

FILED

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

MAY 02 2024

AT 8:30 *16-2711*
CLERK, U.S. DISTRICT COURT - DNJ M

UNITED STATES OF AMERICA	:	Hon. Susan D. Wigenton
v.	:	Crim. No. 2:24-cr-00299
DMITRY YURYEVICH	:	<u>Count 1</u>
KHOROSHEV (Дмитрий Юрьевич	:	18 U.S.C. § 371
Хорошев),	:	<u>Count 2</u>
a/k/a "LockBitSupp,"	:	18 U.S.C. § 1349
a/k/a "LockBit,"	:	<u>Counts 3-10</u>
a/k/a "putinkrab"	:	18 U.S.C. § 1030(a)(5)(A)
	:	18 U.S.C. § 2
	:	<u>Counts 11-19</u>
	:	18 U.S.C. §§ 1030(a)(7)(B)
	:	18 U.S.C. § 2
	:	<u>Counts 20-26</u>
	:	18 U.S.C. §§ 1030(a)(7)(C)
	:	18 U.S.C. § 2
	:	<u>FILED UNDER SEAL</u>

**TRUE AND CERTIFIED COPY****Michael Dixon****3:15 pm, May 03 2024**

I N D I C T M E N T

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges as follows:

General Allegations

1. Since at least as early as in or around September 2019, the defendant, DMITRY YURYEVICH KHOROSHEV (Дмитрий Юрьевич Хорошев) ("KHOROSHEV"), has been the leader, developer, and administrator of the LockBit ransomware group. Operating under the online aliases of, among others, "LockBit," "LockBitSupp," and "putinkrab," KHOROSHEV began developing and promoting

LockBit at least as early as September 2019 and has continued acting as LockBit’s administrator through the present. During that time, KHOROSHEV grew LockBit into a massive criminal organization that has, at times, ranked as the most prolific and destructive ransomware group in the world. KHOROSHEV and his subordinate LockBit members (collectively, the “Coconspirators”) extorted hundreds of millions of dollars in ransom payments from thousands of victims in the United States, including the District of New Jersey, and around the world—which victims have included hospitals, schools, nonprofit organizations, critical infrastructure, and government and law-enforcement agencies—and caused broader losses and damage of billions of U.S. dollars.

2. At times relevant to this Indictment:

KHOROSHEV and His LockBit Coconspirators

- a. KHOROSHEV was a citizen of, and resided in, the Russian Federation.
- b. Mikhail Pavlovich Matveev (Михаил Павлович Матвеев) (“Matveev”), also known as “Wazawaka,” “m1x,” “Boriselcin,” and “Uhodiransomwar,” a Coconspirator who was previously charged for his participation in the LockBit group, was a citizen of, and resided in, the Russian Federation.
- c. Ruslan Magomedovich Astamirov (Руслан Магомедович Астамиров) (“Astamirov”), also known as “Betterpay,” “Offtitan,” and “Eastfarmer,” a Coconspirator who was previously charged for his participation in the LockBit group, was a citizen of, and resided in, the Russian Federation.
- d. Mikhail Vasiliev (“Vasiliev”), also known as “Ghostrider,” “Free,” “Digitalocean90,” “Digitalworld99,” “Digitalwaters99,” and “Newwave110,” a

Coconspirator who was previously charged for his participation in the LockBit group, was a citizen of both Canada and the Russian Federation and resided in Canada.

e. Artur Sungatov (Артур Сунгатов) (“Sungatov”), a Coconspirator who was previously charged for his participation in the LockBit group, was a citizen of, and resided in, the Russian Federation.

f. Ivan Kondratyev (Иван Кондратьев) (“Kondratyev”), also known as “Bassterlord,” a Coconspirator who was previously charged for his participation in the LockBit group, was a citizen of the Russian Federation and resided in either Ukraine or the Russian Federation.

