ORIGINAL

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF GEORGIA

ATLANTA DIVISION

UNITED STATES OF AMERICA
v.
JOHN DOE,
a/k/a Gribodemon, and
HAMZA BENDELLADJ,
a/k/a Bx1,
Defendants.

CRIMINAL INDICTMENT

NO. 1: 11- CR-557

UNDER SEAL

THE GRAND JURY CHARGES THAT:

COUNT ONE
(Wire and Bank Fraud Conspiracy)

1. Beginning on an unknown date, but at least by in or about December 2009, through in or about September 2011, the exact dates being unknown to the Grand Jury, in the Northern District of Georgia and elsewhere, Defendants JOHN DOE, a/k/a Gribodemon, and HAMZA BENDELLADJ, a/k/a Bx1, together and with others known and unknown to the Grand Jury, did knowingly conspire to

(A) violate Title 18, United States Code, Section 1343, that is, to devise and intend to devise a scheme and artifice to defraud financial institutions and individuals, and to obtain money and property from those financial institutions and individuals, by means of materially false and fraudulent pretenses, representations, and promises, as well as by omission of material facts; and for the purpose of executing such scheme and artifice, and attempting to do so, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain signs, signals, and sounds, that is, computer commands to be made between places outside of the State of Georgia and a computer server within the Northern District of Georgia; and

(B) violate Title 18, United States Code, Section 1344, that is, to execute and attempt to execute a scheme and artifice (1) to defraud a financial institution, the deposits for which were at the time insured by the Federal Deposit Insurance Corporation; and (2) to obtain and attempt to obtain moneys, funds, credits, assets, and other properties owned by and under the custody and control of a financial institution, the deposits for which were at the time insured by the Federal Deposit Insurance Corporation, by means of materially false and fraudulent pretenses, representations, and promises, as well as by omission of material facts.

BACKGROUND

2. A "bot" (an abbreviation for "robot") is a computer (most often a personal computer) that contains a software program that interacts with network services. A collection of bots forms a "botnet" (an abbreviation for "robot network"). Malicious software ("malware") associated with a particular botnet allows infected computers (individually known as bots) to be remotely controlled by a master computer commonly referred to as a "command and control" ("C&C") server. Thus, botnets are composed of numerous computers

that serve various roles in the botnet, and these computers fall into two major categories: C&C servers that administer the botnet, and bots that follow the orders given to them through the C&C servers.

3. Botnets are created by installing and executing computer code known as configuration files (or simply "config files") on multiple computers. Config files configure the initial settings for computer programs. In this instance, what is more commonly known as a computer virus makes up part of the config files.

4. Each C&C server in a botnet is assigned an Internet Protocol address (or simply "IP address"). An IP address is a unique numeric address used by computers on the Internet, and looks like a series of four numbers, each in the range 0-255, separated by periods (for example, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. A domain name is an identification label (such as example.com) that allows users to easily locate a website. Domain names resolve back to specific IP addresses, although multiple domain names can resolve back to the same IP address.

MANNER AND MEANS

5. SpyEye is a malware toolkit specifically designed to automate the theft of confidential personal and financial information, such as online banking credentials. Among other things, SpyEye facilitates the theft of confidential personal and financial information by numerous methods. For example, SpyEye obtains such information through a data grabber or keystroke logger, and at times fraudulently presents a fake bank web page or portions of a bank web page to trick a user into entering personal and financial information.

6. Defendant JOHN DOE, a/k/a GRIBODEMON (hereinafter "GRIBODEMON"), is the principal author of SpyEye. Other co-conspirators including Defendant HAMZA BENDELLADJ, a/k/a Bx1 (hereinafter "BENDELLADJ"), also developed SpyEye components.

7. SpyEye allows users to create customized malware resulting in (1) a SpyEye C&C server operated through a web interface; and (2) SpyEye config files.

8. SpyEye C&C servers are used to monitor, manipulate, and update bots under the servers' control. In particular, SpyEye C&C servers send instructions to bots under their control, which contain the SpyEye config files that, when triggered, tell the bots to automatically send specified information back to the C&C servers.

