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

Representing the United States of America

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

UNITED STATES OF AMERICA, Plaintiff, v. EGOR IGOREVICH KRIUCHKOV, Defendant.	Case No: 3:20-mj-83-WGC COMPLAINT FOR VIOLATION OF: Title 18, United States Code, Section 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)

BEFORE the Honorable William G. Cobb, United States Magistrate Judge for the District of Nevada, the undersigned complainant being first duly sworn states:

Count One

(Conspiracy to Intentionally Cause Damage to a Protected Computer)

From at least on or about July 15, 2020, and continuing to on or about August 22, 2020, in the State and District of Nevada and elsewhere, defendant EGOR IGOREVICH KRIUCHKOV did conspire and agree with unknown coconspirators 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).

Purpose of the Conspiracy

1. The purpose of the conspiracy was to recruit an employee of a company to surreptitiously transmit malware provided by the coconspirators into the company's computer system, exfiltrate data from the company's network, and threaten to disclose the data online unless the company paid the coconspirators' ransom demand.

Manner and Means of the Conspiracy

2. The object of the conspiracy was carried out, in substance, as follows:

   a. EGOR IGOREVICH KRIUCHKOV and his coconspirators agreed to recruit an employee of a targeted company to facilitate the transmission of malware into the targeted company's computer system;

   b. EGOR IGOREVICH KRIUCHKOV and a coconspirator communicated with the employee of a targeted company, and explained that the conspirators will pay the employee to facilitate the

transmission of the malware into the targeted company's computer system.

c. The executed malware would provide the conspirators access to data in the targeted company's network. Thereafter the conspirators could threaten to disclose this data online unless the targeted company paid their ransom demand.

Overt Acts

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

a. On or about July 16, 2020, EGOR IGOREVICH KRIUCHKOV used his WhatsApp account to contact the employee of Victim Company A and arranged to visit in person in the District of Nevada.

b. On or about July 28, 2020, EGOR IGOREVICH KRIUCHKOV entered the United States using his Russian Passport and a B1/B2 tourist visa.

c. On or about July 29, 2020, EGOR IGOREVICH KRIUCHKOV purchased a cellular telephone in the United States.

d. On or about July 31, 2020, EGOR IGOREVICH KRIUCHKOV rented a vehicle in San Francisco, California, and drove to Reno, Nevada.

e. On or about July 31, 2020, EGOR IGOREVICH KRIUCHKOV rented a hotel room in Sparks, Nevada.

f. Between on or about August 1, 2020 and on or about August 3, 2020, EGOR IGOREVICH KRIUCHKOV visited with the employee and associates of the employee numerous times, at the employee's residence, or at public locations.

g. On or about the evening of August 3, 2020, EGOR IGOREVICH KRIUCHKOV meet with the employee in person and invited the employee to participate in a "special project" with him and his coconspirators. KRIUCHKOV explained the following:

i. The coconspirators would provide the employee with malware to surreptitiously transmit into Victim Company A's computer system.

ii. The coconspirators would engage in a Distributed Denial of Service Attack to divert attention from the malware.

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

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

v. Both KRIUCHKOV and the employee would be compensated.

h. On or about August 7, 2020, EGOR IGOREVICH KRIUCHKOV again met with the employee 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 and told the employee to think about it until the next meeting.

i. On or about August 16, 2020, EGOR IGOREVICH KRIUCHKOV used his WhatsApp account to contact the employee to set up another meeting.

j. On or about August 17, 2020, EGOR IGOREVICH KRIUCHKOV met with the employee, and during this meeting, KRIUCHKOV used his WhatsApp account to telephone an unidentified coconspirator. KRIUCHKOV, the unidentified coconspirator, and the employee discussed the following:

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

ii. The employee would be expected to transfer malware to Victim Company A's computer system.

iii. KRIUCHKOV and the unidentified coconspirator advised the employee that the computer used to receive the malware transmission should remain running for six to eight hours.