KHOROSHEV’s LockBit Ransomware Variant and Group

g. “Ransomware” was a type of malware that allowed a perpetrator to encrypt some or all of the data stored on a victim computer, transmit some or all of the victim’s data to another computer under the perpetrator’s control and then publish that stolen data, or both. After a ransomware attack, a perpetrator typically demanded a ransom payment from the victim in exchange for decrypting the victim’s data, both refraining from publishing and deleting the perpetrator’s copy of the victim’s stolen data, or both.

h. As with other major ransomware variants, KHOROSHEV designed LockBit to operate through the “ransomware-as-a-service,” or “RaaS,” model. The RaaS model involved two related groups of ransomware perpetrators: developers and affiliates. The developers designed the ransomware code itself, much as a software company would, and maintained the infrastructure, such as servers, on which LockBit operated. The developers then recruited and marketed their

ransomware product to affiliates, who actually deployed the ransomware product designed by the developers against victim computer systems and steal victim data.

i. KHOROSHEV has acted as the LockBit ransomware group's developer and administrator since LockBit's inception at least as early as in or around September 2019 through in or around May 2024. During that time, KHOROSHEV revised the LockBit ransomware variant in at least three separate iterations that he referred to as "versions." Matveev, Astamirov, Vasiliev, Sungatov, and Kondratyev have each acted at various times as LockBit affiliates, along with several other Coconspirators both known and unknown to the Grand Jury.

j. As with other RaaS variants, KHOROSHEV designed LockBit to operate through a "control panel" that KHOROSHEV made available to LockBit affiliate Coconspirators. In the ransomware context, a "control panel" was a software dashboard made available to an affiliate by the developer(s) of a variant to both provide that affiliate with tools necessary for the deployment of ransomware attacks and to allow developers to monitor their affiliates' activities. The LockBit control panel designed and maintained by KHOROSHEV allowed affiliates to, among other things, generate custom executable payloads, or "builds," of the LockBit ransomware for deployment against particular victims, communicate with LockBit victims for ransom negotiation, and publish data stolen from LockBit victims to a website KHOROSHEV also created and operated to aid in the extortion of those victims (the "LockBit Data Leak Site").

k. KHOROSHEV created and hosted much of the LockBit infrastructure, including the various LockBit control panels and the LockBit Data

Leak Site, at various locations on the dark web. The “dark web” comprised Internet content that required specialized software or configurations to access and was intended for anonymous and untraceable online communication.

l. Through the LockBit infrastructure KHOROSHEV created and maintained, KHOROSHEV closely monitored the activities of his subordinate affiliate Coconspirators. For example, the LockBit control panel included a chat feature that allowed affiliates to conduct ransom negotiations with their victims. KHOROSHEV both monitored those negotiations and at times even participated in them. KHOROSHEV also maintained on his infrastructure databases listings of each LockBit affiliate Coconspirator with that affiliate’s victims. In some cases, KHOROSHEV demanded identification documents from his affiliate Coconspirators, which he also maintained on his infrastructure.

m. KHOROSHEV also developed and operated a tool for LockBit affiliate Coconspirators called “StealBit” intended to complement LockBit by aiding affiliates in storing data exfiltrated from LockBit victims and transmitting that stolen data for posting on the LockBit Data Leak Site. KHOROSHEV operated StealBit on multiple servers located throughout the world, including within the District of New Jersey and in Europe.

n. Operating under his online aliases “LockBit” and “LockBitSupp,” KHOROSHEV promoted and spoke for LockBit throughout the conspiracy, including on various cybercriminal forums on the dark web. Among other things, KHOROSHEV, under the alias “LockBitSupp,” posted to a cybercriminal forum on at

least one occasion offering to pay \$1,000 to any individual who received a tattoo of the LockBit logo—and did in fact pay that amount to multiple such individuals.

o. Again operating under his online aliases “LockBit” and “LockBitSupp,” KHOROSHEV recruited LockBit affiliates through a variety of means, including through promotion on cybercriminal forums. At times, KHOROSHEV sought to recruit affiliates of other RaaS groups that had previously been disrupted by law enforcement. Once a new affiliate joined the LockBit ransomware conspiracy, KHOROSHEV provided that affiliate with their own control panel at a unique domain name on the dark web, hosted and operated on KHOROSHEV’s infrastructure.

