

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA

v.

**SERGEY VOVNENKO,
a/k/a "Sergey Vovnencko,"
a/k/a "Tomas Rimkis,"
a/k/a "Flycracker,"
a/k/a "Flyck,"
a/k/a "Fly,"
a/k/a "Centurion,"
a/k/a "MUXACC1,"
a/k/a "Stranier," and
a/k/a "Darklife"**

: Hon.

: Criminal Number:

14-cr-237(FSH)

: 18 U.S.C. § 1028A(a)(1)

: 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(i)

: 18 U.S.C. § 1349

: 18 U.S.C. § 2

I HEREBY CERTIFY that the above and foregoing is a true and correct copy of the original on file in my office.

ATTEST

WILLIAM T. WALSH, Clerk
United States District Court
District of New Jersey

By:

William T. Walsh
Deputy Clerk

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges:

COUNT ONE

(Wire Fraud Conspiracy)
(18 U.S.C. § 1349)

OVERVIEW OF THE HACKING CONSPIRACY

1. From at least as early as in or about September 2010 through at least as late as August 2012, defendant SERGEY VOVNENKO, a/k/a "Sergey Vovnencko," a/k/a "Tomas Rimkis," a/k/a "Flycracker," a/k/a "Flyck," a/k/a "Fly," a/k/a "Centurion," a/k/a "MUXACC1," a/k/a "Stranier," and a/k/a "Darklife," ("VOVNENKO") and his co-conspirators operated an international criminal organization that hacked into the computers of individual users and of companies in the United States and elsewhere, and used that access to steal data, including, among other things, user names and passwords for bank accounts and other online services ("Log-In Credentials") as well as debit and credit card numbers and related personal identifying information ("Payment Card Data").

2. After stealing the Log-In Credentials and Payment Card Data, defendant

VOVNENKO and his co-conspirators used that information to illegally access and withdraw money from bank accounts and to incur unauthorized charges using the Payment Card Data. Defendant VOVNENKO and his co-conspirators also sold the stolen Log-In Credentials and Payment Card Data using on-line forums and other means to individuals and groups that, in turn, used the stolen information to illegally access and withdraw money from bank accounts and to incur unauthorized charges using the Payment Card Data.

RELEVANT ENTITIES, INDIVIDUALS, AND TERMS

3. At various times relevant to this Indictment:

a. VOVNENKO resided in or near Naples, Italy. As set forth more fully below, defendant VOVNENKO was a computer hacker who was part of a sophisticated group that specialized in penetrating and gaining access to the computer networks of multinational corporations; harvesting data, including Log-In Credentials and Payment Card Data from within the compromised networks; and exfiltrating that data out of the compromised networks. In addition, defendant VOVNENKO sold, among other things, stolen Log-In Credentials and Payment Card Data and administered websites that facilitated the sale of such data as well as the purchase of hacking services.

b. Victim #1 was a global financial institution, as defined in Title 18, United States Code, Section 20, with millions of customer accounts. Victim #1 maintained significant infrastructure in New Jersey, including computer servers housing banking information located in New Jersey.

c. "Malware" was malicious computer software programmed to, among other things, gain unauthorized access to computers and to identify, store, and export information from hacked computers, including Payment Card Data.

d. A “botnet” was a collection of computers infected with malware without the users’ authorization and controlled by a hacker using a central “command and control” computer.

e. An Internet Protocol address (or “IP” address) was a unique numeric address (e.g., 123.45.67.891) used by computers connected to the Internet.

THE CONSPIRACY

4. From at least as early as in or about September 2010 through at least as late as in or about August 2012, in Somerset County, in the District of New Jersey, and elsewhere, defendant

**SERGEY VOVNENKO,
a/k/a “Sergey Vovnencko,”
a/k/a “Tomas Rimkis,”
a/k/a “Flycracker,”
a/k/a “Flyck,”
a/k/a “Fly,”
a/k/a “Centurion,”
a/k/a “MUXACC1,”
a/k/a “Stranier,” and
a/k/a “Darklife,”**

did knowingly and intentionally conspire and agree with others to devise a scheme and artifice to defraud and to obtain money and property from Victim #1 and other corporations, their customers, and the financial institutions that issued credit and debit cards to those customers, by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing the scheme and artifice to defraud, transmitted and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

OBJECT OF THE CONSPIRACY

5. It was the object of the conspiracy for defendant VOVNENKO and others to

hack into the computer networks of Victim #1 and other corporations in order to steal and then sell Log-In Credentials and Payment Card Data, or to otherwise profit from their unauthorized access.

