

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

Alexandria Division

UNITED STATES OF AMERICA

v.

Ruslan Yeliseyev,
a/k/a, Ruslan Eliseev,
a/k/a, Ruslan Yeliseev, and
a/k/a, Ruslan Yeliseiev
Defendant.

CRIMINAL NO.: 1:16-CR-310

Count 1: Conspiracy to Commit Wire Fraud
(18 U.S.C. § 1349)

Count 2: Wire Fraud
(18 U.S.C. §§ 1343 and 2(a))

Count 3: Access Device Fraud
(18 U.S.C. §§ 1029(a)(3) and 2(a))

Forfeiture Notice

DECEMBER TERM – AT ALEXANDRIA, VIRGINIA

INDICTMENT

THE GRAND JURY CHARGES THAT:

At all times material to this Indictment:

1. Defendant RUSLAN YELISEYEV, a/k/a “Ruslan Eliseev,” a/k/a “Ruslan Yeliseev,” a/k/a “Ruslan Yeliseiev,” is a Ukrainian national that has resided in Odessa, Ukraine.
2. The term “carding” refers to various criminal activities associated with stealing, typically through computer hacking, financial information and personal identification information belonging to other individuals, including information associated with credit cards, bank cards, debit cards, or other access devices (collectively, “payment cards”) – and using that

information to obtain money, goods, or services without the victims' authorization or consent.

The stolen payment card information often includes, among other things, the card type (e.g., credit or debit), account holder's name, account number, card verification value or code, and the expiration date of the card.

3. In a typical payment card transaction, after a payment card is swiped through a magnetic stripe reader, the software at the point-of-sale terminal transmits payment card information and transactional information (e.g., price and merchant identification number) electronically to an acquirer. An acquirer is a financial institution that initiates and maintains contractual agreements with merchants for the purpose of accepting and processing payment card transactions. The acquirer electronically routes the transactional and payment card information it receives through the appropriate card network (e.g., Banknet for MasterCard and VisaNet for Visa cards) to the cardholder's issuing bank to be approved or declined. The credit card issuer receives the transaction information through the card network and checks, among other things, whether the transaction is valid, the cardholder has a sufficient balance, and the account is in good standing. The card issuer then electronically transmits an approval or declination response code through the appropriate card network to the acquirer, which forwards it to the merchant.

4. The terms "track data" or "dumps" refer to data that is encoded on the magnetic stripe on the back of a stolen payment card. Track data contains information including the card number and expiration date, and certain personally identifiable information ("PII") of the account holder. Track data can be used to create a counterfeit payment card that can be used to make an in-person purchase at a retail location. The terms "cc" or "fullz" refer to information from a stolen payment card that can be used to make purchases over the Internet, often referred to as "Card Not Present" or "CNP" transactions, which include the account number, expiration

date, certain PII of the account holder, as well as a card verification code, usually printed on the back of the card, that is often referred to as the “CVC” or “CVV” code.

5. The term “card shop” refers to an online store that sells stolen payment card information. Card shops often sell both stolen track data and cc data.

6. The term “carding forum” refers to black market websites where subjects involved in payment card fraud came together to discuss and commit criminal activities typically related to payment card fraud, computer hacking, and other related criminal activity.

7. The term “botnet” refers to a network of hacked computers. Cybercriminals oftentimes install malware onto the victim computers of a botnet designed to steal the victim users’ login credentials to online accounts, including their “financial accounts,” which include online banking accounts or any other account capable of being used to receive or send funds.

8. The term “account takeovers” refers to the unauthorized use of an online financial account for the purpose of unlawfully siphoning funds from the account, or for the purpose of transferring funds through an account in order to launder the proceeds of criminal activity.

9. At all times material to this Indictment, the data center of a particular online instant messaging service (“Instant Messaging Service”) that was used to transmit and receive all communications between its users was located in Dulles, Virginia, in the Eastern District of Virginia.

10. At all times material to this Indictment, the data centers of a particular major U.S. credit card company (“Company-A”) for processing payment card transactions were located in Richmond, Virginia, in the Eastern District of Virginia and elsewhere.

