US unseals complaint against Russian-Israeli accused of working for LockBit

By Alexander Martin

Published: 2024-12-20 · Archived: 2026-04-05 18:20:22 UTC

The U.S. unsealed a criminal complaint on Friday against a dual Russian and Israeli national who is accused of being a software developer for the LockBit ransomware group.

Rostislav Panev, 51, is currently detained in Israel, where the U.S. is seeking to have him extradited to face trial on 40 counts, including for computer damage and extortion.

According to the unsealed complaint, Panev worked for the cybercrime group from 2019 up until February 2024 — the same month that law enforcement disrupted the LockBit scheme by seizing its darknet website and infrastructure.

The complaint states that U.S. authorities had already developed significant independent evidence at the time of the LockBit disruption linking Panev to a moniker used on a darknet cybercrime forum.

Speaking to the media following the lifting of a gag order yesterday, Panev's lawyer, Sharon Nahari, told the outlet Ynet: "My client is a computer technician. His role was strictly limited to software development, and he was neither aware of nor involved in the primary offenses he has been accused of, including fraud, extortion, and money laundering."

According to the complaint, an interview by Israeli authorities "yielded overwhelming evidence further establishing PANEV's role as a LockBit developer—and, specifically, as a developer of code for multiple LockBit builders and other critical LockBit facilities."

The authorities also found Panev's computer had access to the LockBit control panel, which they say was only available to LockBit members who have undergone a vetting process and not to the general public.

"Notably," the complaint states, the panel included a handle to communicate with the panel's user on an unidentified decentralized, end-to-end encrypted messaging platform. The user's handle was "FUCKFBI" followed by other characters.

A .onion domain was also discovered that hosted a Git repository — a tool for software developers to collaborate on projects — that Panev is suspected of using to create several LockBit builders, the custom software used to generate the malware to infect the ransomware gang's victims.

According to the complaint, Panev has agreed to multiple voluntary interviews with Israeli authorities while in custody during which time he admitted performing "multiple coding jobs for LockBit in exchange for compensation."

These included writing code to disable Windows Defender antivirus; to propagate additional code throughout a network via Windows Active Directory; and writing code "to print a given text on all printers on a given network (presumably, the LockBit ransom note)."

Panev also told Israeli authorities that he was regularly paid $10,000 in cryptocurrency on a monthly basis — in total "at least approximately $230,000" — in exchange for his software development services, including code "for encryption malware and providing technical assistance."

The complaint states that Panev claimed — dubiously, in the assessment of the U.S. authorities — that it was only over time he came to realise his work with LockBit may have been unlawful, although once he did he continued to work for the group "for the money."

Israeli judicial authorities are currently considering the U.S. extradition request.

Panev's arrest would be the latest in a series of law enforcement activities targeting the ransomware group's associates and affiliates. Several have been identified and arrested.

One, a Russian national called Aleksandr Ryzhenkov, was exposed and accused of also being one of the main members of the Evil Corp cybercrime group.

Following the takedown, the cybercrime gang's pseudonymous leader, LockBitSupp, was subsequently exposed as Russian national Dmitry Khoroshev. The U.S. indicted him and imposed financial sanctions, as did the United Kingdom and Australia. LockBitSupp claimed the wrong man had been identified.

"The arrest of Mr. Panev reflects the Department's commitment to using all its tools to combat the ransomware threat," said U.S. Deputy Attorney General Lisa Monaco. "We started this year with a coordinated international disruption of LockBit — the most damaging ransomware group in the world. Fast forward to today and three LockBit actors are in custody thanks to the diligence of our investigators and our strong partnerships around the world. This case is a model for ransomware investigations in the years to come."

Alexander Martin

is the UK Editor for Recorded Future News. He was previously a technology reporter for Sky News and a fellow at the European Cyber Conflict Research Initiative, now Virtual Routes. He can be reached securely using Signal on: AlexanderMartin.79