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

k. On or about August 18, 2020, EGOR IGOREVICH KRIUCHKOV met with the employee, and explained that the conspirators agreed to pay the employee $1,000,000 USD after the malware was transmitted,

but that they had never made an up-front payment and would not do so in this situation.

l. During the August 18, 2020 meeting, EGOR IGOREVICH KRIUCHKOV stated that his share of the payment had been reduced because the group had agreed to pay the employee $1,000,000 USD.

m. 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 conspirators.

n. On or about August 19, 2020, EGOR IGOREVICH KRIUCHKOV met with the employee and assisted the employee to download an application call "Tor Browser" to facilitate anonymous access to the internet. KRIUCHOV advised the employee to set up a bitcoin wallet through Tor Browser.

o. During this meeting, EGOR IGOREVICH 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."

p. On August 21, 2020, EGOR IGOREVICH KRIUCHKOV met with the employee. During this meeting:

i. EGOR IGOREVICH KRIUCHKOV provided the employee with a cellular telephone.

ii. EGOR IGOREVICH KRIUCHKOV instructed the employee to leave the telephone in "airplane" mode until the employee

received a signal via WhatsApp from a coconspirator referred to as "Kisa."

iii. EGOR IGOREVICH KRIUCHKOV also instructed the employee how to use the telephone, and EGOR IGOREVICH KRIUCHKOV told the employee he should delete messages after using the communications applications on the telephone.

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

q. Also during this meeting, EGOR IGOREVICH KRIUCHKOV spoke with a coconspirator using his telephone's speaker phone. EGOR IGOREVICH KRIUCHKOV informed the coconspirator that he left the phone with the employee and that he had told the employee to leave the phone 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. EGOR IGOREVICH KRIUCHKOV said that he was not going to maintain contact other than through the new phone.

Each in violation of 18 U.S.C. § 371 (1030(a)(5)(A), 1030(c)(4)(B)(i), and 1030(c)(4)(A)(i)(I)).

Complainant as a special agent with the Federal Bureau of Investigation states there is probable cause to arrest the above-named defendant as set forth in the attached affidavit.

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEVADA

UNITED STATES OF AMERICA v. EGOR IGOREVICH KRIUCHKOV	Case No. 3:20-mj-83-WGC **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
ARREST WARRANT AND CRIMINAL COMPLAINT

1. I, Michael J. Hughes, being first duly sworn, hereby depose and state as follows: I make this affidavit in support of the issuance of an arrest warrant and a Criminal Complaint charging defendant EGOR IGOREVICH KRIUCHKOV with a violation of 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)).

2. I am a Special Agent for the Federal Bureau of Investigation ("FBI"), where I have been employed for 14 years. As a Special Agent, in accordance with Title 18, United States Code, Section 2510(7), I am a Federal Law Enforcement Officer of the United States, who is empowered by law to conduct investigations of and make arrests for offenses enumerated in Title 18, as well as author warrants for search and seizure pursuant to Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure.

3. I am currently assigned to the Reno Resident Agency of the FBI Las Vegas Division, where I have been assigned for three years. Prior to this current assignment, I served as a Special Agent in Las Vegas, Nevada and as a Supervisory Special Agent at FBI Headquarters in Washington, D.C.

4. I have experience conducting national security and criminal investigations, including counterintelligence, counterterrorism, and cyber matters. I am currently responsible for conducting counterintelligence investigations.

5. During my tenure with the FBI, I have conducted surveillance, analyzed phone records, drafted search warrant applications, monitored Title III wiretaps, interviewed witnesses, recruited confidential sources, supervised activities of sources, utilized and analyzed GPS tracking technology, executed search warrants, and executed arrest warrants. I have also received ongoing on-the-job training from other agents and law enforcement officials.

6. Based upon the above experience, I am familiar with the modus operandi of persons involved in fraud related to unauthorized computer access, the theft of trade secrets, intelligence collection against the United States Government and industry within the United States, and other criminal violations. I am aware persons involved in such criminal activities routinely attempt to conceal their identities and actions, including involving third party actors to aid in their criminality.

7. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the issuance of an arrest warrant and a criminal complaint and does not set forth all of my knowledge about this matter.

8. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that EGOR IGOREVICH KRIUCHKOV has committed a violation of 18 U.S.C. § 371 – Conspiracy to Intentionally Cause Damage to a Protected Computer.

\\

PROBABLE CAUSE

9. In August 2020, Victim Company A advised the FBI that a Russian male, identified only as "Egor" had offered to pay a Victim Company A employee (CHS1)[1] US $500,000 to introduce computer malware[2] into the network of Victim Company A. "Egor" claimed the malware would provide "Egor" and his associates with access to the system. "Egor's" associates would then extract data from the network and threaten to make the information public if the Victim Company A did not agree to pay a ransom.

