Russian National Arrested and Charged with Conspiring to Commit LockBit Ransomware Attacks Against U.S. and Foreign Businesses

Press Release

Thursday, June 15, 2023

For Immediate Release
Office of Public Affairs

The Justice Department today announced charges against a Russian national for his involvement in deploying numerous LockBit ransomware and other cyberattacks against victim computer systems in the United States, Asia, Europe, and Africa.

Ruslan Magomedovich Astamirov (АСТАМИРОВ, Руслан Магомедовичь), 20, of Chechen Republic, will make his initial appearance later today.

“This LockBit-related arrest, the second in six months, underscores the Justice Department’s unwavering commitment to hold ransomware actors accountable,” said Deputy Attorney General Lisa O. Monaco. “In securing the arrest of a second Russian national affiliated with the LockBit ransomware, the Department has once again demonstrated the long arm of the law. We will continue to use every tool at our disposal to disrupt cybercrime, and while cybercriminals may continue to run, they ultimately cannot hide.”

According to a criminal complaint obtained in the District of New Jersey, from at least as early as August 2020 to March 2023, Astamirov allegedly participated in a conspiracy with other members of the LockBit ransomware campaign to commit wire fraud and to intentionally damage protected computers and make ransom demands through the use and deployment of ransomware. Specifically, Astamirov directly executed at least five attacks against victim computer systems in the United States and abroad.

“Astamirov is the third defendant charged by this office in the LockBit global ransomware campaign, and the second defendant to be apprehended,” said U.S. Attorney Philip R. Sellinger for the District of New Jersey. “The LockBit conspirators and any other ransomware perpetrators cannot hide behind imagined online anonymity. We will continue to work tirelessly with all our law enforcement partners to identify ransomware perpetrators and bring them to justice.”

According to the criminal complaint, 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 at least as much as tens of millions of dollars in actual ransom payments made in the form of bitcoin.

In furtherance of his LockBit-related activities, Astamirov owned, controlled, and used a variety of email addresses, Internet Protocol (IP) addresses, and other online provider accounts that allowed him and his co-conspirators to deploy LockBit ransomware and to communicate with their victims. Additionally, in at least one circumstance, law enforcement was able to trace a portion of a victim’s ransom payment to a virtual currency address in Astamirov’s control.

“The FBI is committed to pursuing ransomware actors like Astamirov, who have exploited vulnerable cyber ecosystems and harmed victims,” said FBI Deputy Director Paul Abbate. “We, in collaboration with our federal and international partners, are fully committed to the permanent dismantlement of these types of ransomware campaigns that intentionally target people and our private sector partners. We will continue to leverage every resource to prevent this type of malicious, criminal activity.”

Astamirov is charged with conspiring to commit wire fraud and conspiring to intentionally damage protected computers and to transmit ransom demands. If convicted, he faces a maximum penalty of 20 years in prison on the first charge and a maximum penalty of five years in prison on the second charge. Both charges are also punishable by a maximum fine of either $250,000 or twice the gain or loss from the offense, whichever is greatest.

This announcement follows LockBit-related charges in two other cases from the District of New Jersey. In November 2022, the department announced criminal charges against Mikhail Vasiliev, a dual Russian and Canadian national, who is currently in custody in Canada awaiting extradition to the United States. In May 2023, the department announced the indictment of Mikhail Pavlovich Matveev, aka Wazawaka, aka m1x, aka Boriselcin, aka Uhodiransomwar, for his alleged participation in separate conspiracies to deploy LockBit, Babuk, and Hive ransomware variants against victims in the United States and abroad.

The FBI Newark Field Office’s Cyber Crimes Task Force is investigating the case. The Jersey City Police Department, New Jersey State Police, Newark IRS Criminal Investigation, and the international partners from Europol’s European Cybercrime Centre, Eurojust, National Police Agency of Japan, France’s Gendarmerie Nationale Cyberspace Command (Cyber Crime Investigation Unit / C3N), National Crime Agency and South West Regional Organized Crime Unit of the United Kingdom, Kantonspolizei Zürich of Switzerland, Landeskriminalamt Schleswig-Holstein and the Bundeskriminalamt of Germany, and Swedish Police Authority of Sweden also provided valuable assistance.

Trial Attorney Jessica C. Peck and Jorge Gonzalez of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorneys Andrew M. Trombly, Vinay Limbachia, and David E. Malagold for the District of New Jersey's Cybercrime Unit in Newark are prosecuting the case.

The U.S. Attorney's Office for the District of Arizona and the Justice Department's Office of International Affairs also provided significant assistance.

Victims of LockBit ransomware should contact their local FBI field office and visit StopRansomware.gov for further information.

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

Updated June 15, 2023

Topic

Cybercrime

Press Release Number: 23-666