Two Foreign Nationals Plead Guilty to Participation in LockBit Ransomware Group

Published: 2024-07-18 · Archived: 2026-04-05 20:06:21 UTC

NEWARK, N.J. –Two foreign nationals pleaded guilty today in Newark federal court to participating in the LockBit ransomware group – at various times the most prolific ransomware variant in the world – and to deploying LockBit attacks against victims in the United States and worldwide.

According to court documents:

Ruslan Magomedovich Astamirov (АСТАМИРОВ, Руслан Магомедовичь), 21, a Russian national of Chechen Republic, Russia, and Mikhail Vasiliev, 34, a dual Canadian and Russian national of Bradford, Ontario, were members of LockBit. The LockBit ransomware variant first appeared in January 2020. Between that time and February 2024, LockBit grew into what was at times the most active and destructive ransomware group in the world. The LockBit group attacked more than 2,500 victims in at least 120 countries around the world, including 1,800 in the United States. Those victims ranged from individuals and small businesses to multinational corporations, and they included hospitals, schools, nonprofit organizations, critical infrastructure, and government and law-enforcement agencies. LockBit's members extracted at least approximately $500 million in ransom payments from their victims and caused billions of dollars in broader losses, including costs like lost revenue and incident response and recovery.

LockBit's "affiliate" members, including Vasiliev and Astamirov, would first identity and unlawfully access vulnerable computer systems. They would then deploy LockBit ransomware on victim computer systems and both steal and encrypt stored data. After a successful LockBit attack, LockBit's affiliate members would then demand a ransom from their victims in exchange for decrypting the victims' data and deleting stolen data. When victims did not pay the demanded ransoms, LockBit's affiliates would then leave the victim's data permanently encrypted and publish the stolen data, including highly sensitive information, on a publicly accessible Internet site under LockBit's control.

> "Astamirov and Vasiliev thought that they could deploy LockBit from the shadows, wreaking havoc and pocketing massive ransom payments from their victims, without consequence. They were wrong. We, in New Jersey, along with our domestic and international law enforcement partners will do everything in our power to hold LockBit's members and other cybercriminals accountable, disrupt and dismantle their operations, and put a spotlight on them as wanted criminals – no matter where they hide.

U.S. Attorney Philip R. Sellinger

"Today's convictions reflect the latest returns on the Department's investment in disrupting ransomware threats, prioritizing victims, and holding cybercriminals accountable," said Deputy Attorney General Lisa Monaco. "In executing our all-tools cyber enforcement strategy, we've dealt significant blows to destructive ransomware groups like LockBit, as we did earlier this year, seizing control of LockBit infrastructure and distributing

decryption keys to their victims. Today's actions serve as a warning to ransomware actors who would attack Americans: we will find you and hold you accountable."

"The defendants committed ransomware attacks against victims in the United States and around the world through LockBit, which was one of the most destructive ransomware groups in the world," said Principal Deputy Assistant Attorney General Nicole M. Argentieri, head of the Justice Department's Criminal Division. "But thanks to the work of the Computer Crime and Intellectual Property Section, along with its domestic and international partners, LockBit no longer claims that title. Today's convictions represent another important milestone in the Criminal Division's ongoing effort to disrupt and dismantle ransomware groups, protect victims, and bring cybercriminals to justice."

"It's a common misconception that cyber hackers won't get caught by law enforcement because they're smarter and savvier than we are," FBI – Newark Special Agent in Charge James E. Dennehy said. "Two members of the LockBit affiliate pleading guilty to their crimes in U.S. federal court illustrate we can stop them and bring them to justice. These malicious actors believe they can operate with impunity – and don't fear getting caught because they sit in a country where they feel safe and protected. FBI Newark and our law enforcement partners around the globe have the technology and intelligence to go after these criminals – regardless of where they hide."