10. From the subsequent investigation, the FBI identified "Egor" as EGOR IGOREVICH KRIUCHKOV ("KRIUCHKOV"), a Russian national who entered the United States on July 28, 2020. KRIUCHKOV's date of birth was a certain day in 1993 known to your affiant and he was born in Russia. He used Russian Passport number ending in 7322 to enter the United States on a B1/B2 tourist visa, which was issued on October 3, 2019 and is valid for three years, expiring on October 1, 2022.

11. CHS1 advised that on or around July 16, 2020, KRIUCHKOV contacted the CHS1 via WhatsApp, having been provided the number by a mutual acquaintance.[3] CHS1

---

[1] Confidential Human Source (CHS1) was recruited by the FBI in August 2020, after CHS1 reported KRIUCHKOV's proposed criminal activity to the security office of Victim Company A. CHS1 had no prior experience reporting to the FBI. FBI and law enforcement database records revealed no derogatory information on CHS1, including no criminal history. Through this investigation much of CHS1's reporting has been verified. The investigation has not revealed any information provided to the FBI by CHS1 which has been proven to be false. CHS1 is cooperating with the FBI because of patriotism to the United States and a perceived obligation to Victim Company A. CHS1 has not asked for and has not been offered any form of payment, including consideration regarding immigration or citizenship.

[2] Malware is short for "malicious software" and refers to software programs designed to damage or do other unwanted actions on a computer system.

[3] CHS1 allowed the FBI to search his telephone, and during the consent search of CHS1's phone, the FBI retained screen shots of CHS1's WhatsApp communications with KRIUCHKOV. FBI translation of these messages confirmed CHS1's reporting on the matter.

reported that he knew KRIUCHKOV from contact the two had in 2016. KRIUCHKOV told CHS1 he was traveling from Russia to the United States and would like to visit with CHS1 during his travels. KRIUCHKOV stated he would be in New York before flying to California, and would be willing to drive from California to Nevada to meet with CHS1. In the WhatsApp text messages, CHS1 invited KRIUCHKOV to visit, but stated the visit had to be before August 7, 2020, due to other commitments.

12. Databases available to law enforcement revealed KRIUCHKOV entered the United States on July 28, 2020, in New York, New York, and on July 30, 2020, flew from New York to San Francisco. Other records show that on July 31, 2020, KRIUCHKOV drove a rented vehicle to Nevada to meet with CHS1. Records also show that KRIUCHKOV rented a room at a hotel just off of I-80 in Sparks, Nevada.

13. KRIUCHKOV advised the CHS1 that he purchased a cellular phone in New York shortly after entering the United States[4]. Agents believe that KRIUCHKOV has been using that cellular phone to contact CHS1.

14. The FBI has confirmed KRIUCHKOV rented a grey Toyota Corolla from Hertz Rent-a-Car at San Francisco International Airport. FBI investigation revealed KRIUCHKOV rented room 228 at the Western Village, 815 Nichols Boulevard, Sparks, Nevada. KRIUCHKOV used Booking.com to make the reservation for the room. He reserved the room from July 31, 2020 through August 04, 2020. KRIUCHKOV used a Mastercard credit card to pay the bill, which totaled US $265.00.

[4] AT&T records provided to the FBI confirm the cellular phone was purchased and activated on July 29, 2020, in New York, New York.

15. FBI agents debriefed CHS1 about his contact with KRIUCHKOV in July and August of 2020. According to CHS1, KRIUCHKOV visited CHS1's residence in Nevada on August 1, 2020, twice on August 2, 2020, and once on August 3, 2020. On August 1, 2020, CHS1, KRIUCHKOV, and two other individuals associated with CHS1 traveled to Emerald Pools, near Nevada City, California. On August 2, 2020, KRIUCHKOV, CHS1, and these other two individuals drove to South Lake Tahoe, California. The group toured the area and had dinner. KRIUCHKOV used his rental car to drive the group during this trip.

16. CHS1 noted to agents that, during these excursions, KRIUCHKOV expressed a desire not to be in any photos. For instance, CHS1 reported that, while they were at Lake Tahoe, there was a beautiful sunset, and KRIUCHKOV was resistant to posing with the group. KRIUCHKOV stated he would just remember the beauty of the sunset and did not need a photograph. Eventually, KRIUCHKOV reluctantly agreed to pose with the group. CHS1 also reported CHS1 could not remember KRIUCHKOV using his own phone to take any pictures. Through my training and experience, I know that individuals involved in criminal activity often take efforts not to leave evidence about their locations, including avoiding surveillance cameras and not taking photographs.