Course of a Typical LockBit Attack

p. A LockBit attack typically began with affiliates gaining unauthorized access to vulnerable computer systems through various means, including hacking, network penetration techniques, and the use of stolen access credentials purchased from third parties. Affiliates then deployed a custom build of the LockBit variant generated from the control panel maintained by KHOROSHEV within the victim computer systems, allowing affiliates to exfiltrate documents and data on the victim computer systems and to encrypt the data on the victim computer systems.

q. After LockBit had been deployed, affiliates then left behind a ransom note on the victim computer system—usually generated by the LockBit custom build produced by KHOROSHEV’s control panel—that provided the victim with instructions for how to contact the affiliate and a threat to publicly share the

victim's stolen data and to leave the victim's data encrypted and thus inaccessible if a ransom was not timely paid.

r. After ransom negotiations began, affiliates demanded a ransom payment in exchange for either decrypting the data on the victim's system and/or agreeing to not publicly post data exfiltrated from the victim system on the LockBit Data Leak Site. Affiliates typically demanded payment in Bitcoin, a form of digital currency allowing users to store value in Bitcoin locations called "addresses" and to exchange value between those addresses anonymously.

s. If the victim ultimately agreed to make a ransom payment, the affiliate typically provided the victim with a Bitcoin address to send the demanded ransom. The affiliate and the developer then split the payment between themselves. KHOROSHEV, as the LockBit developer, typically received 20 percent of each ransom payment, and the affiliate received the remaining 80 percent of each ransom payment.

Scale and Impact of KHOROSHEV's LockBit Ransomware Campaign

t. After KHOROSHEV began developing and promoting the LockBit ransomware variant, the first LockBit attack occurred at least as early as in or around January 2020. Approximately four years later, in or around February 2024, LockBit was severely disrupted by a coordinated operation by law-enforcement agencies in the United Kingdom, the United States, and around the world.

u. At that time, U.K. authorities seized control of KHOROSHEV's LockBit infrastructure, rendering it practically inoperable and allowing law enforcement to review the data stored on it—including KHOROSHEV's records

related to particular LockBit affiliate Coconspirators, such as those Coconspirators' victim lists and personal identification documents. Moreover, KHOROSHEV's seized infrastructure contained copies of data stolen from LockBit victims who had paid the demanded ransom, even though KHOROSHEV and his affiliate Coconspirators had falsely promised those victims that they would delete the victims' stolen data after the ransom was paid.

v. Between in or around September 2019 and in or around the time of the February 2024 operation, KHOROSHEV grew LockBit into a massive global criminal operation that at times ranked as the most prolific and destructive ransomware group in the world. During that period, KHOROSHEV and his LockBit Coconspirators attacked at least approximately 2,500 victims, which included at least approximately 1,800 victims located in the United States. At least approximately 55 of those victims were in the District of New Jersey. Beyond the United States, KHOROSHEV's LockBit victims were located in nearly 120 countries around the world, including in the United Kingdom, France, Australia, Germany, Argentina, Kenya, Switzerland, Finland, the Netherlands, Japan, Canada, Spain, Italy, and China. LockBit's victims ranged from major multinational corporations to small businesses and individuals, and they included hospitals, schools, nonprofit organizations, critical infrastructure facilities, and government and law-enforcement agencies. Although KHOROSHEV purported to prohibit LockBit affiliate Coconspirators from attacking victims located in Russia, KHOROSHEV and LockBit Coconspirators also deployed LockBit against multiple Russian victims.

w. In total, KHOROSHEV and his LockBit affiliate Coconspirators successfully extorted at least approximately \$500 million in ransom payments from their victims. KHOROSHEV alone derived at least approximately \$100 million in Bitcoin disbursements from his 20 percent developer share of each victim ransom payment, some of which he used to continue funding the LockBit operation and its infrastructure.

x. The ransom demands that LockBit members made to their victims were extremely large. One victim alone, for example—Victim-15, a multinational aeronautical and defense corporation headquartered in Virginia—received a ransom demand of approximately \$200 million from the LockBit perpetrators.

y. Beyond ransom payments and demands, LockBit attacks also severely disrupted their victims' operations, causing lost revenue and expenses associated with incident response and recovery. With these losses included, LockBit caused damage around the world totaling billions of U.S. dollars. Moreover, the data KHOROSHEV and his LockBit affiliate Coconspirators stole—containing highly sensitive organizational and personal information—remained unsecure and compromised in perpetuity, notwithstanding KHOROSHEV's and his Coconspirators' false promises to the contrary.

z. Shortly after the February 2024 disruption operation, KHOROSHEV attempted to revive the LockBit operation and launch new infrastructure. KHOROSHEV's new LockBit operation, however, was greatly diminished in victim count and reputation compared to the pre-disruption LockBit

operation. Shortly after the February 2024 operation, KHOROSHEV, seeking to restore LockBit’s primacy and to stifle his competition within the criminal RaaS space, communicated with law enforcement and offered his services in exchange for information regarding the identity of his RaaS competitors. Specifically, KHOROSHEV asked law enforcement during that exchange to, in sum and substance, “[g]ive me the names of my enemies.”

