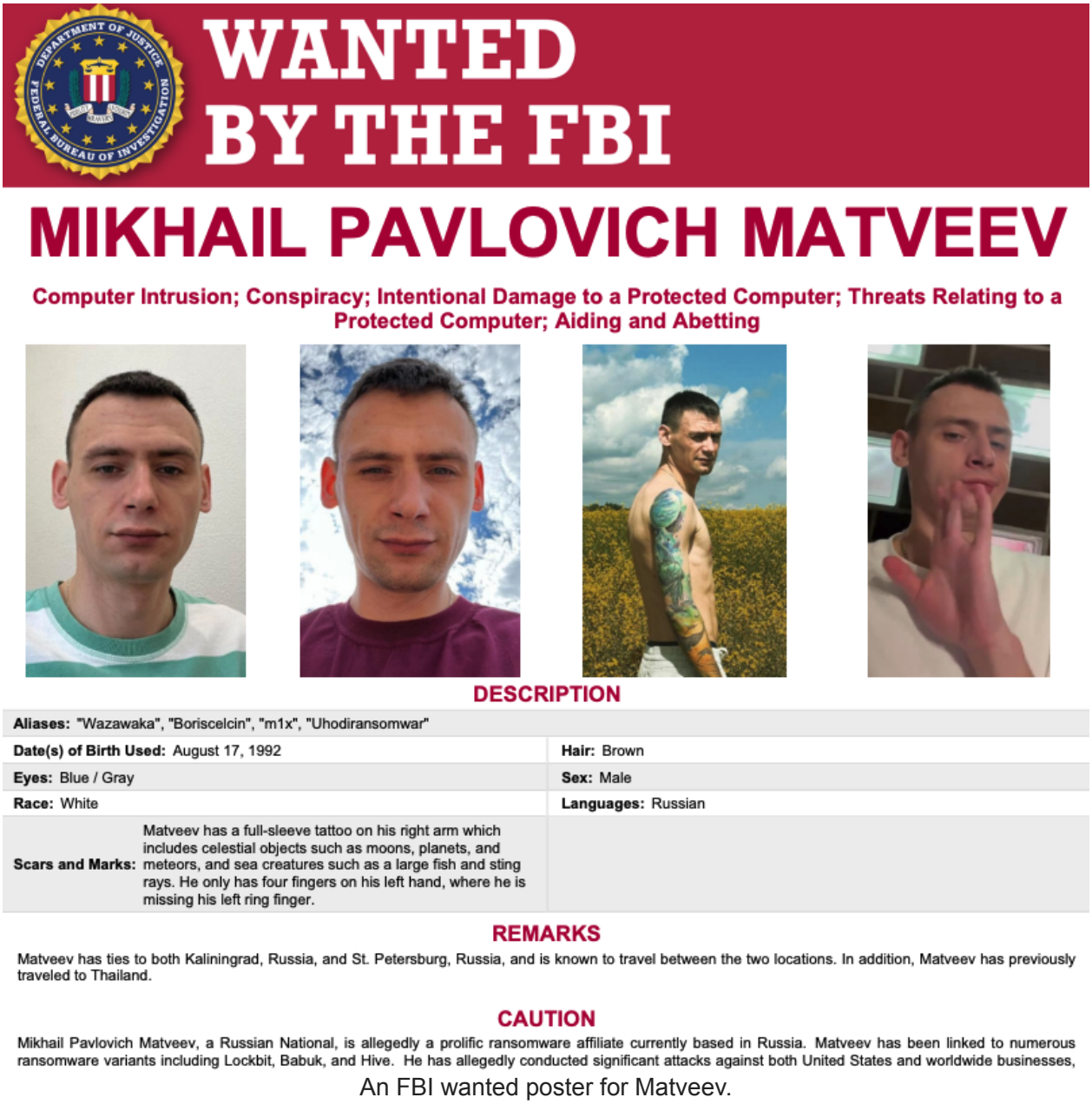
Russian Hacker “Wazawaka” Indicted for Ransomware

