The table below contains affiliate chat logs sourced from the original dump from the LockBit ransomware group data leak in May 2025, with sensitive information redacted. They pertain to LockBit's attack path, business behavior, group features, and ransomware features.

Read the related VicOne blog entry to learn more →

Category	Client	Content
Attack path	246	[2025-04-16 19:16:06] LockBit: 1. http://lockbit[REDACTED] 2-3. We guarantee that we will not blog you or attack you again. 4. We got into your network through a vulnerability in your FortiVPN.
	266	[2025-04-24 14:55:59] LockBit: we got to you through phishing, captured the domain, and then the admin host Vincent [2025-04-24 14:58:02] LockBit: no, you don't have insiders, random phishing through the manager
	167	[2025-02-18 11:25:35] LockBit: al[REDACTED] B[REDACTED]123456 [2025-02-18 11:25:45] LockBit: nice pwd
	138	[2025-02-16 10:32:37] LockBit: backups do not show in the domain [2025-02-16 10:33:00] LockBit: and nas [2025-02-16 10:33:34] LockBit: domain is not a secure infostructure
	154	[2025-02-28 11:42:28] LockBit: we got into the network through a manager with user priv, and dump ntlm local admin access on all the hosts in the domain.
	154	[2025-03-06 06:06:27] LockBit: Hello, you had anydesk installed on many hosts, we just used it to get back

	154	[2025-02-28 11:19:18] LockBit: I followed the work [REDACTED], and waited for him to log into Google Backup [2025-02-28 11:19:41] LockBit: about a month
	138	[2025-02-16 10:28:22] LockBit: host admin needs to be removed from the domain [2025-02-16 10:28:38] LockBit: and close the ports at the admin
Business behavior	138	[2025-02-07 10:59:42] VICTIM: If I provide the IP of a mainland Chinese company, can you attack it? [2025-02-07 11:05:47] LockBit: what china company ?
	113	[2025-03-21 21:30:17] LockBit: I sold your data, wait for a lawsuit
	254	[2025-04-15 19:25:39] LockBit: Are you so sure? Even if your databases fall into the hands of competitors?
	209	[2025-03-27 14:39:05] LockBit: Seems we better message your customers whom data we took. I think they will able to pay.
	245	[2025-04-11 17:22:34] LockBit: Then expect lawsuits from the victims.
	154	[2025-02-12 09:00:09] LockBit: they will also end up with your competitors, and you will be on the verge of closing down
Group features	168	[2025-02-19 09:59:42] LockBit: I am boss Lockbit [2025-02-19 09:59:50] LockBit: only me can decrypt your files

	138	[2025-02-16 09:15:58] VICTIM: Give me five minutes to get approval from my boss. Please provide the address in the meantime. [2025-02-16 09:16:18] LockBit: bc1qvltxkhn7njvd9gq[REDACTED] [2025-02-16 09:17:02] VICTIM: 1BWbqn6xdFat3z[REDACTED] No this one ? [2025-02-16 09:17:29] LockBit: it's affilate wallet, I am boss [2025-02-16 09:17:38] LockBit: you can sent 80% to affilate 20% to me [2025-02-16 09:19:36] VICTIM: You are the boss, so I can give it directly to you in exchange for the password, right? [2025-02-16 09:20:02] LockBit: yes
	266	[2025-04-24 15:24:01] VICTIM: I saw from the ransom letter that I could pay $777 to join you? May I ask what benefits there are after joining? What needs to be done? Could you give me some information? [2025-04-24 15:24:38] LockBit: oh no, that's not for me) [2025-04-24 15:25:31] LockBit: this is for the boss
	234	[2025-04-24 09:17:18] LockBit: There are many people in the affiliate program, and we are not sure. Some novice players may execute multiple encryption strategies at the same time. They always execute automatic programs in batches. We are the attackers who catch whales. You can fully believe that our programs are all executed by professional hackers.
	261	[2025-04-21 14:15:58] LockBit: At the moment, our team of lawyers is studying your financial documentation, wait please.

	241	[2025-04-27 20:39:47] LockBit: Your own policy (section “Cyber Extortion — We will pay on your behalf cyber extortion expenses”) guarantees funds for ransom. Your choice: one clean payment or months of lawsuits, fines, and shareholder rage. Forward this to your insurer and settle, or watch your reputation disintegrate in real time. Our OSINT team collecting contacts of regulators, journalists, and competitors for the data drop in case you refuse to pay.
Ransomware features	158	[2025-02-13 07:16:50] LockBit: There were two modes, encryption by spots and then full encryption.
	36 138 158 167 182 212	LockBit: Procedure for decrypting ESXi: • log in to vCenter • enable ssh access to ESXi • upload decryptor to ESXi via WinSCP or FileZilla; navigate to /tmp folder • login to ssh with root privileges • set permissions to run the decryptor with the command - chmod 777 decrypt • launch decryptor ./decrypt • follow the first method of decrypting by viewing the log file: tail -f /tmp/decrypt.llg, wait for the message at the end of the log - Your system is decrypted • the second way is to check the presence on the disk file decrypt.pid command ls, which protects the decryptor from the restart • the third way - ps | grep decrypt, as soon as decrypt.pid will be removed from the disk, or decrypt will disappear from the running processes, decrypt is complete • check the decrypt.llg log file and see the message at the end that the system was successfully decrypted "Your system is decrypted" • turn on virtual machines in ESXi