17. CHS1 also noted to agents that KRIUCHKOV paid for all the group's activities during the trips to Emerald Pools and Lake Tahoe. CHS1 reported that KRIUCHKOV claimed he had gambled at the hotel and had won some money. KRIUCHKOV stated he wanted to use that money to pay for the expenses incurred by his hosts. Through my training and experience I know individuals involved in intelligence collection and/or criminal activity often spend extravagantly on individuals they are attempting to recruit and/or co-opt for participation in criminal activity.

18. CHS1 reported that, after the group returned from Lake Tahoe, and as KRIUCHKOV was preparing to return to the hotel for the night, he asked to meet with CHS1 the following day, August 3, 2020. KRIUCHKOV stated he wanted to meet with CHS1 alone, so they could discuss "business."

19. CHS1 reported to agents that, on August 3, 2020, KRIUCHKOV used WhatsApp to arrange a meeting with CHS1, and the two met that evening. KRIUCHKOV picked up CHS1, and he drove the pair to a restaurant in the Reno, Nevada area. After eating, the pair went to a nearby bar. They drank heavily until last call. CHS1 insisted on paying at the restaurant as KRIUCHKOV had paid for all the other expenses. KRIUCHKOV paid at the bar.

20. CHS1 reported to agents that, at the bar, CHS1 observed KRIUCHKOV take his cellular phone and place it on top of CHS1's cellular phone before placing the stacked phones arm's length away from the pair. At that point, KRIUCHKOV stated his true reason for traveling to the United States was to visit CHS1. KRIUCHKOV stated he worked for a "group" that works on "special projects." KRIUCHKOV went on to explain that the "group" pays employees of target companies to introduce malware into the target company's computer system. KRIUCHKOV said the "group" has performed these "special projects" successfully on multiple occasions, and identified some of the targeted companies.

21. KRIUCHKOV described the "special projects" as introducing malware into the computer network of Victim Company A. He explained the malware attacks the systems in two ways. Firstly, the malware appears to be an external DDoS attack[5]. This attack occupies the company's computer security staff and conceals the second attack. The second attack exfiltrates

[5] A DDoS (Distributed Denial of Service) attack occurs when multiple systems flood the bandwidth or resources of a targeted computer system, oftentimes causing the system to shut down or "crash."

data from the computer network and into the possession of the "group." The "group" later contacts the company and threatens to make the data public if the company does not pay a large ransom.

22. KRIUCHKOV told CHS1 the "group" would pay CHS1 US $500,000 to introduce the malware to his employer's computer network. KRIUCHKOV said the payment could be delivered as cash or as Bitcoin[6]. Observing that CHS1 was hesitant to be involved, KRIUCHKOV offered to entice CHS1 with an unspecified additional payment coming from KRIUCHKOV's payment from the "group." If CHS1 agreed to this arrangement, the "group" would provide the malware to CHS1 in either a thumb drive to be inserted into a computer's USB drive or an email with an attachment containing malware. CHS1 would choose the delivery method.

23. KRIUCHKOV told CHS1 to consider the proposal over the next several days. KRIUCHKOV stated he was traveling to the Los Angeles, California area the following day, (August 4, 2020). KRIUCHKOV admonished CHS1 to not tell anyone about the proposal.

24. At approximately 3:00 am on August 7, 2020, CHS1 received a WhatsApp text message from KRIUCHKOV[7], requesting to meet after CHS1 finished work. KRIUCHKOV instructed CHS1 to not tell anyone about the meeting. When CHS1 attempted to make excuses to delay or postpone the meeting, KRIUCHKOV insisted on a short meeting and stated he had

---

[6] Bitcoin is a type of digital currency which can be transferred from one digital wallet to another. Each transaction is recorded in a public list called a block chain. The use of Bitcoin is popular in illicit activities due to ease of transfer and perceived protection from law enforcement scrutiny.

[7] The details of these WhatsApp text messages were provided to the FBI during a debriefing of CHS1. Additionally, CHS1 authorized the interviewing Special Agents to take photographs of CHS1's phone containing the WhatsApp messages. These WhatsApp messages were translated by the FBI and were consistent with the reporting provided by CHS1.

not driven for 12 hours to not meet with CHS1. CHS1 relented and sent a text message of an address and proposed to meet at 5:00 pm.

