

UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

United States District Court
District of Connecticut
FILED AT NEW HAVEN

Jan 18 2007
KEVIN F. ROWE, Clerk
By P. A. Villano
Deputy Clerk

UNITED STATES OF AMERICA :

: No.

v. :

: 3:07 cr 12 (JCH)

CIPRIAN DUMITRU TUDOR,
OVIDIU-IONUT NICOLA-ROMAN,
MIHAI CRISTIAN DUMITRU,
PETRU BOGDAN BELBITA,
RADU-MIHAI DOBRICA,
CORNEL IONUT TONITA,
and CRISTIAN NAVODARU,

: VIOLATION: 18 U.S.C. § 1029(b)
: (Conspiracy to Commit Fraud in
: Connection with Access
: Devices); 18 U.S.C. § 1349
: (Conspiracy to Commit Bank
: Fraud); U.S.C. § 1028A
: (Aggravated Identity Theft)

Defendants. :

I N D I C T M E N T

The Grand Jury charges that, at all times relevant to this Indictment:

COUNT ONE

(Access Device Fraud Conspiracy)

1. A "phishing" scheme is a scheme directed against multiple individuals on the Internet to obtain private personal and financial information, such as names, addresses, bank account numbers, credit card numbers, Social Security account numbers, and personal identification numbers, through fraud and deceit.

2. From in or about 2005 through in or about 2007, in the District of Connecticut and elsewhere, CIPRIAN DUMITRU TUDOR, OVIDIU-IONUT NICOLA-ROMAN, MIHAI CRISTIAN DUMITRU, PETRU BOGDAN BELBITA, RADU-MIHAI DOBRICA, CORNEL IONUT TONITA, and CRISTIAN NAVODARU, defendants herein, and others known and unknown, knowingly did conspire, combine, confederate, and agree to obtain

wrongfully private personal and financial information through a phishing scheme and to use that information further to obtain money, goods, and services to which they were not entitled.

Defendants and Conspirators

3. CIPRIAN DUMITRU TUDOR, a defendant herein, was a resident of Craiova, Romania.

4. OVIDIU-IONUT NICOLA-ROMAN, a defendant herein, was a resident of Craiova, Romania.

5. MIHAI CRISTIAN DUMITRU, a defendant herein, was a resident of Craiova, Romania.

6. PETRU BOGDAN BELBITA, a defendant herein, was a resident of Craiova, Romania.

7. RADU-MIHAI DOBRICA, a defendant herein, was a resident of Galati, Romania.

8. CORNEL IONUT TONITA, a defendant herein, was a resident of Galati, Romania.

9. CRISTIAN NAVODARU, a defendant herein, was a resident of Galati, Romania.

The Scheme to Defraud

10. A phishing scheme uses the Internet to communicate with large numbers of potential victims, only a fraction of whom respond and are actually victimized. Such schemes often work by sending fraudulent and counterfeit email, i.e., "spam," to potential victims. The email, which appears to originate from

legitimate banks, companies, or services providers, requests that potential victims provide or update private personal and financial information.

11. In this case, for example, one of the spam emails used by the defendants purported to be from People's Bank, which is based in Bridgeport, Connecticut. The email was sent, in or about June, 2005, to an individual in Madison, Connecticut, among others. The email read, in pertinent part:

Dear People's Bank Client,
For your security, the profile that you are using to access People's Bank Online Banking has been locked because of too many failed login attempts. You can unlock this profile online by selecting an option below:

Unlock your profile with:

My ATM/Visa Check Card number and PIN.

Other personal information (Social Security Number, Account #, etc)

E-mail address.

We regret any inconvenience this may cause you.

Sincerely,

People's Bank Account Review Department.

12. An individual who clicked on the spam email purporting to be from People's Bank would be re-directed to one or more fraudulent Web pages that falsely appeared to originate from People's Bank. In fact, the fraudulent Web pages were actually hosted on a compromised computer unrelated to People's Bank, without the knowledge or permission of the computer's owner.

13. An individual re-directed to the fraudulent Web pages would be asked to provide private personal and financial information, such as first name, last name, date of birth, Social Security number, credit card number, expiration date, CVV code, personal identification number ("PIN"), and telephone number. Any information provided by the individual would be sent by email to a "collector" account, i.e., an email account used by the defendants to receive and collect the information obtained through the phishing scheme.

14. CIPRIAN DUMITRU TUDOR, OVIDIU-IONUT NICOLA-ROMAN, and MIHAI CRISTIAN DUMITRU, three of the defendants herein, used and shared a number of collector accounts, including "pulawork@yahoo.com," "vercartil@yahoo.com," and "fly4hell@yahoo.com," "raize2hell@yahoo.com," "raize4hell@yahoo.com," and "raize2hell@gmail.com."

