Inside LockBit: The Inner Workings of a Ransomware Giant

Archived: 2026-04-05 16:18:59 UTC

Blog

Executive Summary

In May 2025, reports emerged indicating that the LockBit ransomware group had themselves suffered a data breach. This incident revealed a trove of sensitive information, including ransomware build records, chat transcripts between affiliates and victims, and configuration data. The leak offers an unprecedented glimpse into the daily operations of one of the most notorious ransomware-as-a-service (RaaS) ecosystems to date. The exposed data was made available via the Tor network hidden service, appearing on what seemed to be a LockBit 'onion URL'.

The leaked files, although created in 2024, only came to light this month. They provide valuable insights into LockBit's operations, including its communication strategies with victims as well as its affiliate programme.

This blog presents our key findings, including:

- Patterns in payload creation and projected ransom demands by user ID
- Insights into the structure and tactics of ransom negotiations
- Operational insights into LockBit's internal processes

Who are LockBit?

LockBit are a notable and highly active ransomware group that employs the Ransomware-as-a-Service (RaaS) model, enabling affiliates to utilise their services. The group develops ransomware capable of encrypting and decrypting victims' data. Affiliates, typically individual cybercriminals or small collectives, leverage this malware to target organisations. In exchange for their services, LockBit earns a percentage of the ransom when attacks are successful, or they may charge an upfront cost, or even a subscription fee.

Source of the Leak

The source of the leak originated from an onion URL which is tied to LockBit, indicating the attacker had breached their infrastructure and then hosted the leaked information on their own Tor Service website. This was quickly taken down, and is no longer available through the Tor network.

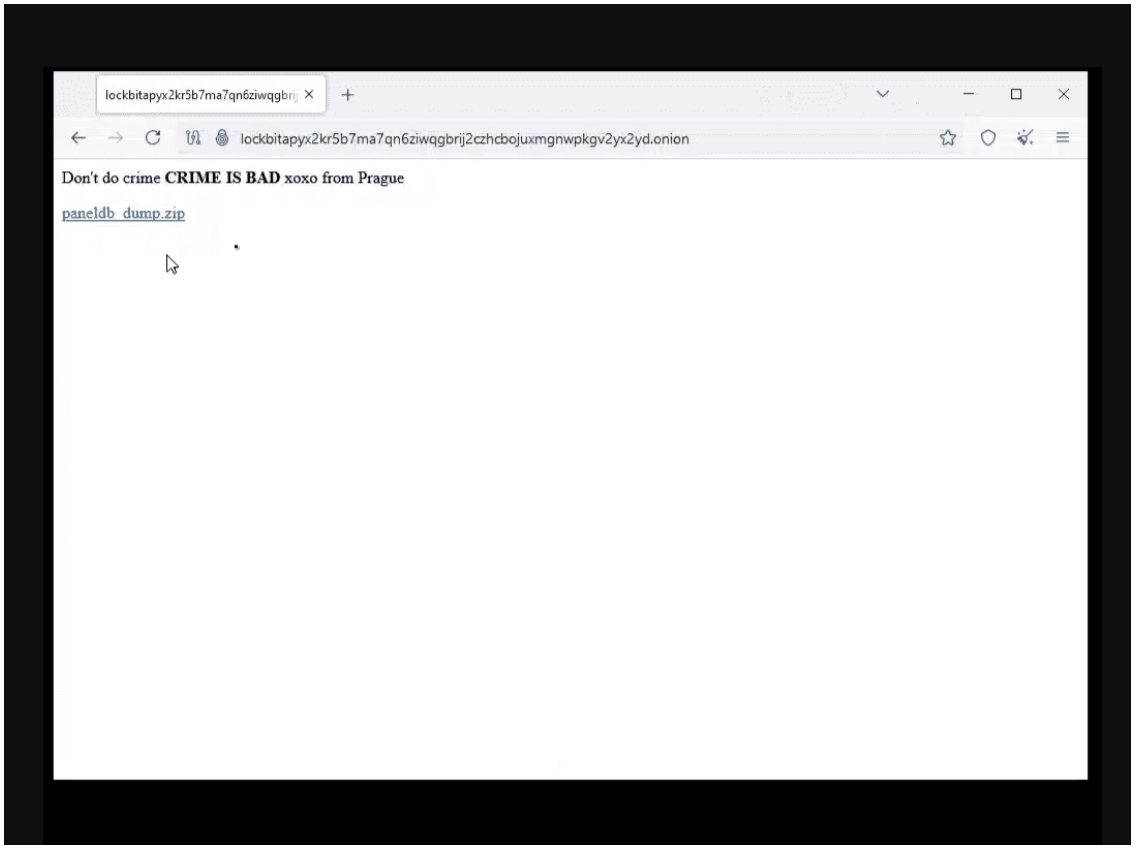


Figure 1 – Lockbit onion URL

What was Leaked?

