

1541

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA

v.

EVGENIY BOGACHEV

) Criminal No. 14-127
) (18 U.S.C. §§ 371, 1343,
) 1030(a)(2), 1030(c)(2)(B),
) 1344, 1957(a) and 1956(i)(1)(B))
) UNDER SEAL

FILED

MAY 19 2014

CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

INDICTMENT

The grand jury charges:

Introduction

At all times material to this Indictment, unless otherwise alleged:

1) Malicious software ("malware") is a software program designed to disrupt computer operations, gather sensitive information, gain access to private computer systems, or do other unwanted action on a computer system. Common examples of malware include viruses, worms, Trojan horses, rootkits, keyloggers, spyware, and others.

2) Keystroke logging is the action of recording (or logging) the keys struck on a keyboard. This action is usually done surreptitiously by a computer program (i.e., keylogger) to capture the keys typed on a computer without the typist's knowledge. Malware that uses keystroke logging often will provide the captured keystrokes to the individual who caused the malware to be installed or to a place designated by the individual. Through keystroke logging, individuals are able to obtain online banking credentials as soon as the user of the

infected computer logs into their account. After obtaining this information, these individuals can access the victim's online bank account and execute unauthorized electronic funds transfers ("EFT"), such as Automated Clearing House ("ACH") payments or wire transfers,¹ to accounts that they control.

3) Web injects introduce (or inject) malicious computer code into a victim's web browser while the victim browses the Internet and "hijacks" the victim's Internet session. Different injects are used for different purposes. Some web injects are used to display false online banking pages into the victim's web browser to trick the victim into entering online banking information, which is then captured by the individual employing the web inject.

4) "Bot," which is short for "robot," is a computer that has been infected by malware and does tasks at the malware's direction.

¹ Electronic funds transfers ("EFT") are the exchange and transfer of money through computer-based systems using the Internet. ACH payments allow the electronic transferring of funds from one bank account to another bank account within the ACH network without any paper money changing hands. The ACH network is a network of participating depository financial institutions across the United States, and the network provides for interbanking clearing of electronic payments. Because ACH payments require the network to clear the transaction, the funds are not immediately available. Wire transfers also allow electronic transferring of funds from one bank account to another bank account without any paper money changing hands; however, unlike ACH payments, wire transferred funds are immediately available.

5) A "botnet" is a network of bots. It is a collection of bots that are connected to each other and that can communicate with each other through some network architecture.

6) Peer-to-peer networking is an advanced decentralized networking architecture. In command and control networks, computers in the network are connected to a central server. When a computer wants to communicate with another device in the network, it communicates with the central server and the central server then communicates with the other device. In peer-to-peer networks, the computers are connected directly to other computers in the network. Computers can communicate with other computers in the network without the use of a centralized server.

7) Zeus is malware specifically designed to automate the theft of confidential personal and financial information, such as online banking credentials, from infected computers through the use of keystroke logging and web injects.

8) Peer-to-Peer Zeus, also known as GameOver Zeus, is a more sophisticated variant of the Zeus malware that utilizes peer-to-peer networking for its botnet. Peer-to-Peer Zeus was developed based on the original Zeus code. Like Zeus, Peer-to-Peer Zeus is specifically designed to automate the theft of confidential personal and financial information through the use of keystroke logging and web injects.

9) "Phishing" is a fraud technique used by computer attackers in an attempt to acquire sensitive information such as usernames, passwords, and other account credentials by sending electronic mails (emails) or other electronic communications which falsely claim to be from an established legitimate entity. One type of phishing email directs the user to click on a hyperlink in the email. By clicking this link, the victim causes the installation of malware without the victim's consent or knowledge.

10) The National Automated Clearing House Association ("NACHA") managed the development, administration, and governance of the ACH network. Although NACHA is not directly involved in ACH payments, it provides the operating rules of the ACH network and oversees the ACH network.

11) A "mule" or "money mule" is a person who received stolen funds into their bank account, and then moved the money to other accounts, or withdrew the funds and transported the funds overseas as smuggled bulk cash.

12) PNC Bank was a financial institution insured by the Federal Deposit Insurance Corporation. It was engaged in the business of providing the means to do electronic funds transfers. It was headquartered in the Western District of Pennsylvania and offered online banking services through

computer servers located in the Western District of Pennsylvania.

13) Haysite Reinforced Plastics was a business located in the Western District of Pennsylvania.

14) The defendant, EVGENIY BOGACHEV, was a resident of Russia. He was an administrator of the Peer-to-Peer Zeus botnet.

SCHEME AND ARTIFICE

15) From in and around September 2011, the exact date being unknown to the grand jury, and continuing to the present, in the Western District of Pennsylvania and elsewhere, the defendant, EVGENIY BOGACHEV, and co-conspirators, known and unknown to the grand jury, did devise, and intend to devise, a scheme and artifice to defraud and to obtain money and property by means of material false and fraudulent pretenses, representations, and promises by using the unauthorized installation of malware on victim computers to steal or attempt to steal millions of dollars from numerous bank accounts in the United States and elsewhere and to transfer the stolen funds overseas.

16) It was a part of the scheme and artifice that the defendant, EVGENIY BOGACHEV, and co-conspirators known and unknown to the grand jury, sent phishing emails through the

Internet that falsely represented to be legitimate emails from legitimate companies, associations, and organizations.

17) It was further a part of the scheme and artifice that the defendant, EVGENIY BOGACHEV, and co-conspirators, known and unknown to the grand jury, created the phishing emails to fraudulently induce recipients to click on a hyperlink falsely represented to be a legitimate link containing business or personal information, when in truth and fact, it installed malware without the email recipients' consent or knowledge.

18) It was further a part of the scheme and artifice that the defendant, EVGENIY BOGACHEV, and co-conspirators, known and unknown to the grand jury, without authorization, installed and caused the installation of the Peer-to-Peer Zeus malware on Internet-connected victim computers.

19) It was further a part of the scheme and artifice that the Peer-to-Peer Zeus malware was designed to automate the theft of confidential personal and financial information, such as online banking credentials. The Peer-to-Peer Zeus malware facilitated the theft of confidential personal and financial information by a number of methods. For example, the Peer-to-Peer Zeus malware may obtain such information through keystroke logging. Alternatively, the Peer-to-Peer Zeus malware may allow computer intruders to hijack a computer session and use web

injects to present a fake online banking webpage to trick a user into entering personal and financial information.

20) It was further a part of the scheme and artifice that the defendant, EVGENIY BOGACHEV, and co-conspirators known and unknown to the grand jury, used the Peer-to-Peer Zeus malware on infected computers to capture the user's confidential personal and financial information, such as online banking credentials, by keystroke logging or by hijacking the computer session and presenting a web inject, i.e., fake online banking webpages.

21) It was further a part of the scheme and artifice that the defendant, EVGENIY BOGACHEV, and co-conspirators known and unknown to the grand jury, used the captured information without authorization to falsely represent to banks that the Defendant and co-conspirators were victims or employees of victims who have authorization to access the victims' bank accounts and to make electronic funds transfers from the victims' bank accounts.

22) It was further a part of the scheme and artifice that the defendant, EVGENIY BOGACHEV, and co-conspirators known and unknown to the grand jury, used the captured banking credentials to cause banks to make unauthorized wire transfers, ACH payments, or other electronic funds transfers from the

victims' bank accounts, without the knowledge or consent of the account holders.

23) It was further a part of the scheme and artifice that the defendant, EVGENIY BOGACHEV, and co-conspirators known and unknown to the grand jury, used money mules to receive the wire transfers, the ACH payments, or other electronic funds transfers from the victims' bank accounts.

24) It was further a part of the scheme and artifice that the defendant, EVGENIY BOGACHEV, and co-conspirators known and unknown to the grand jury, used the money mules to further transfer the stolen funds to ultimately reach the control of the Defendant and his co-conspirators overseas.

25) It was further a part of the scheme and artifice that, on or about October 18, 2011, the defendant, EVGENIY BOGACHEV, and co-conspirators known and unknown to the grand jury, engaged in interstate and foreign wire communications over the Internet by sending to an employee at Haysite Reinforced Plastics, who was located in the Western District of Pennsylvania, a phishing email, which falsely alleged that said communication originated from NACHA and which fraudulently induced the employee to click on a malicious hyperlink falsely represented to be a legitimate link containing information concerning a canceled ACH payment, when in truth and fact, it installed malware without the employee's consent or knowledge.

26) It was further a part of the scheme and artifice that, on or about October 18, 2011, in the Western District of Pennsylvania, the defendant, EVGENIY BOGACHEV, and co-conspirators known and unknown to the grand jury, caused malware to be installed, without authorization, on an Internet-connected computer used by Haysite Reinforced Plastics.

27) It was further a part of the scheme and artifice that, on or about October 20, 2011, in the Western District of Pennsylvania, the defendant, EVGENIY BOGACHEV, and co-conspirators known and unknown to the grand jury, used the installed malware to hijack, without authorization, a computer session of an employee at Haysite Reinforced Plastics and to insert, without authorization, a web inject, i.e., a fake online banking website, in order to obtain the online banking credentials of three Haysite Reinforced Plastics employees known to the grand jury as NK, SC, and AE.

28) It was further a part of the scheme and artifice that, on or about October 20, 2011, the defendant, EVGENIY BOGACHEV, and co-conspirators known and unknown to the grand jury, used the fraudulently obtained online banking credentials to falsely represent to PNC Bank that Defendant and his co-conspirators were persons authorized to access the online banking accounts of Haysite Reinforced Plastics and to cause, or

attempt to cause, the transfer of funds out of Haysite Reinforced Plastics' bank accounts maintained with PNC Bank.

29) It was further a part of the scheme and artifice that, on or about October 20, 2011, in the Western District of Pennsylvania, the defendant, EVGENIY BOGACHEV, and co-conspirators known and unknown to the grand jury, fraudulently caused the electronic transfer of \$198,234.93 from a PNC Bank account belonging to Haysite Reinforced Plastics to a money mule's bank account under the name of Lynch Enterprises LLC and maintained at SunTrust Bank in Atlanta, Georgia.

30) It was further a part of the scheme and artifice that, on or about October 21, 2011, the defendant, EVGENIY BOGACHEV, and co-conspirators known and unknown to the grand jury, used the money mule associated with Lynch Enterprises LLC to execute the electronic transfer of the stolen funds to bank accounts located in Great Britain.

COUNT ONE
(Conspiracy)

The grand jury further charges:

31) Paragraphs 1 through 30 above of the Introduction and Scheme and Artifice are hereby realleged and incorporated by reference herein, as if fully stated.

