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

Alexandria Division

UNITED STATES OF AMERICA v. ALEKSANDR BROVKO, a/k/a, Alexander Brovko, Defendant.	CRIMINAL NO.: 1:18-CR-407

STATEMENT OF FACTS

The United States and the defendant, ALEKSANDR BROVKO ("BROVKO"), agree that the following facts are true and correct, and that had this matter proceeded to trial, the United States would have proven them beyond a reasonable doubt with admissible and credible evidence.

1. From at least on or about 2007 through at least on or about February 2019, the defendant, ALEKSANDR BROVKO, who was 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 co-conspirators to commit the following crimes:

   a. to devise or intend to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmit or cause to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of

executing such scheme or artifice, 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.

2. 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. During the conspiracy, BROVKO possessed and trafficked in at least 202,534 unauthorized access devices, specifically personally identifiable information ("PII") and financial account information stolen from victims' computers.

Manner and Means

3. As part of the conspiracy, BROVKO obtained botnet logs from other co-conspirators who operated botnets. The term "botnet" refers to a group of computers (known as "bots") that have been infected with malicious software that allows the operator of the botnet to covertly access the bots and steal information, such as online banking passwords, login credentials, and PII. Data logs from these botnets, or "botnet logs," often contained data stolen from the compromised computers, and could be used to make fraudulent financial transactions or repackaged and sold to other criminals.

4. Once BROVKO and/or his co-conspirators obtained botnet logs, they shared them with one another.

5. In order to communicate about topics such as the theft of personal and financial information from computers, the use of that stolen information to commit fraud, and the monetization of that stolen information, BROVKO and his co-conspirators used instant messaging platforms, such as ICQ and Jabber. From at least 2009 through at least August 2014, ICQ transmitted and received instant messaging communications between its users through servers located in Dulles, Virginia, as well as other locations, within the Eastern District of Virginia. ICQ communications between BROVKO and his co-conspirators during this time period caused wires to be transmitted into and outside servers located in the Eastern District of Virginia.

6. It was further part of the conspiracy that BROVKO and co-conspirators, such as a convicted cybercriminal, A.T., both manually reviewed the botnet logs and used technical means to identify stolen financial information that could be used to commit fraud.

7. It was further part of the conspiracy that once BROVKO and A.T. identified stolen financial information and PII in botnet logs, they passed the information to the co-conspirator who had provided them with the botnet logs in exchange for a share of the profits generated from illicit financial transactions accomplished using that information. Alternatively, BROVKO and A.T. worked together to conduct the fraudulent transactions themselves and provided a share of the profits to the co-conspirator who had provided them with the botnet logs.

8. It was further part of the conspiracy that BROVKO advertised his services – parsing botnet logs to identify stolen financial information – on a website referenced herein as "Forum A" in order to conspire with forum members to identify and use stolen financial information obtained from compromised computers. Forum A is an elite, members-only cybercriminal website that caters to Russian speakers. Members of the website post within the

forum about cybercrime-related topics, such as how to find vulnerabilities in certain computer operating systems, and members advertise and sell hacked financial and personal data to other members.

9. 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 making illicit transfers of money from those accounts.

Acts in Furtherance of Conspiracy

10. 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 of America account and was seeking to either sell the bank credentials or obtain the help of others who could transfer money out of this account. At all times relevant to this Statement of Facts, Bank of America 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).

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, A.T. and BROVKO communicated on Jabber, discussing how to access and transfer money out of compromised Capital One accounts. At all times relevant to this Statement of Facts, the headquarters of

Capital One, a major bank that issues payment cards and hosts online bank accounts, was located within the Eastern District of Virginia. Capital One 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.

d. On or about January 5, 2017, A.T. messaged BROVKO via Jabber and provided suggestions on how to use stolen financial and personal information to establish business accounts at Capital One and use them to 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, A.T. messaged BROVKO via Jabber and passed along stolen account information A.T. 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 A.T. links to two documents via Jabber. When A.T. asked, "What's there?" BROVKO responded, "50-300 k" and "7 accts, 6 with logins". A.T. then forwarded this information to another co-conspirator, who was a botnet operator.

g. Between on or about February 2014 through November 2016, A.T. sent 46 payments totaling approximately $137,000 to BROVKO's Webmoney account. Webmoney is a form of digital currency that is popular among Eastern European individuals. These payments represented BROVKO's share of proceeds from a portion of the activities in furtherance of conspiracy described above.

Conclusion

18. The Statement of Facts includes those facts necessary to support the defendant's guilty plea. It does not include each and every fact known to the defendant or to the government, and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

19. The actions of the defendant, as recounted above, were in all respects knowing, voluntary, and intentional, and were not committed by mistake, accident, or other innocent reason.

G. Zachary Terwilliger
United States Attorney

By: _____
Kellen S. Dwyer
Assistant United States Attorney

Laura Fong
Senior Trial Attorney
Computer Crime & Intellectual Property Section
U.S. Department of Justice

Defendant's Signature: After consulting with my attorney, and having had it explained or translated into Russian to the extent necessary, I hereby stipulate that the above Statement of Facts is true and accurate and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

SQ Date: ~~January~~ February 14, 2020

Aleksandr Brovko
Defendant

Defense Counsel Signature: I am Aleksandr Brovko's attorney. I have carefully reviewed the above Statement of Facts with him and have had it explained or translated into Russian. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

SQ Date: ~~January~~ February 20, 2020

Shannon Quill, Esq.
Counsel for the Defendant