2019R01049/AMT/DEM/JCP

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. Susan D. Wigenton
	:	
v.	:	Criminal No. 22- 825
	:	
MIKHAIL PAVLOVICH MATVEEV a/k/a "Wazawaka" a/k/a "m1x" a/k/a "Boriselcin" a/k/a "Uhodiransomwar"	:	Count 1 – 18 U.S.C. § 371 (Conspiracy – LockBit Ransomware) Counts 2 and 3 – 18 U.S.C. § 1030(a)(5)(A) (Intentional Damage to a Computer) Count 4 – 18 U.S.C. § 371 (Conspiracy – Babuk Ransomware) Count 5 – 18 U.S.C. § 371 (Conspiracy – Hive Ransomware) Count 6 – 18 U.S.C. § 1030(a)(5)(A) (Intentional Damage to a Computer) **FILED UNDER SEAL**

INDICTMENT

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

Overview

1. From at least as early as 2020, the defendant, MIKHAIL PAVLOVICH MATVEEV, a Russian national and resident, was an active member of at least three different global ransomware conspiracies: LockBit, Babuk, and Hive, each of which ranked among the most active and destructive cybercriminal threats in the world. MATVEEV and the other members of these three ransomware conspiracies attacked at least as many as 2,800 victims in

the United States and around the world and made ransom demands to these victims of at least $400 million. Actual ransom payments from these victims to these perpetrators amounted to over $200 million. These victims include government agencies, including law enforcement agencies, hospitals, schools, and nonprofit organizations. As a member of these three ransomware conspiracies, MATVEEV identified and hacked vulnerable computer systems, deployed ransomware within these systems, and transmitted ransom demands to these victims, in many cases threatening the public disclosure of the victims' private and highly sensitive data if the victims did not pay the demanded ransom.

General Allegations

2. At various times relevant to this Indictment:

a. "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.

b. MATVEEV, also known as "Wazawaka," "m1x," "Boriselcin," and "Uhodiransomwar," was a Russian national and resident. He was a

member of at least three different global ransomware conspiracies: LockBit, Babuk, and Hive. Each of these global ransomware conspiracies targeted as victims government agencies, including law enforcement agencies, hospitals, schools, and nonprofit organizations, including churches and charity organizations.

i. LockBit was a ransomware variant that first appeared at least as early as in or around January 2020. Between then and the present, members of the LockBit conspiracy, including MATVEEV, have executed at least around 1,400 LockBit attacks against victim systems both in the United States and around the world, making at least approximately $100 million in ransom demands to victims and receiving at least as much as $75 million in actual ransom payments.

ii. Babuk was a ransomware variant that first appeared at least as early as in or around December 2020. Between then and at least as recently as September 2021, members of the Babuk conspiracy, including MATVEEV, executed at least as many as around 65 Babuk attacks against victim systems both in the United States and around the world, making at least approximately $49 million in ransom demands to victims and receiving as much as $13 million in actual ransom payments.

iii. Hive was a ransomware variant that first appeared at least as early as in or around June 2021. Between then and the present, members of the Hive conspiracy, including MATVEEV, have executed at least around 1,400 Hive attacks against victim systems both in the United States and around the world, making at least approximately $270 million in ransom demands to victims and receiving as much as $120 million in actual ransom payments.

c. The LockBit, Babuk, and Hive conspiracies operated in largely the same general manner:

i. First, members of each conspiracy would identify and unlawfully access vulnerable computer systems. Conspiracy members would sometimes do so through their own hacking and network penetration techniques; at other times, they would do so by purchasing stolen access credentials from third parties.

ii. Second, members of each conspiracy would deploy that conspiracy's variant within the victim computer system, allowing the perpetrators to either encrypt or steal the data stored on that system, or both.

iii. Third, members of each conspiracy would send a ransom note to the victim providing the victim with instructions for contacting the conspiracy members and threatening either to leave

the victim's data encrypted and inaccessible, or to publicly share the victim's stolen data, or both, if the victim did not make a payment.

iv. Finally, members of each conspiracy would negotiate a ransom amount with a victim, promising to either decrypt locked data or delete stolen data (or both) if the victim paid an acceptable ransom amount. Conspiracy members would accept ransom payments in cryptocurrency. If a victim did not make a ransom payment, conspiracy members would often cause that victim's private data to be publicly posted on the Internet on a website under each conspiracy's control (often called a "data leak site").

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

1. The General Allegations section of this Indictment is realleged here.

The Conspiracy

2. From at least as early as in or about January 2020 through the present, in Passaic County, in the District of New Jersey, and elsewhere, the defendant,

MIKHAIL PAVLOVICH MATVEEV,
a/k/a "Wazawaka,"
a/k/a "m1x,"
a/k/a "Boriselcin,"
a/k/a "Uhodiransomwar,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly and intentionally conspire and agree with others (collectively, the "LockBit 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 one-year period from the LockBit 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 one-year period, contrary to Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B); 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 MATVEEV and the LockBit Coconspirators to enrich themselves by: (a) developing the LockBit ransomware variant, maintaining LockBit infrastructure, 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.

