAINT

CASE NUMBER: 10-93M (AEG)

I, Brett E. Banner, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief. **Count One:** Between at least January 2007 and the present, in the State and Eastern District of Wisconsin and elsewhere, the defendant knowingly, in and affecting interstate commerce, materially falsified header information in multiple commercial electronic mail messages and intentionally initiated the transmission of such messages, in which the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during a 24-hour period, 25,000 during a 30-day period, and 250,000 during a 1-year period, to wit, the defendants altered the header information of spam e-mails that they transmitted via the Internet to disguise the e-mails' true origin, in violation of 18 U.S.C. § 1037(a)(3); and **Count Two:** On or about November 2, 2009, for the purpose of executing a scheme to defraud by failing to send purchased prescription drugs, the defendant knowingly caused to be sent and delivered by the Postal Service, the following matter: a package from Herbal Health Fulfillment House, 6 University Dr., Ste. 206-273, Amherst, MA 01002, containing 60 pills of "VPXL - #1 Dietary Supplement for Men, to an address in Milwaukee, State and Eastern District of Wisconsin, in violation of 18 U.S.C. § 1341.

I further state that I am a Special Agent of the U.S. Department of Justice, Federal Bureau of Investigation, and this complaint is based on the following facts:

Please see the attached affidavit.

Continued on the attached sheet and made a part hereof: X Yes ___ No

Signature of Complainant: Brett E. Banner

Sworn to before me and subscribed in my presence,

November 3 ,2010
Date

at Milwaukee, Wisconsin
City and State

The Honorable Aaron E. Goodstein
United States Magistrate Judge
Name & Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Brett E. Banner, being first duly sworn, hereby depose and state as follows:

A. INTRODUCTION

1. I have been employed by the FBI since November 7, 1999, and am currently assigned to the FBI Milwaukee Division, Cyber Crimes Squad. In that capacity, I am charged with conducting investigations of violations of federal law including violations of the CAN-SPAM Act, Title 18, United States Code, § 1037 and related offenses. I have experience in these investigations through previous case investigations, formal training, and consultation with law enforcement partners in local, state, and federal law enforcement agencies. Prior to my assignment in Milwaukee, I was assigned to the Detroit Division where I was the administrator for the Mid-Michigan Area Computer Crimes Task Force from June 2004 to September 2009. I have also been employed in the state of Wisconsin as a certified law enforcement officer from 1993 to 1999.

2. The facts in this affidavit come from my personal knowledge and investigation, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the issuance of a criminal complaint and arrest warrant and does not set forth all of my knowledge about this matter.

3. The FBI, assisted by the FTC, is investigating Oleg Nikolaenko for violations of the CAN-SPAM Act, 18 U.S.C. § 1037(a)(3) and aiding and abetting violations of the mail fraud statute, 18 U.S.C. § 1341. The investigation to date has included witness interviews and the review of e-mail communications and wire transfer information relating to Nikolaenko's botnet, dubbed the "Mega-D" botnet by computer security experts in the United States.

4. Based on previous investigation in the United States and abroad, the FBI and FTC have

determined that, by at least January 2007, and continuing to the present, Oleg Nikolaenko sent billions of spam emails on behalf of Jody Smith, Lance Atkinson, and others who were selling counterfeit Rolexes, non-FDA approved herbal remedies, and counterfeit prescription medications. In return, Nikolaenko was paid hundreds of thousands of dollars.

