

# U.S. and U.K. Disrupt LockBit Ransomware Variant

[justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant](https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant)



Press Release

Tuesday, February 20, 2024

## For Immediate Release


Office of Public Affairs

U.S. Indictment Charges Two Russian Nationals with Attacks Against Multiple U.S. and International Victims; FBI Seizes Infrastructure; and Department of Treasury Takes Additional Action Against LockBit

The Department of Justice joined the United Kingdom and international law enforcement partners in London today to announce the disruption of the LockBit ransomware group, one of the most active ransomware groups in the world that has targeted over 2,000 victims, received more than \$120 million in ransom payments, and made ransom demands totaling hundreds of millions of dollars.

The U.K. National Crime Agency's (NCA) Cyber Division, working in cooperation with the Justice Department, Federal Bureau of Investigation (FBI), and other international law enforcement partners disrupted LockBit's operations by seizing numerous public-facing websites used by LockBit to connect to the organization's infrastructure and 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.

"For years, LockBit associates have deployed these kinds of attacks again and again across the United States and around the world. Today, U.S. and U.K. law enforcement are taking away the keys to their criminal operation," said Attorney General Merrick B. Garland. "And we are going a step further — we have also obtained keys from the seized LockBit infrastructure to help victims decrypt their captured systems and regain access to their data. LockBit is not the first ransomware variant the Justice Department and its international partners have dismantled. It will not be the last."

Additionally, the NCA, in cooperation with the FBI and international law enforcement partners, has developed decryption capabilities that may enable hundreds of victims around the world to restore systems encrypted using the LockBit ransomware variant. Beginning today, victims targeted by this malware are encouraged to contact the FBI at <https://lockbitvictims.ic3.gov/>  to enable law enforcement to determine whether affected systems can be successfully decrypted.

“Today’s actions are another down payment on our pledge to continue dismantling the ecosystem fueling cybercrime by prioritizing disruptions and placing victims first,” said Deputy Attorney General Lisa Monaco. “Using all our authorities and working alongside partners in the United Kingdom and around the world, we have now destroyed the online backbone of the LockBit group, one of the world’s most prolific ransomware gangs. But our work does not stop here: together with our partners, we are turning the tables on LockBit — providing decryption keys, unlocking victim data, and pursuing LockBit’s criminal affiliates around the globe.”

The Justice Department also unsealed an indictment obtained 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. Today, additional criminal charges against Kondratyev were unsealed in the Northern District of California related to his deployment in 2020 of ransomware against a victim located in California.

Finally, the Department also unsealed two search warrants issued in the District of New Jersey that authorized the FBI to disrupt multiple U.S.-based servers used by LockBit members in connection with the LockBit disruption. As disclosed by those search warrants, those servers were used by LockBit administrators to host the so-called “StealBit” platform, a criminal tool used by LockBit members to organize and transfer victim data.

“Today, the FBI and our partners have successfully disrupted the LockBit criminal ecosystem, which represents one of the most prolific ransomware variants across the globe,” said FBI Director Christopher A. Wray. “Through years of innovative investigative work, the FBI and our partners have significantly degraded the capabilities of those hackers responsible for launching crippling ransomware attacks against critical infrastructure and other public and private organizations around the world. This operation demonstrates both our capability and commitment to defend our nation’s cybersecurity and national security from any malicious actor who seeks to impact our way of life. We will continue to work with our domestic and international allies to identify, disrupt, and deter cyber threats, and to hold the perpetrators accountable.”

According to the indictment obtained in the District of New Jersey, from at least as early as January 2021, Sungatov allegedly deployed LockBit ransomware against victim corporations and took steps to fund additional LockBit attacks against other victims. Sungatov allegedly deployed LockBit ransomware against manufacturing, logistics, insurance, and other companies located in Minnesota, Indiana, Puerto Rico, Wisconsin, Florida, and New Mexico. Additionally, as early as August 2021, Kondratyev similarly began to allegedly deploy LockBit against multiple victims. Kondratyev, operating under the online alias “Bassterlord,” allegedly deployed LockBit against municipal and private targets in Oregon, Puerto Rico, and New York, as

well as additional targets located in Singapore, Taiwan, and Lebanon. Both Sungatov and Kondratyev are alleged to have joined in the global LockBit conspiracy, also alleged to have included Russian nationals Mikhail Pavlovich Matveev and Mikhail Vasiliev, as well as other LockBit members, to develop and deploy LockBit ransomware and to extort payments from victim corporations.

