RMT:AFM/JSY
F. #2014R00176

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- X

UNITED STATES OF AMERICA

- against -

DENIS GENNADIEVICH KULKOV,
also known as "Kreenjo,"
"Nordex" and "Nordexin"

Defendant.

- X

AFFIDAVIT AND COMPLAINT IN SUPPORT OF AN APPLICATION FOR AN ARREST WARRANT

(T. 18, U.S.C., §§ 1029(b)(2), 1029(h), 2 and 3551 et seq.)

No. 19-M-1179

EASTERN DISTRICT OF NEW YORK, SS:

RICHARD PENA-ARIET, being duly sworn, deposes and states that he is a Special Agent with the United States Secret Service, duly appointed according to law and acting as such:

In or about and between January 1, 2005 and December 17, 2019, both dates being approximate and inclusive, in the Eastern District of New York and within the extraterritorial jurisdiction of the United States, the defendant DENIS GENNADIEVICH KULKOV, also known as "Kreenjo," "Nordex" and "Nordexin," together with others, did knowingly and with intent to defraud conspire to: (1) traffic in and use one or more unauthorized access devices during any one-year period, and by such conduct obtain anything of value aggregating $1,000 or more during that period; (2) possess fifteen or more unauthorized access devices; (3) effect transactions with one or more access devices issued to another person or persons, to receive payment or any other thing of value during any one-

year period the aggregate value of which is equal to or greater than $1,000; and (4) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicit a person for the purpose of selling information regarding or an application to obtain an access device, all of which conduct affected interstate and foreign commerce, contrary to Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3), 1029(a)(5) and 1029(a)(6), and such offenses involved one or more access devices issued, owned, managed and controlled by one or more financial institutions, account issuers, credit card system members and other entities within the jurisdiction of the United States.

(Title 18, United States Code, Sections 1029(b)(2), 1029(h), 2 and 3551 et seq.)

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I am a Special Agent with the United States Secret Service ("USSS") and have been a Special Agent with the USSS since 2014. I am currently assigned to the Global Investigative Operations Center in Washington, D.C., where I conduct analysis of non-traditional data sources to coordinate agency operations in order to disrupt and dismantle illicit activities and criminal networks. I was previously assigned to the Electronic Crimes Task Force ("ECTF") in the New York Field Office of the USSS, where my work included the investigation of mail, wire and computer fraud. As a member of the ECTF, I was

[1] Because the purpose of this complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

responsible for conducting and assisting in investigations into the activities of individuals and criminal groups who use computers and computer networks to pursue illegal activities. These investigations are conducted both in an undercover and overt capacity. I have received training in investigative techniques specific to computer fraud investigations. As a result of my training and experience, I am familiar with the methods employed by individuals using computers to facilitate illegal activities, as well as the techniques and methods of operation that these individuals use to conceal their activities from detection by law enforcement authorities.

2. I am familiar with the facts and circumstances set forth below from my participation in the investigation, from my review of documents obtained pursuant to the investigation, and from reports of other law enforcement officers involved in the investigation. When I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated. In addition, many of the statements described herein are based on draft English translations of communications that were not originally made in English, and are subject to revision.

I. The Defendant

3. DENIS GENNADIEVICH KULKOV, also known as "Kreenjo," "Nordex" and "Nordexin," is a 39-year-old male Russian national who resides in Samara, Russia.

II. Background Regarding Online Credit Card Fraud and "Card Checking" Services

4. Based on my knowledge, training and experience, cybercriminals steal millions of credit card numbers every year by breaching corporate databases and hacking into payment systems, among other methods. These numbers are then resold in bulk

through online message boards, known as "carding forums."[2] Carding forums serve as marketplaces where thieves can sell batches of stolen credit card numbers, and as virtual meeting places where cybercriminals communicate, advertise and access necessary services.

5. A batch of stolen credit card numbers has a limited and unpredictable lifespan. Of the thousands or millions of cards in any batch, many are already inactive when stolen, or are deactivated soon afterward when the cardholders or issuers become aware of the breach or detect suspicious activity.

6. Thus, one of the most important auxiliary services in the carding world is provided by so-called "card checking" services. These websites permit cybercriminals to quickly verify the authenticity of stolen credit card numbers, and to determine the percentage of cards in a batch that are still active. Without credible and efficient third-party verification, credit card batches would be difficult to sell, because buyers would have no way to reliably ascertain the value of the data being offered.

