U.S. DEPARTMENT OF THE TREASURY

Treasury Sanctions Russian Ransomware Actor Complicit in Attacks on Police and U.S. Critical Infrastructure

May 16, 2023

Treasury imposes consequences on key ransomware actor

WASHINGTON — Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), designated Mikhail Matveev (**Matveev**) for his role in launching cyberattacks against U.S. law enforcement, businesses, and critical infrastructure. Concurrently, the U.S. District Courts for the District of New Jersey and the District of Columbia unsealed indictments against **Matveev**. Additionally, the U.S. Department of State announced an award of up to $10 million for information that leads to the arrest and/or conviction of Matveev under its Transnational Organized Crime Rewards Program.

"The United States will not tolerate ransomware attacks against our people and our institutions," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "Ransomware actors like Matveev will be held accountable for their crimes, and we will continue to use all available authorities and tools to defend against cyber threats."

The impacts of ransomware attacks are far-reaching, with victims experiencing the loss and disclosure of sensitive information and disruption of critical services. Russia is a haven for ransomware actors, enabling cybercriminals like **Matveev** to engage openly in ransomware attacks against U.S. organizations. According to analysis conducted by Treasury's Financial Crimes Enforcement Network (FinCEN), 75 percent of ransomware-related incidents reported between July and December 2021 were linked to Russia, its proxies, or persons acting on its behalf. Russia-linked ransomware variants such as Hive, LockBit, and Babuk, which Matveev helped to develop and deploy, have been responsible for millions of dollars in losses to victims in the United States and around the world. The Hive ransomware group alone has targeted more than 1,500 victims in over 80 countries, including hospitals, school districts, financial firms, and other critical infrastructure.

MIKHAIL MATVEEV: KEY ACTOR IN THE RUSSIAN RANSOMWARE ECOSYSTEM

Matveev has been a central figure in the development and deployment of the Hive, LockBit, and Babuk ransomware variants, among others. In 2021, Babuk ransomware affiliates attacked the police department of a major U.S. city. The hackers who infiltrated the police department's computer network stole the home addresses, cellphone numbers, financial data, medical histories, and other personal details of police officers, along with sensitive information about gangs, suspects of crimes, and witnesses. In a public interview, **Matveev** claimed responsibility for posting the police department's stolen data online.

In addition to attacks on public institutions, **Matveev** has been linked to ransomware intrusions against numerous U.S. businesses, including a U.S. airline.

Matveev has been vocal about his illegal activities. He has provided insight into his cybercrimes in media interviews, disclosed exploit code to online criminals, and stated that his illicit activities will be tolerated by local authorities provided that he remains loyal to Russia.

OFAC is designating **Matveev** pursuant to section 1(a)(ii)(C) of Executive Order (E.O.) 13694, as amended by E.O. 13757, for being responsible for or complicit in, or having engaged in, directly or indirectly, a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant disruption to the availability of a computer or network of computers.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated individual that are in the United States or in the possession or control of U.S. persons must be blocked and reported to OFAC. OFAC's regulations generally prohibit all dealings by U.S. persons or within the United States (including transactions transiting the United States) that involve any property or interests in property of blocked or designated persons.

In addition, persons that engage in certain transactions with the individual designated today may themselves be exposed to designation.

The power and integrity of sanctions derive not only from OFAC's ability to designate and add persons to the Specially Designated Nationals and Blocked Persons (SDN) List but also from OFAC's willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer

to OFAC's Frequently Asked Question 897. For detailed information on the process to submit a request for removal from an OFAC sanctions list, please refer to OFAC's website.

For more information on the individual designated today.

See OFAC's Updated Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments here for information about actions that OFAC would consider to be mitigating factors in any related enforcement action involving ransomware payments with a potential sanctions risk. For information on complying with sanctions applicable to virtual currency, see OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry here.

####