25. The FBI conducted physical surveillance of this meeting and observed KRIUCHKOV meet with CHS1. KRIUCHKOV arrived in a rental vehicle, different from the rented vehicle he had been driving when he previously met with CHS1. The meeting occurred inside KRIUCHKOV's vehicle in the parking lot of a gas station in Reno, Nevada, and was witnessed by several FBI Special Agents. The Special Agents were able to positively identify KRIUCHKOV and CHS1.

26. During this meeting, which the FBI had consensually recorded, KRIUCHKOV reiterated some of the details of the criminal activity previously proposed to CHS1.[8] KRIUCHKOV described the malware attack as he did before, adding that the first part of the attack (DDoS attack) would be successful for the "group" but the Victim Company's security officers would think the attack had failed. KRIUCHKOV again listed prior companies the "group" had targeted. KRIUCHKOV stated each of these targeted companies had a person working at those companies who installed malware on behalf of the "group." To ease CHS1's concerns about getting caught, KRIUCHKOV claimed the oldest "project" the "group" had worked on took place three and a half years ago and the "group's" co-optee still worked for the company. KRIUCHKOV also told CHS1 the "group" had technical staff who would ensure the malware could not be traced back to CHS1. In fact, KRIUCHKOV claimed the group could

[8] All of the audio-recorded conversations between KRIUCHKOV and CHS1, as well as audio conversations with other coconspirators, took place in Russian. As reported throughout this affidavit, the contents of these conversations are based on summary translations, not transcriptions, of these conversations performed by an FBI translator and the translations are subject to revision.

attribute the attack to another person at Victim Company A, should there be "someone in mind CHS1 wants to teach a lesson."

27. During the meeting, CHS1 expressed how concerned and stressed CHS1 had been over the request. CHS1 stated if CHS1 were to agree to install the malware, CHS1 would need more money. KRIUCHKOV asked how much, and CHS1 responded US $1,000,000. KRIUCHKOV was sympathetic to the request and said he understood, but would have to contact the "group" before agreeing to this request.[9] KRIUCHKOV confided that the "group" was paying KRIUCHKOV US $500,000 for his participation in getting CHS1 to install the malware, and he was willing to give a significant portion of the payment (US $300,000 to US $450,000) to CHS1 to entice his involvement.[10]

28. CHS1 said CHS1 would need money upfront to ensure KRIUCHKOV would not have him install the software and then not pay him. Again, KRIUCHKOV asked how much, and CHS1 responded US $50,000. KRIUCHKOV said this was an acceptable amount and a reasonable request but he would have to work on this because he only had US $10,000 with him due to U.S. Customs restrictions on the amount of money he could bring into the country. KRIUCHKOV also questioned what would prevent CHS1 from taking the up-front money and then not following through on installing the malware. CHS1 stated CHS1 was sure

---

[9] During this discussion KRIUCHKOV referred to what appear to be two other individuals, instead of the "group." He specifically mentioned a need to convince one of these individuals of CHS1's willingness to participate in the criminal activity, when discussing getting approvals for additional payment.

[10] In the consensually recorded conversation, while they were discussing payment for CHS1's participation, KRIUCHKOV stated he would be splitting US $1,000,000 with CHS1 (i.e.: US $500,000 each). KRIUCHKOV then stated it would be sufficient for him to make US $200,000 on the deal. Later in the conversation, KRIUCHKOV stated he would not care if he ended up making US $50,000 to US $100,000 because that would be good enough for him.

KRIUCHKOV or the "group" would figure a way to apply leverage against CHS1 to ensure CHS1 held up his end of the arrangement. CHS1 and KRIUCHKOV discussed the timing of the next meeting, and KRIUCHKOV said he would return to Reno on or around August 17, 2020.

29. According to CHS1, on August 16, 2020, KRIUCHKOV contacted CHS1 via WhatsApp text message to inform CHS1 that he was back in Reno. CHS1 told KRIUCHKOV, CHS1 was not available to meet on August 16, 2020, and arranged to meet with KRIUCHKOV after work on August 17, 2020.

