NICHOLAS A. TRUTANICH
United States Attorney
Nevada Bar Number 13644
RICHARD B. CASPER
Assistant United States Attorney
Nevada Bar Number 8980
400 South Virginia, Suite 900
Reno, Nevada 89501
Telephone: (775) 784-5438
Richard.Casper@usdoj.gov

CANDINA S. HEATH
Senior Counsel
Computer Crime and Intellectual Property Section
U.S. Department of Justice
Washington, D.C. 20005
Telephone: (202) 307-1049
Candina.Heath2@usdoj.gov

Attorneys for Plaintiff
The United States of America

FILED ____ RECEIVED
____ ENTERED ____ SERVED ON
COUNSEL/PARTIES OF RECORD
SEP - 3 2020
CLERK US DISTRICT COURT
DISTRICT OF NEVADA
BY: _____ DEPUTY

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

UNITED STATES OF AMERICA,

Plaintiff,

vs.

EGOR IGOREVICH KRIUCHKOV,

Defendant.

3:20-CR-0045-MMD-CLB

CRIMINAL INDICTMENT

VIOLATIONS:

18 U.S.C. § 371 – Conspiracy to Intentionally Cause Damage to a Protected Computer (conspiracy to violate 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B)(i), and (c)(4)(A)(i)(I)) – Count One

THE GRAND JURY CHARGES THAT:

Introduction

1. At all times material to this Indictment:

a. EGOR IGOREVICH KRIUCHKOV was a Russian national whose residence was in Russia.

b. Victim Company A was a United States Company with a facility located in the State and District of Nevada.

c. Victim Company A maintained a corporate network, which included protected computers located in the Sparks, Nevada area.

d. The employee of Victim Company A, discussed herein, had access to at least one protected computer in Victim Company A's corporate network.

e. The employee of Victim Company A resided in and worked in Nevada.

f. A Distributed Denial of Service (DDoS) attack is an attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

g. Tor is a free and open-source software for enabling anonymous communication. Tor directs Internet traffic through a free, worldwide, volunteer overlay network to conceal a user's location and usage.

h. Bitcoin is a digital or virtual currency which operates independently of a central bank.

COUNT ONE
Conspiracy to Intentionally Cause Damage to a Protected Computer
(18 U.S.C. § 371)

The Object of the Conspiracy

2. From at least on or about July 16, 2020, and continuing up to and including on or about August 22, 2020, in the State and Federal District of Nevada, and elsewhere,

EGOR IGOREVICH KRIUCHKOV ("KRIUCHKOV"),

the defendant herein, and others known and unknown to the Grand Jury, knowingly combined, conspired, confederated, and agreed to commit an offense against the United States in violation of Title 18, United States Code, Section 371, that is: to knowingly cause

the transmission of a program, information, code, and command and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause a loss to one or more persons during any 1-year period aggregating at least $5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i) and 1030(c)(4)(A)(i)(I).

3. The purpose of the conspiracy was to recruit an employee of Victim Company A to surreptitiously transmit malware provided by the coconspirators into a protected computer in Victim Company A's network, exfiltrate data from the network, and threaten to disclose the data unless Victim Company A paid the coconspirators' ransom demand.

Manner and Means of the Conspiracy

4. The object of the conspiracy was carried out, and to be carried out, in substance, as follows:

a. KRIUCHKOV and his coconspirators agreed to recruit an employee of Victim Company A to facilitate the transmission of malware into Victim Company A's network;

b. KRIUCHKOV and a coconspirator advised an employee of Victim Company A that the coconspirators would pay the employee to facilitate the transmission of malware into the Victim Company A's network.

c. KRIUCHKOV and a coconspirator advised the employee of Victim Company A that the malware, when executed, would alter Victim Company A's network to allow the coconspirators access the network to extract data.

d. KRIUCHKOV and a coconspirator advised the employee of Victim Company A that the employee would not be paid until the employee had transmitted the malware into Victim Company A's network.

e. KRIUCHKOV advised the employee of Victim Company A, that once the data was extracted, the conspirators would threaten to make this data public unless Victim Company A paid their ransom demand.

