

Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington.

FEBRUARY 2 2012

WILLIAM M. McZOO, Clerk

By

Deputy

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

SERGEY KAMRATOV,
DMYTRO VOLOKITIN,
YEVGEN FATYEYEV,
VICTOR MAUZE, and
MIKAEL PATRICK SALLNERT

Defendants.

CR 12

NO 2

025 MJP

INDICTMENT

(FILED UNDER SEAL)

The Grand Jury charges that:

COUNT 1

(Conspiracy to Commit Wire Fraud)

A. The Offense

1. Beginning at a date uncertain, but no later than in or around 2006, and continuing until on or about June 21, 2011, within the Western District of Washington and elsewhere, SERGEY KAMRATOV, DMYTRO VOLOKITIN, YEVGEN FATYEYEV, VICTOR MAUZE, and MIKAEL PATRICK SALLNERT (hereinafter "PATRICK SALLNERT"), and others known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, confederate and agree together to commit an offense against the United States, to wit: to knowingly and willfully devise and execute, attempt to execute, and aid and abet, a scheme and artifice to defraud, and for obtaining money and property by means of material false and fraudulent pretenses, representations,

1 and promises; and in executing, attempting to execute, and aiding and abetting this
2 scheme and artifice, to knowingly cause to be transmitted in interstate and foreign
3 commerce, by means of wire communication, certain signs, signals and sounds as further
4 described below, in violation of Title 18, United States Code, Sections 1343 and 2.

5 **B. The Object of the Conspiracy**

6 2. The object of the scheme and artifice to defraud was to fraudulently obtain
7 money from consumers by falsely representing to consumers that their computers were
8 infected with malicious software. After falsely informing consumers that their computers
9 were infected with malicious software, the defendants would fraudulently market their
10 rogue computer security software to the targeted consumers as a means of eliminating the
11 infection. As the defendants then well knew, the malicious software purportedly detected
12 on consumers' computers did not exist. During the course of the scheme and artifice to
13 defraud, SERGEY KAMRATOV, DMYTRO VOLOKITIN, VICTOR MAUZE,
14 YEVGEN FATYEYEV, and PATRICK SALLNERT and others known and unknown,
15 fraudulently obtained at least \$71,000,000.00 from consumers who were fraudulently
16 misled into purchasing the defendants' rogue security programs.

17 **C. Manner and Means of the Conspiracy**

18 3. It was part of the conspiracy that the defendants created rogue security
19 software that purported to be computer security software, but was in fact malicious code
20 that did not perform a legitimate computer security function and, in many cases, caused
21 victims' computers to be further compromised by silently downloading additional
22 malicious code without victims' knowledge or consent.

23 4. It was further part of the conspiracy that the defendants created software
24 that was designed to falsely represent to consumers that their computers were infected
25 with malicious software in order to intimidate and deceive victims into purchasing the
26 defendants' rogue security software to rid their computers of security threats that did not
27 exist.

28 //

1 5. It was further part of the conspiracy that the defendants employed a
2 marketing model in which co-conspirators, known as “affiliates,” were paid to direct
3 online traffic to the defendants’ websites that then infected the victims’ computers with
4 malicious code.

5 6. It was further part of the conspiracy that the defendants and their co-
6 conspirator affiliates employed a variety of methods to direct victims to websites that
7 delivered malicious code, including “social engineering” tactics whereby the defendants
8 tricked consumers into downloading the defendants’ malicious code by misrepresenting
9 the nature of the download.

10 7. It was further part of the conspiracy that the defendants’ malicious code
11 caused graphics to be displayed on victims’ computers that falsely indicated the computer
12 was infected with security threats, and then also conveyed the message that the threats
13 could be removed if the victim agreed to purchase the full version of the defendants’
14 rogue security software.

15 8. It was further part of the conspiracy that the defendants’ malicious code
16 would continue to display intrusive and disruptive alerts falsely indicating the presence of
17 malicious code on the victims’ computers until the victims agreed to purchase the full
18 version of the defendants’ rogue security software.

19 9. It was further part of the conspiracy that the defendants used a network of
20 computer servers throughout the world to support the scheme and artifice to defraud.
21 This network of computer servers included: (a) victim-facing servers that hosted the
22 defendant’s malicious code as well as “ruse sites” that duped victims into downloading
23 the malicious code; (b) affiliate-facing servers that tracked affiliate commissions, pay outs
24 and other affiliate-related information; and (c) back-end servers that performed
25 administrative functions such as data backup, filtering of traffic and payment processing.

26 10. It was further part of the conspiracy that when victims chose to purchase the
27 defendants’ rogue security software, they would be required to make a credit card
28 payment via the Internet.

