

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

UNITED STATES OF AMERICA	:	Hon. Susan D. Wigenton
	:	
v.	:	Crim. No. 24-
	:	
MIKHAIL VASILIEV,	:	18 U.S.C. § 371
a/k/a “Ghostrider,”	:	18 U.S.C. § 1030(a)(5)(A), and § 2
a/k/a “Free,”	:	18 U.S.C. § 1030(a)(7)(C), and § 2
a/k/a “Digitalocean90,”	:	18 U.S.C. § 1349
a/k/a “Digitalworld99,”	:	
a/k/a “Digitalwaters99,”	:	
a/k/a “Newwave110”	:	

INFORMATION

The defendant having waived in open court prosecution by Indictment, the United States Attorney for the District of New Jersey charges:

COUNT 1

(Conspiracy to Commit Fraud and
Related Activity in Connection with Computers)

Overview

1. From in or around September 2019 through in or around October 2022, defendant Mikhail Vasiliev, a/k/a “Ghostrider,” a/k/a “Free,” a/k/a “Digitalocean90,” a/k/a “Digitalworld99,” a/k/a “Digitalwaters99,” a/k/a “Newwave110” (“VASILIEV”), and others (collectively, the “Conspirators”) were part of a conspiracy to deploy a ransomware variant known as “LockBit,” a prolific form of malware and, at relevant times, the most deployed ransomware variant across the world. Since in or around January 2020 and continuing through the present, LockBit has been deployed against more than 2,500 victims, including victims in the District of New Jersey, and the Conspirators have received approximately \$500 million in ransom payments.

VASILIEV personally deployed LockBit against at least 12 victims and caused more than approximately \$500,000 in losses to victims.

Relevant Individuals, Entities, and Terms

2. At times relevant to this Information:

a. VASILIEV was a citizen of both Canada and the Russian Federation and resided in Canada.

b. Dmitry Yuryevich Khoroshev (Дмитрий Юрьевич Хорошев) (“Khoroshev”), also known as “LockBitSupp,” “LockBit,” and “putinkrab,” one of the Conspirators who was previously charged for his participation in the LockBit conspiracy, was a citizen of, and resided in, the Russian Federation. Khoroshev acted as the leader, developer, and administrator of the LockBit ransomware group.

c. Mikhail Pavlovich Matveev (“Matveev”), also known as “Wazawaka,” “m1x,” “Boriselcin,” and “Uhodiransomwar,” one of the Conspirators who was previously charged for his participation in the LockBit conspiracy, was a citizen of, and resided in, the Russian Federation.

d. Ruslan Magomedovich Astamirov (“Astamirov”), also known as “Ruslan Astamirov,” “Руслан Магомедович Астамиров,” “BETTERPAY,” “Offtitan,” “Eastfarmer,” one of the Conspirators who was previously charged for his participation in the LockBit conspiracy, was a citizen of, and resided in, the Russian Federation.

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

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

g. Victim-1 was a law enforcement agency in Passaic County, New Jersey.

h. Victim-2 was a business in West Palm Beach, Florida.

i. Victim-3 was a business in Dakota, Minnesota with operations and computers in New Jersey.

j. Victim-4 was a business headquartered in Tokyo, Japan.

k. Victim-5 was a business in Virginia Beach, Virginia.

l. Victim-6 was a municipality in Burlington County, New Jersey.

m. Victim-7 was a law enforcement agency in Monmouth County, New Jersey.

n. Victim-8 was a business in Rouen, France.

o. Victim-9 was a business in Essex County, New Jersey.

p. Victim-10 was a business in Macomb County, Michigan.

q. Victim-11 was a business in the Isle of Man.

r. Victim-12 was an educational facility in Berkshire, England.

s. Victim-13 was a business in Aberdeen, Scotland.

t. Victim-14 was a business in Appenzell, Switzerland.

u. Victim-15 was an association in Savigny, Switzerland.

v. Victim-16 was a business in London, England.

- w. Victim-17 was a business in Wangen bei Olten, Switzerland.
- x. Victim-18 was a business in Grosswangen, Switzerland.
- y. Victim-19 was a school in Saint-Légier-La Chiésaz, Switzerland.
- z. Victim-20 was a business in Lausanne, Switzerland.
- aa. Victim-21 was a business in Schwerzenbach, Switzerland.
- bb. Victim-22 was a school in Rotkreuz, Switzerland.
- cc. Victim-23 was a municipal utilities operator in Gloucester

County, New Jersey.

dd. Victim-24 was a business in Nairobi, Kenya.

ee. “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, or both. After a ransomware attack, a perpetrator would typically demand a ransom payment from the victim in exchange for decrypting the victim’s data, deleting the perpetrator’s copy of the victim’s stolen data, or both.