The leaked database offers a rare, comprehensive look inside LockBit's ransomware-as-a-service (RaaS) operations. Key components include:

BTC Addresses – 59,975 Bitcoin Wallets

- A massive table mapping unique Bitcoin addresses to:
  - advid (affiliate ID)
  - target_id (likely victim or campaign ID)
- Enables direct correlation between affiliates and ransom payments.
- Ideal for blockchain analysis and tracking criminal infrastruct

Builds – Payload Creation Records

Contains records of **individual ransomware builds** generated by affiliates.

Fields include:

Affiliate identifiers (implicit in linkage)

Build configurations – Ransomware Customisation

- Stores configuration flags per build:
    - Which **files to encrypt**
    - Which **ESXi servers to avoid** (for stealth or targeting)
    - Optional persistence, file types, kill-switches
- Highlights LockBit's **modular payload architecture**.

Chats – 4,442 Negotiation Messages

- A trove of ransom negotiation transcripts between victims and affiliates.
- Spanning from December 19th, 2024 to April 29th
- Reveals behavioural patterns, negotiation strategies, and sometimes emotional manipulation by operators.

Inside LockBit's Affiliate Infrastructure

In our analysis, we uncovered the Affiliate infrastructure utilised by LockBit within the data leak. This "builds" table serves as a **log of every ransomware payload generated** through the LockBit affiliate panel.

Figure 2 – Payload flowchart

Each example generated by the builder is saved in JSON format, allowing affiliates to customise their entries directly within the builder panel. Once the modifications are confirmed, as described in the previous steps, the information is securely stored in the backend to create the payload. This payload comprises essential details, including the ID, target, and revenue, which may either be declared or represent the intended ransom demand – it is not a recorded payment.

```
{
  "buildModel": {
    "id": "1",
    "parent_id": 0,
    "userid": 3,
    "comment": "Hello",
    "company_website": "example.com",
    "crypted_website": "[encrypted string]",
    "revenue": "10kk",
    "delete_decryptor": true,
    "type": 25,
    "created_at": "2024-12-18 20:05:23"
  },
  "comment": "Hello",
  "company_website": "example.com",
  "revenue": "10kk",
  "running_one": "1",
  "quiet_mode": "0",
  "delete_decryptor": false,
  "not_randomize_keys": "0"
}
```


Figure 3 – JSON data format

Operational Features in Build Configs

The fields provided offer detailed configuration options for LockBits affiliates, enabling precise control over the execution of ransomware on target systems. Our analysis indicates that this activity is documented in a table titled “build_configurations”. The system reveals its design for modularity and operational flexibility, with features ranging from stealth options like “quiet_mode” to post-infection cleanup processes such as “delete_decrypter”. This structure suggests a strong focus on affiliate-driven targeting.

Field	Example Value	Purpose / Behaviour
comment	“company_target“	Internal label used by the affiliate typically a victim name or campaign reference.
company_website	example.com	Victim’s domain, sometimes real, but often test.

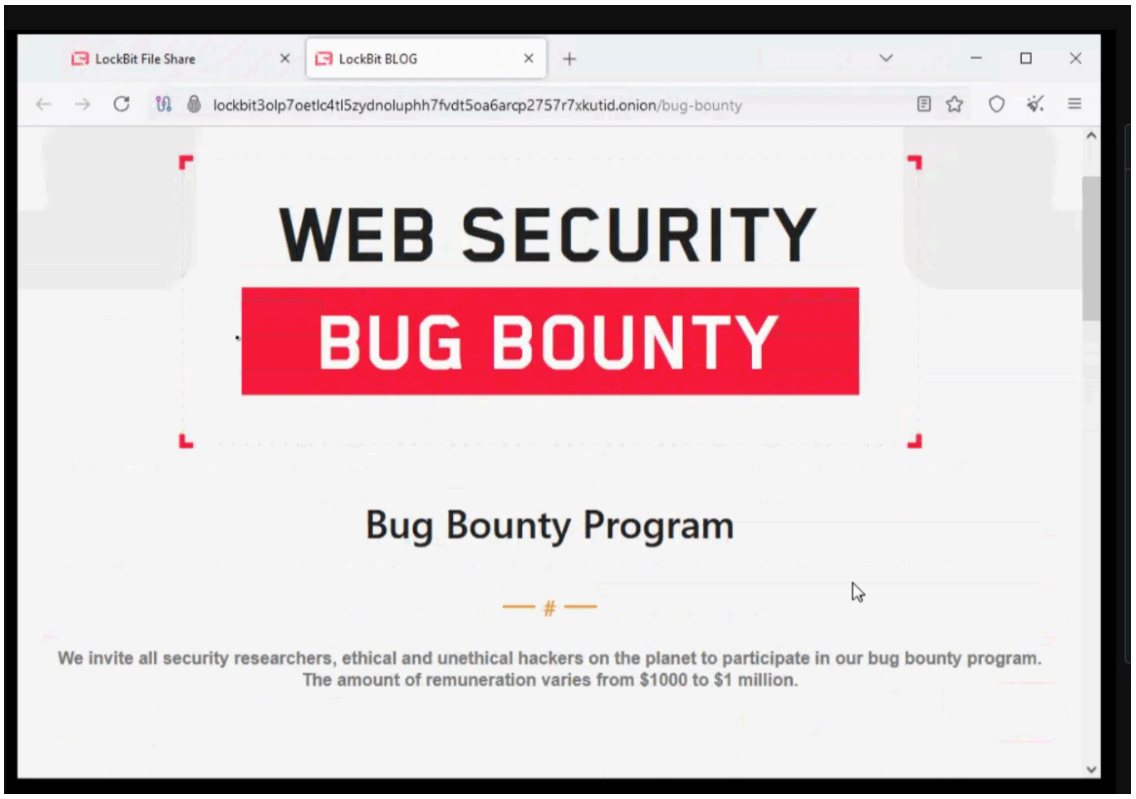
revenue	“15kk“	Declared ransom demand – not a validated or confirmed payment.
userid	25	Internal affiliate ID which is used across builds.
created_at	“2024-12-18 20:05:23”	Timestamp of payload generation.
master_pubkey	(long base64 string)	Public key for file encryption, unique to each build.
master_privkey	(long base64 string)	Private key for decryptor, likely only released after payment.
crypted_website	(encrypted blob)	Possibly contains C2, leak site, or internal config data.
delete_decrypter	true / false	If true, removes decryptor after infection.
quiet_mode	“0” / “1”	Likely suppresses execution output or error logging.
not_randomize_keys	“0” / “1”	Controls whether encryption keys are randomized per file, or static per payload.
running_one	“1” / “0”	Possibly indicates “run once” mode or single execution instance.
type	25, 18 etc.	Variant or profile type – affects payload structure and/or encryption logic.
key_id	0 / Integer	Could reference internal key management system.
stealerid	NULL / Integer	May link to credential stealer module inclusion.
max_file_size	NULL / e.g. 52428800	Limits encryption to files below a certain size e.g. skip files over 50MB in size.