B. BACKGROUND REGARDING COMPUTERS AND BOTNETS

5. Based on my training and experience, I am aware that:

a. The Internet is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of sharing information. Connections between Internet computers exist across state and international borders and information sent between computers connected to the Internet may cross state and international borders, even if those computers are located in the same state.

b. 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 over 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 can be configured so that its sole task is to support a World Wide Web site known simply as a "Web server." Similarly, a server that only stores and processes e-mail is known as a "mail server."

c. An Internet Service Provider (ISP) in 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.

d. Computers connected to the Internet are identified by addresses. Internet addresses are unique and can be resolved to identify a physical location and a specific computer connection. Internet addresses take on several forms, including Internet Protocol addresses, Uniform Resource Locator (URL) addresses, and domain addresses. A domain address is a unique name that identifies a computer within a network; for example, a domain address of "mymachine@mydomain.com"

defines a computer called "mymachine" within the "mydomain.com" Internet domain.

e. The Internet Protocol address (or an IP address) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned a unique IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination.

f. Log files are computer files containing information regarding the activities of computer users, processes/programs running on the system and the activity of computer resources such as networks, modems, and printers. Log files can be used to identify activities that occurred on a specific computer.

g. Bots are software applications that run automated tasks over the Internet. Bots typically perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone. Bots can be implemented when a response speed faster than a human is required. The term is derived from "robot." There are both illegal and legal uses for a bot. However, in this investigation, a bot is malicious in that it is used to send and receive commands on computers that have been illegally compromised.

h. A "botnet" is a collection of software robots, or bots, which run autonomously. The term is derived from "robot network." Botnet is generally used to refer to a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure. A botnet's originator (a.k.a. "botherder") can control the group remotely, often though Internet Relay Chat (IRC) and usually for nefarious purposes. Botnets serve various purposes, including launching and controlling denial-of-service attacks, creating and misusing Simple Mail Transfer Protocols (SMTP) mail relays or proxies for spam, click fraud, and the theft of personal identifying information.

i. Internet Relay Chat (IRC) is a form of real-time Internet text messaging. It is mainly designed for group communication in discussion forums, called channels, but also allows one-to-one communication via private message as well as chat and data transfers. Through the use of an IRC, a botnets originator can control a group of computers remotely. Individual programs manifest as IRC "bots". Often the command and control takes place via an IRC server or a specific channel on a public IRC network. This server is known as the command and control server. A botherder can program their own commanding protocols. These protocols include a server program, client program for operation, and the program that embeds itself

on the victim's machine.

j. An online money transaction service are companies such as Paypal, ePassporte, Western Union, etc., that allow payments and money transfers to be made through the Internet. These services often have accounts that can be funded with an electronic debit from a bank account or by a credit card.

C. SUMMARY OF INVESTIGATION

6. On August 9, 2009, in federal district court for the Eastern District of Missouri, defendant Jody M. Smith pled guilty to a one-count information charging a conspiracy to traffic in counterfeit Rolex watches. The investigation into Smith revealed, and Smith admitted in his guilty plea, that he contracted with "spammers" or senders of spam emails to solicit customers to purchase his counterfeit Rolexes. Smith admitted that he paid more than $2,000,000 to the spammers to send the email messages.

7. As part of the investigation into Smith's case, the FBI, assisted by the FTC, determined that Smith's enterprise, which operated both within and outside the United States, was named "Affking." The FTC received over three million complaints regarding spam messages connected to this operation.

8. In his guilty plea, Smith identified Australian citizen and resident Lance Atkinson as a co-conspirator in the Affking email marketing and counterfeiting operation. Based on other undercover investigations, the FBI and FTC determined that in addition to selling counterfeit Rolexes, Affking also deceptively marketed and sold counterfeit herbal "male enhancement" pills and generic prescription drugs that were falsely advertised as FDA-approved.

9. As part of the ongoing investigation into Smith, Atkinson, and Affking, the United States government sought assistance from Australian and New Zealand authorities. On December 23,

2008, Lance Atkinson was interviewed by the Australian Communications and Media Authority. The purpose of the interview was to get the details of Atkinson's and Smith's spam enterprise. FBI Special Agent Jason Pleming has reviewed a transcript of that interview in connection with the investigation of the instant case and summarized it below.