30. On August 17, 2020, KRIUCHKOV met with CHS1 at a Reno, Nevada restaurant. The meeting was consensually recorded. KRIUCHKOV stated he has personally been involved in two "projects" with the group. KRIUCHKOV said that victim companies usually negotiate with the group to pay less ransom money than the group initially requests, for example on company was ransomed at US $6 million and ultimately paid US $4 million. He said only one company paid the full initial ransom. KRIUCHKOV stated the group has never provided an advance payment to co-optees and was not comfortable giving money upfront to CHS1. KRIUCHKOV said that the group had previously used a program called "Exploit" for an on-line escrow arrangement.

31. During this same meeting, KRIUCHKOV said he would be leaving his cellular phone with CHS1 when KRIUCHKOV left the United States so CHS1 could discuss the details with the group. KRIUCHKOV said the phone and the SIM card were purchased with cash. KRIUCHKOV also referred to the phone as "clean."

32. During the meeting, KRIUCHKOV telephoned a member of the group, First Name Unknown/Last Name Unknown (henceforth: LNU), who agents believe was located overseas. Prior to making the call, KRIUCHKOV asked CHS1 not to mention the fact that he

had told CHS1 of other companies the group had victimized. CHS1 reported that KRIUCHKOV made this call by using a hot spot created on a different cellular phone. KRIUCHKOV then wirelessly tethered a third cellular phone to the hotspot. KRIUCHKOV then placed a WhatsApp call to LNU.

33. During the call, KRIUCHKOV and LNU suggested placing the money to be paid to CHS1 in what appeared to be a kind of online escrow account. LNU explained that the funds would be deposited into a website in advance. KRIUCHKOV asked LNU whether they will be able to assist CHS1 with receiving cash and whether they can use "drops" (i.e., intermediaries) for that. LNU admitted that he could not make such decisions himself. LNU also noted that his team had never paid anyone in advance, although it would not be an issue to transfer the money into the escrow account. LNU told CHS1 that CHS1 would receive the money regardless. LNU told CHS1 that they would tell CHS1 afterwards how CHS1 can withdraw the funds.

34. During the conversation, CHS1 expressed concerns about not being able to trust anyone, and CHS1 wondered whether LNU could transfer US $50,000 into KRIUCHKOV's Bitcoin account, and whether KRIUCHKOV could then cash out the funds. LNU expressed that LNU did not want CHS1 to have any doubts in them, and that he would thus transfer Bitcoins into a real account, and KRIUCHKOV would then cash out the funds. However, LNU also noted that they would give CHS1 the money only after CHS1 completed the job. LNU said that KRIUCHKOV would have the money, and that they should be able to do it by the next evening.

35. At one point in the conversation, CHS1 asked for a description of what CHS1 would have to do in order to complete the task. LNU told CHS1 that CHS1 would need to download all the files. LNU said, after that, they would need to wait for five days. In response to

KRIUCHKOV asking how many hours the computer should be working once CHS1 finished downloading everything, LNU replied that one work shift, six or eight hours, should be enough.

36. CHS1 reported to agents that KRIUCHKOV stated the group had never paid a co-optee as much as they have offered to pay CHS1 (note: US $1 million). CHS1 stated KRIUCHKOV and LNU were not the boss, and that the boss was expected to get US $2 million from this project. CHS1 stated KRIUCHKOV also mentioned another member of the group (not by name) who is a hacker and a high level employee of a government bank in Russia. CHS1 said this group member specializes in encryption and works to ensure the malware cannot be traced back to CHS1 after CHS1 installs it in the network. KRIUCHKOV said the group would be expecting to get US $4 million dollars from Victim Company A. CHS1 reported that KRIUCHKOV said the group had to pay US $250,000 for the malware, which would be written specifically for targeting Victim Company A's computer network. CHS1 reported KRIUCHKOV said after CHS1 and the group come to an agreement it would take ten to twelve days for the group to prepare the malware because it would be designed for Victim Company A's network. CHS1 said the group would also require CHS1's input about Victim Company A's network for the malware development. CHS1 said KRIUCHKOV claimed companies pay because it is easier for the companies to pay the ransom than to fight the group.

37. KRIUCHKOV explained that the "guys" in the group would explain everything to the CHS1 later. KRIUCHKOV admitted he didn't understand the technical part very well.

38. On the evening of August 18, 2020, CHS1 met with KRIUCHKOV. This meeting was consensually monitored and the FBI conducted physical surveillance. KRIUCHKOV claimed to have spoken to the group all night. KRIUCHKOV said the group

communicates through a TOR browser[11] chat system called Jabber[12]. KRIUCHKOV mentioned the names of two members of the group.