Use of Tor for Operational Security

LockBit’s use of Tor is a deliberate OPSEC (operational security) decision**.** By leveraging the Tor network, LockBit operators benefit from strong anonymity and routing obfuscation, allowing them to hide their infrastructure and communications from law enforcement. Unlike websites on the traditional World Wide Web, which can be quickly seized or taken down with proper legal proceedings, Tor-based (.onion) sites are far more

resilient. This enables LockBit to host extortion portals, leak sites, and communication hubs that persist even under global scrutiny, making Tor a crucial part of their cybercriminal infrastructure.

Some of the interesting domains observed from LockBit show the side of the group where they operate like a functional business. Looking through some of the onion sites discovered from the dump, we found a page where LockBit offers a bug bounty reward to security researchers or anyone who can discover flaws in their infrastructure. Refer to the Indicators of Compromise for a comprehensive list of onion domains.



Declared Ransom Demands by Affiliates

Affiliates of LockBit manually input their estimated ransom demands during the payload generation process. These entries provide a glimpse into each affiliate's targeting ambitions, pricing strategies, and even their internal practices. Although this data has not been financially verified, it offers valuable insights into the economic mindset of ransomware operators operating within LockBit's affiliate model.

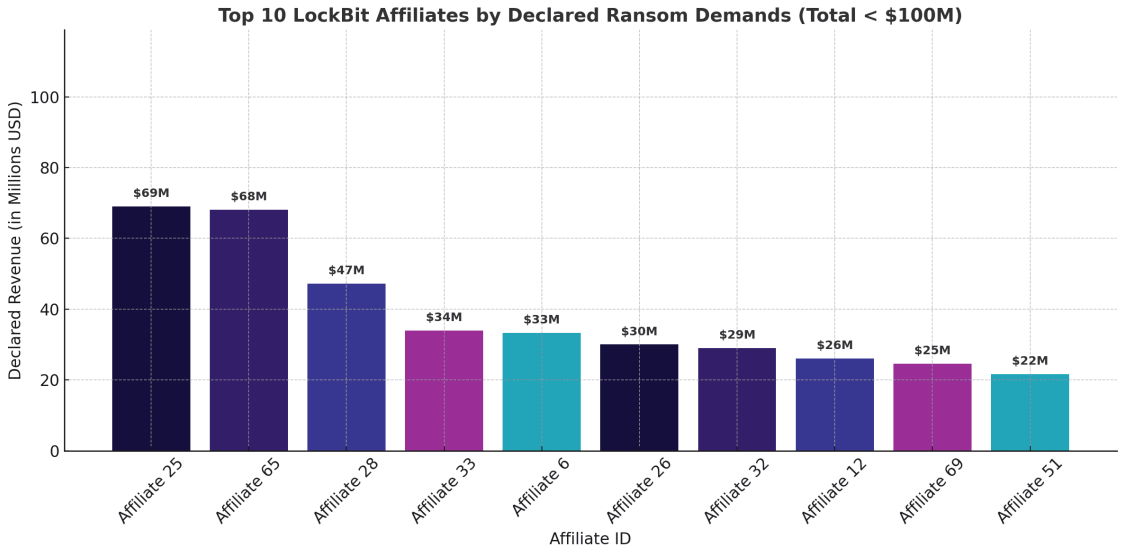


Figure 5 – Top 10 Lockbit Affiliates by Declared Ransow Demands

We have filtered the original data because during our analysis we discovered some exaggerated ransom demands under “revenue“ similar to the following:

“999kk” – $99.9 million

“303kkk” – $303 million

“100kkk” – $100 million

These felt like more of a placeholder or potential test entries that didn’t seem credible. Even if these are real entries there is **no evidence in the leaked panel** that these demands were ever issued to real victims, let alone paid.