32) From in and around September 2011, the exact date being unknown to the grand jury, and continuing to the present, in the Western District of Pennsylvania and elsewhere, the defendant, EVGENIY BOGACHEV, knowingly and willfully did conspire, combine, confederate, and agree with other persons known and unknown to the grand jury, to commit the following offenses against the United States:

(a) to intentionally access a computer without authorization, and exceeding authorization, and thereby obtain, or attempt to obtain, information from a protected computer, which offense was committed in furtherance of a criminal act in violation of Title 18, United States Code, Sections 1343 and 1344 and was committed for the purpose of private financial gain, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B);

(b) to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage, and attempted to cause damage, without authorization, to a protected computer, and the offense did cause and, if completed, would have caused damage

affecting 10 or more protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B);

(c) to devise, and intend to devise, a scheme and artifice to defraud businesses and individuals, and to obtain money from these businesses' and individuals' bank accounts and property, that is, confidential personal and financial information, by means of material false and fraudulent pretenses, representations, and promises, and for purpose of executing such scheme and artifice, to transmit, and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, and pictures, which affected financial institutions, in violation of Title 18, United States Code, Section 1343;

(d) to knowingly execute, and attempt to execute, a scheme and artifice to defraud a financial institution and to obtain any of the moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, a financial institution by means of material false or fraudulent pretenses, representations, and promises in violation of Title 18, United States Code, Section 1344; and

(e) to knowingly engage, and attempt to engage, in monetary transactions affecting interstate and foreign commerce, by and through a financial institution, in criminally derived property of a value greater than \$10,000, said property being

derived from a specific unlawful activity, that is, an act that is indictable under Title 18, United States Code, Sections 1343 and 1344, as more particularly described in paragraphs 1 through 23 and paragraphs 25 through 29, knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1957(a).

OVERT ACTS

33) In furtherance of the conspiracy, and to effect the objects of the conspiracy, the defendant, EVGENIY BOGACHEV, and other persons both known and unknown to the grand jury, did commit and cause to be committed, the following overt acts, among others, in the Western District of Pennsylvania and elsewhere:

(a) On or about October 18, 2011, the defendant and co-conspirators sent to an employee at Haysite Reinforced Plastics a phishing email purporting to be from NACHA and fraudulently inducing the employee to click on a malicious hyperlink, which was falsely represented as a legitimate link.

(b) On or about October 18, 2011, the defendant and co-conspirators caused malware to be installed, without authorization, on a computer used by Haysite Reinforced Plastics.

(c) On or about October 20, 2011, the defendant and co-conspirators used the malware to hijack a computer session of an employee at Haysite Reinforced Plastics and inserted a fake online banking website.

(d) On or about October 20, 2011, the defendant and co-conspirators used the malware and the fake online banking website to request different employees at Haysite Reinforced Plastics to enter their online banking credentials.

(e) On or about October 20, 2011, the defendant and co-conspirators used the installed malware to obtain the online banking credentials of three Haysite Reinforced Plastics employees known to the grand jury as NK, SC, and AE.

(f) On or about October 20, 2011, the defendant and co-conspirators used the fraudulently obtained online banking credentials to falsely represent to PNC Bank that defendant and his co-conspirators were authorized to access online banking accounts of Haysite Reinforced Plastics.

(g) On or about October 20, 2011, the defendant and co-conspirators caused, or attempted to cause, the transfer of funds out of the Haysite Reinforced Plastics' bank accounts maintained with PNC Bank.

(h) On or about October 20, 2011, the defendant and co-conspirators caused the transfer of \$198,234.93 from a PNC Bank account belonging to Haysite Reinforced Plastics to a money

mule's bank account under the name of Lynch Enterprises LLC that was maintained at SunTrust Bank in Atlanta, Georgia.

(i) On or about October 20, 2011, the defendant and co-conspirators caused the transfer of \$175,756.91 from a PNC Bank account belonging to Haysite Reinforced Plastics to a bank account for a jewelry store that was maintained at Herald National Bank in New York, New York.

(j) On or about October 21, 2011, the defendant and co-conspirators used a money mule to cause the transfer of \$99,822.00, which was fraudulently obtained from Haysite Reinforced Plastics and PNC Bank, from a SunTrust Bank account belonging to Lynch Enterprises LLC to a bank account located in Great Britain.

(k) On or about October 21, 2011, the defendant and co-conspirators used a money mule to cause the transfer \$88,550.00, which was fraudulently obtained from Haysite Reinforced Plastics and PNC Bank, from a SunTrust Bank account belonging to Lynch Enterprises LLC to a bank account located in Great Britain.

In violation of Title 18, United States Code, Section 371.

COUNT TWO
(Wire Fraud)

The grand jury further charges:

34) Paragraphs 1 through 33 above are hereby realleged and incorporated by reference herein, as if fully stated.

35) On or about October 18, 2011, in the Western District of Pennsylvania and elsewhere, the defendant, EVGENIY BOGACHEV, for the purpose of executing, and attempting to execute, the scheme and artifice to defraud and to obtain property from others, that is, control of a computer and banking credentials, by means of material false and fraudulent pretenses, representations, and promises, well knowing at the time that the pretenses, representations, and promises were false and fraudulent when made, as set forth above in Paragraphs 1 through 17 and paragraphs 25 through 26, knowingly did transmit, and cause to be transmitted, in interstate and foreign commerce, by means of a wire communication, from the IP address 188.121.144.240, which was then located in the Islamic Republic of Iran, to the IP address 192.168.0.10, which was then located in Erie, Pennsylvania, and belonged to Haysite Reinforced Plastics, certain writings, signs, signals, and pictures that is, a phishing email that falsely purported to be from NACHA, that falsely represented that an ACH payment had been canceled, and that falsely represented that a hyperlink within the email

was a legitimate link containing information concerning a canceled ACH payment.

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

COUNT THREE
(Computer Fraud)

The grand jury further charges:

36) Paragraphs 1 through 33 above are hereby realleged and incorporated by reference herein, as if fully stated.

37) On or about October 20, 2011, within the Western District of Pennsylvania, the defendant, EVGENIY BOGACHEV, intentionally accessed a computer belonging to Haysite Reinforced Plastics without authorization, and thereby obtained information, that is, online banking credentials of Haysite Reinforced Plastics from employees known to the grand jury as NK, SC, and AE, from a protected computer, and the offense was committed for purpose of private financial gain and was committed in furtherance of a criminal act in violation of the laws of the United States, that is, Title 18, United States Code, Sections 1343 and 1344.

In violation of Title 18 United States Code, Sections 1030(a)(2) and 1030(c)(2)(B).

COUNTS FOUR THROUGH TWELVE
(Bank Fraud)

The grand jury further charges:

38) Paragraphs 1 through 33 above are hereby realleged and incorporated by reference herein, as if fully stated.

39) On or about the dates set forth below, in the District of Western Pennsylvania and elsewhere, the defendant, EVGENIY BOGACHEV, having devised and intended to devise the scheme and artifice to defraud PNC Bank and to obtain moneys and funds owned by and under the custody and control of PNC Bank by means of material false and fraudulent pretenses, representations and promises, well knowing at the time that the pretenses, representations and promises would be and were false and fraudulent when made, did knowingly execute and attempt to execute the foregoing scheme and artifice, by causing, and attempting to cause, the transfer of funds, with each transfer, and attempted transfer, being a separate count of this indictment as described below:

Count	On or about Date	Execution
4	October 20, 2011	The transfer of \$198,234.93 out of a PNC Bank account belonging to Haysite Reinforced Plastics to an account belonging to Lynch Enterprises LLC
5	October 20, 2011	The transfer of \$175,756.91 out of a PNC Bank account belonging to Haysite Reinforced Plastics to an account belonging to R&R Jewelers
6	October 20, 2011	The attempted transfer of \$39,841.27 out of a PNC Bank account belonging

		to Haysite Reinforced Plastics
7	October 20, 2011	The attempted transfer of \$49,146.58 out of a PNC Bank account belonging to Haysite Reinforced Plastics
8	October 20, 2011	The attempted transfer of \$49,821.53 out of a PNC Bank account belonging to Haysite Reinforced Plastics
9	October 20, 2011	The attempted transfer of \$39,841.64 out of a PNC Bank account belonging to Haysite Reinforced Plastics
10	October 20, 2011	The attempted transfer of \$49,632.64 out of a PNC Bank account belonging to Haysite Reinforced Plastics
11	October 20, 2011	The attempted transfer of \$49,751.62 out of a PNC Bank account belonging to Haysite Reinforced Plastics
12	October 20, 2011	The attempted transfer of \$171,151.50 out of a PNC Bank account belonging to Haysite Reinforced Plastics

In violation of Title 18, United States Code, Section 1344.

COUNT THIRTEEN
(Money Laundering)

The grand jury further charges:

40) Paragraphs 1 through 33 and paragraphs 38 through 39 above are hereby realleged and incorporated by reference herein, as if fully stated.

41) On or about October 21, 2011, in the Western District of Pennsylvania and elsewhere, the defendant, EVGENIY BOGACHEV, did knowingly engage in a monetary transaction affecting interstate and foreign commerce in criminally derived property with a value greater than \$10,000, which property was derived from specified unlawful activity, in that the defendant, EVGENIY BOGACHEV, caused funds fraudulently obtained from Haysite Reinforced Plastics and PNC Bank, as charged in Count Four, in the amount of \$99,822.00 to be withdrawn and transferred by wire from an account in the name of Lynch Enterprises LLC, maintained at SunTrust Bank, to an account in the name of an individual known to the grand jury as A.Z.M., at HSBC Bank PLC, in London, Great Britain, knowing that the transaction involved funds that were derived from a criminal offense, when in fact said funds were derived from violations of Title 18, United States Code, Section 1344.

In violation of Title 18, United States Code, Sections 1957(a) and 1956(i)(1)(B).

COUNT FOURTEEN
(Money Laundering)

The grand jury further charges:

42) Paragraphs 1 through 33 and paragraphs 38 through 39 above are hereby realleged and incorporated by reference herein, as if fully stated.

43) On or about October 21, 2011, in the Western District of Pennsylvania and elsewhere, the defendant, EVGENIY BOGACHEV, did knowingly engage in a monetary transaction affecting interstate and foreign commerce in criminally derived property with a value greater than \$10,000, which property was derived from specified unlawful activity, in that the defendant, EVGENIY BOGACHEV, caused funds fraudulently obtained from Haysite Reinforced Plastics and PNC Bank, as charged in Count Four, in the amount of \$88,550.00 to be withdrawn and transferred by wire from an account in the name of Lynch Enterprises LLC, maintained at SunTrust Bank, to an account in the name of an individual known to the grand jury as G.A.P., maintained at National Westminster Bank PLC, in London, Great Britain, knowing that the transaction involved funds that were derived from a criminal offense, when in fact said funds were derived from violations of Title 18, United States Code, Section 1344.

In violation of Title 18, United States Code, Sections 1957(a) and 1956(i)(1)(B).