Between 2020 and 2023, Astamirov deployed LockBit against at least 12 victims, including businesses in Virginia, Japan, France, Scotland, and Kenya. Operating under the online aliases "BETTERPAY," "offtitan," and "Eastfarmer," he derived at least $1.9 million in ransom payments from those victims. As part of his plea agreement, Astamirov agreed to forfeit, among other assets, $350,000 in seized cryptocurrency that he extorted from one of his LockBit victims. Astamirov was first charged and arrested in this matter in June 2023.

Between 2021 and 2023, Vasiliev, operating under the online aliases "Ghostrider," "Free," "Digitalocean90," "Digitalocean99," "Digitalwaters99," and "Newwave110," deployed LockBit against at least 12 victims, including businesses in New Jersey, Michigan, the United Kingdom, and Switzerland. He also deployed LockBit against an educational facility in England and a school in Switzerland. Through these attacks, Vasiliev caused at least $500,000 in damage and losses to his victims. Vasiliev was first charged in this matter and arrested in Canada by Canadian authorities in November 2022, and extradited to the United States in June.

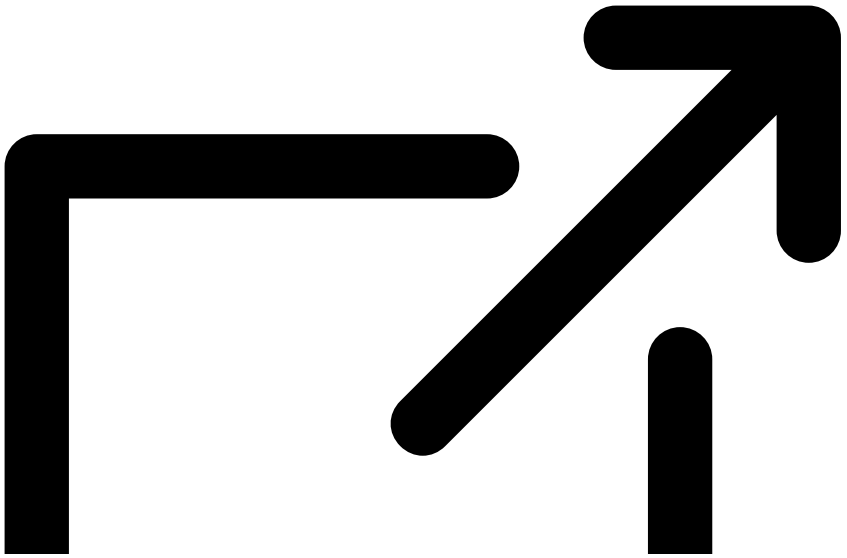
Astamirov pleaded guilty to a two-count information charging him with conspiracy to commit computer fraud and abuse and conspiracy to commit wire fraud. He faces a maximum penalty of 25 years in prison. Vasiliev pleaded guilty to a four-count information charging him with conspiracy to commit computer fraud and abuse, intentional damage to a protected computer, transmission of a threat in relation to damaging a protected computer, and conspiracy to commit wire fraud. He faces a maximum penalty of 45 years in prison. A sentencing date has not yet been set. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The LockBit Investigation

Today's guilty pleas follow a recent a disruption of LockBit ransomware in February by the U.K. National Crime Agency's (NCA) Cyber Division, which worked in cooperation with the Justice Department, FBI, and other international law enforcement partners. As previously announced by the Department, authorities disrupted LockBit by seizing numerous public-facing websites used by LockBit to connect to the organization's

infrastructure and by seizing control of servers used by LockBit administrators, thereby disrupting the ability of LockBit actors to attack and encrypt networks and extort victims by threatening to publish stolen data. This disruption succeeded in greatly diminishing LockBit's reputation and its ability to attack further victims, as alleged by documents filed in this case.

