

CRH:AFM/SKW
F. #2014R00176

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
-----X

UNITED STATES OF AMERICA

I N D I C T M E N T

- against -

DENIS GENNADIEVICH KULKOV,
also known as “Kreenjo,”
“Nordex” and “Nordexin”

Defendant.

Cr. No. 23-CR-00171
(T. 18, U.S.C., §§ 982(a)(1), 982(a)(2),
982(a)(2)(B), 982(b)(1), 1029(a)(3),
1029(a)(5), 1029(c)(1)(C), 1029(c)(2),
1029(h), 1030(a)(4), 1030(c)(3)(A),
1030(i)(1), 1030(i)(2),
1956(a)(1)(B)(1), 1956(h), 2 and 3551
et seq.; T. 21, U.S.C., § 853(p))

-----X

THE GRAND JURY CHARGES:

I N T R O D U C T I O N

At all times relevant to this Indictment, unless otherwise indicated:

I. The Defendant and Try2Check

1. The defendant, DENIS GENNADIEVICH KULKOV, also known as “Kreenjo,” “Nordex” and “Nordexin” (“KULKOV” or “DENIS KULKOV”), was a Russian national born in April 1980 who resided in Samara, Russia and Moscow, Russia.

2. KULKOV created and operated an electronic platform known as Try2Check or Try2Services (hereinafter “Try2Check”) that provided card checking services to individuals involved in computer-enabled criminal activity (hereafter “cybercrime” and “cybercriminals”).

3. Try2Check was one of the most popular card-checking platforms among cybercriminals, processing more than one million card-checking transactions per month, and charging approximately twenty cents per transaction. The platform offered its users—individuals who stole bulk credit card numbers on the internet—the ability to quickly determine the validity of a credit card number.

4. Victim-1, an entity the identity of which is known to the Grand Jury, was a major U.S.-based payment processor. Try2Check obtained unauthorized access to the servers of Victim-1 in order to determine the validity of U.S.-issued cards submitted to its service by users.

II. Background Regarding Online Credit Card Fraud and “Card Checking” Services

5. Cybercriminals stole millions of credit card numbers every year, causing tens of billions of dollars’ worth of losses, by breaching corporate databases and hacking into payment systems, among other methods. The practice of acquiring and trafficking in stolen credit cards was known as “carding.”

6. The credit card numbers obtained through carding activity were often resold in bulk through online message boards, known as “carding forums.” Carding forums served as marketplaces where individuals could sell batches of stolen credit card numbers, and as virtual meeting places where cybercriminals communicated, advertise and access necessary services.

7. A batch of stolen credit card numbers had a limited and unpredictable lifespan. Of the thousands or millions of cards in any batch, many were inactive when stolen, or were deactivated soon afterward when the cardholders or issuers became aware of the breach or detected suspicious activity.

8. Thus, one of the most important auxiliary services to cybercriminals involved in carding was provided by so-called “card checking” services. Websites involved in card checking permitted cybercriminals to quickly verify the authenticity of stolen credit card numbers, and to determine the percentage of cards in a batch that were still active. Without credible and efficient third-party verification that credit card information was active and usable, credit card batches would be difficult to sell because buyers would be unable to reliably ascertain the value of the data being offered.

III. KULKOV’s Criminal Scheme

9. In or around 2005, the defendant DENIS KULKOV created Try2Check, which came to serve as a crucial tool for cybercriminals trafficking in stolen credit cards. At all times relevant to this Indictment, Try2Check was usable both via the openly accessible internet and via the dark web, an alternative network that granted a measure of anonymity both to browsers and to website operators, often with the goal of impeding investigations by law enforcement.

10. The Try2Check platform enabled users to upload thousands of credit card numbers at one time. Try2Check then sent an immediate report of the percentage of the credit card numbers that were active and valid. As of February 2022, a single “check” cost the amount of bitcoin that corresponded to \$0.20 (USD) at the time of purchase.