9. The SpyEye config files contain the malicious computer code to be installed and executed on victim computers. The config files also contain the IP address, domain name, or both for the location of a C&C server to which the bot should "call home" -- that is, the C&C server to which the bot should send at least some information.

10. SpyEye can be customized by those who purchase SpyEye to, among other things, (1) target information from specific financial institutions; and (2) define the type of information that is obtained from the victim computers without the computer users' knowledge or consent, such as online banking credentials, and the method for obtaining the information, such as through a data grabber or keystroke logger.

11. Those who purchase SpyEye can customize their version with "web injects." Web injects introduce (or "inject") malicious computer code into a victim's web browser while the victim browses the Internet, "hijacking" the victim's Internet session. Different injects are used for different purposes. Some are used to steal specific data, such as confidential identity information, credit card information, or specific online banking information. Other web injects are used to present false online banking pages to trick a victim into entering online banking information.

12. A SpyEye botnet is created by infecting multiple computers (bots) with the SpyEye config files without the users' of

the victim computers' knowledge or consent. As a result, the commands sent between a SpyEye C&C server and bots under its control are unauthorized, and essentially create a secret computer network between the server and bots.

13. A method of communication between the bots and their C&C servers is known as a "GET" request, and the bots and C&C servers contain logs reflecting those requests. A GET request refers to the act of a computer sending information to or receiving information from another computer, that is, a GET request is a type of computer command.

14. Co-conspirators including GRIBODEMON and BENDELLADJ communicated through email, instant messaging programs, and web forums to discuss, among other things, (1) purchasing; (2) updating; (3) customizing; (4) developing components for; and (5) the price for SpyEye. The co-conspirators also discussed the operation of various SpyEye components.

15. Co-conspirators including GRIBODEMON and BENDELLADJ sold various versions of SpyEye and SpyEye components on the Internet. The components included different methods for obtaining confidential personal and financial information without victims' knowledge or consent, such as different web injects to accomplish that purpose.

16. Co-conspirators including BENDELLADJ operated SpyEye botnets through SpyEye C&C servers. Individuals like BENDELLADJ

who operate SpyEye botnets through SpyEye C&C servers are also known as "bot herders."

17. One of BENDELLADJ's SpyEye C&C servers was located in Atlanta, Georgia, and a log on that server reflected GET requests between the server and bots from on or about February 21, 2011 through on or about February 24, 2011. A SpyEye config file related to this C&C server targeted information from approximately 253 unique financial institutions, deposits for some of which were at the time insured by the Federal Deposit Insurance Corporation. The GET requests indicated that some of the communications were between the C&C server in Atlanta, Georgia and bots located in different States and foreign countries.

18. After confidential personal and financial information is obtained through a SpyEye botnet, it is available to the bot herder to use or provide to other co-conspirators. Among other things, the information is used by co-conspirators to access victim accounts held at financial institutions without the knowledge or consent of the account holders.

In violation of Title 18, United States Code, Section 1349.

COUNTS TWO THROUGH ELEVEN
(Wire Fraud)

19. The Grand Jury re-alleges and incorporates by reference Paragraphs 2 through 18 of this Indictment as if fully set forth here.

20. From on or about February 21, 2011, through on or about February 24, 2011, in the Northern District of Georgia and elsewhere, Defendant HAMZA BENDELLADJ, a/k/a Bx1, aided and abetted by others known and unknown to the Grand Jury, for the purpose of executing and attempting to execute the aforementioned scheme and artifice, such scheme having been devised and intended to be devised to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, as well as by omission of material facts, did knowingly cause to be transmitted in interstate and foreign commerce, by means of a wire communication, certain signs, signals, and sounds, that is, did knowingly cause computer commands to be transmitted in interstate and foreign commerce.