Today's guilty pleas also follow charges brought in the District of New Jersey against other LockBit members, including its alleged creator, developer, and administrator, Dmitry Yuryevich Khoroshev. An indictment against Khoroshev unsealed in May alleges that Khoroshev began developing LockBit as early as September 2019, continued acting as the group's administrator through 2024, a role in which Khoroshev recruited new affiliate members, spoke for the group publicly under the alias "LockBitSupp," and developed and maintained the infrastructure used by affiliates to deploy LockBit attacks. Khoroshev also took 20 percent of each ransom paid by LockBit victims, allowing him to personally derive at least $100 million over that period. Khoroshev is currently the subject of a reward of up to $10 million through the U.S. Department of State's Transnational Organized Crime (TOC) Rewards Program, with information accepted through the FBI tip website at www.tips.fbi.gov



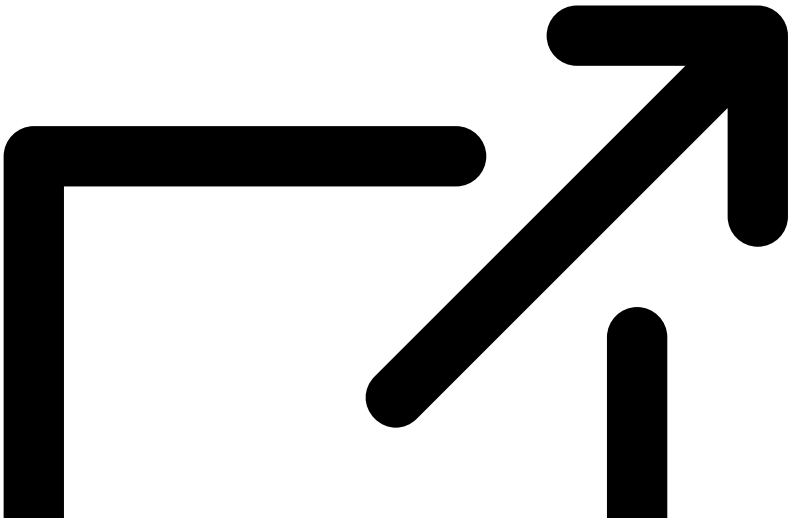
.

Both defendants are scheduled to be sentenced on Jan. 8, 2025.

A total of six LockBit members, including Khoroshev, the alleged developer, and Astamirov and Vasiliev, both affiliates, have now been charged in the District of New Jersey. Other LockBit charges include:

- In February, in parallel with the disruption operation, an indictment was unsealed in the District of New Jersey charging Russian nationals Artur Sungatov and Ivan Kondratyev, also known as Bassterlord, with deploying LockBit against numerous victims throughout the United States, including businesses nationwide in the manufacturing and other industries, as well as victims around the world in the semiconductor and other industries.
- In May 2023, two indictments were unsealed in Washington, D.C., and the District of New Jersey charging Mikhail Matveev, also known as Wazawaka, m1x, Boriselcin, and Uhodiransomwar, with using different

ransomware variants, including LockBit, to attack numerous victims throughout the United States, including the Washington, D.C., Metropolitan Police Department. Matveev is currently the subject of a reward of up to $10 million through the U.S. Department of State's TOC Rewards Program, with information accepted through the FBI tip website at www.tips.fbi.gov/



.

The U.S. Department of State's TOC Rewards Program is offering rewards of:

