

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