Top Affiliates by Likely Realistic Demands

NOTE: These are still **affiliate-entered estimates**, not confirmed ransom notes or payments.

Affiliate ID	Total Revenue	Average Ransom	Number of Valid Builds
14	$168.8M	$42.2M	4 builds
2	$161.9M	$4.9M	33 builds
70	$153.7M	$1.45M	106 builds
16	$105M	$35M	3 builds
18	$103.2M	$8.6M	12 builds

Financial Scope of LockBit – based on this data

Ransom Payment Insights

Metric	Count
Total victims (clients)	246
Victims who paid ransom	7
Victims with decryption (decrypt_done)	0

- **~2.8% of victims** show a “paid_commission greater than 0” likely indicating successful ransom payment.
- None show “decrypt_done greater than 0”, which could mean:
    - Decryption flag wasn’t updated in the dump.
    - Or actual decryption didn’t occur via system logic.

In conclusion, **none of the victims** in the dataset were recorded as having received a decryption tool. However, this information may not be entirely accurate, as LockBit claims to offer a decryption tool which they provide.

What we can confirm

- The field “paid_commission” is an integer.
- It defaults to “0”, per schema:

```
`paid_commission` int(11) NOT NULL DEFAULT 0
```

- In **7 out of 246** rows, this value was changed to be **greater than 0**.

NOTE: This is still **not proof of payment** from this data alone!

What we cannot confirm

We **cannot** claim that “paid_commission > 0“ means the **victim paid** the ransom. Here’s why:

- This value only confirms LockBit marked a commission as paid to an affiliate.
- However the victim-side payment may have:
    - Been paid without being logged in this table.
    - Been paid but never resulted in affiliate compensation.
    - Been simulated for testing, if this dataset is a development/testing snapshot.

Negotiating With Affiliates: The Human Side

Human Tones in Hostile Chats

During our analysis of the specific “chat” conversations that were listed in the dump, we observed multiple different types of tones from affiliates. You can tell there were significant differences in conversations where some

affiliates were aggressive and would not take any considerations into account when demanding to be paid in BTC or XMR.

- Shifts from formal messaging to being aggressive when a victim attempts to get a discount or makes things difficult.
- Straight to the point and no room for discussion.

```
Victim: "We are a small firm; we cannot pay that much."
```

```
LockBit: "Your size is irrelevant. Your data is valuable."
```

Here are more samples from the conversations:

- “I Don’t Care” Aggression
- Deadline Ultimatum

Timestamp: 2024-12-23 17:20:25

```
I don't care whether you pay me or not, there will be no more talk about discounts
```

```
If you don't make a decision, the price will be 2x tomorrow.
```

- Plea for Lower Price – Timestamp: 2024-12-20 10:55:51

```
Yes, I checked the number of test files. Please lower the price a little.
```

One of the more interesting messages that we discovered was what looked to be a predefined footnote message to the victims, which contains some interesting context that we have only observed from one message to a victim that was discovered from our analysis. From threat to recruitment.

The footnote message indicates the specific version of LockBit in use: “ `(Version: LockBitBlack4.0-rc-001)` ”. See the full footnote message in “Appendix A”

Also within the same chat log, we can also observe the affiliate being questioned, raising concerns about the guarantee of decryption of data.

```
Affiliate:
```

```
 - You must pay us.
```

```
Affiliate:
```

```
- What is the guarantee that we won't scam you? We are the oldest extortion gang on the planet
```

```
- Treat this situation simply as a paid training session for your system administrators.
```

```
- Don't go to the police or the FBI. Don't tell anyone.
```

Part of that message included the following intriguing information within the complete footnote. The messaging acts as a way to introduce people to the world of penetration testing and to come join the programme.

```
Delivered Message (Extracted from LockBit Chat ID 433)
```

```
You have been attacked by LockBit 4.0 - the fastest, most stable and immortal ransomware since 2019.
```

```
- "Want a lamborghini, a ferrari and lots of ti**y girls? Sign up and start your pentester billionai
```

The message indicates the specific version of LockBit in use: “ `(Version: LockBitBlack4.0-rc-001)` ”. See the full footnote message in “Appendix A”

Tactics Used By Affiliates

Based on message patterns, we have observed different tactics used by affiliates to push and secure payment:

- **Standard tactics**:
  - Time threats (“24 hours left”)
  - Bitcoin-only payments
  - “Test file” to prove decryption
- **Psychological tactics**:
  - Guilt: “Your clients will suffer”
  - Shame: “You are irresponsible”
  - Urgency: “Tick-tock, the timer runs”

Operation Cronos

In 2024, multiple law enforcement agencies worked together to take down LockBit, and during a period of last year, the UK’s National Crime Agency infiltrated the group’s infrastructure and took control of its services, and posted a list of usernames and user IDs. However LockBit prevailed, and we are now in a situation where they continue to operate. We have compared the UK NCA data to the user IDs and usernames observed in this dump and found the following.