krebsonsecurity.com/2023/05/russian-hacker-wazawaka-indicted-for-ransomware/

A Russian man identified by KrebsOnSecurity in January 2022 as a prolific and vocal member of several top ransomware groups was the subject of two indictments unsealed by the **Justice Department** today. U.S. prosecutors say **Mikhail Pavolovich Matveev**, a.k.a. “**Wazawaka**” and “**Boriselcin**” worked with three different ransomware gangs that extorted hundreds of millions of dollars from companies, schools, hospitals and government agencies.



WANTED BY THE FBI

MIKHAIL PAVLOVICH MATVEEV

Computer Intrusion; Conspiracy; Intentional Damage to a Protected Computer; Threats Relating to a Protected Computer; Aiding and Abetting

DESCRIPTION

Aliases: "Wazawaka", "Boriscelcin", "m1x", "Uhodiransomwar"	
Date(s) of Birth Used: August 17, 1992	**Hair:** Brown
Eyes: Blue / Gray	**Sex:** Male
Race: White	**Languages:** Russian
Scars and Marks: Matveev has a full-sleeve tattoo on his right arm which includes celestial objects such as moons, planets, and meteors, and sea creatures such as a large fish and sting rays. He only has four fingers on his left hand, where he is missing his left ring finger.	

REMARKS

Matveev has ties to both Kaliningrad, Russia, and St. Petersburg, Russia, and is known to travel between the two locations. In addition, Matveev has previously traveled to Thailand.

CAUTION

Mikhail Pavlovich Matveev, a Russian National, is allegedly a prolific ransomware affiliate currently based in Russia. Matveev has been linked to numerous ransomware variants including Lockbit, Babuk, and Hive. He has allegedly conducted significant attacks against both United States and worldwide businesses,

An FBI wanted poster for Matveev.

Indictments returned in New Jersey and the District of Columbia allege that Matveev was involved in a conspiracy to distribute ransomware from three different strains or affiliate groups, including **Babuk**, **Hive** and **LockBit**.

The indictments allege that on June 25, 2020, Matveev and his LockBit co-conspirators deployed LockBit ransomware against a law enforcement agency in Passaic County, New Jersey. Prosecutors say that on May 27, 2022, Matveev conspired with Hive to ransom a nonprofit behavioral healthcare organization headquartered in Mercer County, New Jersey. And on April 26, 2021, Matveev and his Babuk gang allegedly deployed ransomware against the Metropolitan Police Department in Washington, D.C.

Meanwhile, the **U.S. Department of Treasury** has added Matveev to its list of persons with whom it is illegal to transact financially. Also, the **U.S. State Department**is offering a $10 million reward for the capture and/or prosecution of Matveev, although he is unlikely to face either as long as he continues to reside in Russia.