The Conspiracy

3. From in or around September 2019 through in or around October 2022, in the District of New Jersey and elsewhere, the defendant,

**MIKHAIL VASILIEV,
a/k/a “Ghostrider,”
a/k/a “Free,”
a/k/a “Digitalocean90,”
a/k/a “Digitalworld99,”
a/k/a “Digitalwaters99,”
a/k/a “Newwave110,”**

did knowingly and intentionally conspire and agree with Khoroshev, Matveev, Astamirov, Sungatov, Kondratyev, and other Conspirators 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 Conspirators' 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, Sections 1030(a)(5)(A), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI), 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 any: (i) threat to obtain information from a protected computer without authorization and in excess of authorization and to impair the confidentiality of information obtained from a protected computer without authorization and by exceeding authorized access, and (ii) 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, Sections 1030(a)(7)(B), (a)(7)(C), and (c)(3)(A).

Goal of the Conspiracy

4. The goal of the conspiracy was for VASILIEV, Matveev, Astamirov, Sungatov, Kondratyev, and other Conspirators to enrich themselves by: (a) developing the LockBit ransomware variant, maintaining LockBit infrastructure

(*e.g.*, computer servers and affiliate control panels, among other utilities) 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 Internet through a website known as a "leak site" (the "LockBit Data Leak Site").

Manner and Means of the Conspiracy

5. It was part of the conspiracy that:

a. The LockBit conspiracy operated through the "ransomware-as-a-service" model, or "RaaS". 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.

b. The LockBit ransomware variant relied on a "control panel" for its operation. In the ransomware context, a "control panel" was a software dashboard made available to an affiliate by the developers 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 allowed affiliates to, among other things, generate custom 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 the LockBit Data Leak

Site. Once a new affiliate joined the LockBit ransomware conspiracy, that affiliate was given their own control panel hosted at a unique domain name on the dark web.

c. Much of the LockBit infrastructure, including the various LockBit control panels and the LockBit Data Leak Site, was hosted on the dark web. The “dark web” comprises Internet content that requires specialized software or configurations to access and is intended for anonymous and untraceable online communication.

d. A LockBit attack typically began with affiliates gaining unauthorized access to vulnerable computer systems, through hacking, network penetration techniques, and the use of stolen access credentials purchased from third parties. Affiliates then deployed LockBit 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.

e. After LockBit was deployed, affiliates left behind a ransom note 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 to the victim.

f. 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 digital currency that allows Bitcoin holders to transfer their Bitcoin, stored at locations called “Bitcoin addresses,” to other Bitcoin users at those users’ Bitcoin addresses.

g. If the victim ultimately agreed to make a ransom payment, the affiliate typically sent the victim a Bitcoin address to send the demanded ransom. The affiliate and the developer then split the payment between themselves. Typically, the developer received 20% of the ransom payment and the affiliate received 80% of the ransom payment.

Overt Acts

6. In furtherance of the conspiracy, and to effect its objects, VASILIEV and others 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 Conspirators deployed LockBit against Victim-1.

b. On or about August 15, 2020, Astamirov, Khoroshev, and other Conspirators deployed LockBit against Victim-2.

c. On or about September 14, 2020, Khoroshev, Matveev, and other Conspirators deployed LockBit against Victim-3.

d. On or about September 15, 2020, Astamirov, Khoroshev, and other Conspirators deployed LockBit against Victim-4.

e. On or about October 1, 2020, Astamirov, Khoroshev, and other Conspirators deployed LockBit against Victim-5.

f. On or about October 12, 2021, Khoroshev and other Conspirators deployed LockBit against Victim-6.

g. On or about November 13, 2021, Khoroshev and other Conspirators deployed LockBit against Victim-7.

