What the LockBit 4.0 Leak Reveals About RaaS Groups

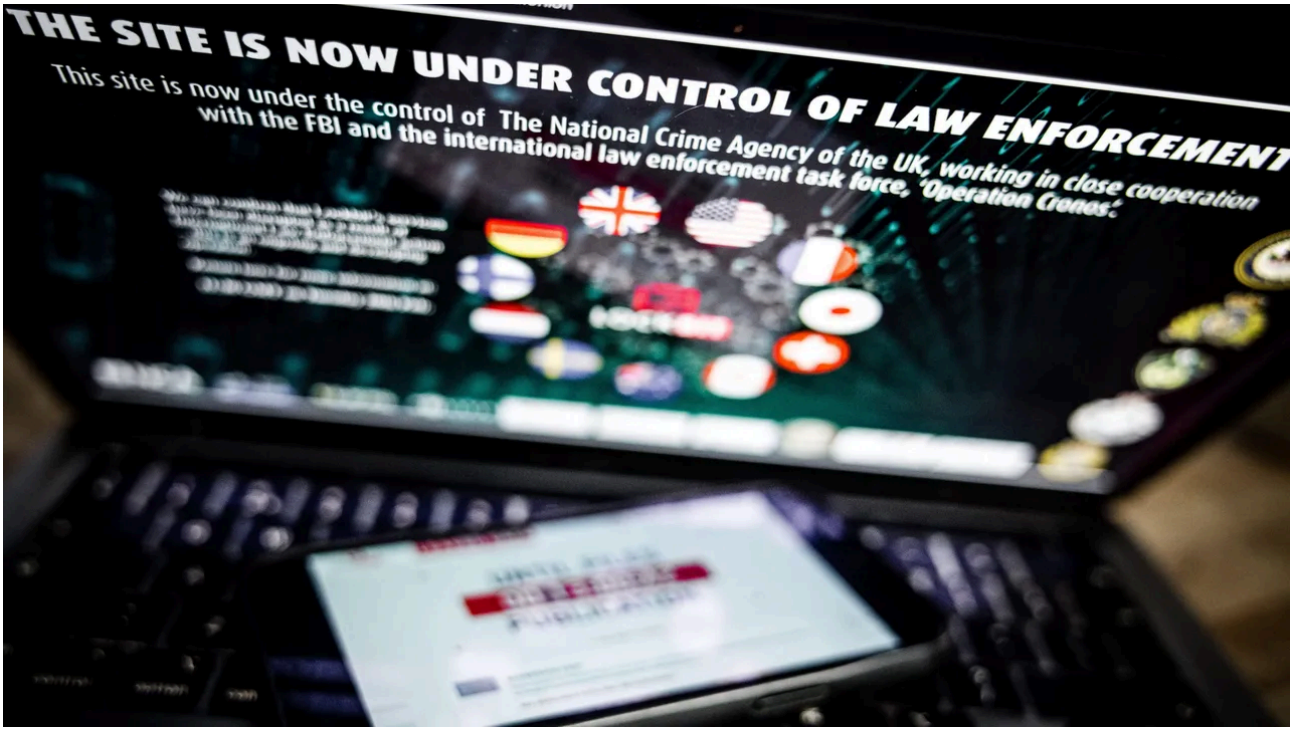
By Michele Campobasso

Published: 2025-08-13 · Archived: 2026-04-05 18:05:23 UTC

Michele Campobasso,Senior Security Researcher, Vedere Labs, Forescout Technologies

August 13, 2025

4 Min Read



Source: ANP via Alamy Stock Photo

COMMENTARY

For years, LockBit has been viewed as the gold standard in ransomware — a sleek, professional, and ruthlessly efficient criminal syndicate with the polish of a Silicon Valley startup.

But the recent leak of LockBit's 4.0 affiliate panel shattered that illusion, exposing a chaotic, backbiting, and wildly inconsistent operation behind the scenes. If you've been picturing ransomware groups as disciplined digital criminal organizations, this leak made one thing clear: The real threat is far more fragmented and unpredictable because of it.

The leak, which occurred in May and included thousands of chats between LockBit affiliates and their victims, uncovered that the ransomware ecosystem remains opportunistic and disorganized. Affiliates ignored victims,

delivered broken decryption tools, dodged payments to their own platform, and even attacked prohibited targets, including Russian state entities.

Related:Automotive Cybersecurity Threats Grow in Era of Connected, Autonomous Vehicles

The Leak That Spilled the Truth: Inside LockBit 4.0

On May 7, LockBit's 4.0 affiliate panel was compromised and replaced with a link to a data dump containing more than 4,000 chat messages, thousands of ransomware builds, internal user tags, and cryptowallet data. After Conti leaks in February 2022 shedding light on the ransomware gang operations, what followed was an unprecedented behind-the-scenes look at how ransomware-as-a-service (RaaS) operations function behind closed doors.