10. In the interview, Atkinson explained his involvement in the Affking and related enterprises, including Affking predecessor companies Genbucks and Sancash. Atkinson admitted that, using a nickname, he posted messages on a pro-spam Internet bulletin boards seeking spammers to promote the herbal pills. Atkinson recalled that his largest spamming affiliates were Russian. Specifically, he recalled that two of his largest Russian spamming affiliates used the online monikers "Docent" and "Dem." Atkinson also admitted that he also used banner advertisements on website and advertisements placed within internet search engines to market the products. Atkinson estimated that 80% of all of the advertising was done by the affiliates via spam emails, with the other 20% done through banner and internet search engine advertisements.

11. As part of its investigation the FTC obtained chat logs which were seized during a search warrant in New Zealand at Atkinson's brother's house. The chat log revealed a conversation between Lance Atkinson's brother, Shane Atkinson, and "Docent" in January 2007. The chat, in pertinent part, reflected that "Docent" was interested in sending additional spam messages on Atkinson's behalf. In the chat, Shane Atkinson indicated that he would have Lance Atkinson get in touch with "Docent" soon.

12. The Director of Malware research at Secure Works, a computer security company which was founded in 1999 to protect organizations from Internet threats while developing propriety technology and processes, determined during the investigation that many of the email messages

touting Affking products were routed without authorization through a vast number of compromised computers, usually referred to as a "botnet." In early 2008, the Director of Malware research identified one botnet, which it named "Mega-D," as one which sent spam promoting Affking's products. The director determined that "Mega-D" was likely the largest botnet in the world, accounting for 32% of all spam. The director estimated that the botnet was capable of sending ten billion spam email messages a day, all of which contained materially falsified header information. A review of some of these emails reflects that the falsified header information was a false "return" address, such that if the recipient's email address did not accept the spam email, it would be sent or bounced back to the false return address.

13. The FTC investigation revealed that Atkinson also controlled an ePassporte[1] online digital currency account in the name of New Pacific Resources, a company registered in the British Virgin Islands. The investigation revealed that between October 2006 and December 2007, Atkinson's ePassporte account received over $1.7 million from Genbucks, the Smith/Atkinson company affiliated with Affking which also sold herbal diet pills, male enhancement pills, and as counterfeit watches and transferred over $1.8 million to other accounts as commissions.

14. Atkinson recalled during his interview that "Docent," the Russian affiliate spammer, used an ePassporte account under the name of "Genbucks_dcent." On November 19, 2009, Agent Pleming received records from ePassporte pursuant to a federal grand jury subpoena. The records

[1]ePassporte offers online accounts which, once logged into, can be used to send or accept payments from other ePassporte account holders and to transfer money to and from a bank account. ePassporte also offers its users a virtual Visa card which can be used to make purchases online, and certain users also receive a physical card which can be used to withdraw funds from ATM machines and make in-store purchases.

revealed that the ePassporte account "Genbucks_dcent" was registered in the name of Oleg Nikolaenko, residing at 28/10 Spasskiy Proezd, Vidnoe 2, Russian Federation, email addresses: ddarwinn@gmail.com and 4docent@gmail.com, telephone number 79265847910. A review of the "Genbucks_dcent" ePassporte account revealed that Atkinson made numerous payments to Nikolaenko's "Genbucks_dcent" ePassporte account. Between June 6, 2007 and December 14, 2007, Lance Atkinson made payments totaling $464,967.12, to "Genbucks_dcent."

15. On November 24, 2009, Agent Pleming received subscriber records for ddarwinn@gmail.com from Google pursuant to a Federal Grand Jury subpoena. The records revealed that email account ddarwinn@gmail.com is registered to Oleg Nikolaenko, residing at 28/10 Spasskiy Pr, Vidnoe 2, Moscow, Russia, telephone number 79265847910.

16. A search warrant was obtained for email addresses ddarwin@gmail.com and 4docent@gmail.com on July 29, 2010.[2] The review of the emails for 4docent@gmail.com reflect emails from Nikolaenko to others, including "Affking1@gmail.com," an email address which is believed to belong to Lance Atkinson. These emails corroborate the business relationship between Nikolaenko and Atkinson, including copies of sample spam messages, references to sending large numbers of emails, selling purported male enhancement products, and transfers of money to Nikolaenko's account.

17. A review of the emails contained in the 4docent@gmail.com account also revealed numerous executable files which were analyzed by the Director of Malware research at Secure Works. In the director's expert opinion, provided to the FBI on October 31, 2010, copies of the

---

[2]Due to a typographical error in the face sheets, email information was not received for the ddarwinn@gmail.com account.

executable files found in the 4docent@gmail.com are samples of the malware family known as Mega-D. Based on my review of the emails to which these executables are attached, I believe that they were being emailed to another individual who, like Lance Atkinson, wanted to use Nikolaenko's botnet to send out spam messages.

18. Based on information reported to the FBI by FireEye, Agent Pleming is aware that network security company FireEye crippled the "Mega-D" botnet on November 4, 2009, by convincing U.S.-based internet service providers to shut down "Mega-D's" command and control computers and to redirect "bots" or infected computers looking for a command and control computer to "sinkholes," which collected information about the botnet, but did not send out any further commands to the infected computers. By doing so, FireEye reduced the spam sent by the Mega-D botnet from 11.8 percent of all spam sent on November 1, 2009, to less than 0.1 percent on November 4, 2009.

19. Based on information obtained through these sinkholes, FireEye was able to identify approximately 509,000 computers infected with the virus which causes computers to become bots seeking direction from the Mega-D command and control computers. An analysis of this data revealed that approximately 136 of the infected computers' IP addresses resolved to addresses in the State of Wisconsin.

20. According to the Director of Malware research at Secure Works, on September 21, 2009, IP address 75.86.208.157 sent Mega-D botnet-generated spam email at 12:04:50 GMT. A review of the email reveals that it purports to advertise male enhancement pills. A review of the email header reflects that it contains materially false information, in that the sender and recipient both appear to be nasreq-archive@ietf.org, when in fact the true sender information reveals that the

email is from jcaparent@alienware.org. This materially false header information makes the email appear as if the recipient sent the email to him/herself, when in fact the email came from an entirely different email account.

21. On November 20, 2009, Agent Pleming received records from Time Warner Cable which revealed that IP address 75.86.208.157 was assigned to G.G. at WXXX NXXXX Red Fox Run, Hartland, Wisconsin, as of November 02, 2009. However, based on conversations with individuals at Time Warner, I believe that IP address is static, meaning that it was also assigned to G.G. on September 21, 2009.

22. According to a November 9, 2009, report from cyber security research firm M86 Security Labs regarding the Mega-D botnet: "We have seen individual Mega-D bots spam at 15,000 messages per hour." Based on my training and experience, I believe that the IP address assigned to G.G. has sent thousands of spam emails with materially falsified header information. However, because the spam is sent to multiple email accounts (rather than targeting the same email account thousands of times), we have, to date, only received one email generated from the IP address associated with G.G.

23. A search of U.S. State Department visa applications revealed that Oleg Yegorovich Nikolaenko, date of birth July 17, 1987, residing at 28/10 Spasskiy Proezd, Vidnoe 2, Russian Federation, email address ddarwinn@gmail.com, telephone number 79265847910 applied for visitor's visa on June 18, 2009. Travel records obtained via grand jury subpoena and U.S. immigration records revealed that Nikolaenko entered the United States in Los Angeles on July 17, 2009, and left on July 27, 2009.

24. Travel records obtained via grand jury subpoena and U.S. immigration records revealed

that Nikolaenko again entered the United States in New York on October 29, 2009, and left from Los Angeles on November 9, 2009. Hotel records reflect that Nikolaenko visited Las Vegas, Nevada, from November 2, 2009, to November 6, 2009. According to information subpoenaed from Google, on the day that Nikolaenko left the United States, November 9, 2009, the email addresses ddarwinn@gmail.com and 4docent@gmail.com were logged into from IP address 65.86.127.226, which is registered to The Tower Hotel, Beverly Hills.