11. Try2Check’s function relied on unauthorized access to computers belonging to Victim-1. Victim-1 functioned as an intermediary, or one of several intermediaries, between credit card issuers and businesses that accepted payment via credit cards. When a consumer inserted a credit card into a point-of-sale machine at a business, the card information traveled to Victim-1’s servers. Victim-1 then determined what issuer

the credit card belonged to, communicated with the issuer on behalf of the business, and sent a signal back to the point-of-sale machine reflecting that the transaction had been authorized.

12. In addition to allowing businesses to charge consumers' credit cards, Victim-1 also performed a service whereby it merely confirmed a card's validity without actually charging the card, known as "preauthorization."

13. Try2Check took advantage of Victim-1's preauthorization function by submitting fraudulent preauthorization requests to determine how many stolen credit cards in a batch remained active, and therefore were of value to a cybercriminal.

14. Specifically, between approximately April 13, 2018 and December 31, 2018, Try2Check submitted at least 16 million fraudulent credit card preauthorization requests, including on behalf of Try2Check users located in the Eastern District of New York. Similarly, between approximately September 24, 2021 and October 25, 2022, Try2Check submitted at least 17 million fraudulent credit card preauthorization requests, including on behalf of Try2Check users located in the Eastern District of New York. In turn, cybercriminals used this information to support their sales of stolen credit card data.

15. KULKOV's receipts from operating Try2Check were significant. In total, between June 2014 and November 2022, KULKOV received at least the equivalent of \$18 million in bitcoin in connection with the scheme, which amount includes only the revenue from the movement of funds visible on the Bitcoin blockchain, excluding alternative means of payment that Try2Check at times offered its users.

16. KULKOV used his proceeds from the scheme to buy luxury goods, including a Ferrari sports car. KULKOV also expressed frequent interest in converting large volumes of bitcoin to fiat currency. For example, on or about February 5, 2019,

KULKOV emailed the general email address of a Swiss law firm and requested assistance with “a scheme so that on a regular basis you can distill bitcoin into a fiat sum of up to 100k per month[.]”

COUNT ONE

(Access Device Fraud – Unauthorized Transactions)

17. The allegations contained in paragraphs one through 16 are realleged and incorporated as though fully set forth in this paragraph.

18. In or about and between January 2005 and April 2023, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant DENIS GENNADIEVICH KULKOV, also known as “Kreenjo,” “Nordex” and “Nordexin,” together with others, did knowingly and with intent to defraud effect transactions with one or more access devices, to wit: credit card account numbers and debit card account numbers, issued to another person or persons, in a manner affecting interstate and foreign commerce, and by such conduct did receive payment and other things of value during any one-year period the aggregate value of which was equal to or greater than \$1,000.

(Title 18, United States Code, Sections 1029(a)(5), 1029(h), 2 and 3551 et seq.)

COUNT TWO

(Access Device Fraud – Possession of Unauthorized Access Devices)

19. The allegations contained in paragraphs one through 16 are realleged and incorporated as though fully set forth in this paragraph.

20. In or about and between January 2005 and April 2023, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant DENIS GENNADIEVICH KULKOV, also known as “Kreenjo,” “Nordex” and

“Nordexin,” together with others, did knowingly and with intent to defraud possess 15 or more counterfeit and unauthorized access devices, to wit: credit and debit card account numbers, in a manner affecting interstate and foreign commerce.

(Title 18, United States Code, Sections 1029(a)(3), 1029(h), 2 and 3551 et seq.)

COUNT THREE

(Computer Intrusion in Furtherance of Fraud)

21. The allegations contained in paragraphs one through 16 are realleged and incorporated as though fully set forth in this paragraph.

22. In or about and between January 2005 and April 2023, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant DENIS GENNADIEVICH KULKOV, also known as “Kreenjo,” “Nordex” and “Nordexin,” together with others, did knowingly and with intent to defraud access without authorization one or more protected computers, to wit: servers belonging to Victim-1, and by means of such conduct did further the intended fraud and obtain something of value, to wit: the use of a computer, information about credit card validity and credit card preauthorization services.