15. In or about October, 2006, the "pulawork@yahoo.com" account held approximately 228 email messages that contained, inter alia, credit card numbers, expiration dates, CVV codes, PIN numbers, and other personal identification information such as names, addresses, telephone numbers, dates of birth, and Social Security numbers.

16. In or about August, 2006, the "raize2hell@yahoo.com," "raize4hell@yahoo.com," and "raize2hell@gmail.com" accounts held approximately 6, 83, and 365

email messages, respectively, that contained, inter alia, credit card numbers, expiration dates, CVV codes, PIN numbers, and other personal identification information such as names, addresses, telephone numbers, dates of birth, and Social Security numbers.

17. In or about March, 2006, the "vercartil@yahoo.com" and "fly4hell@yahoo.com" accounts held approximately 138 and 667 email messages, respectively, that contained, inter alia, credit card numbers, expiration dates, CVV codes, PIN numbers, and other personal identification information such as names, addresses, telephone numbers, dates of birth, and Social Security numbers.

18. Another spam email used by the defendants purported to be from the Brattleboro Savings & Loan Ass'n ("Brattleboro S&L"), an institution based in Brattleboro, Vermont. The email, sent in or about October, 2006, stated that online banking and bill payment services were "temporarily unavailable" and read, in pertinent part:

Dear Customer,

The Brattleboro and Springfield Savings & Loan Assn., F.A. online banking and bill payment service is temporarily unavailable. We are in the process of upgrading the system with enhancements to better serve your banking needs. We hope to have your service restored as soon as possible. Please be assured that any payments or transfers that you previously scheduled for today will be processed as normal.

Thank you for your patience as we work to implement these changes for you.

At this time we need you to confirm your e-mail address with our existing database. As soon as our database will be updated we need to make few

important announcements to our customers so please update your contact information with no delay.

Once you have completed these steps, we will send you an email notifying that online banking and bill payment service is available again.

The information provided will be treated in confidence and stored in our secure database. **If you fail to provide information about your account you'll discover that your account has been automatically deleted from our database.**

Please click on the link below to start the update process:

19. At approximately the same time that the spam email purporting to be from the Brattleboro S&L was sent, the defendants also disabled the real website of the Brattleboro S&L through a denial-of-service attack. In particular, the real website, which is hosted in Avon, Connecticut, was sent a large volume of spurious Internet traffic that was intended to, and which had the effect of, rendering the website inaccessible to the legitimate customers of Brattleboro S&L.

20. Other financial institutions or Internet companies targeted by the defendants' phishing scheme included Ebay/PayPal, Capital One, Citibank, JPMorgan Chase & Co., Comerica Bank, LaSalle Bank, U.S. Bank, and Wells Fargo & Co.

Objects of the Conspiracy

21. From in or about 2005 through in or about 2007, in the District of Connecticut and elsewhere, CIPRIAN DUMITRU TUDOR, OVIDIU-IONUT NICOLA-ROMAN, MIHAI CRISTIAN DUMITRU, PETRU BOGDAN BELBITA, RADU-MIHAI DOBRICA, CORNEL IONUT TONITA, and CRISTIAN

NAVODARU, defendants herein, and others known and unknown, knowingly did conspire, combine, confederate, and agree to commit offenses against the United States, to wit:

- a. knowingly and with intent to defraud, and affecting interstate and foreign commerce, to traffic in and use one and more unauthorized access devices during any one-year period, and by such conduct, to obtain one and more things of value aggregating \$1,000 and more during that period, in violation of Title 18, United States Code, Section 1029(a)(2); and
- b. knowingly and with intent to defraud, and affecting interstate and foreign commerce, to possess fifteen and more counterfeit access devices, in violation of Title 18, United States Code, Section 1029(a)(3).

Manner and Means of the Conspiracy

22. It was a part of the conspiracy that CIPRIAN DUMITRU TUDOR, OVIDIU-IONUT NICOLA-ROMAN, MIHAI CRISTIAN DUMITRU, PETRU BOGDAN BELBITA, RADU-MIHAI DOBRICA, CORNEL IONUT TONITA, and CRISTIAN NAVODARU, defendants herein, and others known and unknown:

- a. devised fraudulent email messages with false header information to induce individual recipients of the messages to click on a link, which would lead to one or

- more fraudulent Web pages requesting the individual's private personal and financial information;
- b. created fraudulent Web pages and gained unauthorized access to Internet servers which they used to host the fraudulent Web pages;
 - c. collected and shared the private personal and financial information that was fraudulently obtained;
 - d. used the private personal and financial information that was fraudulently obtained to access bank accounts and lines of credit and to withdraw funds without authorization; and
 - e. collected and shared the tools, including files, software programs, and email accounts, used to facilitate the phishing scheme.