39. KRIUCHKOV said the group was insistent they never pay co-optees beforehand and would not in this situation. KRIUCHKOV offered to record a video with CHS1 during which KRIUCHKOV would document his agreement to pay CHS1 US $1 million for his part in installing malware on the Victim Company A's network. KRIUCHKOV presented this solution as a contract to pay CHS1 in lieu of an advanced down payment. KRIUCHKOV said that since the group agreed to pay CHS1 US $1 million for his/her participation, KRIUCHKOV's payment was cut to US $250,000.

40. KRIUCHKOV said CHS1 will need to participate in the development of the malware. Specifically, CHS1 will be required to provide information about network authorizations and network procedures.

41. KRIUCHKOV talked about a "project" in which the group targeted another company. This project did not work out because of a failure of the co-optee. KRIUCHKOV also said the Victim Company A project was not the only project the group was working on at the time, and the group was therefore willing to drop the Victim Company A project if they could not come to an agreement with CHS1.

---

[11] A TOR browser allows users to go on the World Wide Web anonymously and serves as an access point to the dark web.

[12] Jabber is a mobile device communication application for texting, voice and video calling, voice messaging, and desktop sharing which utilizes encryption.

42. KRIUCHKOV said, if they came to an agreement and the project was successful, it would take about ten days to get the final payment to CHS1. KRIUCHKOV said his payments for his previous projects with the group were paid in cash.

43. CHS1 told KRIUCHKOV if the group would agree to an advanced payment, CHS1 would acquiesce and accept a down payment via Bitcoin transfer. KRIUCHKOV said he would be leaving Reno, Nevada the next morning (August 19, 2020), to return the rental car in Los Angeles, California. KRIUCHKOV was then planning on returning to Russia. KRIUCHKOV asked to meet with CHS1 the next morning (August 19, 2020) to have one final meeting before he left.

44. In the early morning of August 19, 2020, KRIUCHKOV contacted CHS1 via WhatsApp and requested the morning meeting be cancelled. Instead, KRIUCHKOV asked to meet with CHS1 after work. Additionally, KRIUCHKOV asked CHS1 for a codename. CHS1 asked if the codename was for KRIUCHKOV to set up a Bitcoin and that if it was CHS1 preferred to set it up himself. KRIUCHKOV told CHS1 not to worry about it and to just send a codename. CHS1 instructed him to use "DeadSpace22." KRIUCHKOV then sent a message saying CHS1 would have to do it himself. CHS1 asked why the group changed their mind, to which KRIUCHKOV responded they agreed to the payment because CHS1 was not happy

45. On the evening of August 19, 2020, CHS1 met with KRIUCHKOV in KRIUCHKOV's vehicle. The meeting was consensually recorded and physically surveilled by the FBI. KRIUCHKOV told CHS1 the group had agreed to pay an advance of US $8,500 to $11,000 based on to conversion rate of Bitcoin. KRIUCHKOV took CHS1's phone and downloaded an application called "Tor Browser." This app allows for anonymous access to the internet. KRIUCHKOV then used his identified cellular phone to open instructions for creating

a Bitcoin wallet. CHS1 stopped KRIUCHKOV, and told KRIUCHKOV that CHS1 wanted to set up the wallet[13] and that CHS1 would do this after their meeting. KRIUCHKOV agreed but told CHS1 to set the wallet up through the Tor Browser so it would not be traceable.

46. During the meeting, KRIUCHKOV said he changed his travel plans again so that he could meet with CHS1 the following day. KRIUCHKOV stated he would now be leaving on August 20, 2020, to drive to Los Angeles, California. KRIUCHKOV would return the rental car and then fly out of the Los Angeles area. KRIUCHKOV stated if the project was successful, KRIUCHKOV would return to the United States in November 2020, for his birthday, because his U.S. visa would still be valid. KRIUCHKOV also offered to help CHS1 convert his Bitcoin payment to cash during the November trip.

47. KRIUCHKOV set the next meeting for after CHS1 completed work on August 20, 2020, and said the meeting would be about going over final details and that KRIUCHKOV would give CHS1 the previously-identified phone. KRIUCHKOV implied that the Bitcoin transfer to CHS1's Bitcoin wallet would happen before the meeting.

48. On the morning of August 20, 2020, CHS1 contacted me to confirm that CHS1 provided his Bitcoin wallet information to KRIUCHKOV.

