Russia arrests cybercriminal Wazawaka for ties with ransomware gangs

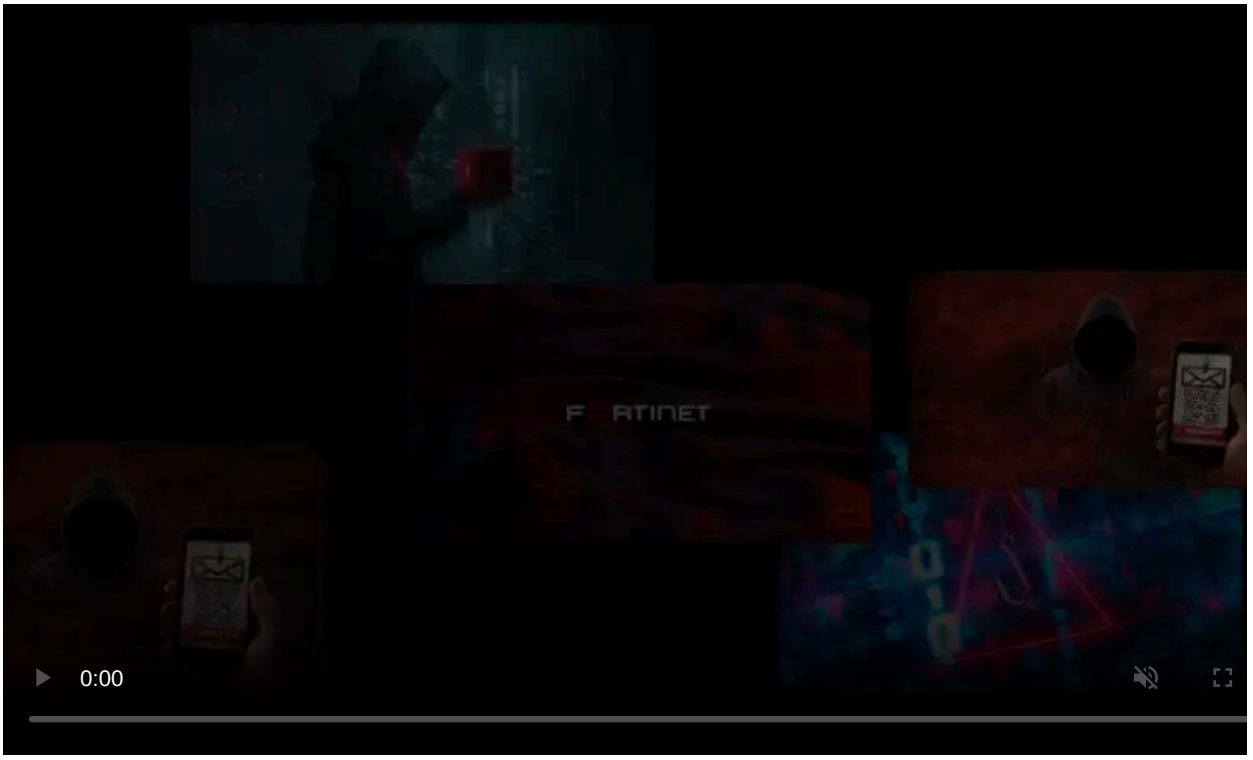
By Sergiu Gatlan

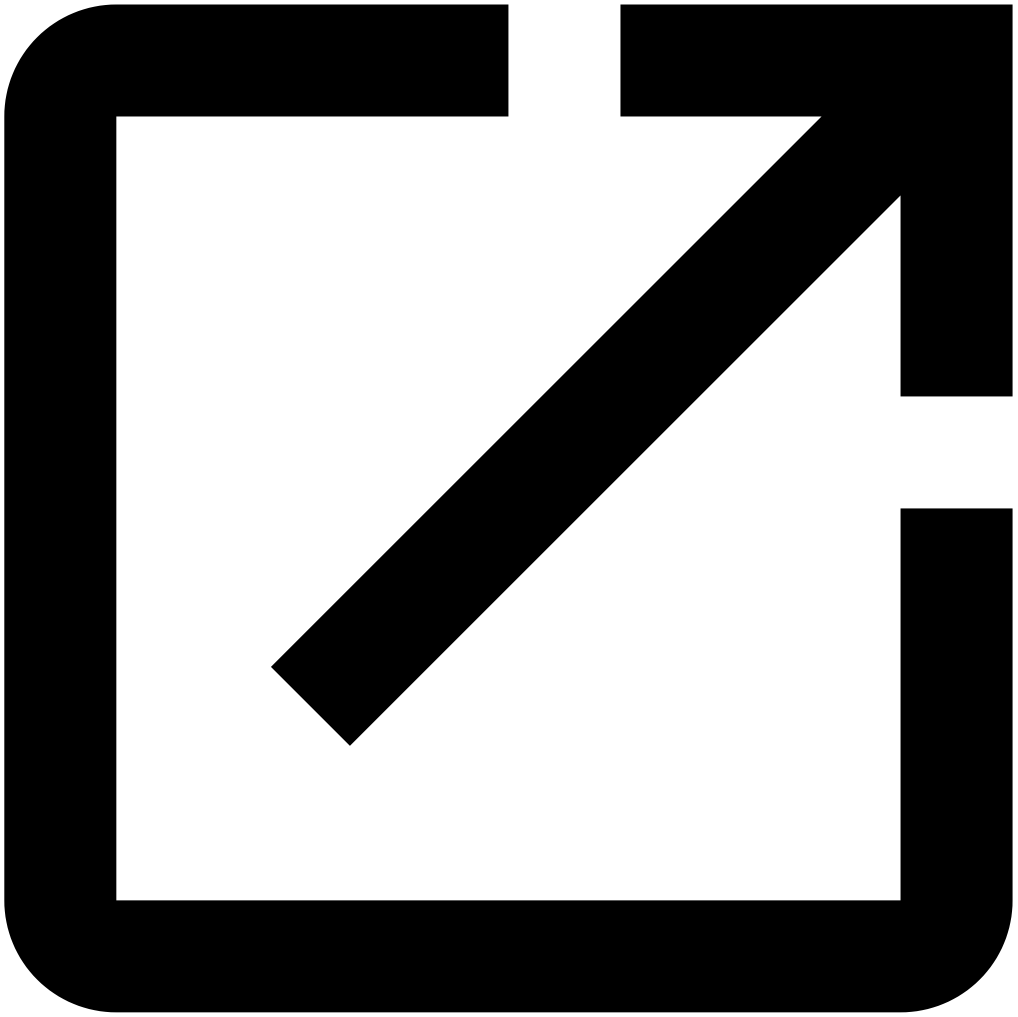
Published: 2024-11-29 · Archived: 2026-04-05 22:09:27 UTC

Russian law enforcement has arrested and indicted notorious ransomware affiliate Mikhail Pavlovich Matveev (also known as Wazawaka, Uhodiransomwar, m1x, and Boriselcin) for developing malware and his involvement in several hacking groups.

While the prosecutor's office has yet to release any details on the individual's identity (described as a "programmer" in court documents), the individual is Matveev, according to an anonymous source of the Russian state-owned news agency RIA Novosti.

"At present, the investigator has collected sufficient evidence, the criminal case with the indictment signed by the prosecutor has been sent to the Central District Court of the city of Kaliningrad for consideration on the merits," the Russian Ministry of Internal Affairs said in a statement.


F RTINET
0:00



As first spotted by cyber policy expert Oleg Shakirov, Matveev is accused of developing ransomware (described by the prosecutor's office notes as "specialized malicious software" that can encrypt files and data) that he planned to use for encrypting the data "of commercial organizations in order to then receive a ransom from them for decryption."

Mikhail Matveev wanted poster (FBI)

Last year, in May 2023, the U.S. Justice Department also filed charges against Matveev for his involvement in the Hive and LockBit ransomware operations that targeted victims across the United States.