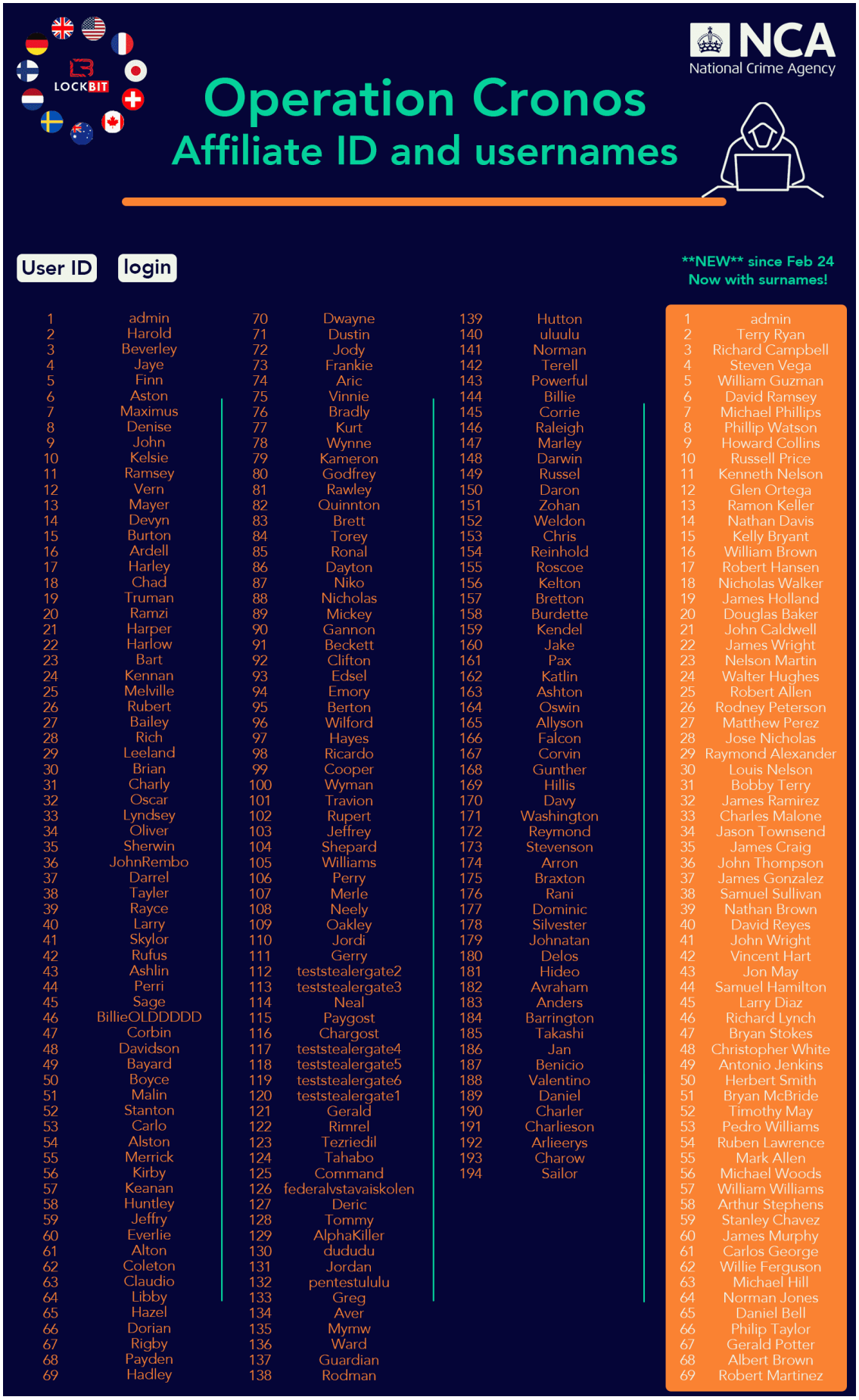
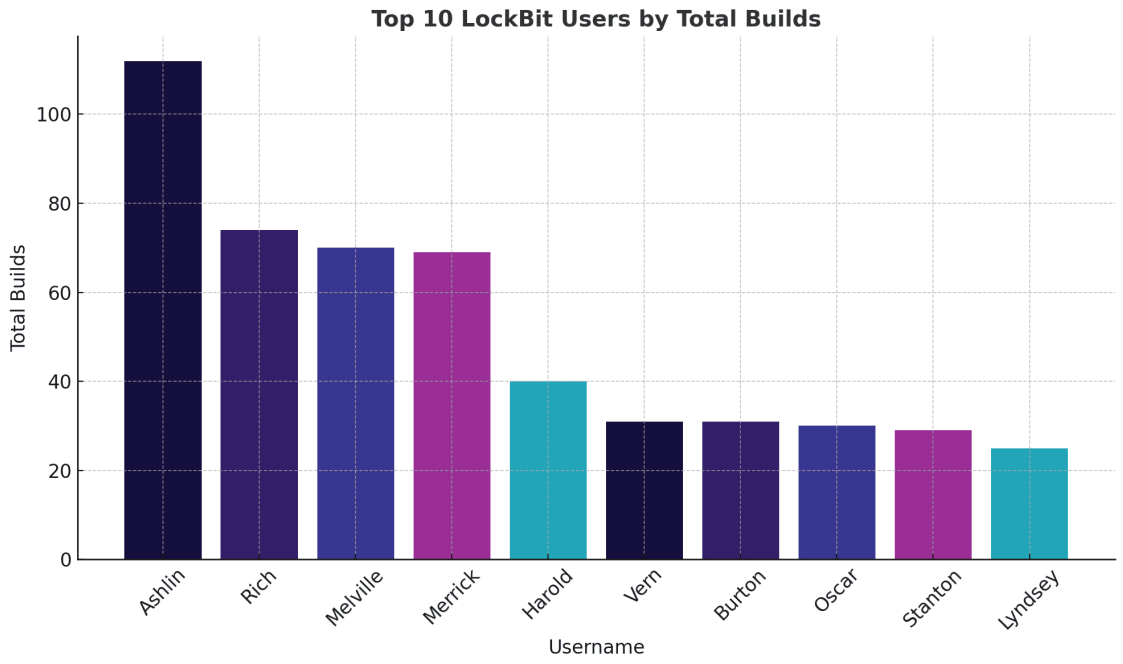