11. YELISEYEV was an online vendor of stolen payment card information who advertised his services on a number of Russian-speaking cybercrime forums. YELISEYEV

obtained the stolen payment card information that he sold through a number of different sources, including through a card shop known as Cardplanet LLC and Cardplanet.cc (“Cardplanet”), which did business through the website www.Cardplanet.cc (the “Cardplanet Website”). The Cardplanet Website, which contained the user interface for customers who bought stolen payment card data, was hosted on a server located outside the United States. Cardplanet sold payment card data for U.S. payment cards, including cards under the Company-A brand. YELISEYEV also used one or more botnets, which gave YELISEYEV and his co-conspirators access to at least 40,000 hacked computers, to steal online credentials of the botnet victims in order to illegally profit from unauthorized account takeovers. To date, YELISEYEV’s criminal conduct is estimated to have caused over \$38,000,000 in losses to various financial institutions and botnet victims.

COUNT ONE

(Conspiracy to Commit Wire Fraud)

12. From at least early February 2008 through at least June 2014, in the Eastern District of Virginia and elsewhere, the defendant,

**RUSLAN YELISEYEV,
a/k/a, "Ruslan Eliseev,"
a/k/a, "Ruslan Yeliseev," and
a/k/a "Ruslan Yeliseiev,"**

did knowingly combine, conspire, confederate, and agree, with other persons known and unknown to the Grand Jury, to devise and intend to devise a scheme and artifice to defraud, and for obtaining money and property, to wit, to obtain stolen payment card information and online credentials for financial accounts for the purpose of using said information to enter into unauthorized financial transactions, such scheme affecting a financial institution, by means of materially false and fraudulent pretenses, representations, and promises, 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 writings, signs, signals, pictures, and sounds, to wit, the transmission via the Internet of stolen payment card information from an overseas server, in violation of Title 18, United States Code, Section 1343.

Manner and Means

13. As a part of the fraudulent scheme, YELISEYEV gained membership to multiple carding forums and used his memberships to advertise the sale of stolen payment card information.

14. As a part of the fraudulent scheme, YELISEYEV became a member of the Cardplanet Website in order to purchase stolen payment card data that he and other co-

conspirators used to enter into unauthorized transactions. YELISEYEV used his membership to purchase stolen payment card information for approximately 213 accounts. YELISEYEV also used a fee-based service offered by the Cardplanet Website to its customers called “checker,” which allowed YELISEYEV to instantly validate stolen payment card information that he purchased.

15. Through his membership in various carding forums, YELISEYEV offered for sale data for approximately 62,000 compromised payment cards – including cards branded in the names of the largest credit card companies in the United States – knowing that such stolen data would be used to make fraudulent purchases.

16. As a further part of the fraudulent scheme, YELISEYEV and others used the stolen payment card data to enter into fraudulent transactions that were processed through Company-A’s credit card processing facility in the Eastern District of Virginia.

17. As a further part of the fraudulent scheme, YELISEYEV had access to 40,000 hacked computers through the use of one or more botnets. YELISEYEV used such access to steal online financial account credentials for numerous botnet victims, and then used those stolen credentials to take over such accounts and to withdraw funds from them without authorization.

Overt Acts

18. It was a further part of the conspiracy that the following acts in furtherance of and to effect the object of the above-described conspiracy were committed in the Eastern District of Virginia and elsewhere:

a. Between in or about February 2008 through October 2009 YELISEYEV used one or more botnets to steal login credentials for financial accounts from the legitimate users of hacked computers. On or about July 30, 2008, YELISEYEV, using one of his Instant

Messaging Service accounts, provided stolen login credentials belonging to a U.S. victim to another co-conspirator.

b. On or about May 3, 2010, YELISEYEV responded to two separate postings related to the purchase and sale of stolen payment card information on a Russian-language carding forum. In response to these solicitations to purchase or sell stolen payment card information, YELISEYEV requested that the poster contact him through one of his Instant Messaging Service accounts.

c. On or about June 22, 2010, YELISEYEV made a posting on a Russian-language carding forum under the topic "Buying/selling cards" that he was looking for a "wholesale" purchaser to buy a database of stolen payment card information relating to approximately 12,000 accounts with account holders from United States.

d. Between on or about November 23, 2011 and on or about June 11, 2012, YELISEYEV purchased stolen payment card information relating to approximately 213 accounts, with account holders from the United States, from a co-conspirator, not named as a defendant herein, who ran the Cardplanet Website. Many of these accounts were for credit card accounts processed by Company-A and were used by YELISEYEV and others to enter into fraudulent transactions with online merchants utilizing servers outside of the Commonwealth of Virginia, that were processed through Company-A's credit card processing facility in the Eastern District of Virginia.

e. On or about December 8, 2011, YELISEYEV made a posting on a Russian-language carding forum advertising the sale of data stolen from botnet victims containing stolen login information relating to thousands of financial accounts.

f. On or about June 19, 2014, YELISEYEV made a posting on a Russian-language carding forum under the topic “Buying/selling cards” that he was looking for a “wholesale” purchaser to buy stolen payment card related information relating to approximately 50,000 accounts with account holders from the United States, Europe, and Asia.