III. Background Regarding Try2Check

7. One of the most visible and popular card checking services in the cybercriminal underworld is a platform called "Try2Check." Try2Check is available on the open, publicly accessible internet and on the dark web, and it offers an application programming interface ("API") that allows it to integrate easily into third-party services. Try2Check offers its users the ability to quickly determine the validity of a credit card number, either singly or in bulk; users can upload thousands of card numbers at a time and

---

[2] The practice of acquiring and trafficking in stolen credit cards is known as "carding."

receive an immediate report as to which numbers are valid. "Checks" can be purchased only in bitcoin and cost whatever amount of bitcoin corresponds to $0.14 (USD) at the time of purchase.

8. Try2Check is currently available at four different domains: Try2services.pm, Try2services.cm, Try2services.vc, and the dark web address Try2checklm32oc3.onion.

9. Although Try2Check has competitors, it appears to be one of the most popular websites of its type among cybercriminals. Users on carding forums who are advertising a batch of cards for sale sometimes include a screenshot of the accompanying report from Try2Check. As discussed further below, Try2Check appears to process tens of millions of card-checking transactions per year.

10. Since 2013, the USSS and the Federal Bureau of Investigation (jointly the "Investigating Agencies") have been conducting an investigation into Try2Check. As set forth below, the Investigative Agencies have determined that DENIS KULKOV operates Try2Check. Further, and as set forth in detail below, the investigation has revealed that Try2Check determines the validity of U.S.-issued cards submitted to its service by obtaining unauthorized access to the servers of a major U.S. payment processor ("Victim-1"). Specifically, Try2Check takes advantage of a system at Victim-1 that allows merchants to access Victim-1's systems in order to "preauthorize" charges on credit cards without actually placing a charge. Try2Check impersonates a merchant seeking preauthorization in order to extract validity information from Victim-1.

IV. Online Accounts and Postings Link DENIS KULKOV with Try2Check

11. As set forth below, Try2Check has historically been associated with certain online nicknames and communication accounts that, in turn, belong to DENIS KULKOV.

a. Try2Check is Associated with the Username "Kreenjo" and Two ICQ Numbers

12. Based on my review of data from the Internet Archive, a publicly accessible web archiving system, Try2Check has been available (under a variety of names) since 2005. The earliest version of Try2Check, which was in operation from 2005 to 2009, was located at the URL "just-buy.it." Records from the Internet Archive reflect that just-buy.it displayed a logo containing a distinctive figure (two opposing, nonaligned semicircles) that also appears on the current versions of Try2Check. The just-buy.it logo contained the text "KreenJo" and the phrase "icq 855377" (the "855 ICQ"), a reference to a point of contact on the chat network ICQ. Moreover, in 2008, a page on just-buy.it contained text indicating that users could seek technical support by sending a message to ICQ number 555724 (the "555 ICQ").

b. "Kreenjo" is Associated with the Username "Nordex"

13. The user named "Kreenjo" also posted on internet forums frequented by cybercriminals.

14. For example, on or about July 18, 2006, a user named "Kreenjo" posted on an online cybercrime forum ("Forum-1"), offering card checking services.[3] In his message, "Kreenjo" offered as points of contact the 855 ICQ and the 555 ICQ. The signature of the message included the 555 ICQ and the URL "check.just-buy.it," which was a web address where Try2Check could be accessed at that time.

15. Records from another online criminal forum ("Forum-2") indicate that in addition to the "Kreenjo" account on Forum-1, there also existed an account with the same username on Forum-2 that was created using the same registration email address. That account was created on or about October 31, 2006, using a computer at IP address 81.25.39.240 (the "81 IP").

16. On that same date, the 81 IP was used to create another account on Forum-2, this one with the registration email address polkas@bk.ru (the "Polkas Email"). The username for that account was "NORDEX."

c. "Nordex" Identifies Himself as "Denis from Samara"

17. The username "Nordex" existed on other forums besides Forum-2. Records from a third online criminal forum ("Forum-3") indicate that a profile called "Nordex" was created on Forum-3 on or about January 19, 2005. The IP address used to register the "Nordex" profile was 193.27.237.66 (the "193 IP") and the associated email address was the Polkas Email. Publicly available IP location data indicates that the 193 IP is assigned to an Internet Service Provider located in Samara, Russia.

---

[3] The records from Forum-1, Forum-2, and Forum-3 referred to herein were obtained by the FBI pursuant to legal process issued in other investigations.