COUNT 1
**(Conspiracy to Commit Fraud, Extortion, and Related Activity in
Connection with Computers – 18 U.S.C. § 371)**

1. Paragraphs 1 and 2 of the General Allegations section of this Indictment are realleged here.

2. From at least as early as in or around September 2019 through in or around May 2024, in the District of New Jersey and elsewhere, the defendant,

DMITRY YURYEVICH KHOROSHEV (Дмитрий Юрьевич Хорошев),
a/k/a “LockBitSupp,”
a/k/a “LockBit,”
a/k/a “putinkrab,”

did knowingly and intentionally conspire and agree with Matveev, Astamirov, Vasiliev, Sungatov, Kondratyev, and other Coconspirators to commit offenses against the United States, that is:

a. 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 loss to persons during a 1-year period from the Coconspirators’ course of conduct affecting protected computers aggregating at least \$5,000 in value, and cause damage affecting 10 or more protected computers during a 1-year period, contrary to Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B)(i); and

b. to knowingly and with intent to extort from any person any money or other thing of value, transmit in interstate and foreign commerce any communication containing a threat to obtain information from a protected computer without authorization and to impair the confidentiality of information obtained from

a protected computer without authorization and by exceeding authorized access, and a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, contrary to Title 18, United States Code, Section 1030(a)(7)(B), (a)(7)(C), and (c)(3)(A).

Goal of the Conspiracy

3. The goal of the conspiracy was for KHOROSHEV, Matveev, Astamirov, Vasiliev, Sungatov, Kondratyev, and other Coconspirators to enrich themselves by: (a) developing the LockBit ransomware variant, maintaining LockBit infrastructure (e.g., computer servers and affiliate control panels, among other facilities), and hacking into and deploying LockBit against victim computer systems; (b) demanding and extracting ransom payments from victims following successful LockBit attacks; and (c) extorting noncompliant victims and intimidating future victims by, among other things, posting those victims' stolen data on the LockBit Data Leak Site.

Manner and Means of the Conspiracy

4. It was part of the conspiracy that KHOROSHEV and the Coconspirators engaged in a number of manner and means, including those described in paragraph 2 of the General Allegations section of this Indictment.

Overt Acts

5. In furtherance of the conspiracy and to effect its illegal objects, KHOROSHEV and the Coconspirators committed the following overt acts, among others, in the District of New Jersey and elsewhere:

a. On or about June 25, 2020, KHOROSHEV, Matveev, and other Coconspirators deployed LockBit against Victim-1, a law-enforcement agency in Passaic County, New Jersey.

b. On or about September 14, 2020, KHOROSHEV, Matveev, and other Coconspirators deployed LockBit against Victim-2, a business in Dakota, Minnesota with operations and computers in New Jersey.

c. On or about August 11, 2021, KHOROSHEV and other Coconspirators deployed LockBit against Victim-3, a multinational consulting firm based in Ireland.

d. On or about October 12, 2021, KHOROSHEV and other Coconspirators deployed LockBit against Victim-4, a municipality in Burlington County, New Jersey.

e. On or about November 13, 2021, KHOROSHEV and other Coconspirators deployed LockBit against Victim-5, a law-enforcement agency in Monmouth County, New Jersey.

f. On or about November 21, 2021, KHOROSHEV, Vasiliev, and other Coconspirators deployed LockBit against Victim-6, a business in Essex County, New Jersey.

g. On or about June 18, 2022, KHOROSHEV and other Coconspirators deployed LockBit against Victim-7, a digital security firm headquartered in Minnesota.

h. On or about June 26, 2022, KHOROSHEV, Sungatov, and other Coconspirators deployed LockBit against Victim-8, a medical-services business based in Florida.

i. On or about November 3, 2022, KHOROSHEV and other Coconspirators deployed LockBit against Victim-9, an automotive parts conglomerate headquartered in Germany.

j. On or about November 9, 2022, KHOROSHEV and other Coconspirators deployed LockBit against Victim-10, a municipal utilities operator in Gloucester County, New Jersey.

