UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

GRAND JURY B-18-1

UNITED STATES OF AMERICA

v.

OLEG KOSHKIN and
PAVEL TSURKAN

CRIMINAL NO. 3:19CR ( )

VIOLATIONS: 3:19cr251(MPS)

18 U.S.C. § 371
(Conspiracy)

18 U.S.C. §§ 1030(a)(5)(A), 1030(b) and 2
(Aiding and Abetting Intentional Damage to a Protected Computer)

INDICTMENT

The Grand Jury charges:

GENERAL ALLEGATIONS

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

1. The defendant OLEG KOSHKIN ("KOSHKIN") is a citizen of Russia who resides in Estonia and Thailand.

2. The defendant PAVEL TSURKAN ("TSURKAN") is a citizen of Estonia who resides in Estonia and Thailand.

3. Peter Yuryevich Levashov, a.k.a. "Petr Levashov," "Peter Severa," "Petr Severa," and "Sergey Astakhov" ("Levashov"), who is not named as a defendant herein, but is charged elsewhere, is a citizen of Russia who last resided in Russia.

4. Jabber is an open source instant messaging and presence protocol that allows for nearly real-time communication.

5. WebMoney is an online payment and money transfer service. WebMoney account holders are assigned a unique WebMoney identifier. A WebMoney user's funds are stored in an electronic "purse." Multiple "purses" can be attributed to each WebMoney identifier.

Background on Malicious Software and Spam

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

7. A "botnet" is a network of computers infected with malware 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." Some botnets 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.

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

9. A "keylogger" is a type of malware that is capable of stealing or recording user keystrokes.

10. "Remote Access Trojans," also known as "rats," are a type of malware that provide the capability to allow covert surveillance or the ability to gain unauthorized access to a computer.

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

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

COUNT ONE
(Conspiracy)

13. Paragraphs 1 to 12 are incorporated by reference.

14. From approximately September 2013 until approximately December 28, 2017, the exact dates being unknown to the Grand Jury, in the District of Connecticut and elsewhere, the defendants KOSHKIN and TSURKAN did knowingly and intentionally combine, conspire, confederate, and agree with each other and with Levashov and others unknown to the Grand Jury to commit offenses against the United States, that is, to knowingly attempt to cause and cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization, to 10 or more protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), and 1030(c)(4)(B).

Manner and Means of the Conspiracy

15. It was part of the conspiracy that between approximately September 2013 and approximately December 28, 2017, the defendants KOSHKIN and TSURKAN controlled and operated an online service known as Crypt4U. Crypt4U was a service that crypted malware in order to avoid detection by antivirus software, including popular antivirus software used by many computer users in the United States. The purpose and intent of the defendants and their co-conspirators in operating Crypt4U was to allow distributers and coders of malware to reduce the chances that the malware would be detected by antivirus software installed on the computers they target. As such, the defendants and co-conspirators knew and intended that Crypt4U would be used to enable and facilitate the installation of malware on computers without the authorization of the computers' owners.

16. It was further part of the conspiracy that other individuals also worked for Crypt4U and assisted the defendants KOSKHIN and TSURKAN in operating Crypt4U.

17. It was further part of the conspiracy that users of Crypt4U were charged a fee to crypt malware.

18. It was further part of the conspiracy that the defendants KOSHKIN and TSURKAN advertised Crypt4U on various websites, including public sites crypt4u.com, crypt4u.net, fud.bz, and fud.re. They also advertised Crypt4U on various online forums known to cater to malware distributors, coders, and other cyber criminals. As a result, the defendants knew and intended that Crypt4U would be used for the facilitation of criminal activity.

19. It was further part of the conspiracy that Levashov controlled and operated the Kelihos botnet. Levashov used the Kelihos botnet to, among others things: (1) 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. Individuals or organizations seeking to have their spam or ransomware distributed by Kelihos paid Levashov, who then commanded the botnet to issue the spam or distribute the malware.

20. It was further part of the conspiracy that Levashov used and paid affiliates to transmit and install the Kelihos malware on victim computers, and thus, grow his botnet.

21. It was further part of the conspiracy that Levashov used Crypt4U to crypt the Kelihos malware so that, when the malware was distributed to victims, antivirus software on any victim's computer would not detect it.

22. It was further part of the conspiracy that because of the way Levashov tracked new installations by a particular affiliate, Levashov could not provide two affiliates with the same

crypted version of Kelihos; thus, he needed to provide unique malware to each affiliate so that he would know which affiliate had distributed it and how much he needed to pay that person as he paid per installation of the malware. This increased Levashov's demand for crypting.

