UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT
Grand Jury B-16-1

UNITED STATES OF AMERICA	:	Criminal No. 3:17CR83(RNC)
	:	
	:	VIOLATIONS:
v.	:	
	:	18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)
PETER YURYEVICH LEVASHOV,	:	18 U.S.C. § 371
aka "Petr Levashov," aka "Peter Severa,"	:	18 U.S.C. §§ 1030(a)(4) and (c)(3)(A)
aka "Petr Severa," aka "Sergey Astakhov"	:	18 U.S.C. § 1343
	:	18 U.S.C. §§ 1030(a)(7)(C) and (c)(3)(A)
	:	18 U.S.C. §§ 1037(a)(2) and (b)(1)
	:	18 U.S.C. §§ 1037(a)(3) and (b)(1)
	:	18 U.S.C. § 1028A
	:	18 U.S.C. § 2
	:	18 U.S.C. § 1030(*i*)
	:	18 U.S.C. § 981(a)(1)
	:	28 U.S.C. § 2461(c)
	:	18 U.S.C. § 1037(c)
	:	21 U.S.C. § 853

INDICTMENT

The Grand Jury charges:

General Allegations

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

1. Defendant PETER YURYEVICH LEVASHOV, a.k.a. "Petr Levashov," "Peter Severa," "Petr Severa," and "Sergey Astakhov" ("LEVASHOV"), is a citizen of Russia and last resided in St. Petersburg, Russia.

2. LEVASHOV uses the alias "Peter Severa" in various online forums and in communications. LEVASHOV also uses online identifiers ICQ number 104967, jabber@honese.com, and peter@severa.biz to chat or communicate with others online.

3. Malicious software ("malware") is a software program designed to disrupt computer operations, gather sensitive information, gain access to a computer, or do other unwanted actions on a computer.

4. A "botnet" is a network of computers infected with malicious software that allows a third party to control the entire computer network without the knowledge or consent of the computer owners. Each of the infected computers is referred to as a "bot." A botnet can be used by spammers to send spam through the network of infected bot computers, using each of the infected computers to transmit the spam email, in order to hide the true origin of the spam, obscure the identity of the spammer, and evade anti-spam filters and other blocking techniques.

5. A Virtual Private Network ("VPN") is a technology that creates a secure network connection over a public network such as the Internet or private network owned by an Internet Service Provider. The user of a VPN can conceal his true Internet Protocol ("IP") address from those with whom he is communicating.

6. A "Trojan" is a type of malware that masquerades as a routine download request or other innocuous file that encourages the victim to open it and thereby unknowingly install malware onto the victim computer, thereby creating an unauthorized access point to the victim computer.

7. "Ransomware" is a type of malware that encrypts an infected computer's files and demands payment to unlock the computer.

8. "Spam" messages are unsolicited bulk commercial email messages.

The Kelihos Botnet

9. The Kelihos botnet is controlled by LEVASHOV through command and control servers, which enable LEVASHOV to issue commands to any and all bots in the Kelihos botnet.

10. LEVASHOV controlled and operated the Kelihos botnet to, among others things: (a) harvest personal information and means of identification (including email addresses, usernames and logins, and passwords) from infected computers; (2) disseminate spam; and (3) distribute malware, including Trojans and ransomware.

11. The computers infected as part of any and all criminal activity associated with the Kelihos botnet were used in and affecting interstate and foreign commerce and communication.

COUNT ONE
(Intentional Damage to a Protected Computer)

12. Paragraphs 1-11 are incorporated by reference.

13. From on or about February 22, 2016, until approximately April 7, 2017, the exact dates being unknown to the Grand Jury, in the District of Connecticut and elsewhere, the defendant, PETER YURYEVICH LEVASHOV, knowingly caused the transmission of a program, code, and command, to wit, the Kelihos botnet, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer and the offense caused (i) loss to one or more persons during any one-year period from LEVASHOV's course of conduct affecting protected computers aggregating to at least $5,000 in value; and (ii) damage affecting ten or more protected computers during any one-year period.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B), and 2.

