U.S. Charges Russian Man as Boss of LockBit Ransomware Group

Published: 2024-05-07 · Archived: 2026-04-05 13:44:33 UTC

The United States joined the United Kingdom and Australia today in sanctioning 31-year-old Russian national **Dmitry Yuryevich Khoroshev** as the alleged leader of the infamous ransomware group **LockBit**. The **U.S. Department of Justice** also indicted Khoroshev and charged him with using Lockbit to attack more than 2,000 victims and extort at least $100 million in ransomware payments.

Image: U.K. National Crime Agency.

Khoroshev (Дмитрий Юрьевич Хорошев), a resident of Voronezh, Russia, was charged in a 26-count indictment by a grand jury in New Jersey.

“Dmitry Khoroshev conceived, developed, and administered Lockbit, the most prolific ransomware variant and group in the world, enabling himself and his affiliates to wreak havoc and cause billions of dollars in damage to thousands of victims around the globe,” **U.S. Attorney Philip R. Sellinger** said in a statement released by the Justice Department.

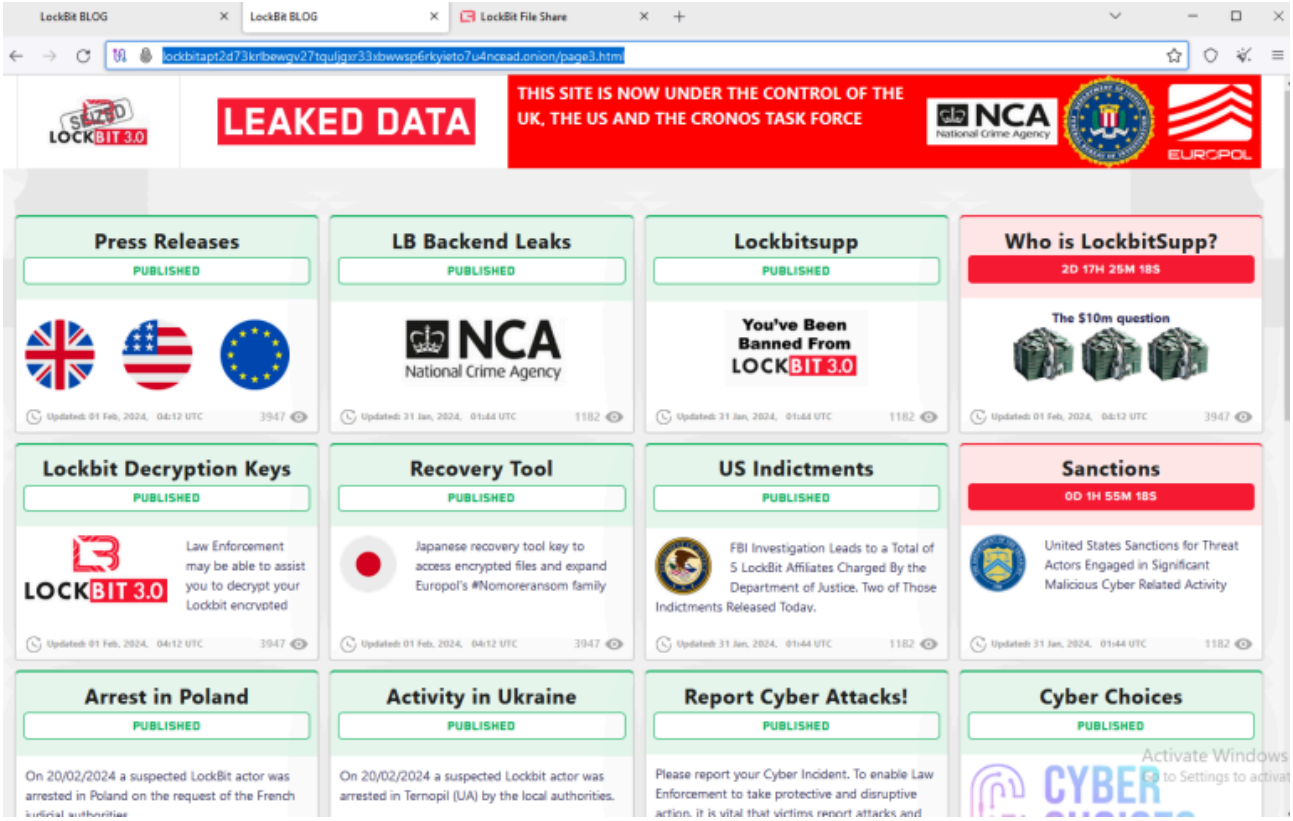
The indictment alleges Khoroshev acted as the LockBit ransomware group’s developer and administrator from its inception in September 2019 through May 2024, and that he typically received a 20 percent share of each ransom

payment extorted from LockBit victims.