- h. On or about November 18, 2021, Astamirov, Khoroshev, and other Conspirators deployed LockBit against Victim-8.
- i. On or about November 21, 2021, VASILIEV, Khoroshev, and other Conspirators deployed LockBit against Victim-9.
- j. On or about January 20, 2022, VASILIEV, Khoroshev, and other Conspirators deployed LockBit against Victim-10.
- k. In or around early February 2022, VASILIEV, Khoroshev, and other Conspirators deployed LockBit against Victim-11.
- l. On or about February 24, 2022, VASILIEV, Khoroshev, and other Conspirators deployed LockBit against Victim-12.
- m. On or about March 27, 2022, VASILIEV, Khoroshev, and other Conspirators deployed LockBit against Victim-13.
- n. On or about April 19, 2022, VASILIEV, Khoroshev, and other Conspirators deployed LockBit against Victim-14.
- o. On or about June 10, 2022, VASILIEV, Khoroshev, and other Conspirators deployed LockBit against Victim-15.
- p. On or about July 14, 2022, VASILIEV, Khoroshev, and other Conspirators deployed LockBit against Victim-16.
- q. On or about July 15, 2022, VASILIEV, Khoroshev, and other Conspirators deployed LockBit against Victim-17.
- r. On or about August 25, 2022, VASILIEV, Khoroshev, and other Conspirators deployed LockBit against Victim-18.

s. On or about August 31, 2022, VASILIEV, Khoroshev, and other Conspirators deployed LockBit against Victim-19 and Victim-20.

t. On or about October 14, 2022, VASILIEV, Khoroshev, and other Conspirators deployed LockBit against Victim-21.

u. On or about October 16, 2022, VASILIEV, Khoroshev, and other Conspirators deployed LockBit against Victim-22.

v. On or about November 9, 2022, Khoroshev and other Conspirators deployed LockBit against Victim-23.

w. In or around March 2023, Astamirov, Khoroshev, and other Conspirators deployed LockBit against Victim-24.

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

COUNT 2

(Intentional Damage to a Protected Computer)

1. The allegations in paragraphs 1, 2, and 4 through 6 of Count 1 of this Information are re-alleged here.

2. On or about November 21, 2021, in the District of New Jersey and elsewhere, the defendant,

**MIKHAIL VASILIEV,
a/k/a “Ghostrider,”
a/k/a “Free,”
a/k/a “Digitalocean90,”
a/k/a “Digitalworld99,”
a/k/a “Digitalwaters99,”
a/k/a “Newwave110,”**

knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, and the offense caused loss to persons during a 1-year period from a related course of conduct affecting protected computers aggregating at least \$5,000 in value, and caused damage affecting 10 or more protected computers during a 1-year period.

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

COUNT 3

(Transmission of a Demand in Relation to
Damaging a Protected Computer)

1. The allegations in paragraphs 1, 2, and 4 through 6 of Count 1 of this Information are re-alleged here.

2. On or about November 21, 2021, in the District of New Jersey and elsewhere, the defendant,

**MIKHAIL VASILIEV,
a/k/a “Ghostrider,”
a/k/a “Free,”
a/k/a “Digitalocean90,”
a/k/a “Digitalworld99,”
a/k/a “Digitalwaters99,”
a/k/a “Newwave110,”**

with intent to extort from any person any money and thing of value, transmitted 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.

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

COUNT 4
(Conspiracy to Commit Wire Fraud)

1. The allegations in paragraphs 1, 2, and 4 through 6 of Count 1 of this Information are re-alleged here.

2. From in or around September 2019 through in or around October 2022, in the District of New Jersey and elsewhere, the defendant,

**MIKHAIL VASILIEV,
a/k/a “Ghostrider,”
a/k/a “Free,”
a/k/a “Digitalocean90,”
a/k/a “Digitalworld99,”
a/k/a “Digitalwaters99,”
a/k/a “Newwave110,”**

did knowingly and intentionally conspire with Khoroshev, Matveev, Astamirov, Sungatov, Kondratyev, and other Conspirators 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, did 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.

FORFEITURE ALLEGATION AS TO COUNTS 1, 2, AND 3

As a result of committing the offenses charged in Counts 1, 2, and 3 of this Information, the defendant,

**MIKHAIL VASILIEV,
a/k/a “Ghostrider,”
a/k/a “Free,”
a/k/a “Digitalocean90,”
a/k/a “Digitalworld99,”
a/k/a “Digitalwaters99,”
a/k/a “Newwave110,”**

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, 2, and 3 of this Information; 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, 2, and 3 of this Information.

FORFEITURE ALLEGATION AS TO COUNT 4

As a result of committing the offense charged in Count 4 of this Information, the defendant,

**MIKHAIL VASILIEV,
a/k/a “Ghostrider,”
a/k/a “Free,”
a/k/a “Digitalocean90,”
a/k/a “Digitalworld99,”**

a/k/a “Digitalwaters99,”
a/k/a “Newwave110,”

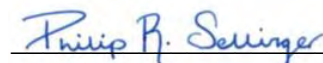
shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of the said offense, and all property traceable 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.


PHILIP R. SELLINGER
United States Attorney