k. In or around February 2023, KHOROSHEV and other Coconspirators deployed LockBit against Victim-11, a parcel delivery service based in the United Kingdom.

l. In or around March 2023, KHOROSHEV, Astamirov, and other Coconspirators deployed LockBit against Victim-12, a business based in Kenya.

m. On or about June 13, 2023, KHOROSHEV and other Coconspirators deployed LockBit against Victim-13, a school district in Somerset County, New Jersey.

n. On or about June 29, 2023, KHOROSHEV, Kondratyev, and other Coconspirators deployed LockBit against Victim-14, a major semiconductor manufacturing company based in Taiwan.

o. On or about October 27, 2023, KHOROSHEV and other Coconspirators deployed LockBit against Victim-15, a multinational aeronautical and defense corporation headquartered in Virginia.

p. On or about November 2, 2023, KHOROSHEV and other Coconspirators deployed LockBit against Victim-16, a healthcare provider in Union County, New Jersey.

q. In or around November 2023, KHOROSHEV and other Coconspirators deployed LockBit against Victim-17, a major financial institution based in China.

r. On or about January 21, 2024, KHOROSHEV and other Coconspirators deployed LockBit against Victim-18, a multinational fast food franchise headquartered in Florida.

s. On or about January 24, 2024, KHOROSHEV and other Coconspirators deployed LockBit against Victim-19, a securities lending platform headquartered in New York.

t. On or about January 29, 2024, KHOROSHEV and other Coconspirators deployed LockBit against Victim-20, a local government authority in Georgia.

In violation of Title 18, United States Code, Section 371.

COUNT 2
(Conspiracy to Commit Wire Fraud – 18 U.S.C. § 1349)

1. Paragraphs 1 and 2 of the General Allegations section of this Indictment and paragraph 5 of Count 1 are realleged here.
2. From at least as early as in or around September 2019 through in or around May 2024, in the District of New Jersey and elsewhere, the defendant,

**DMITRY YURYEVICH KHOROSHEV (Дмитрий Юрьевич Хорошев),
a/k/a “LockBitSupp,”
a/k/a “LockBit,”
a/k/a “putinkrab,”**

did knowingly and intentionally conspire with Matveev, Astamirov, Vasiliev, Sungatov, Kondratyev, and other Coconspirators to devise, and intend to devise, a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice to defraud, to knowingly transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

COUNTS 3 THROUGH 10
(Intentional Damage to a Protected Computer – 18 U.S.C. § 1030(a)(5)(A))

1. Paragraphs 1 and 2 of the General Allegations section of this Indictment and paragraph 5 of Count 1 are realleged here.
2. On or about each of the dates set forth below, in the District of New Jersey and elsewhere, the defendant,

DMITRY YURYEVICH KHOROSHEV (Дмитрий Юрьевич Хорошев),
a/k/a “LockBitSupp,”
a/k/a “LockBit,”
a/k/a “putinkrab,”

did 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 the offense caused loss to persons during a 1-year period from the defendant’s course of conduct affecting protected computers aggregating at least \$5,000 in value, described below for each Count, each transmission constituting a separate Count of this Indictment:

Count	Approximate Date(s)	Victim
3	June 5, 2020	Victim-1
4	September 14, 2020	Victim-2
5	October 12, 2021	Victim-4
6	November 13, 2021	Victim-5
7	November 21, 2021	Victim-6
8	November 9, 2022	Victim-10
9	June 13, 2023	Victim-13
10	November 2, 2023	Victim-16

In violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i), and Section 2.

COUNTS 11 THROUGH 18

**(Extortion in Relation to Information Unlawfully Obtained from a
Protected Computer – 18 U.S.C. § 1030(a)(7)(B))**

1. Paragraphs 1 and 2 of the General Allegations section of this Indictment and paragraph 5 of Count 1 are all realleged here.