MANNER AND MEANS OF THE CONSPIRACY

6. The manner and means by which defendant VOVNENKO and others, sought to accomplish the conspiracy included, among other things, the following.

7. It was part of the conspiracy that to facilitate intrusions into the computer networks of financial institutions, defendant VOVNENKO controlled a botnet of over 13,000 computers infected with malware. Several of the infected computers were in New Jersey.

8. It was further part of the conspiracy that one of the forms of malware that defendant VOVNENKO and others installed on infected computers was known as "Zeus," which was malware designed to steal banking information and record the keystrokes of the users of infected computers.

9. It was further part of the conspiracy that the Log-In Credentials and Payment Card Data that was captured using malware, including the Zeus malware, was sent to defendant VOVNENKO and others.

10. It was further part of the conspiracy that defendant VOVNENKO and others used the stolen Log-In Credentials and Payment Card Data to illegally access and withdraw money from bank accounts and to incur unauthorized charges using the Payment Card Data.

11. It was further part of the conspiracy that defendant VOVNENKO and others also sold the Log-In Credentials and Payment Card Data for a profit.

12. It was further part of the conspiracy that defendant VOVNENKO and

others participated in on-line criminal forums, including Forum #1, Forum #2, and Forum #3 (collectively the "Criminal Forums"). Indeed, defendant VOVNENKO was a high-level administrator of Forum #1 and Forum #2. These forums featured electronic bulletin boards which members used to publicly communicate with all members and also provided the ability to send private messages directly to individual members. The public and private discussions on the Criminal Forums typically pertained to criminal activity, including the purchase, sale, and use of stolen Log-In Credentials and Payment Card Data, as well as discussions related to cybercrime activity such as malicious computer hacking. For example, in or about August 2012, Forum #1 offered various illicit products for sale, including access to compromised computer servers located in the United States. A price was listed for each product, and customers could click an "order" button and purchase the product using "credits" associated with their accounts.

13. It was further part of the conspiracy that defendant VOVNENKO administered and advertised servers that cybercriminals used to discuss criminal activity and to traffic in stolen Log-In Credentials and Payment Card Data via instant messaging (collectively the "Jabber Servers"). Typically, introductions between criminals who were buying or selling Log-In Credentials and Payment Card Data were made on the Criminal Forums. However, the criminals used a more secure mode of communication after initial introductions were made on the forums. These criminals typically used instant messaging servers, using a protocol known as "Jabber," to make and finalize transactions in stolen data. Criminals often use these services because a Jabber server can offer end-to-end encryption of communication, and can be created and hosted by anyone, including the criminals themselves.

14. It was further part of the conspiracy that defendant VOVNENKO and

others used their access to the Criminal Forums, and defendant VOVNENKO used his role as an administrator of Forum #1, Forum #2 and the Jabber Servers to traffic in stolen Log-In Credentials and Payment Card Data.

The Hack of Victim #1

15. It was further part of the conspiracy that the malware that defendant VOVNENKO used to create his botnet infected several computers at Victim #1 in or about 2011, including computers in New Jersey.

16. It was further part of the conspiracy that on or about March 2, 2011, defendant VOVNENKO and his co-conspirators used malware residing on an infected computer at Victim #1 to capture Log-In Credentials belonging to an employee of Victim #1 with the initials "J.H." and exfiltrated that information to a server controlled by defendant VOVNENKO and his co-conspirators.

17. It was further part of the conspiracy that on or about March 3, 2011, defendant VOVNENKO and a co-conspirator discussed how best to use the computers the malware had infected at Victim #1 and worked together to upload additional malware to Victim #1's computers. Defendant VOVNENKO also provided a co-conspirator with access to the list of computers that his botnet controlled. Defendant VOVNENKO and a co-conspirator then compared the IP addresses of infected computers against a public database to determine whether the botnet controlled infected computers located inside financial institutions or other significant corporate entities.