The government says LockBit victims included individuals, small businesses, multinational corporations, hospitals, schools, nonprofit organizations, critical infrastructure, and government and law-enforcement agencies.

“Khoroshev and his co-conspirators extracted at least $500 million in ransom payments from their victims and caused billions of dollars in broader losses, such as lost revenue, incident response, and recovery,” the DOJ said. “The LockBit ransomware group attacked more than 2,500 victims in at least 120 countries, including 1,800 victims in the United States.”

The unmasking of LockBitSupp comes nearly three months after U.S. and U.K. authorities seized the darknet websites run by LockBit, retrofitting it with press releases about the law enforcement action and free tools to help LockBit victims decrypt infected systems.



The feds used the existing design on LockBit’s victim shaming website to feature press releases and free decryption tools.

One of the blog captions that authorities left on the seized site was a teaser page that read, “Who is LockbitSupp?,” which promised to reveal the true identity of the ransomware group leader. That item featured a countdown clock until the big reveal, but when the site’s timer expired no such details were offered.

Following the FBI’s raid, LockBitSupp took to Russian cybercrime forums to assure his partners and affiliates that the ransomware operation was still fully operational. LockBitSupp also raised another set of darknet websites that soon promised to release data stolen from a number of LockBit victims ransomed prior to the FBI raid.

One of the victims LockBitSupp continued extorting was Fulton County, Ga. Following the FBI raid, LockbitSupp vowed to release sensitive documents stolen from the county court system unless paid a ransom demand before LockBit's countdown timer expired. But when Fulton County officials refused to pay and the timer expired, no stolen records were ever published. Experts said it was likely the FBI had in fact seized all of LockBit's stolen data.

LockBitSupp also bragged that their real identity would never be revealed, and at one point offered to pay $10 million to anyone who could discover their real name.

KrebsOnSecurity has been in intermittent contact with LockBitSupp for several months over the course of reporting on different LockBit victims. Reached at the same ToX instant messenger identity that the ransomware group leader has promoted on Russian cybercrime forums, LockBitSupp claimed the authorities named the wrong guy.

> "It's not me," LockBitSupp replied in Russian. "I don't understand how the FBI was able to connect me with this poor guy.

"It's not me," LockBitSupp replied in Russian. "I don't understand how the FBI was able to connect me with this poor guy. Where is the logical chain that it is me? Don't you feel sorry for a random innocent person?"

LockBitSupp, who now has a $10 million bounty for his arrest from the **U.S. Department of State**, has been known to be flexible with the truth. The Lockbit group routinely practiced "double extortion" against its victims — requiring one ransom payment for a key to unlock hijacked systems, and a separate payment in exchange for a promise to delete data stolen from its victims.

But Justice Department officials say LockBit never deleted its victim data, regardless of whether those organizations paid a ransom to keep the information from being published on LockBit's victim shaming website.

Khoroshev is the sixth person officially indicted as active members of LockBit. The government says Russian national **Artur Sungatov** used LockBit ransomware against victims in manufacturing, logistics, insurance and other companies throughout the United States.

Ivan Gennadievich Kondratyev, a.k.a. "Bassterlord," allegedly deployed LockBit against targets in the United States, Singapore, Taiwan, and Lebanon. Kondratyev is also charged (PDF) with three criminal counts arising from his alleged use of the Sodinokibi (aka "REvil") ransomware variant to encrypt data, exfiltrate victim information, and extort a ransom payment from a corporate victim based in Alameda County, California.

In May 2023, U.S. authorities unsealed indictments against two alleged LockBit affiliates, **Mikhail "Wazawaka" Matveev** and **Mikhail Vasiliev**. In January 2022, KrebsOnSecurity published Who is the Network Access Broker 'Wazawaka,' which followed clues from Wazawaka's many pseudonyms and contact details on the Russian-language cybercrime forums back to a 31-year-old Mikhail Matveev from Abaza, RU.

Matveev remains at large, presumably still in Russia. Meanwhile, the U.S. Department of State has a standing $10 million reward offer for information leading to Matveev's arrest.

Vasiliev, 35, of Bradford, Ontario, Canada, is in custody in Canada awaiting extradition to the United States (the complaint against Vasiliev is at this PDF).

In June 2023, Russian national **Ruslan Magomedovich Astamirov** was charged in New Jersey for his participation in the LockBit conspiracy, including the deployment of LockBit against victims in Florida, Japan, France, and Kenya. Astamirov is currently in custody in the United States awaiting trial.

The Justice Department is urging victims targeted by LockBit to contact the FBI at https://lockbitvictims.ic3.gov/ to file an official complaint, and to determine whether affected systems can be successfully decrypted.