FORFEITURE ALLEGATIONS

44) The grand jury realleges and incorporates by reference the allegations contained in Counts One through Fourteen of this Indictment for the purpose of alleging criminal forfeiture pursuant to Title 18, United States Code, Sections 982(a)(1), 982(a)(2)(A), 982(a)(2)(B), 982(a)(4), and 981(a)(1)(C), Title 28, United States Code, Section 2461(c), and Title 21, United States Code, Section 853(p).

45) As a result of the commission of the violations charged in Counts One and Three, the defendant, EVGENIY BOGACHEV, did acquire property that constitutes, and is derived from, the proceeds obtained, directly and indirectly, from such violation, thereby subjecting said property to forfeiture to the United States of America pursuant to Title 18, United States Code, Section 982(a)(2)(B).

46) As a result of the commission of the violations charged in Counts Four through Twelve, the defendant, EVGENIY BOGACHEV, did acquire property that constitutes, and is derived from, the proceeds obtained, directly and indirectly, from such violation, thereby subjecting said property to forfeiture to the United States of America pursuant to Title 18, United States Code, Section 982(a)(2)(A).

47) As a result of the commission of the violations charged in Counts Thirteen through Fourteen, the defendant,

EVGENIY BOGACHEV, did acquire property, real or personal, that was involved in such violation or was traceable to such property thereby subjecting said property to forfeiture to the United States of America pursuant to Title 18, United States Code, Section 982(a)(1).

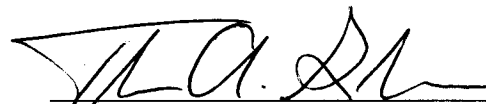
48) As a result of the commission of the violations charged in Counts One and Two, the defendant, EVGENIY BOGACHEV, did acquire property that constitutes, and is derived from, the proceeds obtained, directly and indirectly, from such violation, thereby subjecting said property to forfeiture to the United States of America pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).


49) If through any acts or omission by the defendant, EVGENIY BOGACHEV, any or all of the property described in paragraphs 44 to 48 above (hereinafter the "Subject Properties")

- (a) Cannot be located upon the exercise of due diligence;
- (b) Has been transferred, sold to, or deposited with a third person;
- (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 subdivided without difficulty.

the United States intends to seek forfeiture of any other property of the defendant up to the value of the Subject Properties forfeitable above pursuant to 28 U.S.C. Section 2461(c), which incorporates Title 21, United States Code, Section 853(p).

A True Bill,


FOREPERSON


DAVID J. HICKTON
United States Attorney
PA ID NO. 34524

1541

FILED

MAY 19 2014

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

UNITED STATES OF AMERICA)
)
 v.) Criminal No. 14-127
)
)
 EVGENIY BOGACHEV) **UNDER SEAL**

INDICTMENT MEMORANDUM

AND NOW comes the United States of America, by its attorneys, David J. Hickton, United States Attorney for the Western District of Pennsylvania, and Shardul S. Desai, Assistant United States Attorney for said District, and submits this Indictment Memorandum to the Court:

I. THE INDICTMENT

A Federal Grand Jury returned a fourteen-count Indictment against the above-named defendant for alleged violations of federal law:

<u>COUNTS</u>	<u>OFFENSE/DATE</u>	<u>TITLE/SECTION</u>
1	Conspiracy In and around September 2011-present	18 U.S.C. § 371
2	Wire Fraud On or about October 18, 2011	18 U.S.C. § 1343
3	Computer Fraud On or about October 20, 2011	18 U.S.C. §§ 1030(a)(2) and 1030(c)(2)(B)
4-12	Bank Fraud On or about October 20, 2011	18 U.S.C. § 1344
13-14	Money Laundering On or about October 21, 2011	18 U.S.C. §§ 1957(a) and 1956(i)(1)(B)

II. ELEMENTS OF THE OFFENSES

A. As to Count 1 (Conspiracy):

In order for the crime of Conspiracy, in violation of 18 U.S.C. § 371, to be established, the government must prove all of the following essential elements beyond a reasonable doubt:

1. That two or more persons agreed to commit the offenses against the United States, as charged in the indictment;

2. That the defendant was a party to or member of that agreement;

3. That the defendant joined the agreement or conspiracy knowing of its objectives to commit offenses against the United States and intending to join together with at least one other alleged conspirator to achieve those objectives; that is, that the defendant and at least one other alleged conspirator shared a unity of purpose and the intent to achieve common goals or objectives, to commit offenses against the United States; and

4. That at some time during the existence of the agreement or conspiracy, at least one of its members performed an overt act in order to further the objectives of the agreement.

Third Circuit Model Criminal Jury
Instruction 6.18.371A.

B. As to Count 2 (Wire Fraud):

In order for the crime of Wire Fraud, in violation of 18 U.S.C. § 1343, to be established, the government must prove all of the following essential elements beyond a reasonable doubt:

1. That the defendant devised a scheme to defraud or to obtain money or property by materially false or fraudulent pretenses, representations or promises or willfully participated in such a scheme with knowledge of its fraudulent nature;

2. That the defendant acted with the intent to defraud; and

3. That in advancing, furthering, or carrying out the scheme, the defendant transmitted any writing, signal, or sound by means of a wire, radio, or television communication in interstate commerce or caused the transmission of any writing, signal, or sound of some kind by means of a wire, radio, or television communication in interstate commerce.

Third Circuit Model Criminal Jury
Instruction 6.18.1343.

C. As to Count 3 (Computer Fraud):

In order for the crime of a Unauthorized Access into a Protected Computer, in violation of 18 U.S.C. §§ 1030(a)(2) and

1030(c)(2)(B), to be established, the government must prove all of the following essential elements beyond a reasonable doubt:

1. That the defendant intentionally accessed a computer;
2. That the defendant did so without authorization or in excess of authorization;
3. That the defendant obtained information as a result of the access;
4. That the computer accessed was a protected computer; and
5. That the access of the computer was committed for purposes of a commercial advantage or private financial gain or was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

Authority: 18 U.S.C. §§ 1030(a)(2), 1030(c)(2)(B).

D. As to Count 4-12 (Bank Fraud):

In order for the crime of Bank Fraud, in violation of 18 U.S.C. § 1344, to be established, the government must prove all of the following essential elements beyond a reasonable doubt:

1. That the defendant knowing executed a scheme or artifice to defraud a financial institution or knowingly executed a scheme to obtain the money, funds or other property

owned by or under the control of a financial institution by means of material false or fraudulent pretenses, representations or promises as detailed in the indictment;

2. That the defendant did so with the intent to defraud the financial institution; and

3. That the financial institution was then insured by the Federal Deposit Insurance Corporation or chartered by the United States.

Third Circuit Model Criminal Jury
Instruction 6.18.1344.

E. As to Count 13-14 (Money Laundering):

In order for the crime of Money Laundering, in violation of 18 U.S.C. §§ 1957(a) and 1956(i)(1)(B), to be established, the government must prove all of the following essential elements beyond a reasonable doubt:

1. That the defendant knowingly engaged in a "monetary transaction."

2. The value of the funds or monetary instrument involved in the transaction or attempted transaction exceeded \$10,000.00.

3. The defendant knew that the funds or monetary instrument involved in the transaction or attempted transaction constituted "criminally derived property."

4. The property involved in the transaction (i.e., the funds or monetary instrument) was, in fact, the proceeds of "specified unlawful activity," as defined in 18 U.S.C. § 1956(c)(7).

5. That the offense took place in the United States or in a special maritime or territorial jurisdiction of the United States.

Authority: 18 U.S.C. §§ 1957(a),
1957(d)(1), 1957(f)(1) and 1957(f)(2).

III. PENALTIES

A. As to Count 1: Conspiracy (18 U.S.C. § 371):

1. Individuals - The maximum penalties for individuals are:

(a) imprisonment of not more than 5 years (18 U.S.C. § 371);

(b) a fine not more than the greater of;

(1) \$250,000 (18 U.S.C. § 3571(b)(3));

or

(2) an alternative fine in an amount not more than the greater of twice the gross pecuniary gain to any person or twice the pecuniary loss to any person other than the defendant, unless the imposition of this alternative fine would unduly complicate or prolong the sentencing process (18 U.S.C. § 3571(d));

(c) a term of supervised release of not more than three (3) years (18 U.S.C. § 3583);

(d) Any or all of the above.

B. As to Count 2: Wire Fraud (18 U.S.C. § 1343):

1. Individuals - The maximum penalties for individuals are:

(a) If the violation affects a financial institution, imprisonment of not more than thirty (30) years otherwise imprisonment of not more than 20 years (18 U.S.C. § 1343);

(b) a fine not more than the greater of:

(1) \$250,000 (18 U.S.C. § 3571(b)(3));

(2) If the violation affects a financial institution, a fine of \$1,000,000 (18 U.S.C. § 1343);

or

(3) an alternative fine in an amount not more than the greater of twice the gross pecuniary gain to any person or twice the pecuniary loss to any person other than the defendant, unless the imposition of this alternative fine would unduly complicate or prolong the sentencing process (18 U.S.C. § 3571(d));

(c) a term of supervised release of not more than three (3) years or, if the violation affects a financial institution, of not more than five (5) years (18 U.S.C. §§ 3559, 3583);

(d) Any or all of the above.

C. As to Count 3: Computer Fraud (18 U.S.C. §§ 1030(a)(2) and 1030(c)(2)(B)):

1. Individuals - The maximum penalties for individuals are:

(a) imprisonment of not more than 5 years (18 U.S.C. § 1030(c)(2)(B));

(b) a fine not more than the greater of;

(1) \$250,000 (18 U.S.C. § 3571(b)(3));

or

(2) an alternative fine in an amount not more than the greater of twice the gross pecuniary gain to any person or twice the pecuniary loss to any person other than the defendant, unless the imposition of this alternative fine would unduly complicate or prolong the sentencing process (18 U.S.C. § 3571(d));

(c) a term of supervised release of not more than three (3) years (18 U.S.C. § 3583);

(d) Any or all of the above.

D. As to Count 4-12: Bank Fraud (18 U.S.C. § 1344):

1. Individuals - The maximum penalties for individuals are:

(a) imprisonment of not more than 30 years (18 U.S.C. § 1344);

(b) a fine not more than the greater of:

(1) \$1,000,000 (18 U.S.C. § 1343);

or

(2) an alternative fine in an amount not more than the greater of twice the gross pecuniary gain to any person or twice the pecuniary loss to any person other than the defendant, unless the imposition of this alternative fine would unduly complicate or prolong the sentencing process (18 U.S.C. § 3571(d));

(c) a term of supervised release of not more than five (5) years (18 U.S.C. § 3583);

(d) Any or all of the above.