COUNT TWO
(Conspiracy)

14. Paragraphs 1-11 and 13 are incorporated by reference.

15. From on or about February 22, 2016, until approximately April 7, 2017, the exact dates being unknown to the Grand Jury, in the District of Connecticut and elsewhere, the

defendant, PETER YURYEVICH LEVASHOV, did unlawfully, knowingly, and intentionally conspire, combine, confederate, and agree with others unknown to the Grand Jury, to commit offenses against the United States in connection with the operation and monetization of the Kelihos botnet, that is:

a. to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage, and attempted to cause damage, without authorization, to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A);

b. knowingly and with intent to defraud access protected computers without authorization and by means of such conduct further the intended fraud and obtain something of value, in violation of Title 18, United States Code, Section 1030(a)(4); and

c. to transmit, with intent to extort from persons money and other things of value, in interstate and foreign commerce, a communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, in violation of Title 18, United States Code, Section 1030(a)(7).

Purpose and Object of the Conspiracy

16. A purpose of the conspiracy was for LEVASHOV and his co-conspirators to operate, perpetuate, control, and profit from the Kelihos botnet, and to conceal the conspiracy from others.

Manner and Means of the Conspiracy

17. It was part of the conspiracy that LEVASHOV and his co-conspirators did not seek, nor were they given, permission to install the Kelihos botnet on victims' computers and to use the victims' computers as part of the Kelihos botnet.

18. It was further part of the conspiracy that LEVASHOV operated the Kelihos botnet and advertised spam and other malware dissemination services via the botnet to others for

purchase.

19. It was further part of the conspiracy that the Kelihos botnet obtained and verified, and attempted to obtain and verify, credentials, including email addresses, usernames and logins, passwords, and other means of identification from infected computers.

20. It was further part of the conspiracy that LEVASHOV and his co-conspirators caused malware and spam to be transmitted over the internet, such that they were transmitted in interstate and foreign commerce.

21. It was further part of the conspiracy that LEVASHOV monitored the stability and efficacy of the Kelihos botnet through an on-line dashboard.

22. It was further part of the conspiracy that LEVASHOV and his co-conspirators concealed their true identities and criminal activity through, among other things, using VPNs and proxies, online aliases, and encrypted forms of communication.

23. It was further part of the conspiracy that, in offering and performing spam and malware distribution services via the Kelihos botnet, LEVASHOV enriched himself.

Overt Acts

24. In furtherance of the conspiracy and to effect the objects of the conspiracy, LEVASHOV and his co-conspirators committed and caused to be committed the following overt acts, among others, in the District of Connecticut and elsewhere:

a. On or about February 20, 2016, LEVASHOV monitored the Kelihos botnet via a file called stats.html ("the Dashboard").

b. On or about March 2, 2016, LEVASHOV sent an email from peter@severa.biz to a customer stating that "mailing costs 500 usd per 1 mil emails, 750 us=d per 2mil, 1k per 3mil."

c. From on or about May 5, 2016 to on or about May 9, 2016, LEVASHOV accessed a WebMoney identifier ending in 4986 from a computer with the Internet Protocol address 91.122.62.16.

d. On or about September 22, 2016, LEVASHOV disseminated the JokeFromMars ransomware via the Kelihos botnet.

e. From on or about October 1, 2016 until at least December 8, 2016, LEVASHOV accessed a computer server with an Internet Protocol address of 85.17.31.90.

f. On or about December 15, 2016, Kelihos harvested credentials from a File Transfer Protocol client from a computer in Connecticut.

g. On or about March 21, 2017, LEVASHOV instructed a customer for a spam campaign to pay him by bitcoin and stated that he charged $300 per 1 million emails, but more for phishing and scams.

All in violation of Title 18, United States Code, Section 371.

COUNT THREE
(Accessing Protected Computers in Furtherance of Fraud)

25. Paragraphs 1-11 and 15-24 are incorporated by reference.

26. From on or about February 22, 2016, until approximately April 7, 2017, the exact dates being unknown to the Grand Jury, in the District of Connecticut and elsewhere, the defendant, PETER YURYEVICH LEVASHOV, knowingly and with intent to defraud accessed protected computers without authorization and by means of such conduct furthered the intended fraud and obtained something of value, to wit, thousands of credentials, including email addresses, usernames and logins, and passwords, and the object of the fraud was the use of computers and the value of such use exceeded $5,000 in any one year.

All in violation of Title 18, United States Code, Sections 1030(a)(4), (c)(3)(A), and 2.

