copy

AO 442 (Rev. 11/11) Arrest Warrant

UNITED STATES DISTRICT COURT

UNDER SEAL

for the

Northern District of California

United States of America
v.

DANIL POTEKHIN, a/k/a "cronuswar," and DMITRII KARASAVIDI, a/k/a Dmitriy Karasavidi

Case No. CR-19-0572-CRB

Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) DMITRII KARASAVIDI ,

who is accused of an offense or violation based on the following document filed with the court:

☐ Indictment ☑ Superseding Indictment ☐ Information ☐ Superseding Information ☐ Complaint

☐ Probation Violation Petition ☐ Supervised Release Violation Petition ☐ Violation Notice ☐ Order of the Court

This offense is briefly described as follows:

Defendants are charged with a number of counts associated with a sophisticated phishing campaign targeting users of Poloniex and Binance's virtual currency exchanges, resulting in a loss of at least $15.7 million worth of cryptocurrency, and the subequent money laundering of the proceeds of the fraud.

Date: 2/18/2020

JOSEPH C. SPERO
UNITED STATES MAGISTRATE JUDGE
Issuing officer's signature

City and state: SF, CA

Chief US Magistrate Judge Spero
Printed name and title

Return

This warrant was received on *(date)* _____ , and the person was arrested on *(date)* _____
at *(city and state)* _____ .

Date: _____

Arresting officer's signature

Printed name and title

AO 442 (Rev. 11/11) Arrest Warrant

copy

UNITED STATES DISTRICT COURT UNDER SEAL

for the

Northern District of California

United States of America
v.

DANIL POTEKHIN, a/k/a "cronuswar," and DMITRII KARASAVIDI, a/k/a Dmitriy Karasavidi

Case No. CR-19-0572-CRB

Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) DANIL POTEKHIN,

who is accused of an offense or violation based on the following document filed with the court:

☐ Indictment ☑ Superseding Indictment ☐ Information ☐ Superseding Information ☐ Complaint

☐ Probation Violation Petition ☐ Supervised Release Violation Petition ☐ Violation Notice ☐ Order of the Court

This offense is briefly described as follows:

Defendants are charged with a number of counts associated with a sophisticated phishing campaign targeting users of Poloniex and Binance's virtual currency exchanges, resulting in a loss of at least $15.7 million worth of cryptocurrency, and the subequent money laundering of the proceeds of the fraud.

Date: 2/18/2020

JOSEPH C. SPERO
UNITED STATES MAGISTRATE JUDGE
Issuing officer's signature

City and state: SF, CA

Chief US Magistrate Judge Spero
Printed name and title

Return

This warrant was received on *(date)* _____, and the person was arrested on *(date)* _____
at *(city and state)* _____.

Date: _____

Arresting officer's signature

Printed name and title

United States District Court

FOR THE
NORTHERN DISTRICT OF CALIFORNIA

UNDER SEAL

VENUE: SAN FRANCISCO

UNITED STATES OF AMERICA,

V.

DANIL POTEKHIN, a/k/a "cronuswar," and
DMITRII KARASAVIDI, a/k/a Dmitriy Karasavidi

DEFENDANT(S).

SUPERSEDING INDICTMENT

18U.S.C.§1030(b)–Conspiracy to Commit Computer Fraud & Abuse;
18 U.S.C. §§ 1030(a)(4) and (c)(3)(A) – Unauthorized Access to a Protected Computer To Obtain Value;
18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud;
18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft;
18 U.S.C. § 1956(h) – Money Laundering Conspiracy;
18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j), and 981(a)(1)(C) and 28 U.S.C. § 2461(c) – Forfeiture Allegations

True Bill

A true bill.

Foreman

Filed in open court this 18 day of

February 2020

KAREN L. HOM
Clerk

JOSEPH C. SPERO
~~UNITED STATES MAGISTRATE JUDGE~~

Bail, $ no bail warrants.

3-8

AO 257 (Rev. 6/78)

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT
☒ SUPERSEDING

FILED
FEB 18 2020
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTH DISTRICT OF CALIFORNIA

Name of District Court, and/or Judge/Magistrate Location
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

OFFENSE CHARGED

PLEASE SEE ATTACHMENT

☐ Petty
☐ Minor
☐ Misde-meanor
☒ Felony

PENALTY: PLEASE SEE ATTACHMENT

DEFENDANT - U.S

DMITRII KARASAVIDI, a/k/a Dmitriy Karasavidi

DISTRICT COURT NUMBER
CR-19-0572-CRB

UNDER SEAL

PROCEEDING

Name of Complaintant Agency, or Person (& Title, if any)
USSS

☐ person is awaiting trial in another Federal or State Court, give name of court

☐ this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of:
☐ U.S. ATTORNEY ☐ DEFENSE
} SHOW DOCKET NO.