E. As to Count 13-14: Engaging in Monetary Transactions (18 U.S.C. §§ 1957(a) and 1956(i)(1)(B)):

1. Individuals - The maximum penalties for individuals are:

(a) imprisonment of not more than 10 years (18 U.S.C. § 1957(b)(1));

(b) a fine not more than the greater of:

(1) \$250,000 (18 U.S.C. § 3571(b)(3));

or

(2) an alternative fine of not more than twice the amount of criminally derived property involved in the transaction (18 U.S.C. § 1957(b)(2));

(c) a term of supervised release of not more than three (3) years (18 U.S.C. § 3583);

(d) Any or all of the above.

IV. MANDATORY SPECIAL ASSESSMENT

A mandatory special assessment of \$100.00 must be imposed at each count upon which the defendants are convicted, pursuant to 18 U.S.C. § 3013.

V. RESTITUTION

Restitution may be required in this case as to Counts One through Twelve together with any authorized penalty, as part of the defendant's sentence pursuant to 18 U.S.C. §§ 3663, 3663A, and 3664.

VI. FORFEITURE

As provided in the Indictment, forfeiture may be applicable in this case.

Respectfully submitted,

DAVID J. HICKTON
United States Attorney

By: Shardul S. Desai
SHARDUL S. DESAI
Assistant U.S. Attorney
DC Bar No. 990299

AO 91 (Rev 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Nebraska

SEALED

United States of America

v.

EVGENIY MIKHAYLOVICH BOGACHEV,
a/k/a/ "LUCKY12345"

Case No. 4:14MJ3034

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May, 2009 to May 21, 2010, in the county of Douglas in the District of Nebraska, and elsewhere, the defendant(s) violated:

Code Section

Offense Description

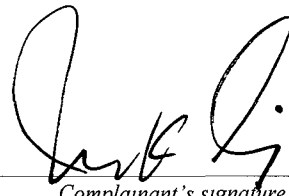
18 U.S.C. § 1349
18 U.S.C. § 1344

Defendant EVGENIY MIKHAYLOVICH BOGACHEV, also known as "LUCKY12345," did knowingly and intentionally conspire with others, both known and unknown, to commit bank fraud, as more specifically described in the attached affidavit, said affidavit incorporated herein by reference.

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT OF SA JAMES CRAIG, INCORPORATED HEREIN BY REFERENCE.

Continued on the attached sheet.



Complainant's signature

JAMES K. CRAIG, SPECIAL AGENT, FBI

Printed name and title

Sworn to before me by telephone and reasonable electronic means:

Date: May 30, 2014.

City and state: Lincoln, Nebraska



Cheryl R. Zwart, United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,

Plaintiff,

v.

EVGENIY MIKHAYLOVICH BOGACHEV,
a/k/a/ "LUCKY12345"

Defendant.

Case No. 4:14MJ3034

UNDER SEAL

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Special Agent James K. Craig, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a criminal complaint against EVGENIY MIKHAYLOVICH BOGACHEV, also known as "lucky12345" (hereinafter, the "DEFENDANT").

2. I am a Special Agent with the FBI and have been since August of 2008. Since July of 2009, my duties include the investigation of offenses including violations of Title 18, United States Code, Section 1030, unauthorized access to computers and computer fraud. I have received specialized training for conducting computer-based investigations, including training regarding computer hardware, networks, network security and computer intrusions. I have received training from the FBI regarding computer crimes and have extensive experience regarding computers, networks and the workings of the Internet.

3. I am currently employed as a Special Agent of the Federal Bureau of Investigation ("FBI"), and am assigned to the Cyber Crime Task Force of the Omaha Field

Office in the District of Nebraska. I have been employed by the FBI since August 2005, and have been a Special Agent since August 2008.

4. The information contained in this affidavit is based upon my personal knowledge, my review of documents and other evidence, my conversations with other law enforcement officers and other individuals, and my training and experience. All conversations and statements described in this affidavit are related in substance and in part unless otherwise indicated. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. I have not, however, excluded any information known to me that would defeat a determination of probable cause.

PROBABLE CAUSE

A. Overview

5. This affidavit establishes probable cause to believe that DEFENDANT has been a member of a long-running conspiracy to employ widespread computer intrusions, malicious software, and fraud to steal millions of dollars from numerous bank accounts in the United States and elsewhere. As more fully described below, DEFENDANT and others have infected thousands of business computers with malicious software that captures passwords, account numbers, and other information necessary to log into online banking accounts, and have then used the captured information to steal millions of dollars from victims' bank accounts.

B. Defendant and Co-Conspirators

6. At all times material to this affidavit:

- a. DEFENDANT was a resident of Russia. He used the online nickname "lucky12345." DEFENDANT was a coder who developed new codes to

compromise banking systems and assisted others in stealing and exploiting banking credentials.

- b. VYACHESLAV IGOREVICH PENCHUKOV was a resident of Ukraine. He used the online nickname “tank.” PENCHUKOV coordinated the exchange of stolen banking credentials and money mules.¹ PENCHUKOV also received alert messages which provided notification once a bank account had been compromised.
- c. IVAN VIKTORVICH KLEPIKOV was a resident of Ukraine. He used the online nickname “petr0vich.” KLEPIKOV was a systems administrator who handled the technical aspects of the criminal scheme. KLEPIKOV also received alerts which provided notification once a bank account has been compromised.
- d. ALEXEY DMITRIEVICH BRON was a resident of Ukraine. He used the online nickname “thehead.” BRON was the financial manager of the criminal operations. BRON managed the transfer of money through an online money system known as Webmoney.
- e. ALEXEY TIKONOV was a resident of Russia. He used the online nickname “kusanagi.” TIKONOV was a coder or developer who assisted the criminal enterprise by developing new codes to compromise banking systems.
- f. YEVHEN KULIBABA was a resident of the United Kingdom. He used the online nickname “jonni.” KULIBABA, who is in custody in the United Kingdom, provided money mules and their associated banking credentials in

¹ “Money mules,” as detailed below, are persons in the United States who are recruited to receive stolen funds via wire and then wire the money outside the United States.

order to facilitate the movement of money which was withdrawn from victim accounts by fraudulent means. He operated the money laundering network in the United Kingdom.

- g. YURIY KONOVALENKO was a resident of the United Kingdom. He used the online nickname “jtk0.” KONOVALENKO, who is in custody in the United Kingdom, provided money mules’ and victims’ banking credentials to KULIBABA and facilitated the collection of victim data from other conspirators.
- h. “AQUA” was a resident of Russia. He used the online nickname “aqua.” “AQUA” provided money mules and their associated banking credentials in order to facilitate the movement of money which was withdrawn from victim accounts by fraudulent means.
- i. “MRICQ” was a resident of Ukraine. He used the online nickname “mricq.” “MRICQ” was a coder who developed new codes to compromise the banking system and passed user credentials to other conspirators.

C. Selected Victims

- 7. At all times material to this affidavit:
 - a. APC PROPERTIES LLC was a business located in Lafayette, Louisiana.
 - b. ARBEN GROUP LLC was a business located in Pleasantville, New York.
 - c. BANK OF ALBUQUERQUE was a subsidiary of BANK OF OKLAHOMA, a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Albuquerque, New Mexico.
 - d. BANK OF GEORGETOWN was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Washington, District of

Columbia.

- e. BASTRIRE EDWARDS, CPAS was a business located in Visalia, California.
- f. BULLITT COUNTY FISCAL COURT was a municipal government office in Shepherdsville, Kentucky.
- g. CALIFORNIA BANK AND TRUST was a financial institution insured by the Federal Deposit Insurance Corporation, and was headquartered in San Diego, California.
- h. CAPITAL ONE BANK was a financial institution insured by the Federal Deposit Insurance Corporation, and was headquartered in Glen Allen, Virginia.
- i. DOLL DISTRIBUTING was a business located in Des Moines, Iowa.
- j. DOWNEAST ENERGY AND BUILDING SUPPLY was a business located in Brunswick, Maine.
- k. ESCROW SCOURCE was a business located in Seattle, Washington.
- l. FIRST FEDERAL SAVINGS BANK was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Elizabethtown, Kentucky.
- m. FIRST NATIONAL BANK OF OMAHA was a financial institution insured by the Federal Deposit Insurance Corporation, and was headquartered in Omaha, Nebraska. It offered online banking services through computer servers located in Nebraska.
- n. GCM FEDERAL CREDIT UNION was a financial institution insured by the National Credit Union Share Insurance Fund, and was located in Saint Paul, Minnesota.

- o. GENLABS was a business located in Chino, California.
- p. HUSKER AG, LLC was a business located in Plainview, Nebraska.
- q. KEY BANK was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Sylvania, Ohio.
- r. LIEBER'S LUGGAGE was a business located in Albuquerque, New Mexico.
- s. PARAGO, INC. was a business located in Lewisville, Texas.
- t. PARKINSON CONSTRUCTION was a business located in Brentwood, Maryland.
- u. SALISBURY BANK & TRUST was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Salisbury, Massachusetts.
- v. TOWN OF EGREMONT was a town in Massachusetts with its own municipal government.
- w. UNION BANK AND TRUST was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Lincoln, Nebraska.
- x. VISALIA COMMUNITY BANK was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Visalia, California.
- y. WEBSTER BANK was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Waterbury, Connecticut.

D. Overview of the Scheme

8. DEFENDANT, being a person employed by and associated with the Jabber Zeus Crew, conspired with PENCHUKOV, KLEPIKOV, BRON, TIKONOV, KULIBABA,

KONOVALENKO, “AQUA,” and “MRICQ” (hereinafter “CO-CONSPIRATORS”),² and with others both known and unknown to devise and execute a scheme and artifice to defraud several depository institutions insured by either the Federal Deposit Insurance Corporation or the National Credit Union Share Insurance Fund.

9. It was part of the scheme that DEFENDANT AND CO-CONSPIRATORS used computer intrusions, malicious software, and fraud to steal or attempt to steal millions of dollars from several bank accounts in the United States, and elsewhere. DEFENDANT AND CO-CONSPIRATORS infected thousands of business computers with software that captured passwords, account numbers, and other information necessary to log into online banking accounts, and then used the captured information to steal millions of dollars from account holding victims’ bank accounts. Account-holding victims included APC PROPERTIES, ARBEN GROUP, BASTRIRE EDWARDS, CPAS, BULLITT COUNTY FISCAL COURT, DOLL DISTRIBUTING, DOWNEAST ENERGY AND BUILDING SUPPLY, ESCROW SOURCE, GCM FEDERAL CREDIT UNION, GENLABS, HUSKER AG, LLC, LIEBER’S LUGGAGE, PARKINSON CONSTRUCTION, PARAGO, INC., and TOWN OF EGREMONT.

10. DEFENDANT AND CO-CONSPIRATORS intended and foresaw that their conduct would defraud banks in the District of Nebraska.