Execution of the Scheme and Artifice

21. On or about each date and time listed in Column B, in the Northern District of Georgia and elsewhere, for the purpose of executing the scheme and artifice to defraud and to obtain money and property as set out in Count One of this Indictment, Defendant HAMZA BENDELLADJ, a/k/a Bx1, aided and abetted by others known and unknown to the Grand Jury, did knowingly cause computer commands to

be made between a SpyEye C&C server with the IP address 75.127.109.16, which was then located in the Northern District of Georgia, and the computer with the IP address listed in Column C and located in the State listed in Column D:

A	B	C	D
Count	**Date/Time**	**IP Address**	**Location**
2	24 February 2011 at 09:07:52 ET	69.132.77.22	North Carolina
3	21 February 2011 at 00:05:06 ET	70.60.121.239	North Carolina
4	21 February 2011 at 00:05:17 ET	71.75.209.112	North Carolina
5	21 February 2011 at 00:05:03 ET	75.176.16.11	North Carolina
6	24 February 2011 at 09:08:07 ET	75.183.121.215	North Carolina
7	22 February 2011 at 19:11:03 ET	98.14.177.88	New York
8	24 February 2011 at 09:08:17 ET	174.96.209.222	North Carolina
9	21 February 2011 at 00:05:02 ET	174.108.10.227	North Carolina
10	23 February 2011 at 16:48:33 ET	174.76.158.53	California

A	B	C	D
Count	**Date/Time**	**IP Address**	**Location**
11	21 February 2011 at 00:05:07 ET	71.0.91.4	Virginia

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

<u>COUNT TWELVE</u>
(Computer Fraud and Abuse Conspiracy)

22. The Grand Jury re-alleges and incorporates by reference Paragraphs 2 through 18 of this Indictment as if fully set forth here.

23. Beginning on an unknown date, but at least by in or about December 2009, through in or about September 2011, the exact dates being unknown to the Grand Jury, in the Northern District of Georgia and elsewhere, Defendants JOHN DOE, a/k/a Gribodemon (hereinafter "GRIBODEMON"), and HAMZA BENDELLADJ, a/k/a Bx1 ("BENDELLADJ"), together and with others known and unknown to the Grand Jury, did knowingly conspire to

(A) intentionally access a computer without authorization and exceeding authorization, and thereby obtain or attempt to obtain information from a protected computer, and the offense 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)(i);

(B) knowingly and with intent to defraud access a protected computer without authorization and exceeding authorization, and by means of such conduct further the intended fraud and obtain things of value, in violation of Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A); and

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

OVERT ACTS

24. In furtherance of the conspiracy and to achieve the objects thereof, the conspirators committed the following overt acts, among others, in the Northern District of Georgia and elsewhere:

(A) On or about January 10, 2010, GRIBODEMON joined the www.darkode.com web forum for the purpose of advertising the sale of SpyEye.

(B) On or about June 29, 2010, GRIBODEMON advertised on the www.darkode.com web forum that, among other things, "SpyEye - this is a bank Trojan with form grabbing possibility," meaning malware designed to steal bank information.

(C) On or about July 06, 2010, BENDELLADJ, using the nickname Bx1, commented on the www.darkode.com web forum that he was a client of GRIBODEMON and vouched for him.

(D) On or about September 16, 2010, GRIBODEMON advertised another version of SpyEye on the www.darkode.com web forum indicating that it includes a "cc grabber." A "cc grabber" scans all the bots on the botnet for credit card credentials.

(E) From on or about February 21, 2011, through on or about February 24, 2011, BENDELLADJ knowingly caused GET request communications between victim computers and a SpyEye C&C server located in the Northern District of Georgia, each of which was an act in furtherance of the conspiracy.

(F) In or about April 2011, BENDELLADJ, using the YouTube account danielhb1988, uploaded a video on YouTube.com setting forth that he is "Bx1" and that he has his own version of SpyEye to sell.

(G) On or about July 6, 2011, GRIBODEMON negotiated and agreed to sell SpyEye for $8,500 to an online, undercover law enforcement officer.

(H) On or about July 6, 2011, GRIBODEMON, in response to receiving $8,500 from an online, undercover law enforcement officer, uploaded a version of the SpyEye toolkit on www.sendspace.com.