LOCKBIT
NCA
National Crime Agency
Operation Cronos
Affiliate ID and usernames
User ID
login
NEW since Feb 24
Now with surnames!
1 admin
2 Harold
3 Beverley
4 Jaye
5 Finn
6 Aston
7 Maximus
8 Denise
9 John
10 Kelsie
11 Ramsey
12 Vern
13 Mayer
14 Devyn
15 Burton
16 Ardell
17 Harley
18 Chad
19 Truman
20 Ramzi
21 Harper
22 Harlow
23 Bart
24 Kennan
25 Melville
26 Rubert
27 Bailey
28 Rich
29 Leeland
30 Brian
31 Charly
32 Oscar
33 Lyndsey
34 Oliver
35 Sherwin
36 JohnRembo
37 Darrel
38 Tayler
39 Rayce
40 Larry
41 Skylor
42 Rufus
43 Ashlin
44 Perri
45 Sage
46 BillieOLDDDDD
47 Corbin
48 Davidson
49 Bayard
50 Boyce
51 Malin
52 Stanton
53 Carlo
54 Alston
55 Merrick
56 Kirby
57 Keanan
58 Huntley
59 Jeffry
60 Everlie
61 Alton
62 Coleton
63 Claudio
64 Libby
65 Hazel
66 Dorian
67 Rigby
68 Payden
69 Hadley
70 Dwayne
71 Dustin
72 Jody
73 Frankie
74 Aric
75 Vinnie
76 Bradly
77 Kurt
78 Wynne
79 Kameron
80 Godfrey
81 Rawley
82 Quinnton
83 Brett
84 Torey
85 Ronal
86 Dayton
87 Niko
88 Nicholas
89 Mickey
90 Gannon
91 Beckett
92 Clifton
93 Edsel
94 Emory
95 Berton
96 Wilford
97 Hayes
98 Ricardo
99 Cooper
100 Wyman
101 Travion
102 Rupert
103 Jeffrey
104 Shepard
105 Williams
106 Perry
107 Merle
108 Neely
109 Oakley
110 Jordi
111 Gerry
112 teststealergate2
113 teststealergate3
114 Neal
115 Paygost
116 Chargost
117 teststealergate4
118 teststealergate5
119 teststealergate6
120 teststealergate1
121 Gerald
122 Rimrel
123 Tezriedil
124 Tahabo
125 Command
126 federalvstavaiskolen
127 Deric
128 Tommy
129 AlphaKiller
130 dududu
131 Jordan
132 pentestululu
133 Greg
134 Aver
135 Mymw
136 Ward
137 Guardian
138 Rodman
139 Hutton
140 uluulu
141 Norman
142 Terell
143 Powerful
144 Billie
145 Corrie
146 Raleigh
147 Marley
148 Darwin
149 Russel
150 Daron
151 Zohan
152 Weldon
153 Chris
154 Reinhold
155 Roscoe
156 Kelton
157 Bretton
158 Burdette
159 Kendel
160 Jake
161 Pax
162 Katlin
163 Ashton
164 Oswin
165 Allyson
166 Falcon
167 Corvin
168 Gunther
169 Hillis
170 Davy
171 Washington
172 Reymond
173 Stevenson
174 Arron
175 Braxton
176 Rani
177 Dominic
178 Silvester
179 Johnatan
180 Delos
181 Hideo
182 Avraham
183 Anders
184 Barrington
185 Takashi
186 Jan
187 Benicio
188 Valentino
189 Daniel
190 Charler
191 Charlieson
192 Arlieerys
193 Charow
194 Sailor
1 admin
2 Terry Ryan
3 Richard Campbell
4 Steven Vega
5 William Guzman
6 David Ramsey
7 Michael Phillips
8 Phillip Watson
9 Howard Collins
10 Russell Price
11 Kenneth Nelson
12 Glen Ortega
13 Ramon Keller
14 Nathan Davis
15 Kelly Bryant
16 William Brown
17 Robert Hansen
18 Nicholas Walker
19 James Holland
20 Douglas Baker
21 John Caldwell
22 James Wright
23 Nelson Martin
24 Walter Hughes
25 Robert Allen
26 Rodney Peterson
27 Matthew Perez
28 Jose Nicholas
29 Raymond Alexander
30 Louis Nelson
31 Bobby Terry
32 James Ramirez
33 Charles Malone
34 Jason Townsend
35 James Craig
36 John Thompson
37 James Gonzalez
38 Samuel Sullivan
39 Nathan Brown
40 David Reyes
41 John Wright
42 Vincent Hart
43 Jon May
44 Samuel Hamilton
45 Larry Diaz
46 Richard Lynch
47 Bryan Stokes
48 Christopher White
49 Antonio Jenkins
50 Herbert Smith
51 Bryan McBride
52 Timothy May
53 Pedro Williams
54 Ruben Lawrence
55 Mark Allen
56 Michael Woods
57 William Williams
58 Arthur Stephens
59 Stanley Chavez
60 James Murphy
61 Carlos George
62 Willie Ferguson
63 Michael Hill
64 Norman Jones
65 Daniel Bell
66 Philip Taylor
67 Gerald Potter
68 Albert Brown
69 Robert Martinez