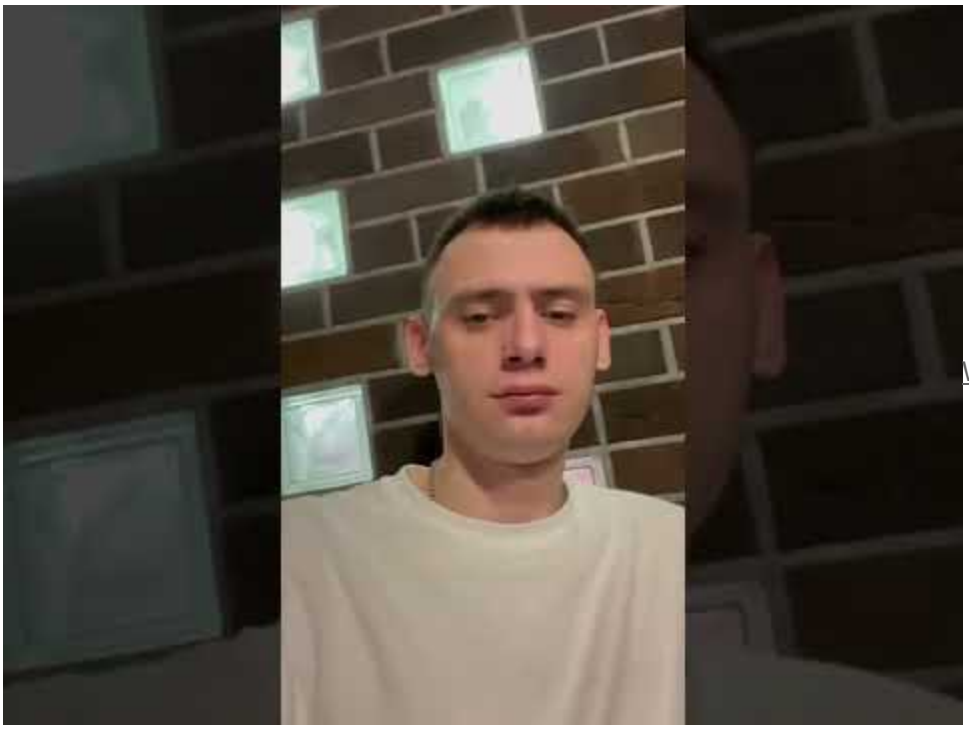
In a January 2021 discussion on a top Russian cybercrime forum, Matveev's alleged alter ego Wazawaka said he had no plans to leave the protection of "Mother Russia," and that traveling abroad was not an option for him.

"Mother Russia will help you," Wazawaka concluded. "Love your country, and you will always get away with everything."

In January 2022, KrebsOnSecurity published Who is the Network Access Broker 'Wazawaka,' which followed clues from Wazawaka's many pseudonyms and contact details on the Russian-language cybercrime forums back to a 33-year-old Mikhail Matveev from Abaza, RU (the FBI says his date of birth is Aug. 17, 1992).

A month after that story ran, a man who appeared identical to the social media photos for Matveev began posting on Twitter a series of bizarre selfie videos in which he lashed out at security journalists and researchers (including this author), while using the same Twitter account to drop exploit code for a widely-used virtual private networking (VPN) appliance.

"Hello Brian Krebs! You did a really great job actually, really well, fucking great — it's great that journalism works so well in the US," Matveev said in one of the videos. "By the way, it is my voice in the background, I just love myself a lot."



Watch Video At:

https://youtu.be/G1LclbndLaM

Prosecutors allege Matveev used a dizzying stream of monikers on the cybercrime forums, including "**Boriselcin**," a talkative and brash personality who was simultaneously the public persona of Babuk, a ransomware affiliate program that surfaced on New Year's Eve 2020.

Previous reporting here revealed that Matveev's alter egos included "**Orange,**" the founder of the **RAMP** ransomware forum. RAMP stands for "Ransom Anon Market Place, and analysts at the security firm Flashpoint say the forum was created "directly in response to several large Dark Web forums banning ransomware collectives on their site following the Colonial Pipeline attack by ransomware group 'DarkSide."

As noted in last year's investigations into Matveev, his alleged cybercriminal handles all were driven by a uniquely communitarian view that when organizations being held for ransom decline to cooperate or pay up, any data stolen from the victim should be published on the Russian cybercrime forums for all to plunder — not privately sold to the highest bidder.

In thread after thread on the crime forum **XSS**, Matveev's alleged alias "**Uhodiransomwar**" could be seen posting download links to databases from companies that have refused to negotiate after five days.

Matveev is charged with conspiring to transmit ransom demands, conspiring to damage protected computers, and intentionally damaging protected computers. If convicted, he faces more than 20 years in prison.

Further reading:

Who is the Network Access Broker “Wazawaka?”

Wazawaka Goes Waka Waka

The New Jersey indictment against Matveev (PDF)

The indictment from the U.S. attorney’s office in Washington, D.C. (PDF)