UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term

Grand Jury Sworn in on September 15, 2022

UNITED STATES OF AMERICA	:	**CRIMINAL NO. 22-cr-**
	:	
v.	:	**GRAND JURY ORIGINAL**
	:	
MIKHAIL PAVLOVICH MATVEEV,	:	**FILED UNDER SEAL**
a/k/a "Wazawaka"	:	
a/k/a "m1x"	:	**VIOLATIONS:**
a/k/a "Boriscelcin"	:	
a/k/a "Uhodiransomwar,"	:	**18 U.S.C. §§ 1030(a)(5), 2**
	:	**(Intentional Damage to a Protected**
Defendant.	:	**Computer, and Aiding and Abetting)**
	:	
	:	**18 U.S.C. §§ 1030(a)(7), 2**
	:	**(Threats Relating to a Protected**
	:	**Computer, and Aiding and Abetting)**

INDICTMENT

The Grand Jury charges that, at times material to this Indictment, on or about the dates and at the approximate times stated below:

GENERAL ALLEGATIONS

1. From at least as early as 2020, the defendant, MIKHAIL PAVLOVICH MATVEEV, also known as "Wazawaka," "m1x," "Boriselcin," and "Uhodiransomwar," was a Russian national and resident.

2. From at least as early as 2020, MATVEEV was an active member of Babuk, a global ransomware campaign, which ranked among the most active and destructive cybercriminal threats in the world.

3. "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.

4. 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 May 2021, MATVEEV, along with others known and unknown to the Grand Jury, and aiding and abetting each other, executed Babuk attacks against victim systems both in the United States and around the world.

5. On April 26, 2021, computer systems of the Metropolitan Police Department of the District of Columbia ("MPD") were intentionally infected with Babuk ransomware. As part of the ransomware attack, the MPD was threatened with the disclosure of sensitive information unless payment was made.

COUNT ONE

6. Paragraphs 1 through 5 are incorporated herein.

7. On April 19, 2021, and continuing through May 9, 2021, within the District of Columbia and elsewhere, the defendant,

MIKHAIL PAVLOVICH MATVEEV,

conspiring with others, 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, and MIKHAIL PAVLOVICH MATVEEV knowingly aided and abetted others in doing the same.

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

COUNT TWO

8. Paragraphs 1 through 5 are incorporated herein.

9. On April 19, 2021, and continuing through May 9, 2021, within the District of Columbia and elsewhere, the defendant,

MIKHAIL PAVLOVICH MATVEEV,

conspiring with others, with intent to extort from MPD money and other things of value, transmitted in interstate and foreign commerce a communication containing a threat to impair the confidentiality of information obtained from a protected computer without authorization, and knowingly aided and abetted others in doing the same.

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

FORFEITURE ALLEGATIONS

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

MIKHAIL PAVLOVICH MATVEEV,

shall forfeit to the United States: 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 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

11. 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

FOREPERSON

Matthew M. Graves/jph

MATTHEW M. GRAVES
ATTORNEY FOR THE UNITED STATES
IN AND FOR THE DISTRICT OF COLUMBIA