1 11. It was further part of the conspiracy that the defendants established shell
2 companies for the purpose of processing the credit card payments for the rogue security
3 software.

4 12. It was further part of the conspiracy that the defendants used shell
5 companies to establish credit card payment accounts with banks and other processing
6 facilities.

7 13. It was further part of the conspiracy that the defendants misrepresented the
8 nature of their business and their product to the banks and other processing facilities.

9 **D. Overt Acts**

10 14. Counts 2 through 11 of this Indictment are incorporated by reference herein
11 and are alleged as separate overt acts in furtherance of the conspiracy and to accomplish
12 one or more of its objects as if fully set forth herein. In addition, SERGEY
13 KAMRATOV, DMYTRO VOLOKITIN, VICTOR MAUZE, YEVGEN FATYEYEV,
14 and PATRICK SALLNERT, and others known and unknown to the Grand Jury,
15 committed the following overt acts within the Western District of Washington and
16 elsewhere, in furtherance of the conspiracy:

17 a. On or about December 13, 2006, DMYTRO VOLOKITIN created
18 the e-mail account "divofix@gmail.com";

19 b. On or about December 20, 2006, SERGEY KAMRATOV created
20 the e-mail account "ddarkmaster@gmail.com";

21 c. On or about February 11, 2007, SERGEY KAMRATOV created the
22 e-mail account "greyx11@gmail.com";

23 d. On or about September 20, 2007, SERGEY KAMRATOV registered
24 the domain name "xpantivirus.com";

25 e. On or about November 20, 2007, SERGEY KAMRATOV created
26 the e-mail account "pro.directly@gmail.com";

27 f. On or about December 29, 2007, SERGEY KAMRATOV registered
28 the domain name "trafficconverter.biz";

1 g. On or about May 6, 2008, VICTOR MAUZE sent an e-mail to
2 ayleon@rambler.ru with source code for a rogue security program called "AntiSpyGuard
3 2007";

4 h. On or about July 1, 2008, YEVGEN FATYEYEV created the e-mail
5 account "ibragimimus@gmail.com";

6 i. On or about August 22, 2008, SERGEY KAMRATOV established
7 an account with Limestone Networks for a computer server with the Server ID: LSN-
8 D1816;

9 j. In or around September 2008, SERGEY KAMRATOV, DMYTRO
10 VOLOKITIN and YEVGEN FATYEYEV started a company named "Smart Systems";

11 k. In or around September 2008, SERGEY KAMRATOV and
12 DMYTRO VOLOKITIN caused E.C. to create a company called "Heliana Limited";

13 l. On or about October 20, 2008, PATRICK SALLNERT sent an e-
14 mail to cd@europaymentgroup.com regarding a company named Bolzar and a merchant
15 payment processing account application for spyware-protector.com;

16 m. On or about October 28, 2008, SERGEY KAMRATOV established
17 an account with Limestone Networks for a computer server with the Server ID: LSN-
18 D1092;

19 n. On or about November 26, 2008, SERGEY KAMRATOV and
20 DMYTRO VOLOKITIN applied for a merchant processing account at Wirecard Bank in
21 Germany for Heliana Limited, doing business as "http://badware-protector.com;"

22 o. On or about April 5, 2009, PATRICK SALLNERT met with
23 representatives of Europayment Group in Germany;

24 p. On or about December 14, 2010, YEVGEN FATYEYEV established
25 an account with Sentris Networks for a server with the IP address 63.223.110.21 and
26 Server ID: CyberUSA22;

27 q. On or about June 3, 2011, YEVGEN FATYEYEV transferred
28 approximately 25 gigabyts (26,028 MB) of data from the server with IP address

1 72.9.108.154 and server ID Amhost1, to a server with IP address 64.120.225.130 and
2 server ID Amhost 21;

3 All in violation of Title 18, United States Code, Section 1349.

4
5 **COUNTS 2 - 11**

6 **(Wire Fraud and Attempted Wire Fraud)**

7 **A. The Offense**

8 15. Beginning at a date uncertain, but no later than in or around 2006, and
9 continuing until on or about June 21, 2011, within the Western District of Washington
10 and elsewhere, SERGEY KAMRATOV, DMYTRO VOLOKITIN, VICTOR MAUZE,
11 YEVGEN FATYEYEV, and PATRICK SALLNERT, and others known and unknown to
12 the Grand Jury, did knowingly and willfully devise and execute and attempt to execute a
13 scheme and artifice to defraud, and for obtaining money and property by means of
14 material false and fraudulent pretenses, representations, and promises; and in executing
15 and attempting to execute this scheme and artifice, did knowingly cause to be transmitted
16 in interstate commerce by means of wire communication, certain signs, signals and
17 sounds.

