# Ransomware Operation LockBit Relaunches Dark Web Leak Site

## After Operation Cronos, LockBit Leader LockBitSupp Vows to Continue Hacking

David Perera (@daveperera) • February 24, 2024 (link)

Russian-speaking ransomware operation LockBit reestablished a dark web leak site Saturday afternoon and posted a lengthy screed apparently authored by its leader, who vowed not to retreat from the criminal underground world.

In a lengthy missive, the LockBit leader said the FBI appears to have used a vulnerability, tracked as CVE-2023-3824, in web-scripting language PHP to penetrate the ransomware-as-a-service operation's servers. LockBit didn't patch the vulnerability "because for five years of swimming in money I became very lazy."

Law enforcement did not take down backup servers that didn't have PHP installed, LockBit said.

"All FBI actions are aimed at destroying the reputation of my affiliate program, my demoralization, they want me to leave and quit my job, they want to scare me because they can not find and eliminate me, I can not be stopped, you can not even hope, as long as I am alive I will continue to do pentest with postpaid," the missive states.

The FBI told Information Security Media Group that it declines to comment on this afternoon's developments.

British, U.S. and European law enforcement on Monday executed the takeover of the LockBit website, which kicked off a week of timed announcements touting the seizure of decryption keys, source code and cryptocurrency wallets (see: Breach Roundup: More Fallout From the LockBit Takedown).

Law enforcement agencies behind the takedown, acting under the banner of Operation Cronos, suggested they would reveal on Friday the identity of LockBit leader LockBitSupp - but did not. "We know who he is. We know where he lives. We know how much he is worth. LockBitSupp has engaged with Law Enforcement :)," authorities instead wrote on the seized leak site (see: No Big Reveal: Cops Don't Unmask LockBit's LockBitSupp).

That statement "is a very interesting way to say: 'LockBitSupp is a Russian security apparatus implant since 2021,'" said Yelisey Bohuslavskiy, chief research officer, RedSense.*

Whoever is behind LockBitSupp, "LockBit has been seriously damaged by this takedown and his air of invincibility has been permanently pierced. Every move he has taken since the takedown is one of someone posturing, not of someone actually in control of the situation," said Allan Liska, principal intelligence analyst, Recorded Future.

The reestablished leak site includes victim entries apparently made just before Operation Cronos executed the takedown, including one for Fulton County, Georgia. LockBit previously claimed responsibility for a January attack that had disrupted the county court and tax systems. County District Attorney Fani Willis is pursuing a case against former President Donald Trump and 18 codefendants for allegedly attempting to stop the transition of presidential power in 2020.

The LockBit message also claims that the FBI may have used a PHP zero-day and captured only 1,000 of the 20,000 ransomware decryptors on the LockBit server - and that the takedown was an effort to prevent the operation from leaking documents stolen from Fulton County.

"The FBI obtained a database, web panel sources, locker stubs that are not source as they claim and a small portion of unprotected decryptors," the message states. It also asserts that the names on a list of nearly 200 affiliates "have nothing to do with their real nicknames on forums and even nicknames in messengers."

The ransomware operation also said it would make future takedowns harder by decentralizing the hosting of its administrative panel.

LockBitSupp is known to exaggerate and has drawn criticism - even in criminal circles - for erratic behavior.

"This dude is all about deflection," said ransomware tracker Jon DiMaggio, chief security strategist at Analyst1. "He likes to say stupid things."

LockBit's assertion that the FBI apparently used a PHP flaw to gain control of its infrastructure looks like a credible statement, but the other assertions should be taken "with a grain of salt," DiMaggio told ISMG.

Operation Cronos remains a success despite LockBit's attempt at a comeback, DiMaggio said. Doubt and fear in the criminal underground about LockBit's reliability and possible lingering exposure to law enforcement will stymie a quick return to form, he said, adding that affiliates have plenty of other operations to choose from.

The FBI "didn't just take him down, they humiliated him," DiMaggio said, referring to LockBitSupp. "This was such an impactful takedown that it's going to permanently affect his reputation, and it embarrasses him."

**Updated Feb. 26, 2024, 09:01 UTC: This story has been updated to include additional comments.*