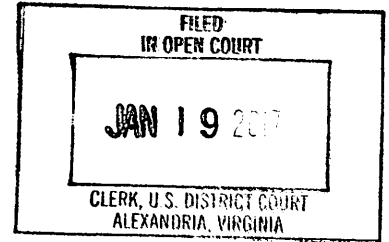


IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA



Alexandria Division

UNITED STATES OF AMERICA

v.

ALEXANDER KONSTANTINOVICH
TVERDOKHLEBOV,

Defendant

CRIMINAL NO.: 1:17-CR-9

Counts 1-4: Wire Fraud (18 U.S.C. § 1343)

Forfeiture Notice

Filed Under Seal

JANUARY TERM 2017 – AT ALEXANDRIA, VIRGINIA

INDICTMENT

At all times relevant to this Indictment:

1. The defendant, ALEXANDER TVERDOKHLEBOV, was a Russian national residing in California.
2. V.P. was a Russian national residing outside of the United States.
3. “ICQ” was a brand of software used for instant chat messaging. At all times relevant to this Indictment, ICQ transmitted and received all communications between its users through servers located in Dulles, Virginia, within the Eastern District of Virginia.
4. The term “botnet” refers to a group of computers (known as “bots”) that have been infected with malicious software that typically allows the operator of the botnet to covertly access the bots and steal information, such as online banking passwords and login credentials. Botnet operators frequently use the stolen information to commit fraud, or to sell to others who intend to use the information to commit fraud.
5. From on or about May 2008 through on or about February 2010, TVERDOKHLEBOV used ICQ to communicate with V.P. for the purposes of devising and

executing a scheme to defraud. In particular, TVERDOKHLEBOV devised a scheme to defraud whereby he used a botnet, and similar methods of unlawful computer intrusions, to steal passwords and login credentials for online banking accounts. As part of the scheme, TVERDOKHLEBOV, and accomplices such as V.P., would then use the stolen passwords and login credentials to make fraudulent purchases and/or fraudulent withdrawals from the victim's online banking accounts.

6. As stated in paragraph 3 above, each ICQ message between TVERDOKHLEBOV and V.P. caused a wire communication to be transmitted into and out of servers located in the Eastern District of Virginia.

COUNTS ONE THROUGH FOUR
(Wire Fraud)

THE GRAND JURY CHARGES THAT:

7. The factual allegations in Paragraphs 1 through 6 are re-alleged and incorporated as if fully set forth here.

8. On or about the dates set forth below, each date constituting a separate count, in the Eastern District of Virginia and elsewhere, the defendant, ALEXANDER TVERDOKHLEBOV, having devised and intending to devise a scheme or artifice to defraud, and for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, namely, the fraudulent scheme described in paragraph 5 above, transmitted and caused to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme or artifice. At all times, the scheme described in this paragraph and paragraph 5 above affected a financial institution, as used in 18 U.S.C. § 1343 and defined in 18 U.S.C. § 20.

9. In particular, TVERDOKHLEBOV sent the following wire transmissions, via the instant messaging service ICQ, to his accomplice V.P. for the purpose of executing the scheme described in paragraphs 5 and 8 above. Each message was transmitted into and out of servers located in the Eastern District of Virginia.

| Count | Date | Description of Wire Transmissions |
|-------|------------|---|
| 1 | 10/28/2008 | TVERDOKHLEBOV sent ICQ messages to V.P. providing V.P. with stolen online banking passwords and login credentials and asking for assistance in making fraudulent transfers of funds from the compromised account. |
| 2 | 10/29/2008 | TVERDOKHLEBOV sent ICQ messages to V.P. discussing how they could use a botnet to steal online banking passwords and login credentials for the purpose of engaging in fraudulent transactions. |
| 3 | 11/15/2008 | TVERDOKHLEBOV sent ICQ messages to V.P. discussing which method should be used to mine stolen data to find the victims' online banking passwords and login credentials. |
| 4 | 11/17/2008 | TVERDOKHLEBOV sent ICQ messages to V.P. telling him how to access banking passwords and login credentials that had been stolen through their botnet and directing V.P. to make fraudulent purchases using these stolen passwords and credentials. |

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

NOTICE OF FORFEITURE

1. There is probable cause that the property described in this NOTICE OF FORFEITURE is subject to forfeiture pursuant to the statutes described herein.
2. Upon conviction of any of the offenses set forth in Counts 1 through 4 of this Indictment, the defendant, ALEXANDER TVERDOKHLEBOV, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(2)(A), any property constituting, or derived from, proceeds traceable to such violation, and pursuant to Title 18, United States Code, Section 1029(c)(1)(C), any personal property used or intended to be used to commit the offense.
3. The defendant is hereby notified, pursuant to Fed.R.Crim.P. 32.2(a), that upon conviction of any count in this Indictment, the defendant, ALEXANDER TVERDOKHLEBOV, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(2)(A), any property constituting, or derived from, proceeds the person obtained directly or indirectly, as the result of such violation.
4. If any of the property described above as being forfeitable pursuant to Title 18, United States Code, Section 982(a)(2)(A) and (B) and 1029(c)(1)(C), 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 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 intention of the United States of America, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and

1029(c)(2), to seek forfeiture of all other property of the defendant as described in paragraph 3 above.

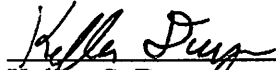
(All pursuant to Title 18, United States Code, Sections 982(a)(2)(A) and (B); and 1029(c)(1)(C))

A TRUE BILL:

Pursuant to the E-Government Act,
the original of this page has been filed
under seal in the Clerk's Office.

Foreperson of the Grand Jury

DANA J. BOENTE
UNITED STATES ATTORNEY



Kellen S. Dwyer

Laura Fong

Assistant United States Attorneys