Overt Acts

23. In furtherance of the conspiracy, and in order to effectuate the objects thereof, CIPRIAN DUMITRU TUDOR, OVIDIU-IONUT NICOLA-ROMAN, MIHAI CRISTIAN DUMITRU, RADU-MIHAI DOBRICA, PETRU BOGDAN BELBITA, CORNEL IONUT TONITA, and CRISTIAN NAVODARU, defendants herein, and others known and unknown, committed the following overt acts, among others, within the District of Connecticut and elsewhere:

- a. In or about June, 2005, one or more of the co-conspirators transmitted a spam email purporting to be

from People's Bank to an individual in Madison, Connecticut.

- b. In or about June, 2005, one or more of the co-conspirators withdrew \$3,409.99 from the account of a People's Bank customer without authorization, using ATM machines in Craiova, Romania and private personal and financial information that had been obtained through phishing.
- c. In or about October, 2006, MIHAI CRISTIAN DUMITRU accessed the collector account "pulawork@yahoo.com" from an IP address assigned to Romania.
- d. In or about March, 2006, CIPRIAN DUMITRU TUDOR and OVIDIU-IONUT NICOLA-ROMAN accessed the collector account "fly4hell@yahoo.com" from IP addresses assigned to Romania.
- e. In or about January, 2006, CIPRIAN DUMITRU TUDOR and OVIDIU-IONUT NICOLA-ROMAN accessed the collector account "vercartil@yahoo.com" from IP addresses assigned to Romania.
- f. In or about February, 2006, CIPRIAN DUMITRU TUDOR sent an email message to PETRU BOGDAN BELBITA which contained tools designed for phishing against Bank of America.

- g. In or about April, 2006, RADU-MIHAI DOBRICA sent an email message to OVIDIU-IONUT NICOLA-ROMAN which contained two Visa credit card numbers with associated Social Security numbers, dates of birth, CVV codes, and PIN numbers.
- h. In or about July, 2005, CORNEL IONUT TONITA forwarded an email message containing bank identification numbers to CRISTIAN NAVODARU that TONITA had received from CIPRIAN DIMUTRU TUDOR.
- i. In or about October, 2006, one or more of the co-conspirators caused to be transmitted a large volume of spurious Internet traffic to the Brattleboro S&L Internet site, rendering the site inaccessible, while sending at approximately the same time, spam emails stating that online banking and bill paying services were unavailable.

All in violation of Title 18, United States Code, Section 1029(b)(2).

COUNT TWO

(Conspiracy to Commit Bank Fraud)

24. Each allegation set forth in paragraphs 1 through 20 is incorporated as if fully set forth herein.

Objects of the Conspiracy

25. From in or about 2005 through in or about 2007, in the District of Connecticut and elsewhere, CIPRIAN DUMITRU TUDOR,

OVIDIU-IONUT NICOLA-ROMAN, MIHAI CRISTIAN DUMITRU, PETRU BOGDAN BELBITA, RADU-MIHAI DOBRICA, CORNEL IONUT TONITA, and CRISTIAN NAVODARU, defendants herein, and others known and unknown, knowingly did conspire, combine, confederate, and agree to commit an offense against the United States, to wit:

- a. knowingly to execute, and attempt to execute, a scheme to defraud a financial institution, and to obtain moneys, funds, credits, assets, and other property owned by, and under the custody and control of, a financial institution, by means of material false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344.

Manner and Means of the Conspiracy

26. Each allegation set forth in paragraph 22 is incorporated as if fully set forth herein.

Overt Acts

27. Each allegation set forth in paragraph 23 is incorporated as if fully set forth herein.

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

COUNT THREE

(Aggravated Identity Theft)

28. Each allegation set forth in paragraphs 1 through 21 is incorporated as if fully set forth herein.


29. From in or about 2005 through in or about 2007, in the District of Connecticut and elsewhere, CIPRIAN DUMITRU TUDOR, OVIDIU-IONUT NICOLA-ROMAN, MIHAI CRISTIAN DUMITRU, PETRU BOGDAN BELBITA, RADU-MIHAI DOBRICA, CORNEL IONUT TONITA, and CRISTIAN NAVODARU, defendants herein, knowingly did transfer, possess, and use, without lawful authority, a means of identification of another person, to wit, names, Social Security account numbers, credit card numbers, personal identification numbers, and dates of birth, during and in relation to violations of Title 18, United States Code, Section 1029, conspiracy to commit fraud in connection with access devices, as charged in Count 1 of this Indictment.

In violation of Title 18, United States Code, Section
1028A(a)(1) and (c)(4).

A TRUE BILL

FOREPERSON

UNITED STATES OF AMERICA


KEVIN J. O'CONNOR
UNITED STATES ATTORNEY

ANTHONY E. KAPLAN
SUPERVISORY ASSISTANT
UNITED STATES ATTORNEY


EDWARD CHANG
ASSISTANT UNITED STATES ATTORNEY