☐ this prosecution relates to a pending case involving this same defendant

☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under
} MAGISTRATE CASE NO.

Name and Office of Person Furnishing Information on this form: DAVID L. ANDERSON
☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned): Cynthia Frey, AUSA, Tax Div.

DEFENDANT

IS *NOT* IN CUSTODY

1) ☒ Has not been arrested, pending outcome this proceeding. If not detained give date any prior summons was served on above charges ▶

2) ☐ Is a Fugitive

3) ☐ Is on Bail or Release from (show District)

IS IN CUSTODY

4) ☐ On this charge

5) ☐ On another conviction } ☐ Federal ☐ State

6) ☐ Awaiting trial on other charges
If answer to (6) is "Yes", show name of institution

Has detainer been filed? ☐ Yes ☒ No } If "Yes" give date filed

DATE OF ARREST ▶ Month/Day/Year

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY ▶ Month/Day/Year

☐ This report amends AO 257 previously submitted

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:
☐ SUMMONS ☐ NO PROCESS* ☒ WARRANT Bail Amount:
If Summons, complete following:
☐ Arraignment ☐ Initial Appearance
Defendant Address:

Date/Time: Before Judge:

Comments:

** Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment*

UNDER SEAL

PENALTY SHEET ATTACHMENT:
DMITRII KARASAVIDI

Count 1: 18 U.S.C. § 1030(b) – Conspiracy to Commit Computer Fraud and Abuse

Maximum Penalties: (1) 10 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 2: 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A) – Unauthorized Access to a Protected Computer To Obtain Value;

Maximum Penalties: (1) 5 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 3: 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud

Maximum Penalties: (1) 20 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Counts 4 & 5: 18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft

Maximum Penalties: (1) 2 years imprisonment (to run consecutive to any other term imposed); (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 6: 18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering

Maximum Penalties: (1) 20 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

AO 257 (Rev. 6/78)

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT
☒ SUPERSEDING

Name of District Court, and/or Judge/Magistrate Location
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

OFFENSE CHARGED

PLEASE SEE ATTACHMENT

☐ Petty
☐ Minor
☐ Misde-meanor
☒ Felony

PENALTY: PLEASE SEE ATTACHMENT

DEFENDANT - U.S

FILED
FEB 18 2020
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTH DISTRICT OF CALIFORNIA

▶ DANIL POTEKHIN, a/k/a "cronuswar"

DISTRICT COURT NUMBER
CR-19-0572-CRB

PROCEEDING

Name of Complaintant Agency, or Person (& Title, if any)
USSS

☐ person is awaiting trial in another Federal or State Court, give name of court

☐ this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of:
☐ U.S. ATTORNEY ☐ DEFENSE
} SHOW DOCKET NO.

☐ this prosecution relates to a pending case involving this same defendant

☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under
} MAGISTRATE CASE NO.

DEFENDANT

IS *NOT* IN CUSTODY

1) ☒ Has not been arrested, pending outcome this proceeding. If not detained give date any prior summons was served on above charges ▶

2) ☐ Is a Fugitive

3) ☐ Is on Bail or Release from (show District)

UNDER SEAL

IS IN CUSTODY

4) ☐ On this charge

5) ☐ On another conviction } ☐ Federal ☐ State

6) ☐ Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

Has detainer been filed? ☐ Yes ☒ No } If "Yes" give date filed

DATE OF ARREST ▶ Month/Day/Year

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY ▶ Month/Day/Year

Name and Office of Person Furnishing Information on this form: DAVID L. ANDERSON
☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned): Cynthia Frey, AUSA, Tax Div.

☐ This report amends AO 257 previously submitted

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:
☐ SUMMONS ☐ NO PROCESS* ☐ WARRANT Bail Amount:
If Summons, complete following:
☐ Arraignment ☐ Initial Appearance
Defendant Address:

** Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment*

Date/Time: Before Judge:

Comments:

PENALTY SHEET ATTACHMENT
DANIL POTEKHIN

UNDER SEAL

Count 1: 18 U.S.C. § 1030(b) – Conspiracy to Commit Computer Fraud and Abuse

Maximum Penalties: (1) 10 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 2: 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A) – Unauthorized Access to a Protected Computer To Obtain Value;

Maximum Penalties: (1) 5 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 3: 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud

Maximum Penalties: (1) 20 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Counts 4 & 5: 18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft

Maximum Penalties: (1) 2 years imprisonment (to run consecutive to any other term imposed); (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 6: 18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering

Maximum Penalties: (1) 20 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Forfeiture Allegations: 18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j), and 981(a)(1)(C) and 28 U.S.C. § 2461(c)

DAVID L. ANDERSON (CABN 149604)
United States Attorney

UNDER SEAL

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

CR19572CRB

UNITED STATES OF AMERICA, Plaintiff, v. DANIL POTEKHIN, a/k/a "cronuswar," and DMITRII KARASAVIDI, a/k/a Dmitriy Karasavidi Defendants.	CASE NO. VIOLATIONS: 18 U.S.C. § 1030(b) – Conspiracy to Commit Computer Fraud and Abuse; 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A) – Unauthorized Access to a Protected Computer to Obtain Value; 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud; 18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft; 18 U.S.C. § 1956(h) – Money Laundering Conspiracy; 18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j), and 981(a)(1)(C) and 28 U.S.C. § 2461(c) – Forfeiture Allegations SAN FRANCISCO VENUE

SUPERSEDING INDICTMENT

The Grand Jury charges:

Background

At all times relevant to this Indictment:

1. DANIL POTEKHIN, a/k/a "cronuswar," is a resident of the Russian Federation.

2. DMITRII KARASAVIDI, a/k/a Dmitriy Karasavidi, is a resident of the Russian Federation.

3. Poloniex, LLC ("Poloniex") is a digital currency exchange platform based in Wilmington, Delaware.

4. Bittrex is a digital currency exchange platform, based in Seattle, Washington.

5. Binance is a digital currency exchange platform that was originally based in Hong Kong, China, and is currently headquartered in Malta.

6. Bitfinex is a digital currency exchange platform based in the British Virgin Islands.

7. Gemini Trust Company LLC ("Gemini") is a digital currency exchange platform based in New York, New Work.

8. Bitcoin ("BTC") is a form of decentralized, convertible digital currency that exists through the use of an online, decentralized ledger system, referred to as a "blockchain." While Bitcoin mainly exists as an Internet-based form of currency, it is possible to "print out" the necessary information and exchange Bitcoin via physical medium. The currency is not issued by any government, bank, or company, but rather is generated and controlled through computer software operating via a decentralized network. Bitcoin is typically acquired by purchasing it from a Bitcoin seller or "exchanger." It is also possible to "mine" Bitcoin by verifying other users' transactions. Bitcoin is just one form of digital currency, and there are many other varieties of digital currency.

9. Bitcoin exchangers typically accept payments in the form of fiat currency (such as dollars, euros, or other currency that derives its value from its support by governments), or other convertible digital currencies. When a user wishes to purchase Bitcoin from an exchanger, the user will typically send payment in the form of fiat currency, often via bank wire or ACH, or other convertible digital currency to an exchanger, for the corresponding quantity of Bitcoin, based on a fluctuating exchange rate. The exchanger, often for a commission, will then typically attempt to broker the purchase with another user of the exchange that is trying to sell Bitcoin, or, in some instances, will act as the seller itself. If the exchanger can place a buyer with a seller, then the transaction can be completed.

10. When a user acquires Bitcoin, ownership of the Bitcoin is transferred to the user's Bitcoin address. The Bitcoin address is somewhat analogous to a bank account number, and is comprised of a case-sensitive string of letters and numbers amounting to a total of 26 to 35 characters. The user can then conduct transactions with other Bitcoin users, by transferring Bitcoin to their Bitcoin

addresses, via the Internet. "Bitcoin address clustering" is a process that attempts to de-anonymize a user by identifying all of the addresses that they control.

11. Little to no personally identifiable information about the payer or payee is transmitted in a Bitcoin transaction itself. Bitcoin transactions occur using a public key and a private key. A public key is used to receive Bitcoin, and a private key is used to allow withdrawals from a Bitcoin address. Only the Bitcoin address of the receiving party and the sender's private key are needed to complete the transaction. These two keys by themselves rarely reflect any identifying information.

12. Digital currencies, including Bitcoin, have many known legitimate uses. However, much like cash, Bitcoin can be used to facilitate illicit transactions and to launder criminal proceeds, given the ease with which Bitcoin can be used to move funds with high levels of anonymity. In some circumstances Bitcoin payments may be traced to accounts at traditional financial institutions using the blockchain.

13. Ethereum ("ETH") is a digital currency that is open source, public, has a blockchain, and is distributed on a platform that uses "smart contract" technology. By definition, smart contracts are computer protocols that automatically enforce a pre-arranged negotiation between individuals conducting a transaction. These protocols are also sometimes called self-executing contracts.

14. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH. Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided without any type of middle-man or counterparty controlling a desired outcome. Smart contract technology is one of Ethereum's main selling points and an important tool for companies or individuals executing trades on the ETH blockchain. The ETH platform allows developers to build and deploy software and decentralized applications using the blockchain protocol. The ETH blockchain protocol allows smart contracts to operate without fraud, censorship, or third-party interference.

15. Gnosis is a platform built as a decentralized application on the Ethereum network. GNO is the digital currency token used on the Gnosis platform.

16. NEO, formerly called as AntShares, is China's first open source blockchain platform. GAS is the digital currency token used to pay the cost of execution on the NEO blockchain.

17. Poloniex, Binance, and Gemini are exchanges that offer their users the ability to trade digital currencies, such as BTC, ETH, GAS, and GNO via the Internet. Users of these exchanges could access their accounts with their email address and a unique password, and through this account, could store, access, move, or trade digital currency. Poloniex places transaction limitations on certain accounts. Where such limitations were in place at Poloniex, the transaction limits could be increased by linking their accounts to other accounts.

18. The computer servers used by Poloniex, Binance, and Gemini in operating their exchanges and user accounts were used to facilitate interstate and foreign commerce and communication, including by interstate and foreign electronic signals, and constituted "protected computers" as defined in Title 18, United States Code, Section 1030(e)(2)(B).

The Conspiracy and Scheme to Defraud

19. As part of the conspiracy and scheme to defraud, the defendants used the Internet to launch a sophisticated phishing campaign targeting users of Poloniex, Binance, and Gemini's digital currency exchanges. The defendants purchased and deployed multiple websites that appeared to users to be the legitimate Poloniex, Binance, and Gemini digital currency exchanges. However, when users would log into these fraudulent websites, the defendants were able to steal their credentials, in the form of an email address, and their password information, enabling the defendants to control their actual Poloniex, Binance, and Gemini accounts, withdraw some or all of their digital currency, and manipulate the market for digital currency. This resulted in losses of digital currencies valued at approximately $17 million for Poloniex, Binance, and Gemini customers, including customers in the Northern District of California.

COUNT ONE: (18 U.S.C. § 1030(b) – Conspiracy to Commit Computer Fraud and Abuse)

20. Paragraphs 1 through 19 of this Indictment are re-alleged and incorporated as if fully set forth here.

21. Beginning at a time unknown to the Grand Jury, but no later than on or about June 8, 2017, and continuing through a date unknown, but at least through on or about April 15, 2018, in the Northern District of California, and elsewhere, the defendants,

DANIL POTEKHIN, and
DMITRII KARASAVIDI,

did knowingly and willfully conspire and agree with each other and with others, to commit computer fraud and abuse, namely, with intent to defraud, accessed a protected computer used in interstate and foreign commerce without authorization and exceeding authorized access, and by means of such conduct furthered the below-described fraud and obtained something of value, in violation of 18 U.S.C. § 1030(a)(4).

22. In furtherance of the conspiracy, the defendants used the following manner and means to accomplish the object and purpose of the conspiracy:

a. Using fraud, deception, and social engineering techniques to gain access to the user identification and passwords of victim users of the Poloniex, Binance, and Gemini exchange platforms;

b. Using identification of others without lawful authority, and fictitious identities to create fictitious Poloniex, Binance, Gemini, and Bittrex accounts to facilitate the fraud scheme;

c. Using information obtained from victim customers of the Poloniex, Binance, and Gemini exchange platforms to access their digital currency addresses and transfer cryptocurrencies owned by the victims without authority;

d. Using unauthorized access to victim customer Poloniex accounts to manipulate the digital currency markets and take advantage of the immediate increase in digital currency value to their benefit; and

e. Using multiple digital currency addresses and clusters to deposit the stolen digital currencies and using a layered process for withdrawal and deposits to conceal the nature, source, location, ownership, or control of the digital currency.