23. It was further part of the conspiracy that Levashov used Crypt4U from at least May 2014, until April 7, 2017, and paid the operators of Crypt4U approximately $3,000 per month. Over the course of his dealings with Crypt4U, Levashov was provided with multiple WebMoney purses to which he was instructed to transfer payment.

24. It was further part of the conspiracy that by April 7, 2017, the Kelihos botnet infected at least 50,000 computers, including computers in Connecticut. The computers infected with the Kelihos botnet were used in and affecting interstate and foreign commerce and communication.

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

Overt Acts

26. In furtherance of the conspiracy and to effect the objects thereof, KOSHKIN, TSURKAN, Levashov, and other co-conspirators committed, and caused to be committed the following overt acts in the District of Connecticut and elsewhere:

a. On or about September 20, 2013, an advertisement was posted for Crypt4U on an online criminal forum known to the Grand Jury.

b. On or about September 2, 2013, KOSHKIN registered the domain name crypt4u.com.

c. On or about January 7, 2014, KOSHKIN registered the domain name crypt4u.net.

d. On or about May 21, 2014, TSURKAN, using an alias, registered the domain name fud.bz.

e. On or about June 1, 2014, a Crypt4U representative sent a message via Jabber to Levashov advising Levashov to send money to a WebMoney purse, which is known to the Grand Jury, and is associated with an account that TSURKAN created in his former wife's name.

f. On or about June 4, 2014, the fud.bz website, which advertised the crypting service, stated "Crypter works with most softs: botnets, rats, keloggers, stealers, miners, etc." The website further provided a list of a number of large anti-virus companies next to each of which was the term "[OK]." The purpose of these statements was to advertise Crypt4U's ability to crypt malware so that it would not be detected by the listed antivirus software.

g. On or about January 24, 2015, KOSHKIN registered the domain name fud.re.

h. On or about December 12, 2015, Levashov and a Crypt4U representative exchanged messages via Jabber discussing a complaint that Levashov had with Crypt4U, during which "Oleg" [KOSHKIN] was identified as Crypt4U's "Admin."

i. On or about January 28, 2016, Levashov and a Crypt4U representative exchanged messages via Jabber discussing a complaint that Levashov had with Crypt4U, during which the Jabber ID for the Crypt4U programmer was identified as olegvic@jabber.no.

j. On or about March 24, 2016, a Crypt4U representative sent a Jabber message to Levashov providing him with an internet protocol ("IP") address for a file transfer

protocol server so that Levashov could transfer the Kelihos malware to Crypt4U in order to be crypted.

k. On or about August 19, 2016, TSURKAN sent messages via Jabber to Levashov discussing Levashov's malware and how the crypted malware could bypass antivirus software.

l. Between approximately December 29, 2016, and March 13, 2017, the exact date being unknown to the Grand Jury, the Kelihos malware was transmitted and installed on a computer assigned internet protocol ("IP") address 96.67.50.137.

m. Between approximately December 29, 2016, and March 13, 2017, the exact date being unknown to the Grand Jury, the Kelihos malware was transmitted and installed on a computer assigned IP address 24.218.138.137.

n. Between approximately December 29, 2016, and March 13, 2017, the exact date being unknown to the Grand Jury, the Kelihos malware was transmitted and installed on a computer assigned IP address 69.94.24.124.

o. Between approximately December 29, 2016, and March 13, 2017, the exact date being unknown to the Grand Jury, the Kelihos malware was transmitted and installed on a computer assigned IP address 69.126.128.244.

p. Between approximately December 29, 2016, and March 13, 2017, the exact date being unknown to the Grand Jury, the Kelihos malware was transmitted and installed on a computer assigned IP address 24.2.180.202.

q. On December 28, 2017, the registration of the domain fud.re, registered to the Name.com user OlegVic, was successfully renewed.

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

COUNT TWO
(Aiding and Abetting Intentional Damage to a Protected Computer)

27. Paragraphs 1 to 25, and 26(g)-(q), are incorporated by reference.

28. From approximately October 2014 until approximately April 7, 2017, the exact dates being unknown to the Grand Jury, in the District of Connecticut and elsewhere, the defendants KOSHKIN and TSURKAN aided and abetted Levashov to knowingly attempt to cause and cause the transmission of a program, information, 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 damage affecting 10 or more protected computers during any one-year period.

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

A TRUE BILL

/s/

FOREPERSON

UNITED STATES OF AMERICA

LEONARD C. BOYLE
FIRST ASSISTANT UNITED STATES ATTORNEY

VANESSA RICHARDS
ASSISTANT UNITED STATES ATTORNEY

NEERAJ N. PATEL
ASSISTANT UNITED STATES ATTORNEY