REDACTED

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

Alexandria Division

UNITED STATES OF AMERICA

v.

ALEKSANDR BROVKO,

a/k/a,

Александр Владимирович БРОВКО,

a/k/a,

Alexander Brovko,

Defendant.

CRIMINAL NO.: 1:18-CR-407

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

Count 2: Conspiracy to Commit Access Device Fraud (18 U.S.C. § 1029(b)(2))

Forfeiture Notice

Filed Under Seal

NOVEMBER TERM 2018 – AT ALEXANDRIA, VIRGINIA

INDICTMENT

At all times relevant to this Indictment:

1. The defendant, ALEKSANDR BROVKO, who also went by the names Александр Владимирович БРОВКО and Alexander Brovko, was a Russian national residing in the Czech Republic.

2. [redacted] is an individual who was indicted by a grand jury in the Eastern District of Virginia for hacking and carding-related crimes and convicted of wire fraud in 2017. At the time of all acts listed in this indictment, [redacted] was residing in California.

3. Jabber is an instant messaging platform.

4. The term "botnet" refers to a network of compromised computers (known as "bots"). Botnet operators are able to covertly access the bots for a variety of malicious purposes,

including stealing financial information, such as online banking passwords and login credentials, from the bots. Botnet operators frequently use the stolen information to commit fraud, or sell it to others who intend to use the information to commit fraud.

5. At all times material to this Indictment, the corporate headquarters of Bank A, a major bank that issues payment cards and hosts online bank accounts, were located within the Eastern District of Virginia. At all times material to this Indictment, Bank A was a "financial institution" within the meaning of 18 U.S.C. § 20 in that, among other reasons, it held funds that were insured by the Federal Deposit Insurance Corporation (FDIC).

6. At all times material to this Indictment, Bank B, a major bank based in the United States that issues payment cards, was a "financial institution" within the meaning of 18 U.S.C. § 20 in that, among other reasons, it held funds that were insured by the FDIC.

7. Forum A is an elite, members-only cybercriminal website that caters to Russian speakers. Members of the website post about topics, such as how to find vulnerabilities in certain computer operating systems, and advertise and sell hacked financial and personal data to other members.

8. Webmoney is a form of digital currency that is popular among Eastern European individuals.

COUNT ONE
(Conspiracy to Commit Wire and Bank Fraud)

THE GRAND JURY CHARGES THAT:

9. The factual allegations in paragraphs 1 through 8 are re-alleged and incorporated as if fully set forth here.

10. From at least on or about 2009 through at least on or about February 2017, the defendant, ALEKSANDR BROVKO, who will be first brought to the Eastern District of Virginia, did knowingly combine, conspire, confederate, and agree, in the Eastern District of Virginia and elsewhere, with other persons known and unknown to the Grand Jury, including [redacted], to commit the following crimes:

a. to devise and intend to devise a scheme and artifice to defraud, and for obtaining money and property, 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 counts, in violation of Title 18, United States Code, Section 1343;

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

11. The goal of the conspiracy was to make a financial profit by identifying and using stolen financial information – such as victims' bank logins and passwords, or credit card data – that was obtained from compromised computers.

Manner and Means

12. It was part of the conspiracy that [redacted] and BROVKO obtained botnet logs from other co-conspirators who operated botnets. These logs contained data stolen from the compromised computers that were part of the botnets.

13. It was further part of the conspiracy that [redacted] and BROVKO also shared botnet logs with each other.

14. It was further part of the conspiracy that [redacted] and BROVKO sifted through the botnet logs to identify stolen financial information that could be used to commit fraud.

15. It was further part of the conspiracy that once BROVKO and [redacted] identified stolen financial information in botnet logs, they would either pass it to the co-conspirator who had provided the botnet logs in exchange for a share of the profits generated from illicit transfers of money out of compromised bank accounts, or [redacted] and BROVKO would work together to make the illicit transfers of money out of the compromised bank accounts.

16. It was further part of the conspiracy that BROVKO would advertise his services – sifting through botnet logs to identify stolen financial information – on Forum A to other cybercriminals who were members of Forum A – in order to conspire with them to identify and use stolen financial information obtained from compromised computers.