Manner and Means of the Conspiracy

4. To carry out the conspiracy and effect its illegal objects, MATVEEV

and the LockBit Coconspirators engaged in a number of manner and means, including those described in Paragraph 2(c) of the General Allegations section of this Indictment.

Overt Acts

5. In furtherance of the conspiracy and to effect its illegal objects, MATVEEV and the LockBit Coconspirators committed and caused to be committed the following overt acts in the District of New Jersey and elsewhere:

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

b. On or about August 30, 2020, MATVEEV and the LockBit Coconspirators deployed LockBit against LockBit-Victim-2, a business in Johnson County, Kansas.

c. On or about September 14, 2020, MATVEEV and the LockBit Coconspirators deployed LockBit against LockBit-Victim-3, a business in Dakota, Minnesota with operations and computers in New Jersey.

d. On or about September 14, 2020, MATVEEV emailed a ransom note with the subject line "Ransom" to LockBit-Victim-3 that read:

> Your data was encrypted and copied to our servers!
>
> Data size 964GB
>
> Data includes:
> -Credit cards (full number, exp date, cvv2, holder name\surname)

> -Document scans (passports US Citizens, Latin America Citizens,SSN scans, driver licence scans etc)
> -Personal Data (Names\SSN's\DOB\ZIP\Addresses etc)
> -Payroll
> -Bank documents
> -Accountant and Finance documents
> -Customers databases
> -Employees information
> -Contragents databases
>
> You have 7 days to communicate with us, besides, We will publish information about the hacking in the mass media and social networks
>
> If you won't communicate with us in 7 days, all your data will be published.

e. Later on or about September 14, 2020, MATVEEV emailed a further ransom note to LockBit-Victim-3 that read:

> Also, if you ignore this message, we will find information in the media about the hack

f. On or about September 23, 2020, MATVEEV and the LockBit Coconspirators deployed LockBit against LockBit-Victim-4, a business in Alameda County, California.

g. On or about September 23, 2020, MATVEEV emailed a ransom note with the subject line "lockbit" to LockBit-Victim-4 that read:

> Hello! All communications through this chat, we can not use emails via security reasons. Data recovery is the first part, the second part is that we have copied 334,48gb of data from your servers. Data includes: your member's personal data, driver licenses, payrolls, employees personal data, passport scans, bank\finance\accountant documents etc (next message you can find the dropmefiles link with screenshot of stolen folders, if you need any data samples, please let us know, we will provide it). And

> if we won't reach an agreement, all this data will be leaked in public. About the process: you make the payment and instantly receive master decryptor which you can use to decrypt all your servers. Plus you receive the videorecord which will contain the process of deleting your data from our servers. That's all.

h. On or about September 24, 2020, MATVEEV and the LockBit Coconspirators deployed LockBit against LockBit-Victim-5, a business in Boulder County, Colorado.

All in violation of Title 18, United States Code, Section 371.

COUNTS 2 AND 3
(Intentional Damage to a Protected Computer – 18 U.S.C. § 1030(a)(5)(A))

1. The General Allegations section and paragraphs 5(a), (c), (d), and (e) of Count 1 of this Indictment are realleged here.

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

MIKHAIL PAVLOVICH MATVEEV,
a/k/a "Wazawaka,"
a/k/a "m1x,"
a/k/a "Boriselcin,"
a/k/a "Uhodiransomwar,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, 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	Date	Victim
2	June 25, 2020	LockBit-Victim-1
3	September 14, 2020	LockBit-Victim-3

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

COUNT 4
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers – Babuk – 18 U.S.C. § 371)

1. The General Allegations section of this Indictment is realleged here.

The Conspiracy

2. From at least as early as in or about December 2020 through at least as recently as in or about September 2021, the defendant,

MIKHAIL PAVLOVICH MATVEEV,
a/k/a "Wazawaka,"
a/k/a "m1x,"
a/k/a "Boriselcin,"
a/k/a "Uhodiransomwar,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly and intentionally conspire and agree with others (collectively, the "Babuk 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 one-year period from the Babuk 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

one-year period, contrary to Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B); 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 MATVEEV and the Babuk Coconspirators to enrich themselves by: (a) developing the Babuk ransomware variant, maintaining Babuk infrastructure, and hacking into and deploying Babuk against victim computer systems; (b) demanding and extracting ransom payments from victims following successful Babuk attacks; and (c) extorting noncompliant victims and intimidating future victims by, among other things, posting those victims' stolen data on the Internet.

Manner and Means of the Conspiracy

4. To carry out the conspiracy and effect its illegal objects, MATVEEV

and the Babuk Coconspirators engaged in a number of manner and means, including those described in Paragraph 2(c) of the General Allegations section of this Indictment.