23. In furtherance of the conspiracy and to effect its objects, on or about the dates listed below, in the Northern District of California and elsewhere, POTEKHIN, KARASAVIDI and others, committed the following overt acts, among others:

Poloniex Theft Attack

a. Between on or about July 17, 2017, and at least on or about October 29, 2017, POTEKHIN created and controlled at least 13 separate fake Poloniex domains to be used in a fraud scheme targeting Poloniex and its users.

b. Between on or about July 17, 2017, and at least on or about October 29, 2017, POTEKHIN induced at least 158 victim customers of the Poloniex exchange platform, including Poloniex customers in the Northern District of California, to access the fake Poloniex domains, causing the victim customers to input their user identification and passwords in order to access their Poloniex account, enabling POTEKHIN and others to obtain the customers' user identification, which is the user's email address, and passwords without authorization.

c. Between on or about June 8, 2017 and July 17, 2017, POTEKHIN, KARASAVIDI, and others created five fictitious Poloniex accounts. At least three of those accounts were in the names of individuals from the United Kingdom: A.C., N.B., and C.A. To create these three accounts, the defendants fraudulently used the means of identification of A.C., N.B., and C.A. POTEKHIN and others possessed the means of identification of A.C., N.B., and C.A. prior to the creation of these fictitious accounts. KARASAVIDI also had access to one of the other fictitious Poloniex accounts.

d. Between at least on or about August 3, 2017 and August 23, 2017, POTEKHIN, KARASAVIDI, and others used user identification and passwords obtained without authorization to gain access to the approximately 155 victim customer Poloniex accounts and withdraw digital currency without authorization. POTEKHIN, KARASAVIDI, and others also used some of the five fictitious accounts, described above, along with victim user identification and passwords obtained without authorization, to link to the victim user accounts, enabling them to withdraw larger sums of digital currency from victim accounts without authorization. Approximately $700,000 in BTC was withdrawn without authorization from victim user accounts, including digital currency from T.S. and J.S., who resided in the Northern District of California, and deposited into one BTC cluster.

e. Between on or about July 8, 2017 and July 15, 2017, POTEKHIN, KARASAVIDI and others created three fictitious Bittrex accounts to receive BTC from the fraud scheme. KARASAVIDI had access to one of the fictitious Bittrex accounts, registered using the email account **********659@yahoo.com, which was the same email account used to register one of the five fictitious accounts. POTEKHIN had access to the identity of one of these Bittrex accounts.

//

Between on or about August 10, 2017 and on or about September 19, 2017, approximately 435 Bitcoins were sent from the Bitcoin cluster to these three fictitious Bittrex accounts.

f. Between on or about August 13, 2017 and on or about September 27, 2017, most of the BTC from the three fictitious Bittrex accounts, including one account also in the name of A.C., was converted to approximately 8,816 ETH and through a sophisticated and layered manner was sent through multiple intermediary accounts, before ultimately being deposited into a Bitfinex account controlled by KARASAVIDI.

Poloniex Manipulation Attack

g. Between on or about July 18, 2017 and on or about August 13, 2017, POTEKHIN and others created nine more fictitious Poloniex accounts, each of which provided a residence in Ukraine or Russia. Eight of those fictitious accounts purchased 300 GAS at relatively low prices (the "Eight Fictitious Poloniex Accounts"). One of these eight accounts was controlled by POTEKHIN. One of the eight accounts also purchased GNO. These Eight Fictitious Poloniex Accounts were then used in a manipulation attack targeting three victim Poloniex customer accounts, with a total holdings of approximately $5,243,000 worth of digital currency on or about October 29, 2017.

h. Using the same phishing means set forth above, POTEKHIN and others unlawfully and without authorization obtained the user identification and passwords for these three victim accounts. On or about October 29, 2017, POTEKHIN and others unlawfully and without authorization obtained access to the victim accounts. Using digital currency in one victim Poloniex account, they placed an order to purchase approximately 8,000 GAS, thereby immediately increasing the market price of GAS from approximately $18 to $2,400. POTEKHIN and others then converted the artificially inflated GAS in their own fictitious Poloniex accounts into ETH and BTC. Using digital currency in the other two victim Poloniex accounts, POTEKHIN and others purchased GNO. The total digital currency contained in the Eight Fictitious Poloniex Accounts on October 30, 2017, when Poloniex froze the accounts, was approximately 15,600 ETH and .16 BTC. Before the Eight Fictitious Poloniex Accounts were frozen, POTEKHIN and others transferred approximately 759 ETH to nine digital currency addresses. Through a sophisticated and layered manner, the ETH from these nine

//

digital currency addresses was sent through multiple intermediary accounts, before ultimately being deposited into a Bitfinex account controlled by KARASAVIDI.