18. "Nordex" sent private messages to other Forum-3 users with whom he hoped to do business. For example, on or about December 28, 2006 and January 3, 2007, "Nordex" posted messages offering for sale, respectively, a computer malware tool and a batch of credit card numbers. Both messages indicated that "Nordex" could be contacted at the 555 ICQ—the same ICQ number that was offered as a customer support line on just-buy.it in 2008. In a third message, "Nordex" identified himself as "Denis," a then-24-year-old individual from Samara, Russia.

d. "Nordex" and "Nordexin" are Identified as DENIS KULKOV

19. Records obtained from a cryptocurrency exchange service ("Exchange-1") indicate that there exists an Exchange-1 account with the username "Nordexin." The registered user for that account supplied the name "Denis Kulkov" and an address in Samara, Russia that is known to me (the "Kulkov Street Address"), along with a telephone number with a Russia country code that is known to me (the "Kulkov Phone Number") and two email addresses: nordexin@ya.ru (the "Ya.ru Email")[4] and "Nordexin Platform-1." Nordexin Platform-1 is the email address associated with an account that has the username "Nordexin" and is hosted on an online platform that provides email hosting and cloud backup services.

---

[4] Ya.ru is a domain owned by Yandex, a Russia-based Internet services company. Yandex also controls the domain yandex.ru. An email account with a given username at ya.ru can typically also be reached by emailing the same username at yandex.ru. Thus, the user who receives email at the Ya.ru Email would also typically control the account nordexin@yandex.ru (the "Yandex.ru Email").

The Exchange-1 account holder validated this information by supplying a photograph of KULKOV's passport and his Russian driver's license.

20. According to records provided by Microsoft, the Kulkov Phone Number is also the phone number of record for a Skype account with the username "Nordexin" that is registered in the name the name "Дени Кульков," which transliterates into Latin characters as "Denis Kulkov," and with the Kulkov Street Address.

21. In addition, records obtained from Marriot International, Inc. indicate that in or about June 2018, an individual who supplied the name "Denis Kulkov" stayed at the Ritz Carlton hotel in Moscow, Russia, along with a woman whose surname indicates that she is KULKOV's wife. KULKOV provided the Yandex.ru Email to the hotel in connection with his stay. Both KULKOV and his wife presented internal Russian travel documents to the hotel; the photograph and date of birth on KULKOV's internal travel document match that on his passport and driver's license as provided to Exchange-1, described above.

22. Furthermore, the images of KULKOV shown on his passport, internal travel document and driver's license are identical to photographs of KULKOV and his family that I have reviewed on publicly accessible social media postings. These include photographs of KULKOV and his daughter posted to an Instagram account which was identified in English as belonging to "Denis Kulkov[,] Ferrari owner." The Instagram account, which is no longer publicly available, included numerous photographs of KULKOV, his daughter, and KULKOV's Ferrari and Land Rover. The images of KULKOV on Instagram are, in turn, identical to the profile picture of an account on the social media site Foursquare that has "liked" various businesses in Samara, Russia. The

owner of the Foursquare account is identified as "Дени Кульков," which transliterates in Latin characters to the name "Denis Kulkov."

V. Nordexin Platform-1 reveals that DENIS KULKOV Operates Try2Check

23. In addition to the accounts described above, records provided by Platform-1 show that the individual who registered Nordexin Platform-1 indicated that he lived in Samara, Russia and provided the name "Дени Кульков," which transliterates into Latin characters as "Denis Kulkov." The registrant registered that account with the Kulkov Phone Number and the Kulkov Street Address.

24. On May 31, 2019, the Honorable Ramon E. Reyes, United States Magistrate Judge, issued a search warrant authorizing the search of Nordexin Platform-1.

25. The Investigating Agencies' review of the search warrant returns has confirmed that DENIS KULKOV operates Try2Check.

a. Screenshots of Try2Check's Administrator Panel are Found in Nordexin Platform-1

26. Nordexin Platform-1 contains screenshot images of webpages from Try2Check that I know from my own experience are not publicly available and that, based on my knowledge, training and experience, are accessible only to administrators of Try2Check. These include screenshots of the site's administrative controls, also known as the "administrator panel."

27. One such screenshot is dated January 13, 2019 and depicts a webpage. The URL of the webpage includes the phrase "Try2" and the word "admin." The webpage interface is visually similar to that of Try2Check's public pages, including the logo of two

nonaligned semicircles. On the upper right, where a username would typically appear, is the word "Admin."