11. The actions of DEFENDANT AND CO-CONSPIRATORS to execute the scheme included the following:

- a. Infecting the computers used by small businesses and non-profit organizations with malicious software;

² DEFENDANT was previously charged by indictment in 4:11CR3074, but under his online nickname only.

- b. Obtaining bank account numbers, passwords, PIN numbers, RSA SecureID token codes, and similar information necessary to log into online bank accounts;
- c. Initiating electronic funds transfers from those bank accounts to the bank accounts of “money mules;”
- d. Transferring funds from money mules to overseas;
- e. Obtaining the use of computer servers necessary to obtain banking credentials and provide real-time communications among enterprise members; and
- f. Assigning different members the tasks of writing malicious software, administering computer servers, recruiting money mules, infecting computers, accessing bank accounts to make unauthorized transfers, and receiving transferred funds outside the United States.

E. Electronic Funds Transfer System

12. This investigation has identified numerous unauthorized Electronic Funds Transfers (“EFTs”) initiated from victim bank accounts. There are two primary types of EFTs: wire transfers, and Automated Clearing House (“ACH”) payments. Both of these EFTs are performed through the Federal Reserve Bank System. The primary method used by DEFENDANT AND CO-CONSPIRATORS to steal funds has been through ACH payments.

13. Wire transfers are real-time transfers of funds. After a wire transfer is initiated from a sending bank, the sending bank’s Reserve Account at the Federal Reserve Bank is immediately debited and the receiving bank’s Reserve Account is immediately credited. Wire transfers are typically performed when transactions are time-sensitive or are for large dollar amounts. Recipients of wire transfers have immediate access to the funds through their account at the receiving financial institution.

14. ACH Payments are made through the ACH Network, which is a batch-oriented EFT system wherein batch transfers are settled the next day. The ACH Network is governed by the National Automated Clearing House Association (“NACHA”) regulations. The Federal Reserve and Electronic Payments Network act as the central clearing facilities through which institutions transmit or receive funds. ACH Payments are typically used for direct deposit to payroll, direct payment for consumer bills (mortgages, loans, etc.), electronic checks, business-to-business payments, or e-commerce payments. ACH payments are either credits (also known as direct deposits) or debits (also known as direct payments). An ACH credit is always initiated by the sender whereas ACH debits are initiated by either the sender or receiver. ACH Payments are submitted in batches from the originator (through their financial institution) to the Federal Reserve Bank. One day later, these batch payments are settled and the payment is sent to the receiving depository financial institution. At the time of settlement, funds are debited from the sending financial institution’s account at the Federal Reserve Bank and credited to the receiving financial institution’s account.

15. Larger financial institutions have developed their own software to conduct ACH Payments and wire transfers based on the rules governing EFTs through the Federal Reserve Bank. Smaller financial institutions that do not have their own Information Systems Departments utilize Third-Party Processor systems, which allow these banks to conduct EFTs. There are several companies which have developed systems which are utilized by these smaller financial institutions to conduct EFTs, including FundsXpress, Fiserv, FundTech, CashEdge, Jack Henry, and Metavante. Each of these companies must comply with same regulations that the financial institutions are required to follow. FundsXpress, which is a subsidiary of FirstData, has approximately 600 client financial institutions for which it processes EFTs. This

investigation has uncovered fraudulent EFTs which were processed through several Third-Party Processors.

F. The Zeus Malware

16. FirstData (“FD”) requires all client financial institutions to provide multi-factor authentication for their banking customers in order to conduct Internet-based banking transactions. This multi-factor authentication uses a username, password, and either a security challenge question or a one-time personal identification number (“PIN”). The one-time PINs are mailed to the banking customers for later use. FD also uses electronic behavioral analysis in the login authentication process. For example, for each online login attempt, FD stores the customer’s IP address, Internet browser, cookie, time of day, and frequency of use to build a profile of the user’s activity. If the login behavior differs from their “normal” use, the user is challenged to either enter a one-time PIN or else answer a security question. Therefore, an unauthorized user who attempts to log into the system must not only have the username and password, but the answer to various security questions or the one-time PIN.

17. Beginning in May 2009, the FBI began receiving numerous complaints of fraudulent ACH transfers. Through techniques described later in this affidavit, the FBI was able to determine that a large number of fraudulent transfers were being made by unauthorized users, who were gaining the one-time PINs and security questions in real-time to initiate the transfers. FBI Omaha, the FBI’s Cyber Division, and several other FBI Division offices began coordinating with Internet security researchers, ACH payment processors, and financial institutions in an effort to determine how the unauthorized users were gaining the one-time PINs and security questions in real-time and initiated an effort to determine links between incidents nationwide.

18. On June 1, 2009, Internet security researchers at the company iDefense, a provider of computer security intelligence to corporate clients, discovered a modified version of the “Zeus” malicious software that was capable of sending one-time passwords, such as one-time PINs, directly to the attackers in real-time, through an “instant message” protocol known as “Jabber.” Based on my training and experience, I know that Jabber is a method of sending and receiving text-based communication sent over the Internet, also referred to as “chat.”

19. Based on my training and experience and on information developed during this investigation, I know that Zeus is the name of an identified “keylogger” used to steal online banking information. A keylogger is a form of malicious code which are designed to capture the keystrokes of a user on the machine which the keylogger is installed.³ The primary purpose of a keylogger is to capture the keystrokes for usernames and passwords used to access websites, e-mail, and other services from the victim computer. Keyloggers are often designed to send the captured keystrokes back to the criminal who installed the keylogger on the victim machine. These captured keystrokes are typically sent over the Internet in regular time intervals from the victim machine to a machine controlled by the criminal. An unknown criminal or group of criminals developed this keylogger as part of a toolkit to sell to other criminals. FBI investigations and Internet security company researchers have identified criminals advertising the toolkit for sale on various Internet forums used by criminals to exchange fraud information.

³ Malicious code is a term used to describe any software code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, trojan horses, backdoors, and malicious active content. It is often installed on a victim computer system via the Internet through spam that contains attachments or through a website where code is injected to automatically download onto a victim system when it is viewed through a web browser. When it is installed onto a victim computer system to perform malicious activity, it is often referred to as malware.

Copies of the toolkit have been obtained for analysis. The developers of Zeus gave the toolkit that name. However, it is often detected by anti-virus software under the name “zbot” (short for “Zeus bot”) or “wsnpoem,” based on a directory name created on the victim machine when it is installed. Zeus is referred to as a toolkit because it contains software which enables a criminal to operate a database for storing captured data, operate a command and control server, and to create new variants of the keylogger which are not detectable by anti-virus programs. Simple changes in the software code will change the signature of the keylogger, thus creating a new variant which is not recognized as a Zeus bot even though it is performing the same function as the previous variant.⁴

20. Zeus had become such a notorious toolkit that in January 2009, computer security researchers in Switzerland, who are well known to FBI Cyber investigators, had devoted a website to tracking command and control servers communicating with Zeus bots. Their page is hosted at the URL <https://zeustracker.abuse.ch>. This site is often referred to as the “Zeustracker” site. The Zeus bots on victim computers can be configured to communicate to the command and control servers through a domain name, such as kerchon.com, and not by the command and control server’s IP address. Therefore, a criminal can easily change the computer on which the domain resides (kerchon.com, in this example) and the infected victim computers will communicate with the criminal’s new computer system. The criminal can also send the Zeus bot

⁴ 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 initiate a denial of service attack, send spam, operate as proxies (blindly forwarding Internet data), host phishing sites, or participate in other crime.

a software configuration update with a new domain for the Zeus bot to communicate. It is therefore difficult to quantify how many criminals or criminal groups are operating Zeus command and control servers. Since the creation of the Zeustracker website, the researchers have identified approximately 1,000 unique command and control server computers which talk to Zeus bots.

21. Zeus bots use encoded (not humanly-readable) configuration files that contain the list of banking/web targets for which that particular bot is programmed to capture information. The security researchers referenced above devote time to decoding the configuration files in order to alert the Internet security community of the current and historical target websites. Researchers search for the unique alpha-numeric key that will decode the configuration file. The unique alpha-numeric keys can be used to decode multiple configuration files. This indicates a relationship between the Zeus bots for which the configuration files are decoding, meaning there is reason to believe that the Zeus bots were deployed or controlled by the same criminal or criminal group.

22. iDefense released analysis in iDefense report #486471 on June 4, 2009. The analysis revealed that the modified version of Zeus was capable of sending one-time passwords, such as one-time PINs, directly to the attackers in real-time, through the Jabber instant message protocol.

23. Further analysis published by iDefense stated that stolen login credentials were sent via the Jabber instant-message protocol to the domain incomeet.com, which was hosted on the IP address 66.199.248.195 (hereinafter the "INCOMEET SERVER"). Further, iDefense advised that once the Zeus keylogger was fully installed on a victim system, it would be detected as having the filename "sdra64.exe," if the virus was not already removed by an anti-virus

program.

G. Investigation and Searches of the INCOMEET SERVER

24. Investigation of the Zeus malware led me to believe that a computer with the IP address 66.199.248.195 – i.e., the INCOMEET SERVER – was receiving Jabber instant messages containing the usernames, passwords, PIN numbers, and possibly other credentials necessary to log into victims’ bank accounts.

25. An open source address lookup of the IP address 66.199.248.195 on September 17, 2009, revealed that it hosted the domain incomeet.com. It also revealed that the address corresponded to EZZI.NET. EZZI.NET is a company headquartered at 882 Third Avenue, 9th Floor, Brooklyn, NY 11232. EZZI.NET maintains server computers connected to the Internet. Their customers use those computers to operate servers on the Internet that, in turn, provide services to client computers. In general, customers configure their computers remotely, connecting to them over the Internet through the Secure Shell (“SSH”) protocol.

26. On September 18, 2009, an FBI agent interviewed Mohammed Salim, an employee at EZZI.NET. According to Salim, the INCOMEET SERVER was built by EZZI.NET at the request of the customer, to the customer’s specification. The INCOMEET SERVER had one 500 gigabyte hard drive, 2 gigabytes of RAM, and a dual-core AMD processor. It ran the CentOS 5.0 distribution of the Linux operating system. It was leased to someone who identified himself as “Alexey S.” (no full last name known), who claimed to be associated with a company “IP-Server Ltd,” supposedly located at Komsomolskaya St. 1, Moscow, Russian Federation.

27. Pursuant to search warrants, the FBI searched the INCOMEET SERVER on four occasions: September 28, 2009, December 9, 2009, March 17, 2010, and May 21, 2010.

28. On the INCOMEET SERVER, agents found extensive logs of chat communications. These included usernames, passwords, and temporary token numbers for hundreds of bank and brokerage accounts, username and passwords for Paypal.com and other financial sites, and other information collected from infected victim computers.