Binance Theft Attack

i. Between on or about October 16, 2017 and October 31, 2017, POTEKHIN and others created at least two fictitious Binance accounts using the email accounts of two individuals from the United Kingdom. POTEKHIN and others possessed the email accounts of these individuals prior to the creation of these fictitious accounts.

j. Between at least on or about at least December 19, 2017, until on or about March 2, 2018, POTEKHIN, KARASAVIDI, and others induced at least 142 victim customers of the Binance exchange platform, including at least one Binance customer in the Northern District of California, to access the fake Binance domains, causing the victim customers to input their user identification and passwords in order to access their Binance account, enabling POTEKHIN and others to obtain the customers' user identification, which is the user's email address, and passwords without authorization.

k. POTEKHIN, KARASAVIDI, and others used the user identification and passwords obtained without authorization to gain access to approximately 142 victim customer Binance accounts and withdraw digital currency without authorization. Approximately 566 BTC, with a value of over $10 million BTC (valued on December 19, 2017), was withdrawn without authorization, including digital currency from one victim in the Northern District of California, and deposited into one BTC cluster, as well as several other intermediary digital currency addresses. BTC from the cluster, as well as from several other intermediary digital currency addresses, was then deposited into the two fictitious Binance accounts described above before ultimately being deposited into a Bitfinex account controlled by KARASAVIDI.

Gemini Theft Attack

l. Between on or about October 24, 2017, and November 1, 2017, POTEKHIN, KARASAVIDI, and others induced at least 42 victim customers of the Gemini exchange platform, including at least one Gemini customer in the Northern District of California, to access the fake Gemini domains. The victim customers input their user identification and passwords, believing they were accessing their Gemini accounts instead of the fake Gemini domains. In this manner, POTEKHIN and

others obtained the customers' user identification, which was the users' email address, and passwords without authorization.

m. POTEKHIN, KARASAVIDI, and others used the user identification and passwords obtained without authorization to gain access to victim customer Gemini accounts and withdraw digital currency without authorization. Approximately $1.176 million in United States dollars and digital currencies, was withdrawn without authorization from these accounts, including digital currency from one victim in the Northern District of California. The valuation of the digital currencies was based upon the average value between October 24, 2017 and November 1, 2017. Some of the stolen digital currency was intermingled with funds obtained by the co-conspirators in the Poloniex Market Manipulation Attack. Together, those funds then were moved through several intermediary digital currency addresses before being deposited into a Bitfinex account controlled by KARASAVIDI. Still other digital currency that was stolen from the victim Gemini accounts was deposited into a Binance account that had also received digital currency from the Binance Theft Attack, before it was ultimately deposited into a Bitfinex account controlled by KARASAVIDI.

Money Laundering from the Poloniex, Binance, and Gemini Attacks

n. In total, at least $16,876,000 in digital and fiat currency was reported stolen in the Poloniex, Binance, and Gemini Attacks, which was obtained through the above described fraud scheme by the co-conspirators. These fraud proceeds were then moved through various accounts, in an effort by the co-conspirators to promote the fraud and to conceal and disguise the nature, source, ownership, and control of the funds. Specifically, the digital currency from the Poloniex Manipulation Attack was intermingled with the digital currency from the Poloniex Theft Attack, as well as digital and fiat currencies from the Binance Theft Attack and the Gemini Theft Attack. Through a sophisticated and layered manner, these fraud proceeds were sent through multiple intermediary accounts, before approximately 19,600 ETH was ultimately deposited on March 11, 2018, March 18, 2018, April 9, 2018, and April 15, 2018 into a Bitfinex account controlled by KARASAVIDI.

All in violation of Title 18, United States Code, Section 1030(b).

//

//

COUNT TWO: (18 U.S.C. § 1030(a)(4) – Computer Fraud)

24. Paragraphs 1 through 23 of this Indictment are re-alleged and incorporated as if fully set forth here.

25. On or about June 8, 2017, and continuing through a date unknown, but at least through on or about April 15, 2018, within the Northern District of California and elsewhere, the defendants,

DANIL POTEKHIN, and
DMITRII KARASAVIDI,

knowingly and with intent to defraud accessed a protected computer used in interstate and foreign commerce without authorization and exceeding authorized access, and by means of such conduct furthered the intended fraud and obtained something of value, specifically digital currency addresses and passkeys, containing digital currency later withdrawn without authorization by defendants.

All in violation of 18 U.S.C. Sections 1030(a)(4) and (c)(3)(A).

COUNT THREE: (18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud)

26. Paragraphs 1 through 23 of this Indictment are re-alleged and incorporated as if fully set forth here.

27. Beginning at a time unknown to the Grand Jury, but no later than on or about June 8, 2017, and continuing through a date unknown, but at least through on or about April 15, 2018, in the Northern District of California and elsewhere, the defendants,

DANIL POTEKHIN, and
DMITRII KARASAVIDI,

and others, did knowingly conspire to devise and intend to devise a scheme and artifice to defraud as to a material matter and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and by concealment of material facts, and, for the purpose of executing such scheme or 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, in violation of Title 18, United States Code, Section 1343.

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

COUNT FOUR: (18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft)

28. Paragraphs 1 through 27 of this Indictment are re-alleged and incorporated as if fully set forth here.

29. Between on or about June 8, 2017 and August 23, 2017, in the Northern District of California and elsewhere, the defendants,

DANIL POTEKHIN, and
DMITRII KARASAVIDI,

during and in relation to the crime of Conspiracy to Commit Computer Fraud and Abuse, in violation of 18 U.S.C. § 1030(b); Computer Fraud, in violation of 18 U.S.C. § 1030(a)(4); and Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349, did knowingly transfer, possess, and use, without lawful authority the means of identification of another person, to wit, the username and password of T.S.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

COUNT FIVE: (18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft)

30. Paragraphs 1 through 27 of this Indictment are re-alleged and incorporated as if fully set forth here.

31. Between on or about June 8, 2017 and August 23, 2017, in the Northern District of California and elsewhere, the defendants,

DANIL POTEKHIN, and
DMITRII KARASAVIDI,

during and in relation to the crime of Conspiracy to Commit Computer Fraud and Abuse, in violation of 18 U.S.C. § 1030(b); Computer Fraud, in violation of 18 U.S.C. § 1030(a)(4); and Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349, did knowingly transfer, possess, and use, without lawful authority the means of identification of another person, to wit, the username and password of J.S.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

//

//

//

COUNT SIX: (18 U.S.C. § 1956(h) – Money Laundering Conspiracy)

32. Paragraphs 1 through 27 of this Indictment are re-alleged and incorporated as if fully set forth here.

33. From on or about June 8, 2017, through on or about April 15, 2018, in the Northern District of California and elsewhere, the defendants,

DANIL POTEKHIN, and
DMITRII KARASAVIDI,

did knowingly combine, conspire, and agree with each other and with other persons known and unknown to the Grand Jury to conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, Conspiracy to Commit Computer Fraud and Abuse, in violation of 18 U.S.C. § 1030(b); Computer Fraud, in violation of 18 U.S.C. § 1030(a)(4); and Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349; knowing the property involved in the financial transactions represented the proceeds of some form of unlawful activity and knowing the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

All in violation of Title 18, United States Code, Section 1956(h).

COMPUTER FRAUD FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j))

34. The allegations contained in this Indictment are re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(b) and 1030(i) and (j).

35. Upon conviction for the offenses set forth in Counts One and Two in violation of Title 18, United States Code, Section 1030, set forth in this Indictment, the defendants,

DANIL POTEKHIN, and
DMITRII KARASAVIDI,

shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(b) and 1030(i) and (j), any personal property used or intended to be used to commit or to facilitate the commission of said violation or a conspiracy to violate said provision, and any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses, including, but not limited to:

a. 15,602 ETH and .016 BTC seized by law enforcement on or about December 14, 2017 (with a value of approximately $12,623,627 in USD on that date);

b. 238.32 BTC, $6,164,994.23 USD, .99 Bitcoin Cash (BCH), 196.13 Bitcoin Gold (BTG), 1199.99 NEO, and 50,000 EOS seized by law enforcement on or about August 23, 2019 (with a value of approximately $8,768,000 USD on that date); and

c. a money judgment equal to the total amount of proceeds defendant obtained or derived, directly or indirectly, from the violation, or the value of the property used to commit or to facilitate the commission of said violation.

36. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon 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,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 1030(i)(2).

All pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030, and Federal Rule of Criminal Procedure 32.2.

//

//

//

WIRE FRAUD FORFEITURE ALLEGATION: (18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c))

37. The allegations contained in this Indictment are re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).

38. Upon conviction for the offense set forth in Count Three of this Indictment, the defendants,

DANIL POTEKHIN, and
DMITRII KARASAVIDI,

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), all property, real or personal, constituting, or derived from proceeds the defendant obtained directly and indirectly, as the result of those violations; including but not limited to:

a. 15,602 ETH and .016 BTC seized by law enforcement on or about December 14, 2017 (with a value of approximately $12,623,627 in USD on that date);

b. 238.32 BTC, $6,164,994.23 USD, .99 Bitcoin Cash (BCH), 196.13 Bitcoin Gold (BTG), 1199.99 NEO, and 50,000 EOS seized by law enforcement on or about August 23, 2019 (with a value of approximately $8,768,000 USD on that date); and

c. A money judgment equal to the total amount of proceeds the defendant obtained as a result of the offense.

39. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon 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,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21,

United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

All pursuant to Title 18, United States Code, Section 981(a)(1)(C), Title 28, United States Code, Section 2461(c), and Federal Rule of Criminal Procedure 32.2.

MONEY LAUNDERING FORFEITURE ALLEGATION: (18 U.S.C. § 982(a)(1))

40. The allegations contained in this Indictment are re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 982(a)(1).

41. Upon conviction for the offense set forth in Count Six of this Indictment, the defendant,

DANIL POTEKHIN, and
DMITRII KARASAVIDI,

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), all property, real or personal, involved in said violations, or any property traceable to such property, including, but not limited to:

a. 15,602 ETH and .016 BTC seized by law enforcement on or about December 14, 2017 (with a value of approximately $12,623,627 in USD on that date);

b. 238.32 BTC, $6,164,994.23 USD, .99 Bitcoin Cash (BCH), 196.13 Bitcoin Gold (BTG), 1199.99 NEO, and 50,000 EOS seized by law enforcement on or about August 23, 2019 (with a value of approximately $8,768,000 USD on that date); and

c. A money judgment equal to the total amount of funds involved in the offense.

//

//

//

//

//

//

//

//

42. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon 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,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1).

All pursuant to Title 18, United States Code, Sections 982(a)(1) and (b)(1) and Federal Rule of Criminal Procedure 32.2.

DATED: 2/18/2020

A TRUE BILL.

FOREPERSON

DAVID L. ANDERSON
United States Attorney

CYNTHIA FREY
Assistant United States Attorney

UNDER SEAL

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

FILED

FEB 18 2020

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTH DISTRICT OF CALIFORNIA

CRIMINAL COVER SHEET

Instructions: *Effective November 1, 2016, this Criminal Cover Sheet must be completed and submitted along with the Defendant Information Form, for each new criminal case.*

CASE NAME:	CASE NUMBER:
USA v. DANIL POTEKHIN, a/k/a "cronuswar," and DMITRII KARASAVIDI, a/k/a Dmitriy Karasavidi	CR 19-0572-CRB

Is This Case Under Seal?	**Yes** ✓	**No**	
Total Number of Defendants:	**1**	**2-7** ✓	**8 or more**
Does this case involve ONLY charges under 8 U.S.C. § 1325 and/or 1326?	**Yes**	**No** ✓	
Venue (Per Crim. L.R. 18-1):	**SF** ✓	**OAK**	**SJ**
Is this a potential high-cost case?	**Yes**	**No** ✓	
Is any defendant charged with a death-penalty-eligible crime?	**Yes**	**No** ✓	
Is this a RICO Act gang case?	**Yes**	**No** ✓	

Assigned AUSA (Lead Attorney): CYNTHIA FREY, AUSA **Date Submitted:** 2/18/2020

Comments:

RESET FORM SAVE PDF

UNDER SEAL

FILED

FEB 18 2020

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

DAVID L. ANDERSON (CABN 149604)
United States Attorney

HALLIE HOFFMAN (CABN 210020)
Chief, Criminal Division

CYNTHIA FREY (DCBN 475889)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7200
Fax: (415) 436-7234
cynthia.frey@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. DANIL POTEKHIN, a/k/a "cronuswar," and DMITRII KARASAVIDI, a/k/a Dmitriy Karasavidi Defendants.	No.: CR-19-0572-CRB MOTION TO SEAL SUPERSEDING INDICTMENT AND [~~PROPOSED~~] ORDER (UNDER SEAL)

The government hereby moves the Court for an order sealing the Superseding Indictment, this motion, and the Court's sealing order until execution of the arrest warrant for defendants DANIL POTEKHIN, a/k/a "cronuswar," and DMITRII KARASAVIDI, a/k/a Dmitriy Karasavidi. In order to reduce the chances that the defendants will flee and for reasons of officer safety, the United States requests that the fact of

//

//

//

//

the arrest warrant remain under seal until the warrant is executed. The Court's sealing order will be lifted automatically once the arrest warrant is executed.

DATED: February 13, 2020

Respectfully submitted,

DAVID L. ANDERSON
United States Attorney

CYNTHIA FREY
Assistant United States Attorney

[PROPOSED] ORDER

Based upon the motion of the government and for good cause shown, IT IS HEREBY ORDERED that the Superseding Indictment, this motion, and this sealing order shall be sealed until execution of the arrest warrant for defendants DANIL POTEKHIN, a/k/a "cronuswar," and DMITRII KARASAVIDI, a/k/a Dmitriy Karasavidi or until further order of the Court, whichever occurs first. This sealing order shall not prevent the Clerk from providing copies of the aforementioned documents to the United States upon request of an attorney for the United States.

DATED: 2/14/2020

HON. JOSEPH C. SPERO
Chief United States Magistrate Judge