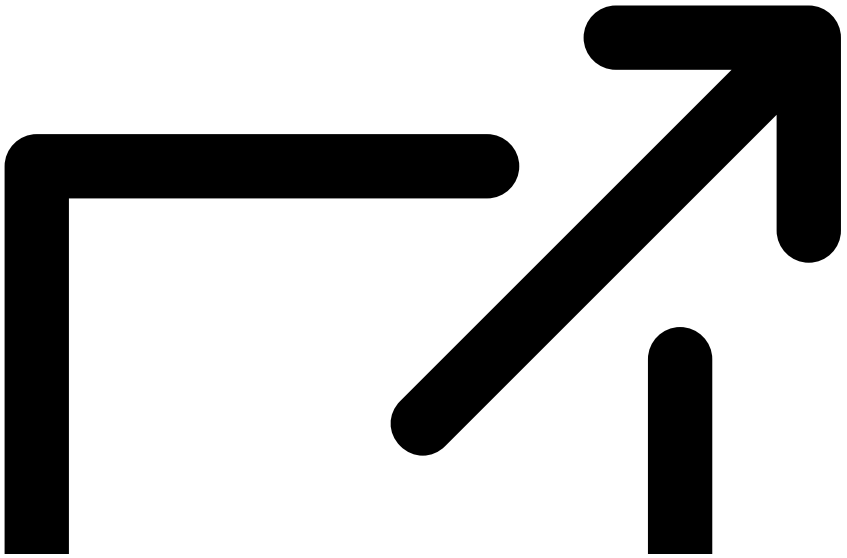
- Up to $10 million for information leading to the arrest and/or conviction in any country of Khoroshev;
- Up to $10 million for information leading to the arrest and/or conviction of Matveev;
- Up to $10 million for information leading to the identification and location of any individuals who hold a key leadership position in LockBit; and
- Up to $5 million for information leading to the arrest and/or conviction in any country of any individual participating or attempting to participate in LockBit.

Information is accepted through the FBI tip website at www.tips.fbi.gov/.

Khoroshev, Matveev, Sungatov, and Kondratyev have also been designated for sanctions by the Department of the Treasury's Office of Foreign Assets Control for their roles in launching cyberattacks.

Victim Assistance

LockBit victims are encouraged to contact the FBI and submit information at https://lockbitvictims.ic3.gov/



. As announced by the Department in February, law enforcement, through its disruption efforts, has developed decryption capabilities that may enable hundreds of victims around the world to restore systems encrypted using the LockBit ransomware variant. Submitting information at the ICE site will enable law enforcement to determine whether affected systems can be successfully decrypted.

LockBit victims are also encouraged to visit https://www.justice.gov/usao-nj/lockbit for case updates and information regarding their rights under U.S. law, including the right to submit victim impact statements and request restitution, in the litigation against Astamirov and Vasiliev.

The FBI Newark Field Office, under the supervision of Special Agent in Charge James E. Dennehy, is investigating the LockBit ransomware variant. The FBI Atlanta Field Office, under the supervision of Special Agent in Charge Keri Farley; U.S. Attorney's Office for the Northern District of Georgia; Ontario Provincial Police in Ontario, Canada; and Crown Attorney's Office in Toronto, Canada, provided significant assistance in the Vasiliev matter. The United Kingdom's NCA; France's Gendarmerie Nationale Cyberspace Command; Germany's Landeskriminalamt Schleswig-Holstein and the Bundeskriminalamt; Switzerland's Federal Office of Police, Public Prosecutor's Office of the Canton of Zurich, and Zurich Cantonal Police; Japan's National Policy Agency; Australian Federal Police; Sweden's Polismyndighetens; Royal Canadian Mounted Police; Politie Dienst Regionale Recherche Oost-Brabant of the Netherlands; Finland's Poliisi; Europol; and Eurojust have provided significant assistance and coordination in both matters and in the LockBit investigation generally.

Assistant U.S. Attorneys Andrew M. Trombly, David E. Malagold, and Vinay Limbachia for the District of New Jersey and Trial Attorneys Jessica C. Peck, Debra Ireland, and Jorge Gonzalez of the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and are prosecuting the charges against Astamirov and Vasiliev.

The Justice Department's Cybercrime Liaison Prosecutor to Eurojust, Office of International Affairs, and National Security Division also provided significant assistance.

Additional details on protecting networks against LockBit ransomware are available at StopRansomware.gov. These include Cybersecurity and Infrastructure Security Agency Advisories AA23-325A, AA23-165A, and AA23-075A.