Figure 6 – Operation Cronos

Comparing the usernames observed in the Cronos Operation, we have discovered multiple usernames within the leaked data that confirm the operation of the same actors. As you can see below, we have put together a visual representation of the top 10 LockBit users by total builds.



What we can take from this:

- **Ashlin** generated the most payloads by a wide margin.
- **Rich**, **Melville**, and **Merrick** followed as high-volume affiliates.

Overall, here is a comprehensive list of all linked usernames derived from the NCA list, and then matched against the leaked dataset to show these usernames match.

UserID	**Username**
1	admin
2	Harold
5	William Guzman
6	David Ramsey
9	Howard Collins
10	Russell Price
12	Vern
13	Mayer

14	Devyn
15	Burton
16	Ardell
17	Harley
18	Chad
19	Truman
21	Harper
24	Kennan
25	Melville
26	Bubet
27	Bailey
28	Rich
31	Charly
32	Oscar
33	Lyndsey
34	Oliver
35	Sherwin
36	JohnRembo
37	Darrel
40	Larry
42	Rufus
43	Ashlin
45	Sage
46	BillieOLDDDDD
48	Davidson
51	Malin
52	Stanton

53	Carlo
54	Alston
55	Merrick
57	Huntley
58	Jeffly
59	Everlie
63	Libby
64	Hazel
65	Dorian
66	Rigby
67	Payden
69	Robert Martinez

Conclusion

The LockBit leak has provided an exceptional insight into how one of the world's most successful and active ransomware groups operates. From chat logs and ransomware build records, to affiliate configurations and ransom demands, the data shows LockBit are both well organised and methodical. Affiliates play a major role in customising attacks, demanding payment, and negotiating with victims. While some payments appear to have been made, it remains unclear how often victims actually received working decryption tools. Overall, the leak confirms that LockBit functions like a traditional business, except with criminal intentions at its core.

References

- https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned
- https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group

Indicators of Compromise

```
1.  http://e4hwk3w4ztqfkyo6l36ss3tfj4bw2jw4ytkmomkx2ugwjgrs4w3lriid.onion
```

```
2.  http://iyuggdvguyt4f4hdk6eudwcdtlsw3ixi5thzhqb6fpydw6jblf3sxlyd.onion
```

3. http://lockbit3753ekiocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2id.onion/

4. http://lockbit3753ekiocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2id.onion/buybitcoin

5. http://lockbit3753ekiocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2id.onion/buybitcoin#mirrors

6. http://lockbit3753ekiocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2id.onion/conditions

7. http://lockbit3753ekiocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2id.onion/rules

8. http://lockbit3g3ohd3katajf6zaehxz4h4cnhmz5t735zpltywhwpc6oy3id.onion/

9. http://lockbit3g3ohd3katajf6zaehxz4h4cnhmz5t735zpltywhwpc6oy3id.onion/conditions