Overt Acts

5. In furtherance of the conspiracy and to effect its illegal objects, MATVEEV and the Babuk Coconspirators committed and caused to be committed the following overt acts:

a. On or about December 30, 2020, MATVEEV and the Babuk Coconspirators deployed Babuk against Babuk-Victim-1, a business in Turin, Italy.

b. On or about January 4, 2021, MATVEEV and the Babuk Coconspirators deployed Babuk against Babuk-Victim-2, a business in Hillsborough County, New Hampshire.

c. On or about March 10, 2021, MATVEEV and the Babuk Coconspirators deployed Babuk against Babuk-Victim-3, a business in Washington County, Oregon.

d. On or about March 12, 2021, MATVEEV emailed Babuk-Victim-3 a link to a dark web location hosting a chat portal to conduct ransom negotiations.

e. On or about April 26, 2021, MATVEEV and the Babuk Coconspirators deployed Babuk against the Metropolitan Police Department in Washington, D.C.

All in violation of Title 18, United States Code, Section 371.

COUNT 5
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers – Hive – 18 U.S.C. § 371)

1. The General Allegations section of this Indictment is realleged here.

The Conspiracy

2. From at least as early as in or about June 2021 through the present, in the District of New Jersey and elsewhere, the defendant,

MIKHAIL PAVLOVICH MATVEEV,
a/k/a "Wazawaka,"
a/k/a "m1x,"
a/k/a "Boriselcin,"
a/k/a "Uhodiransomwar,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly and intentionally conspire and agree with others (collectively, the "Hive 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 one-year period from the Hive 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

one-year period, contrary to Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B); 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 the Hive Coconspirators to enrich themselves by: (a) developing the Hive ransomware variant, maintaining Hive infrastructure, and hacking into and deploying Hive against victim computer systems; (b) demanding and extracting ransom payments from victims following successful Hive attacks; and (c) extorting noncompliant victims and intimidating future victims by, among other things, posting those victims' stolen data on the Internet.

Manner and Means of the Conspiracy

4. To carry out the conspiracy and effect its illegal objects, MATVEEV

and the Hive Coconspirators engaged in a number of manner and means, including those described in Paragraph 2(c) of the General Allegations section of this Indictment.

Overt Acts

5. In furtherance of the conspiracy and to effect its objects, MATVEEV and the Hive Coconspirators committed and caused to be committed the following overt acts in the District of New Jersey and elsewhere:

a. On or about May 27, 2022, the Hive Coconspirators deployed Hive against Hive-Victim-1, a nonprofit behavioral healthcare organization headquartered in Mercer County, New Jersey.

b. On or about June 2, 2022, MATVEEV and the Hive Coconspirators deployed Hive against Hive-Victim-2, a business in Somerset County, New Jersey.

c. On or about June 2, 2022, MATVEEV and the Hive Coconspirators caused a ransom note to be sent to Hive-Victim-2 that read, in part:

> Your network has been breached and all data were encrypted.
> Personal data, financial reports and important documents are ready to disclose.
>
> To decrypt all the data and to prevent exfiltrated files to be disclosed at [Hive data leak site]
> you will need to purchase our decryption software.

All in violation of Title 18, United States Code, Section 371.

COUNT 6
(Intentional Damage to a Protected Computer – 18 U.S.C. § 1030(a)(5)(A))

1. The General Allegations section and paragraphs 5(b) and (c) of Count 6 of this Indictment are realleged here.

2. On or about June 2, 2022, in Somerset County, in the District of New Jersey, and elsewhere, the defendant,

MIKHAIL PAVLOVICH MATVEEV,
a/k/a "Wazawaka,"
a/k/a "m1x,"
a/k/a "Boriselcin,"
a/k/a "Uhodiransomwar,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, 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, namely a protected computer belonging to Hive-Victim-2, 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.

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

FORFEITURE ALLEGATIONS

1. Upon conviction of any of the offenses charged in this Indictment, the defendant,

MIKHAIL PAVLOVICH MATVEEV,
a/k/a "Wazawaka,"
a/k/a "m1x,"
a/k/a "Boriselcin,"
a/k/a "Uhodiransomwar,"

shall forfeit to the United States:

a. pursuant to 18 U.S.C. §§ 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 this Indictment; and

b. pursuant to 18 U.S.C. § 1030(i), all right, title, and interest of the defendant in any personal property that was used or intended to be used to commit or to facilitate the commission of the offenses charged in this Information.

SUBSTITUTE ASSETS PROVISION

2. If any of the property described above, 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 21 U.S.C. § 853(p), as incorporated by 28 U.S.C. § 2461(c), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described above.

A True Bill,

[redacted]

Foreperson

Philip R. Sellinger

PHILIP R. SELLINGER
UNITED STATES ATTORNEY

CASE NUMBER: 22- 825 (SDW)

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

MIKHAIL PAVLOVICH MATVEEV,
a/k/a "Wazawaka," "m1x," "Boriselcin," and "Uhodiransomwar"

INDICTMENT FOR

18 U.S.C. § 371; 18 U.S.C. § 1030(a)(5)(A)

A True Bill,

[redacted]

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

ANDREW M. TROMBLY
DAVID E. MALAGOLD
ASSISTANT UNITED STATES ATTORNEYS, DISTRICT OF NEW JERSEY
NEWARK, NEW JERSEY

JESSICA C. PECK
TRIAL ATTORNEY, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION
WASHINGTON, DISTRICT OF COLUMBIA