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

COUNT THIRTEEN
(Computer Fraud and Abuse)

25. The Grand Jury re-alleges and incorporates by reference Paragraphs 2 through 18 of this Indictment as if fully set forth here.

26. Beginning on an unknown date, but at least by on or about February 21, 2011, through on or about February 24, 2011, the exact dates being unknown to the Grand Jury, in the Northern District of Georgia and elsewhere, Defendant HAMZA BENDELLADJ, a/k/a Bx1, aided and abetted by others known and unknown to the Grand Jury, did knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage and attempt to cause damage without authorization to a protected computer, and the offense caused and would, if completed, 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), 1030(c)(4)(B), and 2.

COUNTS FOURTEEN THROUGH TWENTY THREE
(Computer Fraud and Abuse)

27. The Grand Jury re-alleges and incorporates by reference Paragraphs 2 through 18 of this Indictment as if fully set forth here.

28. Beginning on an unknown date, but at least by on or about February 21, 2011, through on or about February 24, 2011, the exact dates being unknown to the Grand Jury, in the Northern District of Georgia and elsewhere, Defendant HAMZA BENDELLADJ, a/k/a Bx1, aided and abetted by others known and unknown to the Grand Jury, did intentionally access a computer without authorization and exceeding authorization, and thereby obtain or attempt to obtain information from a protected computer for the purpose of private financial gain.

29. On or about the date and time listed in Column B, the following communication between the SpyEye C&C server with the IP address 75.127.109.16, which was then located in the Northern District of Georgia, and the protected computer with the IP address listed in Column C occurred and resulted in accessing the protected computers and obtaining information from the protected computers with the IP addresses listed in Column C:

A	B	C
Count	**Date/Time**	**IP Address**
14	21 February 2011 at 00:05:04 ET	58.7.239.152
15	21 February 2011 at 00:05:00 ET	184.162.222.3
16	21 February 2011 at 01:35.12 ET	84.17.96.70

A	B	C
Count	**Date/Time**	**IP Address**
17	21 February 2011 at 03:16:23 ET	217.112.59.207
18	21 February 2011 at 05:40:10 ET	94.116.162.110
19	21 February 2011 at 00:05:01 ET	95.225.232.28
20	21 February 2011 at 02:27:36 ET	220.255.1.91
21	24 February 2011 at 09:08:01 ET	41.133.136.211
22	24 February 2011 at 09:07:56 ET	83.119.125.35
23	22 February 2011 at 08:18:18 ET	80.249.65.140

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

FORFEITURE

Upon conviction of one or more of the offenses alleged in Counts One through Eleven of this Indictment, the Defendants shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and Title 28, United States Code, Sections 2461(c), any and all property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly, as a result of such offenses, including, but not limited to, the following:

a. A sum of money equal to the amount of proceeds the Defendants obtained as a result of the offenses.

Upon conviction of one or more of the offenses alleged in Counts Twelve through Twenty-Three of this Indictment, the Defendants shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(B), any and all property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly, as a result of such offenses, including, but not limited to, the following:

a. A sum of money equal to the amount of proceeds the Defendants obtained as a result of the offenses.

If any of the above-described forfeitable property, 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 divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), Title 18, United States Code, Section

982(b), and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of said Defendants up to the value of the forfeitable property described above.

A True BILL

FOREPERSON

SALLY QUILLIAN YATES
UNITED STATES ATTORNEY

NICHOLAS A. OLDHAM
ASSISTANT UNITED STATES ATTORNEY
Georgia Bar No. 592701

CAROL L SIPPERLY
TRIAL ATTORNEY
COMPUTER CRIMES & INTELLECTUAL PROPERTY SECTION
UNITED STATES DEPARTMENT OF JUSTICE
Maine Bar No. 009930

600 U.S. Courthouse
75 Spring Street, S.W.
Atlanta, GA 30303
Telephone 404-581-6000
Facsimile 404-581-6181