49. On August 21, 2020, KRIUCHKOV and CHS1 communicated via a WhatsApp chat to arrange for a meeting later that day. In the evening, KRIUCHKOV and CHS1 met in KRIUCHKOV's vehicle. This meeting was consensually monitored by the FBI. During the meeting, KRIUCHKOV stated he was leaving Reno, Nevada the following day. KRIUCHKOV stated that no money would be transferred and that the "project" was being delayed.

---

[13] CHS1 was instructed by the FBI to prevent KRIUCHKOV from setting up a wallet so the FBI could set it up on behalf of CHS1, which would give the FBI access to the wallet.

50. During the same meeting, KRIUCHKOV told CHS1 that he would still give the identified burner phone to CHS1 and instructed CHS1 to leave the phone in airplane mode. "Kisa" would then send CHS1 a smiley face emoji to CHS1's WhatsApp account, which would indicate CHS1 should take the identified burner phone off airplane mode. KRIUCHKOV stated that the Bitcoin transfer would happen, but he didn't know when. KRIUCHKOV said that the transfer could be in a few days. KRIUCHKOV instructed CHS1 not to take any action until CHS1 received the Bitcoin transfer.

51. During the meeting, KRIUCHKOV placed a call to another individual. CHS1 observed KRIUCHKOV use a personal phone (not the phone KRIUCHKOV intended to give to CHS1) to make this call. CHS1 also observed KRIUCHKOV's phone's screen and saw the contact was listed as "Sasha Skarobogatov" ("Skarobogatov"). KRIUCHKOV left a message on the phone stating that he (KRIUCHKOV) needed to talk now and not later. Shortly thereafter, an individual believed to be Skarobogatov called KRIUCHKOV and the call was placed on speaker phone.

52. During this call, KRIUCHKOV informed Skarobogatov that he left the phone with CHS1 and that he had told CHS1 to leave the phone in airplane mode until the money arrives. CHS1 asked when the money would be sent, and Skarabogatov said that was a question for "Pasha." KRIUCHKOV said that he had already talked to Pasha and that Pasha had told KRIUCHKOV that they need to wait for a couple of days. KRIUCHKOV said that he was not going to maintain contact other than through the new phone. Skarobogatov asked KRIUCHKOV to let him [Skarabogatov] know when the phone was active, and KRIUCHKOV said that he would do so. The call ended soon thereafter.

53. CHS1 reported that KRIUCHKOV also told CHS1 the delay in the Victim Company A project was because the group was in the final stage of another project which was supposed to provide a large payout to the group. KRIUCHKOV said getting the money for the advanced payment to CHS1 wasn't a problem, it just wasn't the focus of the group because they were all worried about the other project.

54. During the same meeting, KRIUCHKOV provided a cellular phone and charging cable to CHS1. KRIUCHKOV then instructed CHS1 on how to use the phone. Specifically, KRIUCHKOV instructed CHS1 to delete messages after using the communications applications on the phone. Based on my experience investigating foreign intelligence officials and sophisticated criminal organization I believe KRIUCHKOV's actions during this meeting constitute a communications plan intended to be used to conceal communications between a handler (KRIUCHKOV) and a co-optee (CHS1) for advancing the criminal activity.

55. On August 21, 2020, a Senior Manager for Victim Company A estimated to an FBI agent that the remediation cost for a Distributed Denial of Service attack is estimated to be over ten-thousand dollars. The manger also estimated that the remediation cost for an actual network intrusion would be well over $5,000. Furthermore, in addressing the potential threat posed by KRIUCHKOV and his coconspirators, they have already spent more than US $5,000.

56. Thus, based on my training and experience and a conversation with a Senior Manager for Victim Company A, any remediation efforts due to the malware or a DDoS attack would be an excess of US $5000.

\\

\\

\\

CONCLUSION

Based upon the above facts and my training and experience, I believe the foregoing facts establish that probable cause exists to believe that EGOR IGOREVICH KRIUCHKOV has committed the offense of Conspiracy to Intentionally Cause Damage to a Protected Computer, in violation of 18 U.S.C. § 371 (conspiracy to violate 18 U.S.C. §§ 1030(a)(5)(A); 1030(c)(4)(B)(i) and (c)(4)(A)(i)(I)).

Respectfully submitted,

Michael J. Hughes
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by reliable electronic means on the 23rd day of August, 2020.

WILLIAM G. COBB
UNITED STATES MAGISTRATE JUDGE