“Today’s indictment, unsealed as part of a global coordinated action against the most active ransomware group in the world, brings to five the total number of LockBit members charged by my office and our FBI and Computer Crime and Intellectual Property Section partners for their crimes,” said U.S. Attorney Philip R. Sellinger for the District of New Jersey. “And, even with today’s disruption of LockBit, we will not stop there. Our investigation will continue, and we remain as determined as ever to identify and charge all of LockBit’s membership — from its developers and administrators to its affiliates. We will put a spotlight on them as wanted criminals. They will no longer hide in the shadows.”

With the indictment unsealed today, a total of five LockBit members have now been charged for their participation in the LockBit conspiracy. In May 2023, two indictments were unsealed in Washington, D.C., and the District of New Jersey charging Matveev 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 Transnational Organized Crime Rewards Program, with information accepted through the FBI tip website at <https://tips.fbi.gov>. In November 2022, a criminal complaint was filed in the District of New Jersey charging Vasiliev in connection with his participation in the LockBit global ransomware campaign. Vasiliev, a dual Russian-Canadian national, is currently in custody in Canada awaiting extradition to the United States. In June 2023, Russian national Ruslan Magomedovich Astamirov was charged by criminal complaint in the District of New Jersey for his participation in the LockBit conspiracy, including his deployment of LockBit against victims in Florida, Japan, France, and Kenya. Astamirov is currently in custody in the United States awaiting trial.

Kondratyev, according to the indictment obtained in the Northern District of California and unsealed today, is also charged with three criminal counts arising from his use of the Sodinokibi, also known as REvil, ransomware variant to encrypt data, exfiltrate victim information, and extort a ransom payment from a corporate victim based in Alameda County, California.

The LockBit ransomware variant first appeared around January 2020 and, leading into today’s operation, had grown into one of the most active and destructive variants in the world. LockBit members have executed attacks against more than 2,000 victims in the United States and around the world, making at least hundreds of millions of U.S. dollars in ransom demands and receiving over \$120 million in ransom payments. The LockBit ransomware variant, like other major ransomware variants, operates in the “ransomware-as-a-service” (RaaS) model, in which administrators, also called developers, design the ransomware, recruit other members — called affiliates — to deploy it, and maintain an online software dashboard called a “control panel” to provide the affiliates with the tools necessary to deploy LockBit. Affiliates, in turn, identify and unlawfully access vulnerable computer systems, sometimes through their own hacking or at other times by purchasing stolen access credentials from others. Using the control panel operated by the developers,

affiliates then deploy LockBit within the victim computer system, allowing them to encrypt and steal data for which a ransom is demanded to decrypt or avoid publication on a public website maintained by the LockBit developers, often called a data leak site.


The FBI Newark Field Office is investigating the LockBit ransomware variant.

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 are prosecuting the charges against Sungatov and Kondratyev unsealed today in the District of New Jersey. The Justice Department's Cybercrime Liaison Prosecutor to Eurojust and Office of International Affairs also provided significant assistance.

The disruption announced today was the result of a joint operation between the FBI; NCA South West Regional Organised Crime Unit; 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 Polismyndigheten; Royal Canadian Mounted Police; Politie Dienst Regionale Recherche Oost-Brabant of the Netherlands; Finland's Poliisi; Europol; and Eurojust.

The FBI Phoenix Field Office and Assistant U.S. Attorney Helen L. Gilbert are investigating and prosecuting the case against Kondratyev in the Northern District of California.

Additionally, the Department of the Treasury's Office of Foreign Assets Control announced today that it is designating Sungatov and Kondratyev for their roles in launching cyberattacks.

As mentioned above, victims of LockBit should contact the FBI at <https://lockbitvictims.ic3.gov>  for further information. Additional details on protecting networks against LockBit ransomware are available at [StopRansomware.gov](https://StopRansomware.gov). These include Cybersecurity and Infrastructure Security Agency Advisories AA23-325A, AA23-165A, and AA23-075A.

Watch the Attorney General's remarks:

Updated February 20, 2024

---

## Topic

Cybercrime

Press Release Number: 24-194