29. For example, on March 16, 2010, alone, 16 different Jabber communications that appeared to pertain to stolen banking credentials were passed through the INCOMEET SERVER. Many of these pertained to the same victims. For example, one of those messages read as follows:

```
Panel: http://193.104.41.131/
Template: WebCashMgmt
Added: 2010-03-15 23:48:09
Updated: 2010-03-15 23:48:09
IPv4: 76.79.206.130
BotID:
BotNet:
Country: US
Host: rrcs-76-79-206-130.west.biz.rr.com
UserAgent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR
1.1.4322; AskTB5.6)
Location: https://bob.sovereignbank.com/wcmfd/wcmpw/CustomerLogin
Status: Waitoperator
Data:
Customer/Organization ID: KUS2761
User ID: sysadmin
Password: Kunal[remainder of password redacted]
```

30. From my review of other messages sent through the server, I know that this message represents the transmission of compromised banking credentials. Specifically, this says that a user with user ID “KUS2761,” and a password beginning “Kunal” (the remainder of the password was in the original message but has been redacted from this affidavit) used the IP address 76.79.206.130 to attempt to access an account on Sovereign Bank, which is in the United States.

31. Additionally, the INCOMEET SERVER contained evidence that it was used by

the conspirators to communicate with each other. The INCOMEET SERVER's operators had configured it to record on its hard drive ongoing logs of every chat message sent through the server. These chat communications included discussions among conspirators made as they were in the progress of transferring money out of victim bank accounts. They also discuss the recruitment of "mules" – persons in the United States who are recruited to receive ACH payments and wire the money outside the United States. They also discuss the operation of their botnet. The conspirators communicated in Russian, using both the Cyrillic and Roman alphabets. All chats quoted in this affidavit have been translated into English, using human translators except where indicated. In some cases, immaterial lines of chat have been omitted for brevity's sake.

32. Participants in the chat identified themselves by nicknames. With exceptions, noted below, they do not reveal in chat their real names or other personally identifiable information.

33. On July 2, 2009, a writer for the Washington Post website posted a blog entry entitled "PC Invader Costs Ky. County \$415,000," which began with the lead paragraph, "Cyber criminals based in Ukraine stole \$415,000 from the coffers of Bullitt County, Kentucky this week. The crooks were aided by more than two dozen co-conspirators in the United States, as well as a strain of malicious software capable of defeating online security measures put in place by many banks."⁵ The article generally described the theft of funds from the Bullitt County Fiscal Court in Shepherdsville, Kentucky, as described in this affidavit. The blog entry is accessible at http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud

⁵ In this quotation, and hereinafter in this affidavit, all money/currency amounts are in U.S. dollars, unless otherwise indicated.

part ii.html.

34. Chat logs show that the conspirators viewed this posting and recognized that it described their criminal activity. For example, on July 12, 2009, the user with the online name of “aqua” (i.e., “AQUA”) said the following to user “tank” (later determined to be PENCHUKOV): “But they described the entire scheme. The Bastards. They exposed the texts. They laid out the entire scheme. ... It’s necessary to give to the supporting [people?] to read. I’m really pissed. They exposed the entire deal.”

35. Also on July 12, 2009, user “aqua” and user “tank” had this exchange:

tank: Well, nevertheless, they were writing about us.
aqua: So because of whom did they lock Western Union for Ukraine?
aqua: Tough shit.
tank: *****Originator: BULLITT COUNTY FISCAL Company: Bullitt
County Fiscal Court
aqua: So?
aqua: This is the court system.
tank: Shit.
tank: Yes
aqua: This is why they fucked [nailed?] several drops.
tank: Yes, indeed.
aqua: Well, fuck. Hackers: It's true they stole a lot of money.

36. That same day, user “tank,” while chatting with user “indep,” specifically referenced the URL of the Washington Post blog posting and discussed its contents:

tank: [Are you] there?
indep: Yeah.
indep: Greetings.
tank: [http://voices.washingtonpost.com/securityfix/2009/07/
an_odyssey_of_fraud_part_ii.html#more](http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html#more)
tank: This is still about me.
tank: Originator: BULLITT COUNTY FISCAL Company: Bullitt County Fiscal
Court
tank: He is the account from which we cashed.
tank: Today someone else send this news.
tank: I'm reading and thinking: Let me take a look at history. For
some reason this name is familiar.
tank: I'm on line and I'll look. Ah, here is this shit.
indep: How are you?

tank: Did you get my announcements?
indep: Well, I congratulate [you].
indep: This is just fuck when they write about you in the news.
tank: Whose [What]?
tank: :D
indep: Too much publicity is not needed.
tank: Well, so nobody knows who they are talking about.

37. At roughly the same time that user “tank” was having this chat conversation with user “indep,” user “tank” was also having the following chat conversation with user

“lucky12345” (i.e., DEFENDANT):

tank: Are you [it] there?
tank: This is what they damn wrote about me.
tank: http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html#more
tank: I'll take a quick look at history
tank: Originator: BULLITT COUNTY FISCAL Company: Bullitt County Fiscal Court
tank: Well, you got [it] from that cash-in.
lucky12345: From 200K?
tank: Well, they are not the right amounts and the cash out from that account was shitty.
tank: Levak was written there.
tank: Because now the entire USA knows about Zeus.
tank: :D
lucky12345: It's fucked.

38. On or about July 29, 2009, DOLL DISTRIBUTING, a company that banks with FIRST NATIONAL BANK OF OMAHA, reported that it experienced two fraudulent ACH payments totaling \$59,222. In a chat message sent on July 28, 2009, from user “777” to user “hrd” on the INCOMEET SERVER, it was reported that \$29,383 was transmitted from Doll to KODASH CONSULTING, LLC, and that \$29,839 was transmitted to PANDORA SERVICES, LLC.

39. On July 31, 2009, an FBI agent interviewed Renee Michelli, the proprietor of PANDORA SERVICES, LLC. Michelli stated that she been looking for a job and had posted

her resume on Internet job seeker sites. She was supposedly “hired” as a United States representative for a Russian software company, “1C.” She was told to establish an LLC with a bank account. She was told her job would involve receiving payments and wiring them outside the United States. On October 2, 2009, Heidi Nelson, the proprietor of KODASH CONSULTING, LLC, was interviewed by another FBI agent. Nelson stated that she lost her job in early 2009, and put her resume on Internet job seeker sites. She was contacted by an individual claiming to be an assistant human resources manager for a Russian company. Her job would be to work with clients in the United States, and on occasion to receive payments from them, which she would transmit to Russia. Based on my training and experience and information developed during this investigation, I believe that Michelli and Nelson were “money mules” hired by the DEFENDANT AND CO-CONSPIRATORS to facilitate the transfer of stolen funds.

40. Through the execution of the four search warrants, other agents and I found chat communications on the INCOMEET SERVER describing the transfer of money from a large number of bank accounts, including those held by APC PROPERTIES, ARBEN GROUP, BASTRIRE EDWARDS, CPAS, BULLITT COUNTY FISCAL COURT, DOLL DISTRIBUTING, DOWNEAST ENERGY AND BUILDING SUPPLY, ESCROW SOURCE, GCM FEDERAL CREDIT UNION, GENLABS, HUSKER AG, LLC, LIEBER’S LUGGAGE, PARKINSON CONSTRICTION, PARAGO, INC., and TOWN OF EGREMONT. These chats usually occurred within hours of the transfers in question. Among other things, the chats were used to transmit log-in credentials for victims, report the transfer of funds to mules, and/or request bank account information for mules. DEFENDANT AND CO-CONSPIRATORS referenced herein participated in one or more chats relating to or facilitating thefts of log-in

credentials or fraudulent transfers of funds from victims. Some of those chats are referenced in Overt Acts, below.

THE CONSPIRACY

41. From in or about May 2009, the exact date being unknown, and continuing to on or about May 21, 2010, in the District of Nebraska and elsewhere, DEFENDANT, being a person employed by and associated with the Jabber Zeus Crew, did unlawfully, voluntarily, intentionally and knowingly conspire, combine, confederate, and agree with each other, with CO-CONSPIRATORS, and with others both known and unknown to the Grand Jury to devise and execute a scheme and artifice to defraud BANK OF ALBUQUERQUE, BANK OF GEORGETOWN, CALIFORNIA BANK AND TRUST, CAPITAL ONE BANK, FIRST FEDERAL SAVINGS BANK, FIRST NATIONAL BANK OF OMAHA, GCM FEDERAL CREDIT UNION, KEY BANK, SALISBURY BANK & TRUST, UNION BANK AND TRUST, VISALIA COMMUNITY BANK, and WEBSTER BANK, all of which were depository institutions insured by either the Federal Deposit Insurance Corporation or the National Credit Union Share Insurance Fund.

A. Manner and Means of the Conspiracy

42. It was part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS used computer intrusion, malicious software, and fraud to steal or attempt to steal millions of dollars from several bank accounts in the United States, and elsewhere.

43. It was further part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS installed, without authorization, malicious software known as “Zeus” or “Zbot” on Internet-connected computers without those computers’ owners’ authorization, thereby causing damage to those computers.

44. It was further part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS used that malicious software to capture bank account numbers, passwords, and other information necessary to log into online banking accounts.

45. It was further part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS used that captured information without authorization to falsely represent to banks that DEFENDANTS AND CO-CONSPIRATORS were employees of the victims authorized to make transfers of funds from the victims' bank accounts.

46. It was further part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS used that captured information to cause banks to make unauthorized transfers of funds from the victims' bank accounts.

47. It was further part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS used as "money mules" residents of the United States who received funds transferred over the Automated Clearing House ("ACH") network or through other interstate wire systems from victims' bank accounts into the money mules' own bank accounts, and then withdrew some of those funds and wired the funds overseas to conspirators.

48. It was further part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS maintained Internet-connected computer servers, in the United States and elsewhere, to facilitate communication.

49. It was further part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS knowingly falsely registered a domain name and knowingly used that domain name in the course of the offense, in violation of 18 U.S.C. § 3559(g)(1).

B. Overt Acts

50. In furtherance of the conspiracy and to achieve the objectives thereof, at least one

of the conspirators performed or caused to be performed at least one of the following overt acts,⁶ among others, in the District of Nebraska and elsewhere:⁷

- a. On or about June 22, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by BULLITT COUNTY FISCAL COURT.
- b. On or about June 22, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause FIRST FEDERAL SAVINGS BANK to transfer funds out of a bank account belonging to BULLITT COUNTY FISCAL COURT and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- c. On or about June 27, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by GCM FEDERAL CREDIT UNION.
- d. On July 8, 2009, DEFENDANT sent a chat message to PENCHUKOV which included details of a bank account. The message contained account and company identification information.
- e. On July 8, 2009, DEFENDANT sent another chat message to PENCHUKOV which included details of a bank account. The message contained account and company identification information.