Overt Acts

5. In furtherance of this conspiracy and to accomplish the object, at least one of the coconspirators committed and caused to be committed, in the District of Nevada, and elsewhere, at least one of the following overt acts, among others:

Overt Act No. 1: On or about July 16, 2020, KRIUCHKOV used his WhatsApp account to contact the employee of Victim Company A and arranged to meet with the employee, who was in Nevada, in the District of Nevada.

Overt Act No. 2: On or about July 28, 2020, KRIUCHKOV entered the United States from outside the United States using his Russian passport and a visa.

Overt Act No. 3: On or about July 29, 2020, KRIUCHKOV purchased a cellular telephone in the United States, in the State of New York.

Overt Act No. 4: On or about July 31, 2020, KRIUCHKOV rented a vehicle in the San Francisco, California, area and drove to the Reno, Nevada area.

Overt Act No. 5: On or about July 31, 2020, KRIUCHKOV rented a hotel room in Sparks, Nevada.

Overt Act No. 6: Between on or about August 1, 2020 and on or about August 3, 2020, KRIUCHKOV visited with the employee numerous times, at the employee's residence, or at public locations.

Overt Act No. 7: On or about the evening of August 3, 2020, KRIUCHKOV met with the employee, and invited the employee to participate in a "special project" with him and his coconspirators. KRIUCHKOV explained the following:

a. The coconspirators would provide the employee with malware to surreptitiously transmit into Victim Company A's network.

b. The coconspirators would execute a Distributed Denial of Service attack against Victim Company A's network to divert attention from the malicious operation of the malware.

c. The malware would allow the coconspirators to extract data from Victim Company A's network.

d. Once the data was extracted, the coconspirators would extort Victim Company A for a substantial payment.

e. Both KRIUCHKOV and the employee would be compensated.

Overt Act No. 8: On or about August 7, 2020, KRIUCHKOV again met with the employee in Nevada and continued to encourage the employee's participation in the "special project." KRIUCHKOV advised the employee that either he or his coconspirators could make a partial payment to the employee up-front.

Overt Act No. 9: On or about August 16, 2020, KRIUCHKOV used his WhatsApp account to contact the employee in Nevada to set up another meeting.

Overt Act No. 10: On or about August 17, 2020, KRIUCHKOV met with the employee, and during this meeting, KRIUCHKOV informed the employee that the group would pay the employee $1,000,000 USD, with $50,000 of that to be paid the day the employee completes the assigned task.

Overt Act No. 11: During the same meeting on or about August 17, 2020, KRIUCHKOV used his WhatsApp account to contact an unidentified coconspirator using his telephone's speaker phone. KRIUCHKOV, the unidentified coconspirator, and the employee discussed the following:

a. The unidentified coconspirator discussed various means by which to pay the employee, including payments using cryptocurrency, a guarantor security deposit, or cash.

b. In exchange for the payment, the employee would be expected to transfer malware into Victim Company A's network.

c. KRIUCHKOV and the unidentified coconspirator had a conversation which resulted in the unidentified coconspirator telling KRIUCHKOV and the employee that the computer used to receive the malware transmission should remain running for six to eight hours.

d. The unidentified coconspirator stated that once the coconspirators received access to Victim Company A's data, they would execute a simulated external attack on Victim Company A.

e. The unidentified coconspirator told the employee that another unidentified person would call the employee before the operation and explain to the employee what the employee would need to do.

f. The unidentified coconspirator told the employee that the group would need between 10 and 12 days to prepare for the job after the employee agreed to do the job.

Overt Act No. 12: On or about August 18, 2020, KRIUCHKOV met with the employee, and explained that the coconspirators agreed to pay the employee $1,000,000

USD after the malware was transmitted to Victim Company A's network, but, in previous projects, the group had never prepaid the individual who would be introducing the malware and that it would not do so in this situation.

Overt Act No. 13: During the meeting on or about August 18, 2020, KRIUCHKOV stated that his (KRIUCHKOV's) share of the payment had been reduced because the coconspirators had agreed to pay the employee $1,000,000 USD.