(Title 18, United States Code, Sections 1030(a)(4), 1030(c)(3)(A), 2 and 3551 et seq.)

COUNT FOUR

(Money Laundering Conspiracy)

23. The allegations contained in paragraphs one through 16 are realleged and incorporated as though fully set forth in this paragraph.

24. In or about and between January 2005 and April 2023, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant DENIS GENNADIEVICH KULKOV, also known as “Kreenjo,” “Nordex” and “Nordexin,” together with others, did knowingly and intentionally conspire to transport, transmit and transfer monetary instruments and funds from a place in the United States to and through a place outside the United States and to a place in the United States from and through a place outside the United States, knowing that the monetary instruments and funds involved in the transportation, transmission and transfer represented the proceeds of some form of unlawful activity, and knowing that such transportation, transmission and transfer was designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of specified unlawful activity, to wit: access device fraud, in violation of Title 18, United States Code, Section 1029 and computer intrusion, in violation of Title 18, United States Code, Section 1030, contrary to Title 18, United States Code, Section 1956(a)(2)(B)(i).

(Title 18, United States Code, Section 1956(h) and 3551 et seq.)

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS ONE AND TWO

25. The United States hereby gives notice to the defendant that, upon his conviction of either of the offenses charged in Counts One and Two, the government will seek forfeiture in accordance with: (a) Title 18, United States Code, Section 982(a)(2)(B), which requires any person convicted of such offenses to forfeit any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such offenses; and (b) Title 18, United States Code, Section 1029(c)(1)(C), which requires any person convicted

of such offenses to forfeit any personal property used or intended to be used to commit the offenses.

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

- (a) cannot be located upon the 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;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1029(c)(2), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(2)(B), 982(b)(1), 1029(c)(1)(C) and 1029(c)(2); Title 21, United States Code, Section 853(p))

**CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT THREE**

27. The United States hereby gives notice to the defendant that, upon his conviction of the offense charged in Count Three, the government will seek forfeiture in accordance with Title 18, United States Code, Sections 982(a)(2) and 1030(i)(1), which require any person convicted of such offense to forfeit any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense, and such person's

interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such offense.

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

- (a) cannot be located upon the 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;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1030(i)(2), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(2), 982(b)(1), 1030(i)(1) and 1030(i)(2); Title 21, United States Code, Section 853(p))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT FOUR

29. The United States hereby gives notice to the defendant that, upon his conviction of the offense charged in Count Four, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(1), which requires any person convicted of such offense to forfeit any property, real or personal, involved in such offense, or any property traceable to such property.

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

- (a) cannot be located upon the 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;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(1) and 982(b)(1); Title 21, United States Code, Section 853(p))

A TRUE BILL


/FOREPERSON


BREON PEACE
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK

No.

UNITED STATES DISTRICT COURT
EASTERN *District of* NEW YORK
CRIMINAL DIVISION

THE UNITED STATES OF AMERICA

vs.

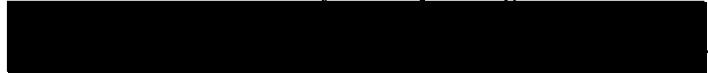
DENIS GENNADIEVICH KULKOV,
also known as "Kreenjo," "Nordex" and "Nordexin,"

Defendant.

INDICTMENT

(T. 18, U.S.C., §§ 982(a)(1), 982(a)(2), 982(a)(2)(B), 982(b)(1),
1029(a)(3), 1029(a)(5), 1029(h), 1030(a)(4), 1030(c)(3)(A),
1030(i)(1), 1030(i)(2), 1956(a)(1)(B)(1), 1956(h), 2 and 3551 et seq.;
T. 21, U.S.C., § 853(p))

A true bill.



Foreperson

Filed in open court this _____ day,

of _____ A.D. 20 _____

Clerk

Bail, \$ _____

Alexander Mindlin and Sara K. Winik, Assistant U.S. Attorneys
(718) 254-7000