⁶ I note that 18 U.S.C. § 1349 does not require proof of an overt act in furtherance of the conspiracy.

⁷ In the description of the overt acts as set forth below, DEFENDANT is specifically identified as an actor. Evidence concerning the attribution of the nickname used by DEFENDANT on the INCOMEET SERVER, “lucky12345,” is set forth below under “ATTRIBUTION.”

- f. On or about July 8, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by TOWN OF EGREMONT.
- g. On or about July 12 and 13, 2009, DEFENDANT, PENCHUKOV, "AQUA," and another individual exchanged online messages about unauthorized withdrawals they had made from a bank account owned by BULLITT COUNTY FISCAL COURT.
- h. On or about July 21, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause GCM FEDERAL CREDIT UNION to transfer funds out of its general ledger account and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- i. On or about July 28, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by DOLL DISTRIBUTING.
- j. On or about July 29, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause SALISBURY BANK & TRUST to transfer funds out of a bank account belonging to TOWN OF EGREMONT and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- k. On or about July 29, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to attempt to cause FIRST NATIONAL BANK OF OMAHA to transfer funds out of a bank account belonging to DOLL DISTRIBUTING and into one or more bank accounts designated by

DEFENDANT AND CO-CONSPIRATORS.

- l. On or about September 1, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by ESCROW SOURCE.
- m. On or about September 1, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause KEY BANK to transfer funds out of a bank account belonging to ESCROW SOURCE and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- n. On or about September 1, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by DOWNEAST ENERGY AND BUILDING SUPPLY.
- o. On or about September 1, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause KEY BANK to transfer funds out of a bank account belonging to DOWNEAST ENERGY AND BUILDING SUPPLY and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- p. On or about September 17, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by GENLABS.
- q. On or about September 17, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause CALIFORNIA BANK AND TRUST to transfer funds out of a bank account belonging to GENLABS and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.

- r. On or about September 18, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by LIEBER'S LUGGAGE.
- s. On or about September 18, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause BANK OF ALBUQUERQUE to transfer funds out of a bank account belonging to LIEBER'S LUGGAGE and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- t. On or about September 28, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by PARAGO, INC.
- u. On or about September 28, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to attempt to cause FIRST NATIONAL BANK OF OMAHA to transfer funds out of a bank account belonging to PARAGO, INC. and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- v. On or about October 28, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by APC PROPERTIES LLC.
- w. On or about October 28, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause CAPITAL ONE BANK to transfer funds out of a bank account belonging to APC PROPERTIES LLC and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- x. On or about November 24, 2009, DEFENDANT AND CO-CONSPIRATORS

caused malicious software to be installed, without authorization, on a computer used by PARKINSON CONSTRUCTION.

- y. On or about November 24, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause BANK OF GEORGETOWN to transfer funds out of a bank account belonging to PARKINSON CONSTRUCTION and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- z. On or about February 10, 2010, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by BASTRIRE EDWARDS, CPAS.
- aa. On or about February 10, 2010, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause VISALIA COMMUNITY BANK to transfer funds out of a bank account belonging to BASTRIRE EDWARDS, CPAS and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- bb. On or about February 16, 2010, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by ARBEN GROUP LLC.
- cc. On or about February 16, 2010, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause WEBSTER BANK to transfer funds out of a bank account belonging to ARBEN GROUP LLC and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- dd. On or about March 3, 2010, DEFENDANT AND CO-CONSPIRATORS caused

malicious software to be installed, without authorization, on a computer used by HUSKER AG, LLC.

ee. On or about March 3, 2010, DEFENDANT AND CO-CONSPIRATORS used stolen access information to attempt to cause UNION BANK AND TRUST to transfer funds out of a bank account belonging to HUSKER AG, LLC and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.

ATTRIBUTION

51. As indicated above, participants in the chat on the INCOMEET SERVER identified themselves by nicknames. As set forth below, the nickname “lucky12345”⁸ is associated with DEFENDANT, and was used in chat communications discussing the overt acts set forth above that involved DEFENDANT.

52. Based on my training and experience, I am aware that there are certain well-known online forums used to facilitate computer crimes by allowing the solicitation of and dissemination of malware and other products and services related to computer intrusions and fraud schemes. On these

⁸ The full address for this nickname at the origination of the conspiracy was lucky12345@jabber.org. Unlike most of the other participants in the scheme possessing Jabber accounts, the communications for “lucky12345” did not originate from the INCOMEET SERVER. The Jabber protocol allows for communications between accounts hosted on different Jabber servers. Thus, the communications related to “lucky12345” stored on the INCOMEET SERVER are only those sent to or from users with accounts on the INCOMEET SERVER; communications that “lucky12345” may have sent to other individuals were not stored there. It should be noted that on January 30, 2010, the INCOMEET SERVER began storing chat communications related to nickname lucky12345@jabber.cz. The INCOMEET SERVER only stored 14 more communications originating from lucky12345@jabber.org after this date, in comparison to tens of thousands involving lucky12345@jabber.org from before this date, and thousands involving lucky12345@jabber.cz from January 30, 2010, onwards. Taking this into account, along with in-context review of the Jabber chat communications from both addresses, I believe that the user of the “lucky12345” nickname switched from using an address ending in jabber.org to one ending in jabber.cz on or about January 30, 2010. For simplicity’s sake, the communications involving the “lucky12345” nickname will be referred to as if they were one account, except where distinguishing between the full lucky12345@jabber.cz and lucky12345@jabber.org addresses are of substantive importance.

forums, individuals can advertise their services and negotiate the purchase of services from other individuals. These forums also permit users to communicate with each other by private messaging system that is not seen by the rest of the users on the forum site. Many of these forums also include subforums dedicated to the buying, selling, and solicitation of credit card numbers, passwords, banking information, and cash out services that provide the means to convert stolen money.

53. In order to post on these forums or to send private messages to individuals on the forum, users must first create an account, which requires a username, a password, and some contact information, such as an e-mail account or Jabber account. Based on my training and experience, I am aware that the e-mail and/or Jabber account associated with the user account usually is used during the registration process to authenticate the user and to activate the account. In addition, the forum usually sends notifications to the e-mail address of the user that he/she has received a private message from another forum member or that there are updates to the forum. Based on my training and experience, I am aware that many of these forums require the user to be vetted before they are allowed to register.

54. Based on my training and experience, I am aware that Mazafaka.info⁹ is a well-known example of one of these online forums, and is dedicated to furthering the above-mentioned criminal activities. Pursuant to a search warrant in another criminal investigation, the FBI obtained a copy of the server hosting Mazafaka.info. On September 5, 2009, a user with the moniker “Lastik” sent a private message to another user stating “icq 427297771 jabber:

⁹ Today, this site is located at mazafaka.ru.

lucky12345@jabber.org.”¹⁰ Similar private messages referencing this Jabber identifier were sent to other users by “Lastik” on September 7, 2009, November 4, 2009, December 14, 2009, and January 22, 2010. On April 5, 2010, “Lastik” sent a private message to another user, providing another contact Jabber address of lucky12345@jabber.cz.¹¹ Similar private messages referencing this Jabber identifier were sent to other users by “Lastik” on other subsequent occasions, including on May 12, 2010.

55. “Lastik” boasted on several occasions of being the author of Zeus malware. On October 5, 2008, “Lastik” sent a private message to another user, stating, “I’m the author, ICQ 427297771, hit me up and post your ports please...” On June 5, 2010, “Lastik” sent a private message to another user, stating, “I’m monster, and not his reincarnation... I’m the author of Zeus.” Furthermore, in response to a private message asking for contact info for the author of Zeus, “Lastik” replied in a May 29, 2010, private message stating, “jabber: bashorg@talking.cc.”

56. “Lastik” also made additional references to the moniker “[M]onster” or a variant thereof on Mazafaka.info. On February 25, 2008, “Lastik” sent a private message to another user stating “MonsterTrack 427-297-771 Software.” On November 14, 2009, “Lastik” sent a private message to another user, stating in pertinent part, “I am Monster 427297771.”

57. The registration information for “Lastik” on Mazafaka.info showed that the user listed the e-mail address alexgarbarchuck@yahoo.com as a means of contact. The

¹⁰ ICQ is an instant messaging program in which each user is provided an account number that also functions as a contact number similar to telephone numbers. ICQ members can exchange messages and files using this program. Based on my training and experience, I know that ICQ numbers function similarly to e-mail addresses in that they can only be registered to one individual at a time.

¹¹ As noted in footnote 8 above, I believe that the user of the “lucky12345” nickname switched from using an address ending in jabber.org to one ending in jabber.cz on or about January 30, 2010.

Mazafaka.info forum required users to authenticate themselves by responding to an e-mail sent to a registration e-mail account; thus, “Lastik” must have had access to the alexgarbarchuck@yahoo.com e-mail account in order to register the account on Mazafaka.info.

58. Analysis of the chat communications on the INCOMEET SERVER involving user “lucky12345” revealed several references to ICQ number 427297771.¹² On November 12, 2009, “lucky12345” had an automatic response message set to state, “Busy restoring contacts, stolen, 427297771, new 312456.” On November 23, 2009, “lucky12345” told user “thehead,” “I talked/communicated with you with icq 427297771.”

59. Further analysis of the INCOMEET SERVER also revealed that the monikers “monster” and “monstertrack” (i.e., alternative monikers referenced by user “Lastik” on Mazafaka.info) were attributed to user “lucky12345.” This information was derived from the buddy lists which were extracted from accounts located on the INCOMEET SERVER.

60. Pursuant to a mutual legal assistance request, Dutch authorities seized a server associated with domain talking.cc (hereinafter “TALKING.CC SERVER”) in or about October 2010. FBI investigators present on-scene were permitted to make a digital forensic image of the TALKING.CC SERVER. Analysis of the server revealed that it was another Jabber communications server.

61. Analysis of the chat communications on the TALKING.CC SERVER revealed that on September 23, 2010, a user with the moniker bashorg@talking.cc (hereinafter “bashorg”)

¹² I am aware that this ICQ number may have also been used by another individual to engage in related criminal conduct in or about 2006 and 2007. This individual is believed to have been working with DEFENDANT at that time. Based on my training and experience, as well as the evidence in this investigation (to and including the information supplied in this affidavit), I believe that DEFENDANT was using ICQ number 427297771 at the times mentioned in this affidavit.

received a message from user “de_baambaataa” stating, “I’m sorry, who are you?” “Bashorg” replied, “Lastik” (i.e., the user on Mazafaka.info with registration e-mail address alexgarbarchuck@yahoo.com). Analysis of the user database on the TALKING.CC SERVER indicated that “bashorg” logged-in to the server using exclusively a client¹³ named “yaya.” Analysis of the user database on the INCOMEET SERVER indicated that user “lucky12345”¹⁴ had also logged-in to that server using exclusively a client named “yaya.”

62. The TALKING.CC SERVER tracked the transmitting IP addresses of its users. From July 17, 2010, until the day the server was seized, “bashorg” usually logged into the server via an IP address located in Amsterdam, the Netherlands, which may have been used as a proxy server.¹⁵ However, on several occasions, “bashorg” transmitted Jabber messages using IP addresses registered in Krasnodar Krai, Russia. Proximate to the times of those transmissions, chat communications also originated from user “odmin”¹⁶ on the TALKING.CC SERVER, from the same IP addresses:

¹³ In technical terms, a computer that accesses a service made available by a server is called a “client.”

¹⁴ Specifically, this user database file concerns user lucky12345@jabber.cz; see footnote 8 above.

¹⁵ A proxy server is an intermediary computer that sits between the user’s computer and the Internet. Proxy servers are often used by cyber criminals to hide their identity and location.

¹⁶ The “odmin” account had administrative privileges. Because of this, I believe it may have been a misspelling of the word “admin,” a typical moniker for the administrator of a system. From my training and experience, I know that system administrators often have their own user accounts on system, apart from an “admin” account.

<u>Date</u>	<u>Time</u> ¹⁷	<u>IP Address</u>	<u>User</u>
August 4, 2010	21:02	94.233.198.22	odmin
August 4, 2010	21:02	94.233.198.22	bashorg
August 16, 2010	17:33	178.34.53.18	odmin
August 17, 2010	00:24	178.34.53.18	bashorg
August 17, 2010	01:20	178.34.53.18	odmin
August 17, 2010	04:19	178.34.53.18	odmin
August 17, 2010	04:32	178.34.53.18	bashorg
August 17, 2010	04:50	178.34.53.18	bashorg

Based on my training and experience, as well the extreme closeness in time between the logins for users “bashorg” and “odmin,” I believe that both of these monikers were used by the same individual during in or about August 2010.¹⁸

63. On or about August 14, 2013, the FBI received records from a U.S. provider of online services (hereinafter “SERVICE PROVIDER ONE”) for an account registered in the name of EVGENIY BOGACHEV, with an associated phone number. SERVICE PROVIDER ONE provided historical login IP addresses and times for this account, several of which were proximate to the times of chat communications originating from “odmin” on the TALKING.CC SERVER, from the same IP addresses registered in Krasnodar Krai, Russia:

¹⁷ All times in the following tables are in UTC, a time scale that couples Greenwich Mean Time, which is based solely on the Earth’s inconsistent rotation rate, with highly accurate atomic time.

¹⁸ The “odmin” account was also accessed at the time of a concurrent login by user “ben” on July 19, 2010. This was the only other concurrent login, and predates August 2010. Further, the login by “ben” did not originate from an IP address in Krasnodar Krai, Russia.

<u>Date</u>	<u>Time</u>	<u>IP Address</u>	<u>Account</u>
August 2, 2010	22:09	94.233.197.170	odmin
August 2, 2010	23:27	94.233.197.170	SERV PROV ONE ¹⁹
August 3, 2010	21:52	94.233.218.62	odmin
August 3, 2010	23:08	94.233.218.62	SERV PROV ONE
August 4, 2010	16:32	94.233.218.62	SERV PROV ONE
August 9, 2010	16:51	178.34.100.42	odmin
August 10, 2010	8:07	178.34.100.42	SERV PROV ONE
August 10, 2010	8:13	178.34.100.42	SERV PROV ONE
August 10, 2010	8:14	178.34.100.42	SERV PROV ONE
August 11, 2010	12:50	178.34.164.128	SERV PROV ONE
August 11, 2010	13:03	178.34.164.128	odmin
August 20, 2010	16:44	178.34.100.62	odmin
August 20, 2010	19:40	178.34.100.62	SERV PROV ONE

Based on my training and experience, as well the extreme closeness in time between the logins for “odmin” and the SERVICE PROVIDER ONE account registered to EVGENIY BOGACHEV, I believe that both of these monikers were used by the same individual.

64. On or about January 18, 2013, in another related investigation, the FBI obtained, via search warrant, the contents of e-mail account charajiang16@gmail.com, which the FBI had probable cause to believe contained discussions related to the criminal operation of a similar computer intrusion and fraud scheme. Within this e-mail account, numerous e-mails were exchanged between charajiang16@gmail.com and e-mail address alexgarbarchuck@yahoo.com (i.e., the registration e-mail address for user “Lastik” on Mazafaka.info). Analysis of the headers of these e-mails revealed the originating IP addresses for the messages sent from alexgarbarchuck@yahoo.com to charajiang16@gmail.com. Several of these transmissions were

¹⁹ Abbreviation of “SERVICE PROVIDER ONE.”

proximate to the login times associated with the SERVICE PROVIDER ONE account registered to EVGENIY BOGACHEV, from the same IP addresses:

<u>Date</u>	<u>Time</u>	<u>IP Address</u>	<u>Account</u>
February 16, 2011	16:31	212.117.170.62	Yahoo!
February 18, 2011	20:28	212.117.170.62	SERV PROV ONE
July 23, 2011	16:10	212.117.170.62	Yahoo!
July 24, 2011	10:32	212.117.170.62	SERV PROV ONE
September 27, 2011	8:59	212.117.170.62	Yahoo!
September 27, 2011	14:10	212.117.170.62	Yahoo!
September 28, 2011	13:39	212.117.170.62	SERV PROV ONE
November 19, 2011	10:44	200.63.44.46	SERV PROV ONE
November 19, 2011	11:05	200.63.44.46	Yahoo!
March 17, 2012	10:13	196.46.189.130	SERV PROV ONE
March 18, 2012	11:37	196.46.189.130	Yahoo!
July 22, 2012	10:04	78.129.189.64	Yahoo!
July 22, 2012	13:04	78.129.189.64	Yahoo!
July 22, 2012	21:19	78.129.189.64	SERV PROV ONE

Based on my training and experience, as well the extreme closeness in time between the logins to the alexgarbarchuck@yahoo.com and the SERVICE PROVIDER ONE account registered to EVGENIY BOGACHEV, I believe that both of these monikers were used by the same individual.

65. In sum, based upon the proximate logins to the above-mentioned accounts, I believe that the following identifiers appear to have been used by the same individual: the alexgarbarchuck@yahoo.com account; the “odmin” and “bashorg” accounts on the TALKING.CC SERVER; and, the SERVICE PROVIDER ONE account registered to EVGENIY BOGACHEV.

66. Further, as detailed above, alexgarbarchuck@yahoo.com was used to register user “Lastik” on Mazafaka.info. “Lastik” was given as an alternative moniker by “bashorg” in chat communications on the TALKING.CC SERVER. In private messages on Mazafaka.info, user “Lastik” provided ICQ number 427297771 and the Jabber user account “lucky12345” from the INCOMEET SERVER as means of contact, as well as identifying himself using monikers “Monster” and “MonsterTrack.” “Lastik” also boasted about being the author of Zeus, and later told another user that the author of Zeus could be reached at the Jabber address for user “bashorg” on the TALKING.CC SERVER. User “bashorg” on the TALKING.CC SERVER had a connecting client name that matched that of user “lucky12345” on the INCOMEET SERVER. User “lucky12345” provided ICQ number 427297771 in chat communications, and was associated with nicknames “monster” and “monstertrack.” Based on my training and experience, I believe that all of these usernames, accounts, and identifiers were used by BOGACHEV, known as “lucky12345” in the communications of the Jabber Zeus Crew.

67. As noted above, records from the SERVICE PROVIDER ONE account registered to EVGENIY BOGACHEV showed that he listed a specific phone number as a means of contact. Records obtained from a business on or about May 29, 2013, indicated the presence of a membership services account in the name of EVGENIY MIKHAYLOVICH BOGACHEV, with the same phone number and a specific e-mail address as a means of contact.

68. Information was obtained on or about July 1, 2013, from another U.S. provider of online services concerning the e-mail address associated with the above-mentioned membership services account. These records indicated that this same e-mail address was registered to an account belonging to EVGENIY BOGACHEV, with a listed home address in Krasnodar Krai, RUSSIA.

69. Based on the information set forth above, and my training and experience, and the information set forth above, I believe that all of the above-mentioned usernames, accounts, and identifiers are controlled by EVGENIY MIKHAYLOVICH BOGACHEV, known as “lucky12345” in the communications of the Jabber Zeus Crew.

CONCLUSION

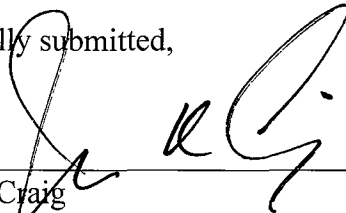
70. Based on the foregoing, I submit there is probable cause to believe that from in or about May 2009, and continuing to on or about May 21, 2010, in the District of Nebraska and elsewhere, EVGENIY MIKHAYLOVICH BOGACHEV, also known as “lucky12345,” together with others known and unknown, did knowingly and intentionally conspire to violate 18 U.S.C. §§ 1344 and 1349, that is, devised and executed a scheme and artifice to defraud BANK OF ALBUQUERQUE, BANK OF GEORGETOWN, CALIFORNIA BANK AND TRUST, CAPITAL ONE BANK, FIRST FEDERAL SAVINGS BANK, FIRST NATIONAL BANK OF OMAHA, GCM FEDERAL CREDIT UNION, KEY BANK, SALISBURY BANK & TRUST, UNION BANK AND TRUST, VISALIA COMMUNITY BANK, and WEBSTER BANK, all of which were depository institutions insured by either the Federal Deposit Insurance Corporation or the National Credit Union Share Insurance Fund.

REQUEST FOR SEALING

71. **It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and complaint. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits via the Internet, and disseminate them to other online criminals as they deem appropriate, e.g., by posting them publicly online. The crimes discussed in this affidavit have already been the subject of**

media attention, and there is a danger that the information in this affidavit could be further disseminated by journalists. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



James K. Craig
Special Agent
FBI

Sworn to before me by telephone and reasonable electronic means:

Date: May 30, 2014.

City and state: Lincoln, Nebraska



Cheryl R. Zwart, United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA)	
)	
)	
vs.)	Criminal No. 14-127
)	
EVGENIY BOGACHEV,)	
)	
Defendant.)	

ORDER

AND NOW, this 23RD day of September, 2015, it appearing that further proceeding cannot be held in this as to defendant EVGENIY BOGACHEV because the defendant is a fugitive and a warrant of arrest has been issued,

IT IS HEREBY ORDERED that the case be returned to the Clerk of Court as to defendant EVGENIY BOGACHEV, until such time as action by the Court may be required against said defendant.

s/ Arthur J. Schwab
United States District Judge

cc/ecf: Shardul S. Desai, Asst. U.S. Atty.