

## REMARKS

May 7, 2024

PHILIP R. SELLINGER,  
U.S. ATTORNEY, DISTRICT OF NEW JERSEY

Good morning. I'm Philip Sellinger, United States Attorney for the District of New Jersey.

In February of this year, I joined law enforcement partners from around the world to announce a coordinated operation that had severely disrupted LockBit, at the time the most prolific and destructive ransomware group in the world. We promised then that our investigation would continue until all of LockBit was held accountable, including its developer.

And we are here again today, to announce a 26-count indictment alleging that Dmitry Yuryevich Khoroshev conceived, developed and administered LockBit, enabling himself and his affiliates to wreak havoc and cause billions of dollars in damage to thousands of victims around the globe. The indictment charges Khoroshev—a Russian national and resident—with committing and conspiring to commit LockBit attacks since September 2019 while operating under the online aliases “LockBit” and “LockBitSupp.”

As alleged in the indictment, Khoroshev designed LockBit so that after hackers secretly gained access to a victim's computer systems, they could encrypt or steal the victim's data, or both. After Lockbit was deployed, hackers sent victims ransom notes, threatening to publicly share the victims' stolen data if a ransom of hundreds of thousands or even millions of dollars was not paid. One victim alone received a ransom demand of \$200 million. If a victim did not pay up, the hackers would allegedly cause that victim's private data to be publicly posted, often on what was called a “data leak site.”

LockBit's alleged victims included hospitals, schools, nonprofit organizations, critical infrastructure facilities, and government and law-enforcement agencies in New Jersey and around the world. They ranged from major multinational corporations to small businesses and individuals in nearly 120 countries, including China and even Russia, even though Khoroshev purportedly claimed to prohibit LockBit affiliate co-conspirators from attacking Russian victims.

All told, LockBit conspirators allegedly extorted approximately half a billion dollars in ransom payments from their victims. Khoroshev—as the developer and leader of LockBit—is accused of receiving 20 percent of each LockBit ransom payment, totaling more than \$100 million. Nobody profited from LockBit more than Khoroshev.

But these ransom payments are only part of the story. As alleged, LockBit attacks also severely disrupted their victims' operations, causing lost revenue and expenses associated with incident response and recovery. Altogether, the total damage allegedly caused by LockBit amounts to billions of U.S. dollars. Moreover, stolen data, some of which was highly sensitive, was compromised. And, as alleged in the indictment, Khoroshev was in charge of it all.

As I mentioned earlier, in February, law enforcement agencies from around the world, joined together to severely disrupt LockBit, seizing its servers and diminishing its reputation and ability to extort victims. That operation was a success. Even though Khoroshev has attempted to revive LockBit following the disruption, the number of LockBit attacks since February has dramatically decreased, and LockBit's brand has been seriously tarnished.

What's more, the servers seized by law enforcement in February contained copies of data allegedly stolen from LockBit victims who had actually paid the demanded ransom. In other words, we now know, that even though Khoroshev and his co-conspirators allegedly promised those victims they would delete the stolen data after the ransom was paid, they didn't. Future ransomware victims should take note: alleged cyber criminals cannot be trusted to do what they say.

With today's indictment of LockBit's leader, a total of six individuals have now been charged in the District of New Jersey for their participation in LockBit including Russian nationals Ruslan Astamirov, who is in custody in the United States; Mikhail Vasiliev, who is in custody in Canada awaiting extradition here, and Mikhail Matveev, Artur Sungatov, and Ivan Kondratyev, who are all at large.

And let me be clear: as I said in February, my office remains determined to hold every LockBit conspirator accountable. Law enforcement agencies around the world continue to work together to carefully analyze LockBit's data and infrastructure, including victim lists and documents which identify affiliates and other co-conspirators.

Shortly after the February 2024 disruption of LockBit, Khoroshev is alleged to have contacted law enforcement to offer his services in exchange for information regarding the identity of his ransomware competitors. As charged, Khoroshev intended to use this information to stifle his competition and restore LockBit's primacy in the ransomware space. "Give me the names of my enemies," he allegedly asked.

The tables have turned. Instead, the Department of Justice has one name to disclose today in this unsealed indictment: and that is Dmitry Yuryevich Khoroshev.

I am also pleased to share that the State Department is offering a reward of up to \$10 million for information that leads to Khoroshev's apprehension. The Treasury Department's Office of Foreign Assets Control has also designated Khoroshev for sanctions based on his role in the LockBit ransomware conspiracy.

To conclude, I want to commend the extraordinary investigative work of the prosecutors assigned to this case – including Assistant U.S. Attorneys Andrew Trombly, David Malagold, and Vinay Limbachia, who led this investigation for my Office, and trial attorneys Jessica Peck, Debra Ireland, and Jorge Gonzalez from the Computer Crimes and Intellectual Property Section of the Department of Justice – as well as the dedicated agents from the FBI.

Because of their work, an alleged cybercriminal no longer hides in the shadows —a grand jury has charged him with multiple federal crimes. Let today's charges be a reminder to cybercriminals everywhere – my office is devoted to combatting ransomware attacks and will spare no resources in bringing cybercriminals to justice.

Thank you.