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

COUNT TWO

(Unauthorized Computer Access)
(18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(i))

1. The allegations set forth in Paragraphs 1 through 3 and 5 through 17 of Count One are hereby repeated, realleged, and incorporated as if fully set forth herein.
2. On or about March 2, 2011, in Somerset County, in the District of New Jersey, and elsewhere, defendant

**SERGEY VOVNENKO,
a/k/a "Sergey Vovnencko,"
a/k/a "Tomas Rimkis,"
a/k/a "Flycracker,"
a/k/a "Flyck,"
a/k/a "Fly,"
a/k/a "Centurion,"
a/k/a "MUXACC1,"
a/k/a "Stranier," and
a/k/a "Darklife,"**

by means of interstate communications, did intentionally access protected computers without authorization, and exceeded authorized access, namely the computer systems used in and affecting interstate and foreign commerce and communication owned by Victim #1 and thereby obtained information from those computers, namely Log-In Credentials, for the purpose of commercial advantage and private financial gain.

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

COUNTS THREE THROUGH SIX

(Aggravated Identity Theft)
(18 U.S.C. §§ 1028A(a)(1))

1. The allegations set forth in Paragraphs 1 through 3 and 5 through 17 of Count One are hereby repeated, realleged, and incorporated as if fully set forth herein.

2. On or about the dates set forth below, in the District of New Jersey and elsewhere, the defendant

**SERGEY VOVNENKO,
a/k/a "Sergey Vovnencko,"
a/k/a "Tomas Rimkis,"
a/k/a "Flycracker,"
a/k/a "Flyck,"
a/k/a "Fly,"
a/k/a "Centurion,"
a/k/a "MUXACC1,"
a/k/a "Stranier," and
a/k/a "Darklife,"**

during and in relation to felony violations of 18 U.S.C. § 1349 and 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(i), as set forth in Counts One and Two of this Indictment, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, as set forth in the individual counts below:

COUNT	APPROXIMATE DATE	MEANS OF IDENTIFICATION
3	March 2, 2011	Log-In Credentials belonging to an individual with the initials "J.H." for the website of a bank.
4	March 4, 2011	Log-In Credentials belonging to an individual with the initials "J.H." for the website of a health insurance plan.
5	March 10, 2011	Log-In Credentials belonging to an individual with the initials "J.H." for internal company resource #1 at Victim #1.
6	March 14, 2011	Log-In Credentials belonging to an individual with the initials "J.H." for internal company resource #2 at Victim #1.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

FORFEITURE ALLEGATION
(COUNTS ONE AND THREE THROUGH SIX)

1. Upon conviction of one or more of the offenses alleged in Counts One and Three through Six of this Indictment, defendant SERGEY VOVNENKO shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such violations.

FORFEITURE ALLEGATION
(COUNT TWO)

2. Upon conviction of the offense alleged in Count Two of this Indictment, defendant SERGEY VOVNENKO shall forfeit to the United States, pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense, and any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense.

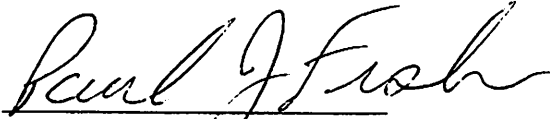
SUBSTITUTE ASSETS PROVISION

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

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third person;
- (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;

it is the intent of the United States, pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. § 982(b), to seek forfeiture of any other property of said defendant up to the value of the above forfeitable property.

A True Bill,



PAUL J. FISHMAN
United States Attorney

PageID: 19

CASE NUMBER: *14-Cr-237(FSH)*

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

SERGEY VOVNENKO,
a/k/a "Sergey Vovnencko,"
a/k/a "Tomas Rimkis,"
a/k/a "Flycracker,"
a/k/a "Flyck,"
a/k/a "Fly,"
a/k/a "Centurion,"
a/k/a "MUXACCI,"
a/k/a "Stranier," and
a/k/a "Darklife"

INDICTMENT FOR

18 U.S.C. § 1028A(a)(1)
18 U.S.C. § 1030(a)(2)(C)
18 U.S.C. § 1349
18 U.S.C. § 2

PAUL J. FISHMAN
U.S. ATTORNEY
NEWARK, NEW JERSEY

DANIEL SHAPIRO
ASSISTANT U.S. ATTORNEY
(973) 353-6087

USA-48AD 8
(Ed. 1/97)