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

COUNT TWO

(Wire Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

19. The factual allegations in Paragraphs 1 through 11 and 13 through 18 are re-alleged and incorporated as if fully set forth here.

20. From at least early February 2008 through at least June 2014,

**RUSLAN YELISEYEV,
a/k/a, "Ruslan Eliseev,"
a/k/a, "Ruslan Yeliseev," and
a/k/a "Ruslan Yeliseiev,"**

did knowingly devise and intend to devise a scheme and artifice to defraud, and for obtaining money and property, to wit, the scheme described in Paragraphs 13 to 18, such scheme affecting a financial institution, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, and attempting to do so, did transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, to wit, payment card-related information was transmitted via the Internet to online merchants utilizing servers outside the Commonwealth of Virginia, which were processed through Company-A's credit card processing facility in the Eastern District of Virginia.

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

COUNT THREE

(Access Device Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

21. The factual allegations in Paragraphs 1 through 11 and 13 through 18 are re-alleged and incorporated as if fully set forth here.

22. From on or about November 23, 2011 through on or about June 11, 2012,

**RUSLAN YELISEYEV,
a/k/a, "Ruslan Eliseev,"
a/k/a, "Ruslan Yeliseev," and
a/k/a "Ruslan Yeliseiev,"**

knowingly and with intent to defraud, did possess fifteen or more unauthorized access devices, to wit, lines of credit associated with numerous payment cards, said possession affecting interstate and foreign commerce, in that the unauthorized access devices were transmitted via the Internet.

(All in violation of Title 18, United States Code, Sections 1029(a)(3) and 2(a))

NOTICE OF FORFEITURE

THE GRAND JURY HEREBY FINDS THAT:

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. The defendant is hereby notified, pursuant to Fed.R.Crim.P. 32.2(a), that upon conviction of the offense set forth in Count 1 and Count 2 of this Indictment, the defendant,

**RUSLAN YELISEYEV,
a/k/a, "Ruslan Eliseev,"
a/k/a, "Ruslan Yeliseev," and
a/k/a "Ruslan Yeliseiev,"**

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), any property, real or personal, constituting, or derived from, proceeds traceable to such violation.

3. Upon conviction of the offense set forth in Count 3 of this Indictment, the defendant,

**RUSLAN YELISEYEV,
a/k/a, "Ruslan Eliseev,"
a/k/a, "Ruslan Yeliseev," and
a/k/a "Ruslan Yeliseiev,"**

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(2)(B), any property, real or personal, involved in such violation, or any property traceable to such property; 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 described in Count 2 of this Indictment.

4. If any of the property described above as being forfeitable pursuant to Title 18, United States Code, Section 981(a)(1)(C); 982(a)(2)(B); 1029(c)(1)(C); and Title 28, United States Code, Section 2461(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 28, United States Code, Section 2461(c); and Title 18, United States Code, Sections 982(b)(1) and 1029(c)(2), to seek forfeiture of all other property of the defendant up to the value of the above-described property.

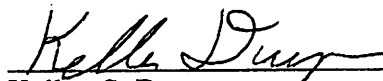
(All pursuant to Title 18, United States Code, Sections 981(a)(1)(C); 982(a)(2)(B); 1029(c)(1)(C), and Title 28, United States Code, Section 2461(c))

A TRUE BILL:

Payment to the Government of
the original of this page has been
under seal in the Clerk's Office

Foreperson of the Grand Jury

DANA J. BOENTE
UNITED STATES ATTORNEY



Kellen S. Dwyer
Assistant United States Attorney

James Silver, Deputy Chief
Andrew S. Pak, Trial Attorney
U.S. Department of Justice
Computer Crime & Intellectual Property Section