Russian National Charged with Ransomware Attacks Against Critical Infrastructure

justice.gov/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure

Press Release

Tuesday, May 16, 2023

For Immediate Release
Office of Public Affairs

Ransomware Attacks Against Law Enforcement Agencies in Washington, D.C. and New Jersey, As Well As Other Victims Worldwide; U.S. Department of State Offers Reward Up to $10M

The Justice Department today unsealed two indictments charging a Russian national and resident with using three different ransomware variants to attack numerous victims throughout the United States, including law enforcement agencies in Washington, D.C. and New Jersey, as well as victims in healthcare and other sectors nationwide.

According to the indictment obtained in the District of New Jersey, from at least as early as 2020, Mikhail Pavlovich Matveev, aka Wazawaka, aka m1x, aka Boriselcin, aka Uhodiransomwar, allegedly participated in conspiracies to deploy three ransomware variants. These variants are known as LockBit, Babuk, and Hive, and Matveev transmitted ransom demands in connection with each. The perpetrators behind each of these variants, including Matveev, have allegedly used these types of ransomware to attack thousands of victims in the United States and around the world. These victims include law enforcement and other government agencies, hospitals, and schools. Total ransom demands allegedly made by the members of these three global ransomware campaigns to their victims amount to as much as $400 million, while total victim ransom payments amount to as much as $200 million.

“From his home base in Russia, Matveev allegedly used multiple ransomware variants to attack critical infrastructure around the world, including hospitals, government agencies, and victims in other sectors,” said Assistant Attorney General Kenneth A. Polite, Jr. of the Justice Department’s Criminal Division. “These international crimes demand a coordinated response. We will not relent in imposing consequences on the most egregious actors in the cybercrime ecosystem.”

On or about June 25, 2020, Matveev and his LockBit coconspirators allegedly deployed LockBit ransomware against a law enforcement agency in Passaic County, New Jersey. Additionally, on or about May 27, 2022, Matveev and his Hive coconspirators allegedly deployed Hive against a nonprofit behavioral healthcare organization headquartered in Mercer County, New Jersey. On April 26, 2021, Matveev and his Babuk coconspirators allegedly deployed Babuk against the Metropolitan Police Department in Washington, D.C.

“From Russia and hiding behind multiple aliases, Matveev is alleged to have used these ransomware strains to encrypt and hold hostage for ransom the data of numerous victims, including hospitals, schools, nonprofits, and law enforcement agencies, like the Metropolitan Police Department in Washington, D.C.,” said U.S. Attorney Philip R. Sellinger for the District of New Jersey. “Thanks to the extraordinary investigative work of prosecutors from my office and our FBI partners, Matveev no longer hides in the shadows – we have publicly identified his criminal acts and charged him with multiple federal crimes. Let today’s charges be a reminder to cybercriminals everywhere – my office is devoted to combatting cybercrime and will spare no resources in bringing to justice those who use ransomware attacks to target victims.”

According to the indictment obtained in the District of Columbia, between April 21, 2021, and May 9, 2021, Matveev allegedly participated in conspiracies to deploy Babuk and to transmit a ransom demand. Specifically, on April 26, 2021, Matveev and his Babuk co-conspirators allegedly deployed Babuk ransomware against the Metropolitan Police Department in Washington, D.C., and then threatened to disclose sensitive information to the public unless a payment was made.

“Data theft and extortion attempts by ransomware groups are corrosive, cynical attacks on key institutions and the good people behind them as they go about their business and serve the public,” said U.S. Attorney Matthew M. Graves for the District of Columbia. “Whether these criminals target law enforcement, other government agencies, or private companies like health care providers, we will use every tool at our disposal to prosecute and punish such offenses. Thanks to exceptional work by our partners here, we identified and charged this culprit.”

“The FBI is steadfast in our commitment to disrupting cybercriminals like Matveev,” said Assistant Director Bryan Vorndran of the FBI’s Cyber Division. “The FBI will continue to impose costs on cyber adversaries through our joint collaboration with our private sector and international partners, and we will not tolerate these criminal acts against American citizens.”

The LockBit ransomware variant first appeared around January 2020. LockBit actors have executed over 1,400 attacks against victims in the United States and around the world, issuing over $100 million in ransom demands and receiving over $75 million in ransom payments.

The Babuk ransomware variant first appeared around December 2020. Babuk actors executed over 65 attacks against victims in the United States and around the world, issuing over $49 million in ransom demands and receiving as much as $13 million in ransom payments.

Since June 2021, the Hive ransomware group has targeted more than 1,400 victims around the world and received as much as $120 million in ransom payments.

The LockBit, Babuk, and Hive ransomware variants operated in the same general manner: first, the ransomware actors would identify and unlawfully access vulnerable computer systems, sometimes through their own hacking, or by purchasing stolen access credentials from others. Second, the actors would deploy the ransomware variant within the victim computer system, allowing the actors to encrypt and steal data thereon. Next, the actors would send a ransom note to the victim demanding a payment in exchange for decrypting the victim's data or refraining from sharing it publicly. Finally, the ransomware actors would negotiate a ransom amount with each victim willing to pay. If a victim did not pay, ransomware actors would often post that victim's data on a public website, often called a data leak site.

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

The FBI Newark Field Office's Cyber Crimes Task Force is investigating the case with valuable assistance from the Jersey City Police Department, New Jersey State Police, Newark IRS Criminal Investigation, and international partners from European Cyber Crime Centre of Europol, National Police Agency of Japan, Gendarmerie Nationale Cyberspace Command of France, National Crime Agency and South West Regional Organized Crime Unit of the United Kingdom, Kantonspolizei Zürich of Switzerland, High-Tech Crime Unit of the Dutch Police Services Agency of the Netherlands, Bundeskriminalamt and Landeskriminalamt of Germany, Mossos d'Esquadra Police Department of Spain, Norwegian Police Service of Norway, and Swedish Police Authority of Sweden.

Trial Attorneys Jessica C. Peck, Benjamin Proctor, and Jorge Gonzalez of the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS); Assistant U.S. Attorneys Andrew M. Trombly and David E. Malagold for the District of New Jersey's Cybercrime Unit in Newark; and Assistant U.S. Attorney Elizabeth Aloi for the District of Columbia's Fraud, Public Corruption, and Civil Rights Section are prosecuting the case.

The FBI Tampa Field Office and Orlando Resident Agency, along with Assistant U.S. Attorney Chauncey Bratt for the Middle District of Florida and CCIPS Trial Attorneys Christen Gallagher and Alison Zitron, made critical contributions to the case. The FBI Washington Field Office and Metropolitan Police Department also provided valuable assistance.

The Justice Department's Office of International Affairs and National Security Division also provided significant assistance.

Victims of LockBit, Babuk, or Hive ransomware should contact their local FBI field office for further information. For additional information on ransomware, including the LockBit, Babuk, and Hive variants, please visit StopRansomware.gov.

Additionally, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) today announced that it is designating the defendant for his role in launching ransomware attacks against U.S. law enforcement, businesses, and critical infrastructure.

Finally, the Department of State has also announced an award of up to $10 million for information that leads to the arrest and/or conviction of this defendant. Information that may be eligible for this award can be submitted at tips.fbi.gov. Congress established the Transnational Organized Crime Rewards Program in 2013 to support law enforcement efforts to dismantle transnational criminal organizations and bring their leaders and members to justice. The Department of State's Bureau of International Narcotics and Law Enforcement Affairs manages the program in coordination with other U.S. federal agencies.

An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Updated May 17, 2023

Topic

Cybercrime

Press Release Number: 23-559