25. Based on Nikolaenko's entry documents, he was expected to stay in the United States until November 11, 2009. However, airline records reveal that Nikoleanko left early. Based on the timing of the Fireye attack on the Mega-D botnet, I believe that Nikolaenko left the U.S. early to repair the damage caused by Fireye. FireEye disabled the Mega-D botnet by disabling its command and control structure, which had an immediate effect on the amount of spam generated by the botnet. M86 Security, the largest provider of Secure Web Gateways and the largest independent provider of web and e-mail content security in the world, reported that by November 9, 2009 the spam had stopped altogether. However, the botnet bounced back, exceeding pre-takedown levels by November 22, 2009, and constituting 17% of worldwide spam by December 13, 2009.

26. On November 2, 2009, Agent Pleming obtained a copy of an email which was sent by Nikolaenko's Mega-D botnet. This email was provided to him by the Director of Malware research at Secure Works. A review of the email header reflects that it contains materially false information, in that the sender and recipient both appear to be yamamoto.kenichiro@somec.co.jp, when in fact the true sender information reveals that the email is from jnaka@4dcsi.com. This materially false header information makes the email appear

as if the recipient sent the email to him/herself, when in fact the email came from an entirely different email account.

27. This email advertised an "Approved Card" within the subject line of the email and appeared to be from "Amazon, Ltd." Acting in an undercover capacity, Agent Pleming clicked on a link in the email which was supposed to unsubscribe him from the mailing list. Instead, clicking on this link took him to a website for a company called "Canadian Pharmacy." This website advertised male enhancement pharmaceuticals and did not appear to have anything to do with approved credit cards or online retailer Amazon.com.

28. Agent Pleming then purchased one pack of "VPXL," a male enhancement pharmaceutical advertised on the website. Agent Pleming purchased a one month supply (one bottle) for $37.91. Agent Pleming also purchased one package of Viagra Professional, which purported to contain 10 prescription Viagra pills, 100 mg each for $64.74. In addition, one package of four Viagra Professional, 100mg each, were included in the order at no charge. Agent Pleming purchased the pharmaceuticals using an undercover identity and an undercover credit card. The pharmaceuticals were to be delivered to an undercover address located in Milwaukee, Wisconsin.

29. Shortly after submitting the order, a receipt for the transaction was provided to him electronically which cited an order number of P95-1420541. The receipt provided the following telephone numbers for customer support: 210-787-1711 and 800-383-7433. In addition, the receipt provided the website http://united-pharmacy-support.net for customers to check on the status of their orders.

30. On November 19, 2009, Agent Pleming traveled to his pre-arranged undercover address located in Milwaukee, Wisconsin, to retrieve a package that had been delivered. Once there,

Agent Pleming recovered a package delivered via the United States Postal Service (USPS) addressed to his undercover identity. The package had a return address of Herbal Health Fulfillment House, 6 University Dr., Ste. 206-273, Amherst, MA 01002. Agent Pleming opened the package and recovered a bottle containing 60 pills of "VPXL - #1 Dietary Supplement for Men." No item which purported to be Viagra was contained in the box.

31. On October 30, 2010, Nikolaenko entered the United States at the port of entry located at JFK airport in New York. According to hotel records, he has checked in at the Bellagio hotel in Las Vegas, Nevada, and is scheduled to stay until November 5, 2010. Based on information obtained by grand jury subpoena, I am aware that Nikolaenko attended the Specialty Equipment Market Association (SEMA) car show in Las Vegas, Nevada last year, which was held November 3-6, 2009. Based on a review of the SEMA website, I am aware that this year's annual SEMA car show is occurring November 2-5, 2010.

G. CONCLUSION

32. Based on the foregoing, I submit that there is probable cause to believe that Oleg Nikolaenko has violated the CAN-SPAM Act, 18 U.S.C. § 1037(a)(3), between at least 2007 and the present by sending multiple emails with materially falsified header information, and has aided and abetted a violation of the mail fraud statute, 18 U.S.C. § 1341, by sending spam emails advertising Viagra, when, in fact, no Viagra is mailed when ordered. Accordingly, a criminal complaint and arrest warrant are requested.