

Exclusive: After LockBit's takedown, its purported leader vows to hack on

By Dina Temple-Raston

Published: 2024-03-15 · Archived: 2026-04-05 23:13:37 UTC

This week, the Click Here podcast landed a rare interview with the purported leader of the LockBit ransomware group — he goes by the name LockBitSupp. He's under pressure because last month [an international police operation](#) infiltrated the group and seized not just their platform, but their hacking tools, cryptocurrency accounts and source code ending a four year ransomware rampage.

“As of today, LockBit is effectively redundant,” Graeme Biggar, the director general of the UK's National Crime Agency, told reporters when he announced the operation on February 19.

Officials had “hacked the hackers,” he said, adding that the fiercest ransomware gang was now “fundamentally disrupted.”

LockBit has been linked to thousands of attacks in recent years, including ones on hospital systems and critical infrastructure. In 2022, the group [attacked](#) Canada's largest pediatric health center shortly before Christmas, causing diagnostic and treatment delays. A September attack against two New York hospitals [forced](#) them to divert ambulances and reschedule most appointments.

So far, several people alleged to be linked to the LockBit gang have been [arrested](#) in Ukraine and Poland with more arrests expected. LockBitSupp, who law enforcement officials and cybersecurity experts believe is Russian, may be shielded from arrest if he indeed resides there. There are conflicting reports about whether he does.

The conversation, conducted over an encrypted messaging app and translated from Russian, has been edited for clarity and length. An audio version of the story with more highlights can be found on [Click Here's](#) Friday feature: Mic Drop.



ILLUSTRATION BY MEGAN J. GOFF

CLICK HERE: How did you find out about the takeover of the LockBit website and infrastructure?

LOCKBITSUPP: I realized this when the site stopped working, and I couldn't log into the server. I released a [detailed explanation of what happened](#).

CH: What was the first thought when it dawned on you that law enforcement was in your systems?

LS: The first thought that came to my mind was that my worst fears had come true. I knew that sooner or later the FBI would hack me and now they had. Initially, I felt fear and panic, but once I figured out how they did it, I started to calm down and began to work on restoring infrastructure.

CH: Is it true that law enforcement had access to your tools, dashboards and even future versions of the LockBit ransomware?

LS: That's true, but it doesn't affect business in any way. I take this as additional advertising and an opportunity to show everyone the strength of my character. I cannot be intimidated. What doesn't kill you makes you stronger.

CH: Were you surprised by the way law enforcement got into your systems? Did you find it more sophisticated than what they've done in the past?

LS: I was very surprised. Over the years my vigilance has relaxed. I got lazy. Now I ask that the FBI hack me more often [so that can't happen again].

CH: Law enforcement took over the LockBit platform, seized your hacking tools, froze accounts ... it is a little bit like what you do when you launch a ransomware attack. Did you feel like one of your victims?

LS: I felt like I was being hunted, like they were trying to destroy me. This is different from what we do because they were not giving me a chance to recover. Our business is very different from this. We do post-payment penetration testing, and we return the systems to their original state after paying the ransom. They were trying to

inflict maximum reputational damage to make me stop working. But [it has had the opposite effect] the FBI just motivated me to work harder. They can't stop me.

CH: You say you do penetration testing after payment to return systems to their original state, but some data you were supposed to destroy after payment was apparently found on your platform. Tell us about that.

LS: This is a bluff and not true, the FBI is trying to tarnish my reputation because they cannot catch me, they hope that if my reputation is destroyed I will stop working. If the FBI could provide at least one piece of evidence, it would be good. [Click Here reached out to the FBI for a response and did not receive one by press time].

CH: How are your partners, the people you work with, responding? Do you think you need to rebuild their trust in you?

LS: Partners, proven over the years, have joined me and continue to work. I don't need to restore their trust because there is no reason not to trust me.

CH: You've said that the raid on LockBit happened because you got lazy. Did you apologize to your affiliates for that?

LS: The best apology to our partners is to continue working and improve security. If the FBI couldn't scare me, my partners will respect me for standing up to them. Have you ever seen an affiliate program continue to work after the FBI hacked?

CH: So everyone has said they still want to work with you?

LS: Some partners got scared, probably those who laundered cryptocurrency poorly. Most partners continue to work though.

CH: Is there any other ransomware group that worries you? Do you see them trying to take advantage of and undermine your position as a leading ransomware group?

LS: Yes, I see that my opponents are trying to take advantage of the situation, but they will not succeed because I am too strong for my opponents. Previously, the only worthy competitor as I saw it was AlphV/BlackCat. But now [they are gone](#), and so now I don't see a single worthy competitor.

CH: How do you think this police action will affect business?

LS: In the short term, profits will decrease. In the long term, I will prove that not even the FBI can stop me. The stronger I stand on my feet, the more my partners will know this is true and trust me. No one ever stood on their feet after the FBI attack.

CH: Not long after the takedown you put up a barebones LockBit leak site... there were [five companies](#) on it. But didn't you launch attacks against them before the platform was seized by police? These are old victims, not new ones.

LS: I am publishing the remaining information to show that the FBI was not able to completely destroy my infrastructure, so that in the future, companies that are attacked by us will know that it is better to pay than to be published on our sites forever. Look, the FBI is not omnipotent; they just found a weak spot and struck. The battle was lost, but the war hasn't been. I will continue to work as long as my heart beats.

CH: So a year from now, five years from now... where is LockBit?

LS: I plan to continue working until my death. I don't have a goal for a year or for five years. My only goal in life is to attack one million companies around the world and go down in human history as the most destructive affiliate program. Once I reach one million businesses on my blog, I will retire forever.

CH: One other thing, why do you use cat emojis in your LockBitSupp messages?

LS: All people love cats.

CH: Maybe. I'm just wondering when law enforcement put a cat emoji on a public message to you, what did you think? Did it make you mad?

LS: It's cute. The FBI can't make me angry, they only teach me and make me stronger. I love the FBI — without the FBI my life wouldn't be as fun, and they're just doing their job. So, how can they make me angry?

 Recorded Future®

Know what matters.

Act first.

Get started





[Dina Temple-Raston](#)

is the Host and Managing Editor of the Click Here podcast as well as a senior correspondent at Recorded Future News. She previously served on NPR’s Investigations team focusing on breaking news stories and national security, technology, and social justice and hosted and created the award-winning Audible Podcast “What Were You Thinking.”



[Sean Powers](#)

is a Senior Supervising Producer for the Click Here podcast. He came to the Recorded Future News from the Scripps Washington Bureau, where he was the lead producer of "Verified," an investigative podcast. Previously, he was in charge of podcasting at Georgia Public Broadcasting in Atlanta, where he helped launch and produced about a dozen shows.

Source: <https://therecord.media/after-lockbit-takedown-its-purported-leader-vows-to-hack-on>