28. The webpage that is visible in the screenshot includes a wide variety of information that, based on my experience using Try2Check, is not available to ordinary users of that site, but is characteristic of the types of information that would be available to a website administrator. For example, the page includes a list of Try2Check users, along with the Bitcoin balance associated with each user's account on Try2Check and that user's unique user number. The page also lists the number of users online at the time the image was made.

29. Also visible, but not selected, are tabs that appear to provide access to panels containing other information typically available only to a website's administrators. Based on the names of the tabs, these include lists of subcategories of Try2Check users, including "blocked," "top" and "new" users; a list of "tickets," or service requests, which indicates fifteen outstanding requests; a list of operative servers; and a collection of site statistics.

30. Nordexin Platform-1 also contains a second screenshot of Try2Check's administrator panel, which indicates that it was created on May 26, 2019. That screenshot appears to show the results of a search for one particular user. The information returned by the search includes the user's Bitcoin balance and the fact that he is a new user and connects to Try2Check via its API.

b. Nordexin Platform-1 Contains Virtual Memory Files with Numerous Try2Check-Related Keywords

31. In addition to the above, Nordexin Platform-1 contains multiple "virtual memory" files, meaning files that contain electronic backups of the contents of a physical computer's memory. Based on the contents of these files, they appear to contain memory data from computers used to operate Try2Check. Keyword searches across the virtual memory files have uncovered references to multiple web addresses associated with Try2Check, both in its open web and dark web versions; multiple instant messaging accounts associated with Try2Check's public-facing communications with its users; and tens of thousands of instances apiece of key phrases associated with Try2Check and its predecessor websites, including "try2admin," "try2check," and "try2services." The virtual memory file also includes what appear to be excerpts of instructions for users of Try2Check to access the site and set up its API.

32. The virtual memory files discovered in Nordexin Platform-1 are in a format that is proprietary to a company that sells digital virtualization services ("Platform-2"). Platform-2 has indicated that it has a customer named "Denis Kulkov," who resides in Samara, Russia. Information provided by Platform-2 indicates that KULKOV's Platform-2 account was registered with the Kulkov Phone Number, the Ya.ru Email, and the Nordexin Platform-1 email address.

c. Emails to and from DENIS KULKOV are found in Nordexin Platform-1

33. In addition to the screenshots and virtual memory files described above, Nordexin Platform-1 contains multiple emails between DENIS KULKOV and others.

Except where noted below, all of the emails are sent from a user identified as "Дени Кульков," which transliterates into Latin characters as "Denis Kulkov."

34. For example, on or about April 10, 2018, DENIS KULKOV used Nordexin Platform-1 to exchange emails with an employee of a business that (according to its publicly available website) specializes in registering companies for its clients ("Business-1"). Writing in Russian, KULKOV asked the employee how much it would cost for Business-1 to set up a Delaware limited liability corporation for KULKOV. The next day, KULKOV added that the newly formed company would "try to get a merchant account in the [Victim-1] system." KULKOV further said that if Business-1, in addition to its corporate formation services, could help KULKOV get an account with Victim-1, KULKOV would "agree to pay for such services."

35. In response to a request from Business-1, KULKOV emailed a photograph of himself holding up the same Russian passport that was used to open KULKOV's Exchange-1 account. The person holding up the passport in the emailed photograph is the same person whose photograph appears in the passport itself, and both photographs match the photographs of KULKOV on other documents and social media postings described above.

36. In another email chain dated on or about February 12, 2019, KULKOV forwarded to the email account associated with Nordexin Platform-1 a copy of a January 31, 2019 message that he had written from the Ya.ru Email to a representative of a company ("Business-2") that (according to its publicly available website) provides U.S.-based corporate services to Russian speakers in Eastern Europe. In the related message chain, KULKOV requested "access" to Victim-1, and stated that he wished to "continue to extend

on the same conditions." Also included in that same chain was an invoice from Business-2 for unspecified consulting services, addressed to "KULKOV, Denis."

37. Nordexin Platform-1 also contains emails reflecting KULKOV's attempts to convert his cryptocurrency holdings into fiat currency. For example, on or about February 6, 2019, KULKOV emailed a representative of a European financial services firm ("Business-3"). In response to a question from KULKOV, the Business-3 employee responded, "Yes, through [Business-3] you can sell cryptocurrency and go fiat. To complete the compliance procedure and open an account, you must provide a photo of a foreign person and a Russian passport." KULKOV responded, "What is the maximum amount which will not cause compliance suspicion"?