18 16. The essence of the scheme and artifice to defraud was to fraudulently obtain
19 money from consumers by falsely representing to consumers that their computers were
20 infected with malicious software. After falsely informing consumers that their computers
21 were infected with malicious software, the defendants would fraudulently market their
22 rogue computer security software to the targeted consumers as a means of eliminating the
23 infection. As the defendants then well knew, the malicious software purportedly detected
24 on consumers' computers did not exist. During the course of the scheme and artifice to
25 defraud, SERGEY KAMRATOV, DMYTRO VOLOKITIN, VICTOR MAUZE,
26 YEVGEN FATYEYEV, and PATRICK SALLNERT, and others known and unknown to
27 the Grand Jury, fraudulently obtained at least \$71,000,000.00 from consumers who were
28 fraudulently misled into purchasing the defendants' rogue security programs.

B. Manner and Means of the Scheme and Artifice

17. The manner and means of the scheme and artifice are set forth in Paragraphs 3 through 13 of Count 1 of this Indictment, and said paragraphs are incorporated by reference as if fully set forth herein.

C. Execution of the Scheme and Artifice to Defraud

18. Beginning at a date uncertain, but no later than in or around 2006, and continuing until on or about June 21, 2011, within the Western District of Washington and elsewhere, SERGEY KAMRATOV, DMYTRO VOLOKITIN, VICTOR MAUZE, YEVGEN FATYEYEV, and PATRICK SALLNERT, and others known and unknown to the Grand Jury, for the purpose of executing the aforementioned scheme and artifice to defraud and to obtain money by means of false and fraudulent pretenses, representations, promises and omissions of material facts, and attempting to do so, did knowingly and intentionally transmit, and did aid, abet, counsel, command, induce and procure the below listed wire transmissions in interstate and/or foreign commerce:

Count	Approximate Date	Wire Transaction	Amount
2	February 1, 2010	RC transmitted his credit card number from Shoreline, Washington, over the Internet to Los Angeles, California and elsewhere, in order to purchase defendants' rogue security software	\$89.90
3	February 2, 2010	MC transmitted his debit card number from Kirkland, Washington, over the Internet to Los Angeles, California and elsewhere, in order to purchase defendants' rogue security software	\$89.90

1	4	February 3, 2010	MT transmitted his credit card number from Bainbridge Island, Washington, over the Internet to Los Angeles, California and elsewhere, in order to purchase defendants' rogue security software	\$89.90
2				
3				
4				
5				
6	5	February 3, 2010	KM transmitted her debit card number from Shoreline, Washington, over the Internet to Los Angeles, California and elsewhere, in order to purchase defendants' rogue security software	\$99.90
7				
8				
9				
10				
11	6	February 4, 2010	LA transmitted her credit card number from Bellevue, Washington, over the Internet to Los Angeles, California and elsewhere, in order to purchase defendants' rogue security software	\$89.90
12				
13				
14				
15	7	February 5, 2010	NK transmitted her debit card number from Seattle, Washington, over the Internet to Los Angeles, California and elsewhere, in order to purchase defendants' rogue security software	\$99.90
16				
17				
18				
19				
20	8	February 7, 2010	RR transmitted his debit card number from Seattle, Washington, over the Internet to Los Angeles, California and elsewhere, in order to purchase defendants' rogue security software	\$99.90
21				
22				
23				
24	9	February 9, 2010	VB transmitted her credit card number from Bellevue, Washington, over the Internet to Los Angeles, California and elsewhere, in order to purchase defendants' rogue security software	\$99.90
25				
26				
27				
28				

10	February 9, 2010	MS transmitted her credit card number from Seattle, Washington, over the Internet to Los Angeles, California and elsewhere, in order to purchase defendants' rogue security software	\$99.90
11	February 10, 2010	JT transmitted her credit card number from Kingston, Washington, over the Internet to Los Angeles, California and elsewhere, in order to purchase defendants' rogue security software	\$89.90

All in violation of Title 18, United States Code, Sections 1343, 1349, and 2.

COUNT 12
(Accessing Protected Computer in Furtherance of Fraud)

19. The Grand Jury realleges and incorporates by reference paragraphs 1 – 13 of this Indictment and further charges that:

20. Beginning no later than February 1, 2010, and continuing until at least January 31, 2011, within the Western District of Washington and elsewhere, SERGEY KAMRATOV, DMYTRO VOLOKITIN, VICTOR MAUZE, YEVGEN FATYEYEV, and PATRICK SALLNERT, and others known and unknown to the Grand Jury, knowingly and with intent to defraud accessed protected computers without authorization and by means of such conduct furthered an intended fraud and obtained something of value, specifically, the defendants caused victims' computers to be infected with malicious code that caused graphics that falsely indicated the computer was infected with security threats to display on victim computers, along with the message that the threats could be removed if the victim computer owner would purchase rogue security software,

//

1 and thereby deceived victims into installing rogue security software and making payments
2 to the defendants for the same that exceeded \$5,000.00 within a 1-year period.

3 All in violation of 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A), and 2.
4

5 **COUNT 13**

6 **(Intentional Damage to a Protected Computer)**

7
8 21. The Grand Jury realleges and incorporates by reference paragraphs 1 – 13
9 of this Indictment and further charges that:

10 22. Beginning no later than February 1, 2010, and continuing until at least
11 January 31, 2011, within the Western District of Washington and elsewhere, SERGEY
12 KAMRATOV, DMYTRO VOLOKITIN, VICTOR MAUZE, YEVGEN FATYEYEV,
13 and PATRICK SALLNERT, and others known and unknown to the Grand Jury,
14 knowingly caused the transmission of a program, information, code, and command,
15 including specifically malicious code that caused graphics that falsely indicated the
16 computer was infected with security threats to display on victim computers, along with
17 the message that the threats could be removed if the victim computer owner would
18 purchase rogue security software, and as a result of such conduct, intentionally caused
19 damage without authorization affecting 10 or more protected computers during a 1-year
20 period.

21 All in violation of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B), and 2.
22

23 **FORFEITURE ALLEGATIONS AS TO COUNTS 1 - 11**

24
25 22. The allegations contained in Counts 1 - 11 of this Indictment are hereby
26 realleged and incorporated by reference for the purpose of alleging forfeitures to the
27 United States pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28,
28 United States Code, Section 2461(c).

23. Upon conviction of the offenses charged in Counts 1 - 11, in violation of Title 18, United States Code, Sections 1343 and 1349 and 2, SERGEY KAMRATOV, DMYTRO VOLOKITIN, YEVGEN FATYEV, VICTOR MAUZE, and PATRICK SALLNERT shall forfeit 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), any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses. The property to be forfeited includes, but is not limited to, the following:

a. Money Judgment. A sum of money representing the proceeds obtained as a result of the offenses charged in Counts 1 - 11 of this Indictment.

24. If any of the property described above, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- 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 of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

All pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).

/////

/////

1 **FORFEITURE ALLEGATIONS AS TO COUNTS 12 AND 13**

2 25. The allegations contained in Counts 12 and 13 of this Indictment are
3 hereby realleged and incorporated by reference for the purpose of alleging forfeitures
4 pursuant to Title 18, United States Code, Section 982(a)(2)(B) and Title 18, United States
5 Code, Section 1030(i) and (j).
6

7 26. Upon conviction of the offenses in Title 18, United States Code, Section
8 1030 set forth in Counts 12 - 13 of this Indictment, the defendants, SERGEY
9 KAMRATOV, DMYTRO VOLOKITIN, VICTOR MAUZE, YEVGEN FATYEYEV,
10 and PATRICK SALLNERT, shall forfeit to the United States of America, pursuant to
11 Title 18, United States Code, Section 982(a)(2)(B) and Title 18, United States Code,
12 Section 1030(i) and (j), any property constituting, or derived from, proceeds obtained,
13 directly or indirectly, as a result of such violations, and any property used or intended to
14 be used to commit or to facilitate the commission of such violations. The property to be
15 forfeited includes, but is limited to, the following:

16 a. Money Judgment. A sum of money representing the proceeds obtained
17 as a result of the offenses charged in Counts 12 - 13 of this Indictment.

18 27. If any of the property described above, as a result of any act or omission
19 of the defendants:

- 20 a. cannot be located upon the exercise of due diligence;
- 21 b. has been transferred or sold to, or deposited with, a third party;
- 22 c. has been placed beyond the jurisdiction of the court;
- 23 d. has been substantially diminished in value; or
- 24 e. has been commingled with other property which cannot be divided
25 without difficulty,

26 the United States of America shall be entitled to forfeiture of substitute property pursuant

27 /////

to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1) and Title 28, United States Code, Section 2461(c).

A TRUE BILL: 2/12/12

DATED:

Signature of Foreperson redacted pursuant to policy of the Judicial Conference.

FOREPERSON

Jenny A. Durkan
JENNY A. DURKAN
United States Attorney

Carl Blackstone
CARL BLACKSTONE
Assistant United States Attorney

Francis Franze-Nakamura
FRANCIS FRANZE-NAKAMURA
Assistant United States Attorney

Carol Sipperly
CAROL SIPPERLY
Trial Attorney

Ethan R. Arenson
ETHAN R. ARENSEN
Trial Attorney

Norman M. Barbosa
NORMAN M. BARBOSA
Assistant United States Attorney

Kathryn A. Warma
KATHRYN A. WARMA
Assistant United States Attorney