He is also believed to be "Orange," the original creator and admin of the Ramp hacking forum and the original admin of the Babuk ransomware operation. The latter split up after members couldn't decide whether to publish data stolen from the Washington DC Capital Police Force.

A Justice Department press release and unsealed indictments in New Jersey and the District of Columbia provide an approximate timeline of his activity while working with the three ransomware gangs:

- In June 2020, Matveev and LockBit coconspirators allegedly deployed LockBit ransomware on the network of a law enforcement agency in Passaic County, New Jersey.
- In April 2021, the defendant and Babuk ransomware coconspirators allegedly deployed malicious payloads on the systems of the Metropolitan Police Department in Washington, D.C.
- In May 2022, Matveev and Hive ransomware gang members allegedly encrypted the systems of a nonprofit behavioral healthcare organization headquartered in Mercer County, New Jersey.

Matveev was also sanctioned by the Department of the Treasury's Office of Foreign Assets Control (OFAC) for launching cyberattacks against U.S. entities, including U.S. law enforcement and critical infrastructure organizations.

The U.S. Department of State is also offering a reward of up to $10 million for any information that could lead to his arrest or conviction for transnational organized crime.

Matveev has had a very vocal online presence. He frequently talked with cybersecurity researchers and professionals and openly discussed his cybercrime activity using his (still active) Twitter account, RansomBoris.

After being sanctioned by the U.S., Matveev openly taunted U.S. law enforcement, tweeting a picture of his wanted poster on a t-shirt.

Source: https://www.bleepingcomputer.com/news/security/russia-arrests-cybercriminal-wazawaka-for-ties-with-ransomware-gangs/