COUNT FOUR
(Wire Fraud)

27. Paragraphs 1-11 and 15-24 are incorporated by reference.

28. From on or about February 22, 2016, until approximately April 7, 2017, the exact dates being unknown to the Grand Jury, in the District of Connecticut and elsewhere, the defendant, PETER YURYEVICH LEVASHOV, willfully, knowingly, and with intent to defraud, devised and intended to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and did transmit and caused to be transmitted by means of wire communications in interstate and foreign commerce writings for the purpose of executing such scheme.

29. On or about March 22, 2017, for the purpose of executing and attempting to execute the above-described scheme and artifice to defraud, LEVASHOV caused a wire to be sent via a chat platform from outside of Connecticut to an individual in Connecticut, whose identity is known to the Grand Jury, concerning "pump and dump" spam.

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT FIVE
(Threatening to Damage a Protected Computer)

30. Paragraphs 1-11 and 15-24 are incorporated by reference.

31. On or about September 22, 2016, in the District of Connecticut and elsewhere, the defendant, PETER YURYEVICH LEVASHOV, with intent to extort from persons money and other things of value, transmitted in interstate and foreign commerce a communication containing a demand and request for money and other things of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.

All in violation of Title 18, United States Code, Sections 1030(a)(7)(C), (c)(3)(A), and 2.

COUNT SIX
(Fraud in Connection with Email)

32. Paragraphs 1-11 and 15-24 are incorporated by reference.

33. From on or about February 22, 2016, until approximately April 7, 2017, the exact dates being unknown to the Grand Jury, in the District of Connecticut and elsewhere, the defendant, PETER YURYEVICH LEVASHOV, knowingly did use a protected computer to relay and retransmit multiple commercial email messages, in and affecting interstate and foreign commerce, with the intent to deceive and mislead recipients, and an Internet access service, as to the origin of such messages; to wit, LEVASHOV transmitted spam messages in furtherance of a felony under the laws of the United States, to wit, 18 U.S.C. §§ 2, 371, 1030, 1028A, and 1343, and the volume of email messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, and 250,000 during any one-year period.

All in violation of Title 18, United States Code, Sections 1037(a)(2), (b)(1), and 2.

COUNT SEVEN
(Fraud in Connection with Email)

34. Paragraphs 1-11 and 15-24 and incorporated by reference.

35. From on or about February 22, 2016, until approximately April 7, 2017, the exact dates being unknown to the Grand Jury, in the District of Connecticut and elsewhere, the defendant, PETER YURYEVICH LEVASHOV, knowingly did, in and affecting interstate and foreign commerce, materially falsify and cause others to materially falsify header information in multiple commercial email messages and intentionally initiate the transmission of such messages, to wit, LEVASHOV transmitted spam messages in furtherance of a felony under the laws of the United States, to wit, 18 U.S.C. §§ 2, 371, 1030, 1028A, and 1343, and the volume of email

messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, and 250,000 during any one-year period.

All in violation of Title 18, United States Code, Sections 1037(a)(3), (b)(1), and 2.

COUNT EIGHT
(Aggravated Identity Theft)

36. Paragraphs 1-11 and 15-24 are incorporated by reference.

37. On or about July 15, 2016, in the District of Connecticut and elsewhere, the defendant, PETER YURYEVICH LEVASHOV, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, to wit, the email address/username and password of Victim S.B., whose identity is known to the Grand Jury, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A, to wit, the violation of 18 U.S.C. § 1030(a)(5)(A) charged in Count One, the violation of 18 U.S.C. § 1030(a)(4) charged in Count Three, the violation of 18 U.S.C. § 1343 charged in Count Four, the violation of 18 U.S.C. § 1030(a)(7)(C) charged in Count Five, the violation of 18 U.S.C. § 1037(a)(2) charged in Count Six, and the violation of 18 U.S.C. § 1037(a)(3) charged in Count Seven, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Sections 1028A and 2.