Overt Act No. 14: During the meeting on or about August 18, 2020, KRIUCHKOV also stated that the employee would have to participate in the development of the malware, by providing information about Victim Company A's network to the coconspirators.

Overt Act No. 15: On or about August 19, 2020, KRIUCHKOV met with the employee in Nevada and assisted the employee to download a Tor browser application to facilitate anonymous access to the internet. KRIUCHKOV advised the employee to set up a Bitcoin wallet through the Tor browser.

Overt Act No. 16: During this meeting on or about August 19, 2020, KRIUCHKOV advised the employee that he (KRIUCHKOV) would give his cellular telephone to the employee, so that the employee could communicate directly with coconspirators more knowledgeable about the technical aspects of the "special project."

Overt Act No. 17: On or about August 21, 2020, KRIUCHKOV met with the employee. During this meeting,

a. KRIUCHKOV provided the employee with a cellular telephone.

b. KRIUCHKOV instructed the employee to leave the telephone in "airplane" mode until the employee received a signal via WhatsApp from KRIUCHKOV.

c. KRIUCHKOV also instructed the employee how to use the telephone, and KRIUCHKOV told the employee that the employee should delete messages after using the communication applications on the telephone.

d. During the meeting, KRIUCHKOV told the employee that the Bitcoin transfer would happen in a few days, and that the employee should not take any action until the employee received the Bitcoin transfer.

Overt Act No. 18: Also during the meeting on or about August 21, 2020, KRIUCHKOV spoke with a coconspirator using the speaker phone on KRIUCHKOV'S telephone. KRIUCHKOV informed the coconspirator that he left the telephone with the employee and that he had told the employee to leave the telephone in airplane mode until the money arrives. The coconspirator told the employee that any questions regarding timing of payment to the employee would need to be addressed by another coconspirator. KRIUCHKOV said that he was not going to maintain contact other than through the new telephone.

Victim Company A's Network

6. From at least on or about July 16, 2020, and continuing up to and including on or about August 22, 2020, Victim Company A's network was in contact with, and communicated with, the Internet.

Damage

7. A Distributed Denial of Service attack on Victim Company A's network and a network intrusion of Victim Company A's network to exfiltrate data would cause a loss to Victim Company A during any 1-year period aggregating at least $5,000 in value.

All in violation of 18 U.S.C. § 371.

FORFEITURE ALLEGATION

Conspiracy to Intentionally Cause Damage to a Protected Computer

1. The allegations contained in Count One of this Criminal Indictment are hereby realleged and incorporated herein by reference for the purpose of alleging forfeiture pursuant to 18 U.S.C. § 1030(i)(1)(A) and (j)(1).

2. Upon conviction of the felony offense charged in in Count One of this Criminal Indictment,

EGOR IGOREVICH KRIUCHKOV,

defendant herein, shall forfeit to the United States of America, any personal property that was used or intended to be used to commit or to facilitate the commission of a violation of 18 U.S.C. § 1030(a)(5)(A), or 18 U.S.C. § 371, conspiracy to violate such offense:

defendant herein, shall forfeit to the United States of America, any personal property used or intended to be used to commit or to facilitate the commission of a violation of 18 U.S.C. § 1030(a)(5)(A), or 18 U.S.C. § 371, conspiracy to violate such offense:

a. an iPhone X, model number A1901, serial number G0NW1D54JCL8; and

b. a LG Phoenix 5, model number LM-K300AM, seral number 007VTHJ0163129, IMEI 353953111881291.

/ / /

/ / /

/ / /

/ / /

/ / /

All pursuant to 18 U.S.C. § 1030(i)(1)(A) and (j)(1), 18 U.S.C. § 371, and 18 U.S.C. § 1030(a)(5)(A).

DATED: this 3RD day of September 2020.

A TRUE BILL:

/s/

FOREPERSON OF THE GRAND JURY

NICHOLAS A. TRUTANICH
United States Attorney

RICHARD B. CASPER
Assistant United States Attorney

CANDINA S. HEATH
Senior Counsel
Computer Crime and Intellectual Property Section
U.S. Department of Justice