17. It was further part of the conspiracy that BROVKO posted on Forum A that he had access to compromised bank account credentials and needed help in making illicit transfers

of money from those accounts so that he could find more co-conspirators to help him steal money from the online bank accounts he had identified in botnet logs.

Acts in Furtherance of Conspiracy

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

a. On or about January 5, 2011, BROVKO posted on Forum A, stating that he had access to a compromised Bank B account and was seeking to either sell the bank credentials or obtain the help of others who could transfer money out of this account.

b. On or about July 25, 2011, BROVKO posted on Forum A, offering to help other Forum A members identify stolen financial information contained within botnet logs.

c. On or about August 9, 2016, [redacted] and BROVKO discussed, via Jabber, accessing and transferring money out of compromised Bank A accounts.

d. On or about January 5, 2017, [redacted] messaged BROVKO via Jabber and provided suggestions on how to use stolen financial and personal information to establish business accounts at Bank A and commit fraud. During this exchange, BROVKO critiqued these suggestions based on tips someone had given him "about the USA" and provided alternative ideas for committing fraud.

e. On or about January 9, 2017, [redacted] forwarded BROVKO, via Jabber, stolen account information [redacted] had received from a botnet operator. BROVKO

subsequently responded that one of the accounts contained $72,000 that could be withdrawn.

f. On January 11, 2017, BROVKO sent [redacted] links to two documents via Jabber. When [redacted] asked, "What's there?" BROVKO responded, "50-300 k" and "7 accts, 6 with logins". [redacted] then forwarded this information to their co-conspirator, who was a botnet operator.

g. Between on or about February 2014 through November 2016, [redacted] sent 46 payments totaling approximately $137,000 to BROVKO's Webmoney account. These payments represented BROVKO's share of proceeds from the conspiracy described above.

(All in violation of 18 U.S.C. § 1349)

COUNT TWO
(Conspiracy to Commit Access Device Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

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

20. From at least on or about 2009 through at least on or about February 2017, the defendant, ALEKSANDR BROVKO, who will be first brought to the Eastern District of Virginia, did knowingly combine, conspire, confederate, and agree, in the Eastern District of Virginia and elsewhere, with other persons known and unknown to the Grand Jury, including [redacted], to commit the following crimes:

a. to knowingly and with intent to defraud traffic in or use one or more unauthorized access devices during any one-year period, and by such conduct obtain anything of value aggregating $1,000 or more during that period, in violation of Title 18, United States Code, Section 1029(a)(2);

b. to knowingly and with intent to defraud possess fifteen or more devices which are counterfeit or unauthorized access devices, in violation of Title 18, United States Code, Section 1029(a)(3).

21. In particular, the goal of the conspiracy was to make a financial profit by stealing financial data from networks of infected computers and then selling that stolen data to others with the intent that the stolen data be used to commit fraud and to use the stolen data themselves to commit fraud.

22. The "manner and means" of the conspiracy charged in this count are those stated in Paragraphs 12 through 17.

23. The "overt acts," or acts committed in furtherance of this conspiracy, include those alleged in Paragraph 18 above.

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

NOTICE OF FORFEITURE

The Grand Jury finds that there is probable cause that the property described in this NOTICE OF FORFEITURE is subject to forfeiture pursuant to the statutes described herein.

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

22. The defendant is hereby notified, pursuant to Fed. R. Crim. P. 32.2(a), that upon conviction of the offenses set forth in Count 2 of this Indictment, the defendant, ALEKSANDR BROVKO, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(2)(B), 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.

23. If any of the property described above as being forfeitable pursuant to Title 18, United States Code, Sections 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(a)(1), 982(b)(1) and 1029(c)(2) to seek forfeiture of all other property of the defendant as described above.

(All pursuant to Title 18, United States Code, Sections 982 and 1029)

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

G. ZACHARY TERWILLIGER
UNITED STATES ATTORNEY

Laura Fong
Kellen S. Dwyer
Assistant United States Attorneys