FORFEITURE ALLEGATIONS

38. Paragraphs 1-11 and 15-24 are incorporated by reference.

FORFEITURE ALLEGATION
(Computer Fraud)

39. Upon conviction of one or more of the computer fraud offenses alleged in Counts One, Two, Three, and Five of this Indictment, the defendant, PETER YURYEVICH LEVASHOV,

shall forfeit to the United States, pursuant to 18 U.S.C. § 1030(*i*), all right, title, and interest in any property, real or personal, constituting, or derived from, proceeds obtained, directly or indirectly, as a result of the violation(s) of 18 U.S.C. §§ 371 and 1030, and any personal property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of the said violation(s), including but not limited to:

a. any computer hardware, servers, proxies, network equipment, and electronic devices used or intended to be used to commit or to facilitate the commission of such offense(s); and

b. a sum of money equal to the total amount of any property, real or personal, which constitutes or is derived from proceeds traceable to violation(s) of, or obtained as a result of, 18 U.S.C. §§ 371 and 1030.

40. If any of the above-described forfeitable property, as a result of any act or omission of the defendant, cannot be located upon the exercise of due diligence, has been transferred, sold to, or deposited with a third party, has been placed beyond the jurisdiction of the court, has been substantially diminished in value, or has been commingled with other property which cannot be divided without difficulty, it is the intent of the United States, pursuant to 21 U.S.C. § 853(p), to seek forfeiture of any other property of said defendant up to the value of the forfeitable property described above.

All in accordance with 18 U.S.C. § 1030(*i*) and 21 U.S.C. § 853, and Rule 32.2(a), Federal Rules of Criminal Procedure.

FORFEITURE ALLEGATION
(Wire Fraud)

41. Upon conviction of the wire fraud offense alleged in Count Four of this Indictment, the defendant, PETER YURYEVICH LEVASHOV, shall forfeit to the United States of America, pursuant to 18 U.S.C. § 982(a)(1)(C) and 28 U.S.C. § 2461(c), all right, title, and interest in any

and all property, real or personal, which constitutes or is derived from proceeds traceable to the violation of 18 U.S.C. § 1343, and all property traceable to such property, including a sum of money equal to the total amount of any property, real or personal, which constitutes or is derived from proceeds traceable to the violation of 18 U.S.C. § 1343 or obtained as a result of such offense.

42. If any of the above-described forfeitable property, as a result of any act or omission of the defendant cannot be located upon the exercise of due diligence, has been transferred, sold to, or deposited with a third party, has been placed beyond the jurisdiction of the court, has been substantially diminished in value, or has been commingled with other property which cannot be divided without difficulty, it is the intent of the United States, pursuant to 21 U.S.C. § 853(p), as incorporated by 28 U.S.C. § 2461(c), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described above.

All in accordance with 18 U.S.C. § 981(a)(1) as incorporated by 28 U.S.C. § 2461(c), and Rule 32.2(a), Federal Rules of Criminal Procedure.

FORFEITURE ALLEGATION
(Email Fraud)

43. Upon conviction of one or more of the email fraud offenses alleged in Counts Six and Seven of this Indictment, the defendant, PETER YURYEVICH LEVASHOV, shall forfeit to the United States, pursuant to 18 U.S.C. § 1037(c), all right, title, and interest in any property, real or personal, constituting, or derived from, proceeds obtained, directly or indirectly, as a result of the violation(s) of 18 U.S.C. § 1037; any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of the said violation(s); a sum of money equal to the total amount of any property, real or personal, which constitutes or is derived from proceeds traceable to violations of, or obtained as a result of the offense, 18 U.S.C. § 1037.

44. If any of the above-described forfeitable property, as a result of any act or omission of the defendant, cannot be located upon the exercise of due diligence, has been transferred, sold to, or deposited with a third party, has been placed beyond the jurisdiction of the court, has been substantially diminished in value, or has been commingled with other property which cannot be divided without difficulty, it is the intent of the United States, pursuant to 21 U.S.C. § 853(p), to seek forfeiture of any other property of said defendant up to the value of the forfeitable property described above.

All in accordance with 18 U.S.C. § 1037(c) and 21 U.S.C. § 853, and Rule 32.2(a), Federal Rules of Criminal Procedure.

A TRUE BILL

FOREPERSON

UNITED STATES OF AMERICA

DEIRDRE M. DALY
UNITED STATES ATTORNEY

VANESSA RICHARDS
ASSISTANT UNITED STATES ATTORNEY

DAVID T. HUANG
ASSISTANT UNITED STATES ATTORNEY