10.http://lockbit3olp7oetlc4tl5zydnoluphh7fvdt5oa6arcp2757r7xkutid.onion/

11.http://lockbit435xk3ki62yun7z5nhwz6jyjdp2c64j5vge536if2eny3gtid.onion/

12.http://lockbit4lahhluquhoka3t4spqym2m3dhe66d6lr337glmnlgg2nndad.onion/

13.http://lockbit6knrauo3qafoksvl742vieqbujxw7rd6ofzdtapjb4rrawqad.onion/

14.http://lockbit7ouvrsdgtojeoj5hvu6bljqtghitekwpdy3b6y62ixtsu5jqd.onion/

15.http://lockbitapiahy43zttdhslabjvx4q6k24xx7r33qtcvwqehmnnqxy3yd.onion

16.http://lockbitapiahy43zttdhslabjvx4q6k24xx7r33qtcvwqehmnnqxy3yd.onion</p>

17.http://lockbitapo3wkqddx2ka7t45hejurybzzjpos4cpeliudgv35kkizrid.onion

18.http://lockbitapo3wkqddx2ka7t45hejurybzzjpos4cpeliudgv35kkizrid.onion<br

19.http://lockbitapp24bvbi43n3qmtfcasf2veaeagjxatgbwtxnsh5w32mljad.onion

20.http://lockbitapp24bvbi43n3qmtfcasf2veaeagjxatgbwtxnsh5w32mljad.onion<br

21.http://lockbitapyum2wks2lbcnrovcgxj7ne3ua7hhcmshh3s3ajtpookohqd.onion

22.http://lockbitapyum2wks2lbcnrovcgxj7ne3ua7hhcmshh3s3ajtpookohqd.onion<br

23.http://lockbitapyx2kr5b7ma7qn6ziwqgbrij2czhcbojuxmgnwpkgv2yx2yd.onion

24.http://lockbitapyx2kr5b7ma7qn6ziwqgbrij2czhcbojuxmgnwpkgv2yx2yd.onion<br

25.http://lockbitfskq2fxclyfrop5yizyxpzu65w7pphsgthawcyb4gd27x62id.onion

26.http://lockbitfskq2fxclyfrop5yizyxpzu65w7pphsgthawcyb4gd27x62id.onion/

27.http://lockbitfss2w7co3ij6am6wox4xcurtgwukunx3yubcoe5cbxiqakxqd.onion

28.http://lockbitfsvf75glg226he5inkfgtuoakt4vgfhd7nfgghx5kwz5zo3ad.onion

29.http://lockbitspbsvke7ucgvegltl4acagjjjfkhoi4efxti7gyw742jgjeyd.onion

30.http://lockbitspchsxta4gug5wj5tdsvvmbtqdjmtqfwdoeqfodqzpkmviyqd.onion

31.http://lockbitspckzvghfqwd6uowk2y6gtb4ltbd3miqp53okfkc3j5rrunqd.onion

32.http://lockbitspfigqwjpd6v3az57xpykygkpdzb4xz2imwnxckxh7oyvxuyd.onion

33.http://lockbitspgsxzkoi2cuwklu6hzvuvoj4qggvqwan3nr4zy7ge3s7rtad.onion

34.http://lockbitspomtxfihje6wepecgif7vuqci6zyl7qgenne5b6lxngf4yqd.onion

35.http://lockbitsppra2sj6gkfrgtavqds7rcnvhaxdio7jvu2xrozdr2ld3ead.onion

36.http://lockbitsppsg2kfcafzzdettjbgc4tx2cl6tfm4v4py6xtndbhnnhsid.onion

```
37.http://lockbitspqldd3mm223vmzcvwntd7honhhan3ke72vpnrxexlrsu5ryd.onion
```

```
38.http://lockbitsprnigidq6imswpysqjg3sewkeagtfbamlybwm7fnonglhlyd.onion
```

```
39.http://lockbitsptqsmaf56cmo7bieqwh5htlsfkodpahsaurxlquoz67zwrad.onion
```

```
40.http://lockbitspudgjptrzadjzi7b4n2nw3yq6aqqqqw6wbrrjkr2ffuhkhyd.onion
```

```
41.http://lockbitspxgtf65ej7uu5h7qtephbevcsc2sk2brxzmt754etrrzhdqd.onion
```

```
42.http://lockbitspxmqqfi6bw4y7f5psnpoaakhlisdx33busmnpgtimart5fad.onion
```

```
43.http://lockbitspyakyequybgwgwauhzqxx7ba2gh3lmlj3zyeuaknrexdzfid.onion
```

```
44.http://rbuqsricjycmlv4hkh6cuwpefhgzzgthhxr2ackqwnv2ex23yqkfmuqd.onion
```

Appendix A

```
(433, 36, 36, 112, 0, 1737142597, 'yes i got this instructions from you\n~~~ You have been attacked
```

Source: https://www.ontinue.com/resource/inside-lockbit-inner-workings-of-ransomware-giant/