The leak revealed that much of the affiliate ransomware ecosystem remains opportunistic and disorganized. Affiliates operate with little oversight, and their professionalism varies widely. Some negotiate payments with care and follow through on decryption, while others vanish the moment a ransom is paid. In one exchange, an affiliate blamed corrupted files on antivirus software and told a victim to wait for the correct decryption tool because "the boss is very busy." This continued until the affiliate eventually stopped replying.

Even the supposed rules of the LockBit platform were ignored by affiliates. LockBit rules state that affiliates should not target Russian organizations, but in February, two Russian government entities were hit. To contain the fallout, LockBit administrators took over and offered free decryptors to save face. The affiliate responsible for the attack was suspended and tagged "ru target."

Even the economics of the operation were unclear. Of the 159 Bitcoin wallets tied to extortion attempts, only 19 received funds. Some affiliates may have negotiated outside LockBit's platform to avoid giving into the platform's 20% cut. One affiliate extorted more than $2 million from a Swiss cloud provider. Most, however, walked away with nothing.

Related:Critical Flaw in Langflow AI Platform Under Attack

Why This Chaos Makes Ransomware Harder to Stop

It's tempting to think that disorganization makes these groups less dangerous. In reality, the opposite is true. The chaos is what makes them harder to defend against.

Without consistent structure or standards, it's harder to come up with a predictable playbook that allows defenders to prepare at their best. One affiliate may offer support and honor payment agreements, while another might disappear after collecting ransom. That unpredictability complicates incident response planning and erodes what little perceived value there is in paying a ransom.

There is also no guarantee that stolen data will be destroyed or kept secret. Data from breaches can surface months later, exposing an organization's private negotiations or security failings even after they believed the crisis has been contained.

Surprisingly, this case shows that the affiliate model incentivizes recklessness. Although brand reputation is key for a successful RaaS enterprise, apart from glaring examples of rules infringement, we found no affiliate repercussions on terms of service breaching, which in turn may make actors confident in taking bigger risks, demanding more money and moving on with minimal or no consequences. We speculate that this may hold true for other RaaS ventures.

Related:Patch Now: Oracle's Fusion Middleware Has Critical RCE Flaw

The only rational defense isn't negotiation; it's preparation. That means segmenting networks, monitoring for lateral movement, implementing multifactor authentication and patching known vulnerabilities. It also means rehearsing incident response with the assumption that help will not come even after a ransom is paid.

The Future of RaaS: More Mayhem for the Unprepared

Undoubtedly, the LockBit leak will not be the last. As pressure from law enforcement agencies continues to increase and financial incentives wane, it's likely organizations will see more infighting within ransomware groups (as suspected by the very same LockBit admins), giving security researchers invaluable real-world data.

This infighting will likely lead to fewer brand-name groups collecting heterogeneous actors operating in short bursts. Attribution will get harder, threat intelligence will get murkier, and the RaaS landscape will resemble less of a corporate hierarchy and more of a crowded and unstable atmosphere.

Too often, defenses become oriented around names — Conti, LockBit, BlackCat — as if fighting a brand means understanding the underlying threat. But these names are disposable identities, built for plausible deniability, technological convenience, and short-term gain. Clinging to them offers a false sense of clarity.

The LockBit 4.0 leak serves as a wake-up call: The ransomware threat isn't (anymore?) too organized, centralized, or consistent. It's fragmented, opportunistic, and growing more chaotic by the day. Being prepared is the cornerstone of a successful defense: those who aren't are going to face uncertainty caused by the lack of attackers' accountability.

But there's hope: Less accountability means less successful RaaS brands, which will result in a reduced set of technical TTPs to inform network defenses; researchers studying negotiation tactics can provide signals to assess the reliability of a threat actor, regardless of their brand, to minimize losses; and finally, the growing awareness of this threat, combined with a more disorganized ecosystem, could make their business unprofitable. Until their next move.

About the Author

Senior Security Researcher, Vedere Labs, Forescout Technologies

Michele Campobasso is a senior security researcher at Vedere Labs' Forescout Technologies. He holds a PhD in Cybercrime Ecosystems obtained at Eindhoven University of Technology. In his work, he integrates concepts from economics and criminology to characterize cybercriminal marketplaces fostering innovation and enabling attacks at scale to identify those posing more damaging real-world threats. Part of his research has been instrumental in the law enforcement operation "Cookie Monster" against Genesis Market, led by EUROPOL, the Dutch National Police, and the FBI. He contributed to a white paper on access-as-a-service, presented to the US Department of Commerce, which led to the NSO Group to be included as a company threatening US national security. His research has received large media and industry attention (Intel471, Troy Hunt, Recorded Future, national media), and has been invited in industrial and scientific symposia as a speaker.