2. On or about each of the dates set forth below, in the District of New Jersey and elsewhere, the defendant,

**DMITRY YURYEVICH KHOROSHEV (Дмитрий Юрьевич Хорошев),
a/k/a “LockBitSupp,”
a/k/a “LockBit,”
a/k/a “putinkrab,”**

did knowingly and with intent to extort from any person any money or other thing of value, transmit in interstate and foreign commerce a communication containing a threat to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access, described below for each Count, each transmission constituting a separate Count of this Indictment:

Count	Approximate Date(s)	Victim
11	June 5, 2020	Victim-1
12	September 14, 2020	Victim-2
13	October 12, 2021	Victim-4
14	November 13, 2021	Victim-5
15	November 21, 2021	Victim-6
16	November 9, 2022	Victim-10
17	June 13, 2023	Victim-13
18	November 2, 2023	Victim-16

In violation of Title 18, United States Code, Sections 1030(a)(7)(B) and (c)(3)(A), and Section 2.

COUNTS 19 THROUGH 26
**(Extortion in Relation to Intentional Damage to a
Protected Computer – 18 U.S.C. § 1030(a)(7)(C))**

1. Paragraphs 1 and 2 of the General Allegations section of this Indictment and paragraph 5 of Count 1 are all realleged here.

2. On or about each of the dates set forth below, in the District of New Jersey and elsewhere, the defendant,

**DMITRY YURYEVICH KHOROSHEV (Дмитрий Юрьевич Хорошев),
a/k/a “LockBitSupp,”
a/k/a “LockBit,”
a/k/a “putinkrab,”**

did knowingly and with intent to extort from any person any money or other thing of value, transmit in interstate and foreign commerce a communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, described below for each Count, each transmission constituting a separate Count of this Indictment:

Count	Approximate Date(s)	Victim
19	June 5, 2020	Victim-1
20	September 14, 2020	Victim-2
21	October 12, 2021	Victim-4
22	November 13, 2021	Victim-5
23	November 21, 2021	Victim-6
24	November 9, 2022	Victim-10
25	June 13, 2023	Victim-13
26	November 2, 2023	Victim-16

In violation of Title 18, United States Code, Sections 1030(a)(7)(C) and (c)(3)(A), and Section 2.

FORFEITURE ALLEGATION AS TO COUNTS 1 AND 3 THROUGH 26

1. As a result of committing the offenses charged in Counts 1 and 3 through 26 of this Indictment, the defendant,

DMITRY YURYEVICH KHOROSHEV (Дмитрий Юрьевич Хорошев),
a/k/a “LockBitSupp,”
a/k/a “LockBit,”
a/k/a “putinkrab,”

shall forfeit to the United States:

a. pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of the offenses charged in Counts 1 and 3 through 26 of this Indictment; and

b. pursuant to Title 18, United States Code, Section 1030(i), all right, title, and interest in any personal property that was used or intended to be used to commit or to facilitate the commission of the offenses charged in Counts 1 and 3 through 26 of this Indictment.

FORFEITURE ALLEGATION AS TO COUNT 2

2. As a result of committing the offense charged in Count 2 of this Indictment, the defendant,

DMITRY YURYEVICH KHOROSHEV (Дмитрий Юрьевич Хорошев),
a/k/a “LockBitSupp,”
a/k/a “LockBit,”
a/k/a “putinkrab,”

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, all property, real and

personal, that constitutes or is derived from proceeds traceable to the commission of the said offense, and all property traceable thereto.

SUBSTITUTE ASSETS PROVISION
(Applicable to All Forfeiture Allegations)

3. 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 person;
 - (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 subdivided without difficulty,

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.

A TRUE BILL

[Redacted]
FOREPERSON

Philip R. Sellinger
PHILIP R. SELLINGER
UNITED STATES ATTORNEY

CASE NUMBER: 2:24-cr-00299

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

DMITRY YURYEVICH KHOROSHEV (Дмитрий Юрьевич Хорошев)
a/k/a “LockBitSupp,” “LockBit,” “putinkrab”

INDICTMENT FOR

18 U.S.C. §§ 371; 1349;
1030(a)(5)(A); 1030(a)(7)(B); 1030(a)(7)(C); 2

A True Bill,

[REDACTED]
Foreperson

PHILIP R. SELLINGER
UNITED STATES ATTORNEY
FOR THE DISTRICT OF NEW JERSEY

ANDREW M. TROMBLY, DAVID E. MALAGOLD, AND VINAY LIMBACHIA
ASSISTANT U.S. ATTORNEYS
NEWARK, NEW JERSEY

JESSICA C. PECK, DEBRA IRELAND, AND JORGE GONZALEZ
TRIAL ATTORNEYS
COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION
WASHINGTON, DISTRICT OF COLUMBIA