38. Similarly, on or about February 5, 2019, KULKOV emailed the general email address of a Swiss law firm ("Law Firm-1") with a subject heading indicating that he had found Law Firm-1's information on a web forum devoted to discussions about bitcoin.[5] KULKOV wrote: "Hello. Can you help build a scheme so that on a regular basis you can distill bitcoin into a fiat sum of up to 100k per month?"

39. In addition the messages described above, Nordexin Platform-1 also contains numerous personal communications attributable to KULKOV. These include an email between KULKOV and his wife regarding an online purchase, and a backup of an

---

[5] At present, the website of Law Firm-1 contains text specifying that "the information in this web site is not intended to constitute legal advice or to create an attorney-client relationship." Nordexin Platform-1 does not contain a response to KULKOV from Law Firm-1, or any other communication suggesting that KULKOV and Law Firm-1 entered into an attorney-client relationship.

instant message between KULKOV and his wife regarding school tuition for KULKOV's daughter.

VI. Victim-1 Provides Information Regarding Try2Check

40. As set forth in brief above, the Investigating Agencies have determined that Try2Check authenticates U.S.-issued credit cards by carrying out unauthorized access to computers belonging to a U.S. company ("Victim-1"). Victim-1 functions as an intermediary between credit card issuers and businesses that accept payment via credit cards. When a consumer inserts a credit card into a point-of-sale machine at a business, the card information travels to Victim-1's servers. Victim-1 then determines what issuer the credit card belongs to, communicates with the issuer on behalf of the business, and sends a signal back to the point-of-sale machine reflecting that the transaction has been authorized. According to public information, Victim-1 processed billions of transactions in 2018.

41. In addition to allowing businesses to charge consumers' credit cards, Victim-1 also offers a service whereby it merely confirms a card's validity without actually charging the card, known as "preauthorization." For example, when a guest checks into a hotel, the hotel might request that Victim-1 preauthorize a charge on the guest's card to confirm that it is valid and has the necessary credit available, but typically will not charge the card until the guest checks out.

42. Data provided by Victim-1 indicates that Try2Check takes advantage of this preauthorization service. Specifically, in or around November 2018, the Investigating Agencies used an undercover online persona to load bitcoin into a Try2Check account belonging to the persona. Using a computer located in the Eastern District of New York, an agent then logged into that account and ran twenty credit card numbers through Try2Check's

card checking system (the "Undercover Transactions"). The credit card numbers had been newly created for this purpose and were not otherwise in circulation.

43. Victim-1 monitored its systems at the same time that the Undercover Transactions were taking place. Victim-1 reported that the credit cards involved in the Undercover Transactions appeared in its systems as if they were being submitted by U.S. merchants for preauthorization, and were accompanied by numerical codes ("merchant identifiers") corresponding to real merchants in Victim-1's systems. However, the accompanying merchant names were not genuine, did not match the merchant identifiers, and consisted of garbled letters and numbers.

44. Data provided by Victim-1 further indicated that the scope of Try2Check's activity is vast. During the Undercover Transactions, Victim-1 identified five external IP addresses that were directly involved in submitting the 20 credit card numbers for preauthorization, as well as four additional IP addresses that had previously submitted transactions using the same merchant identifiers, accompanied by similarly garbled merchant names. Victim-1 reported that these nine IP addresses had collectively submitted over 16 million credit card numbers for preauthorization over the approximately nine-month period on or about and between April 13, 2018 and December 31, 2018. Merchants located in the Eastern District of New York were among those whose merchant identifiers were used in connection with these transactions.

WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for the defendant DENIS GENNADIEVICH KULKOV, also known as "Kreenjo," "Nordex" and "Nordexin," so that he may be dealt with according to law.

IT IS FURTHER REQUESTED that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including this Affidavit and the arrest warrant for the defendant DENIS GENNADIEVICH KULKOV, with the exception that the complaint and arrest warrant can be unsealed for the limited purpose of disclosing the existence of, or disseminating, the complaint and/or arrest warrant to relevant United States, foreign, or intergovernmental authorities, at the discretion of the United States and in connection with efforts to prosecute the defendant or to secure the defendant's arrest, extradition or expulsion. Based on my training and experience, I have learned that criminals actively search for criminal affidavits on the Internet and disseminate them to other criminals as they deem appropriate, such as by posting them publicly through online forums. Premature disclosure of the contents of this Affidavit and related documents will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior and notify confederates.

[redacted]

RICHARD PENA-ARIET
Special Agent
United States Secret Service

Sworn to before me this
17th day of December, 2019

[redacted]

THE HONORABLE ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK