Black Basta Leak Analysis

medium.com/@a-poc/black-basta-leak-analysis-add723b179a5

May 19, 2025

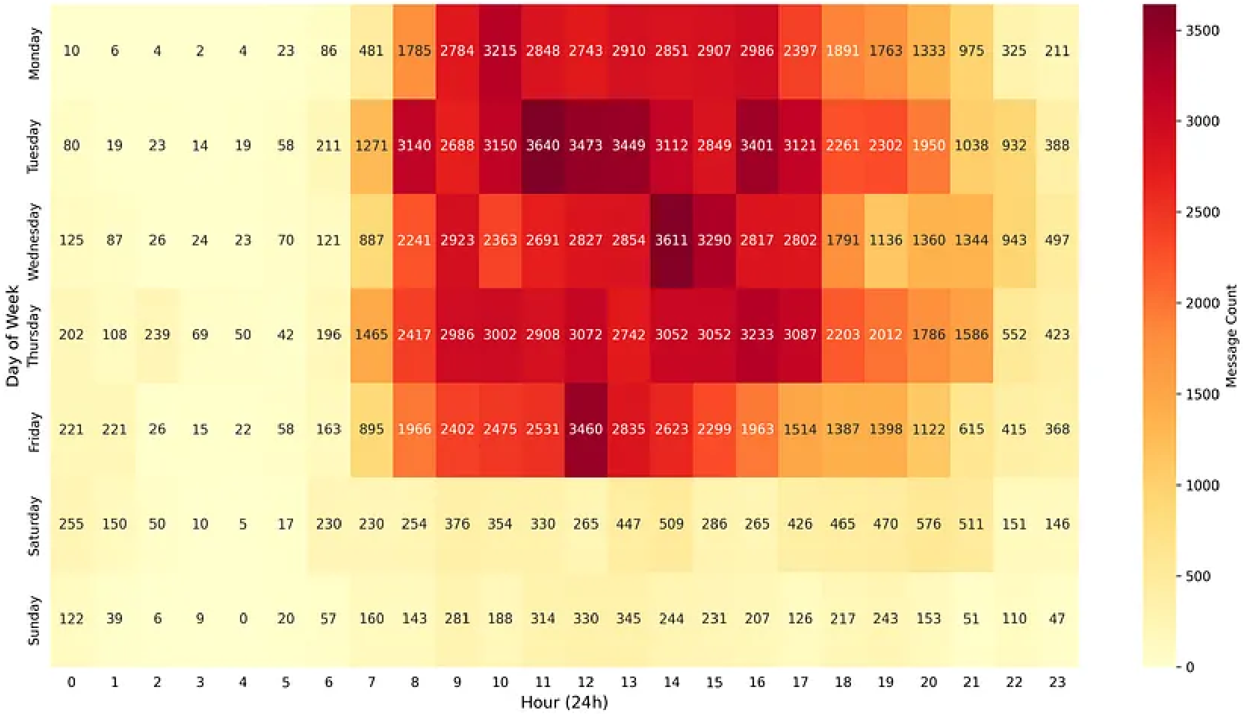
On the 20th of February 2025, the Matrix server chat logs from the notorious ransomware group Black Basta were uploaded to MEGA. This caused a wave of activity from cyber security firms and individuals looking for needles in the 200k message haystack.

The leak provides a fascinating peek behind the curtain of a major ransomware operation and an opportunity to identify data trends.

Working Hours

From September 2023 until June 2024, the Black Basta chat server was most active each week from approximately **07:00 until 21:00**.

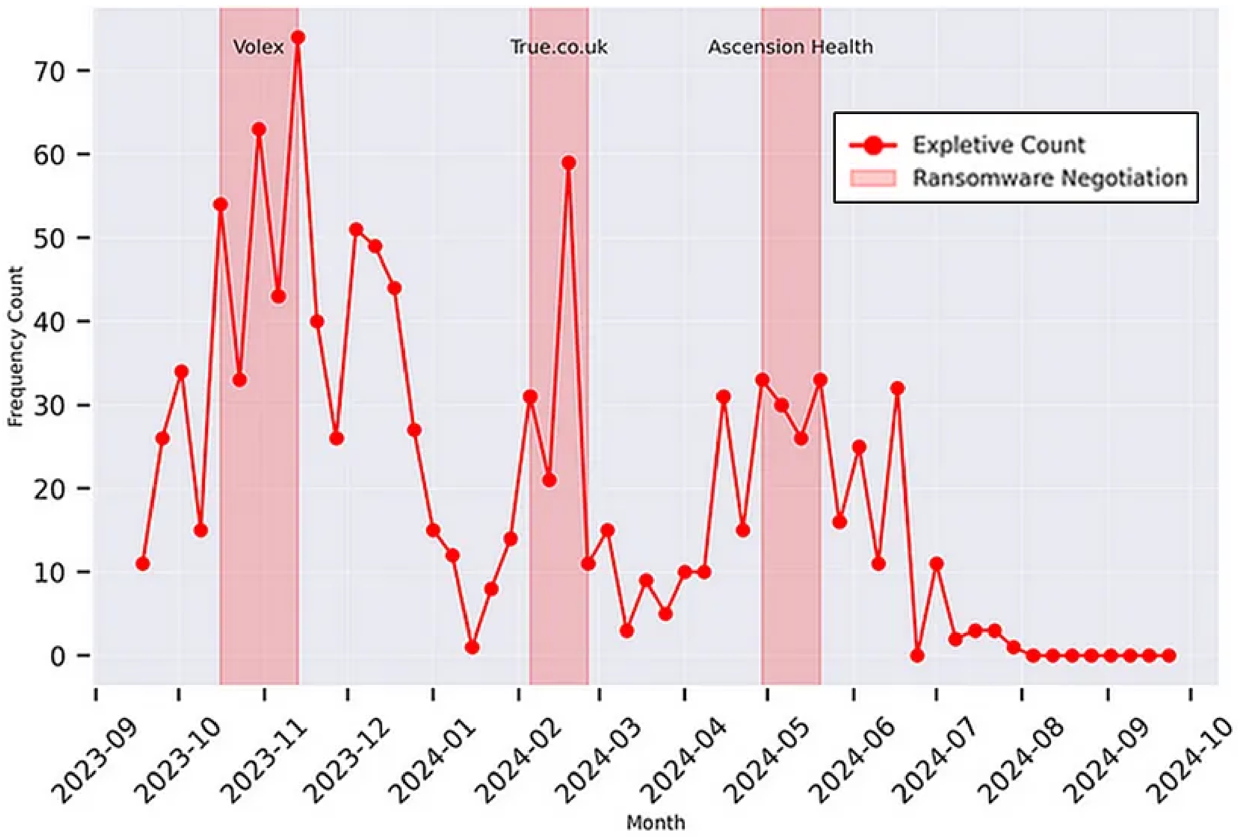
The number of messages sent on Friday afternoons differed from those on other afternoons in the week, and weekends were much quieter.



A heat map of message activity on the Black Basta matrix server

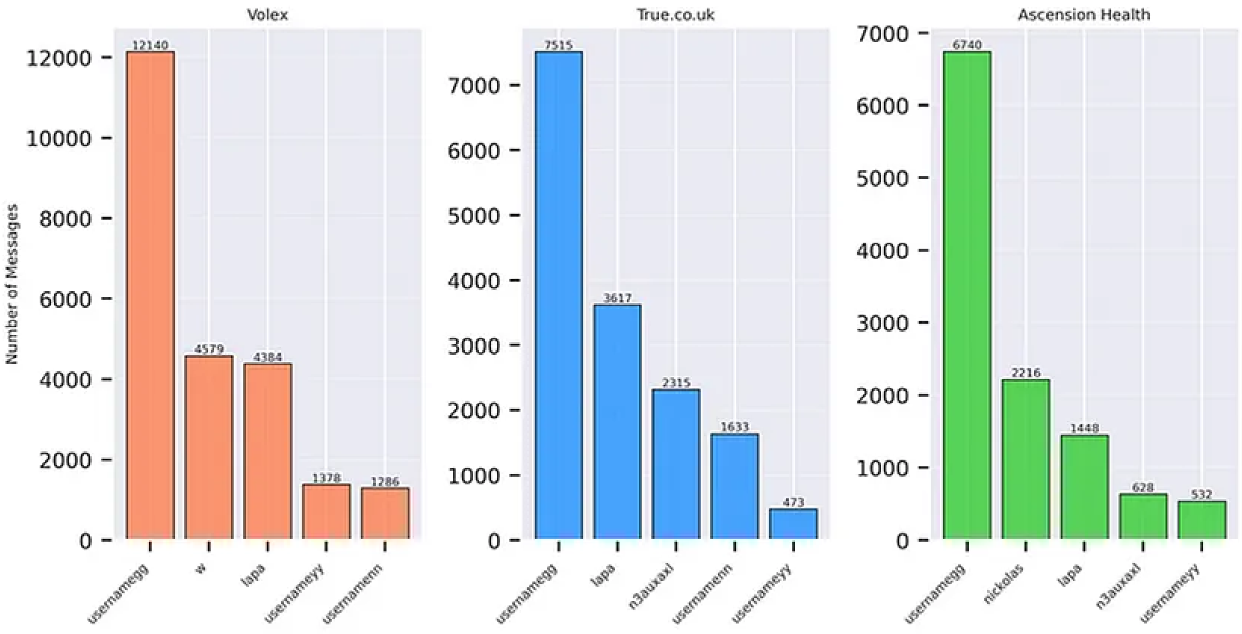
Ransom Negotiations

During active ransomware negotiations (, and) Black Basta members communicated with each other using more expletives than usual.



Graph showing the number of expletives used throughout the year in relation to key negotiation events

and when these negotiations were taking place, specific user message volume patterns outline lead members.



Charts showing the number of messages sent by Black Basta members during periods of negotiation

Some members appeared to be involved in all negotiation discussions:

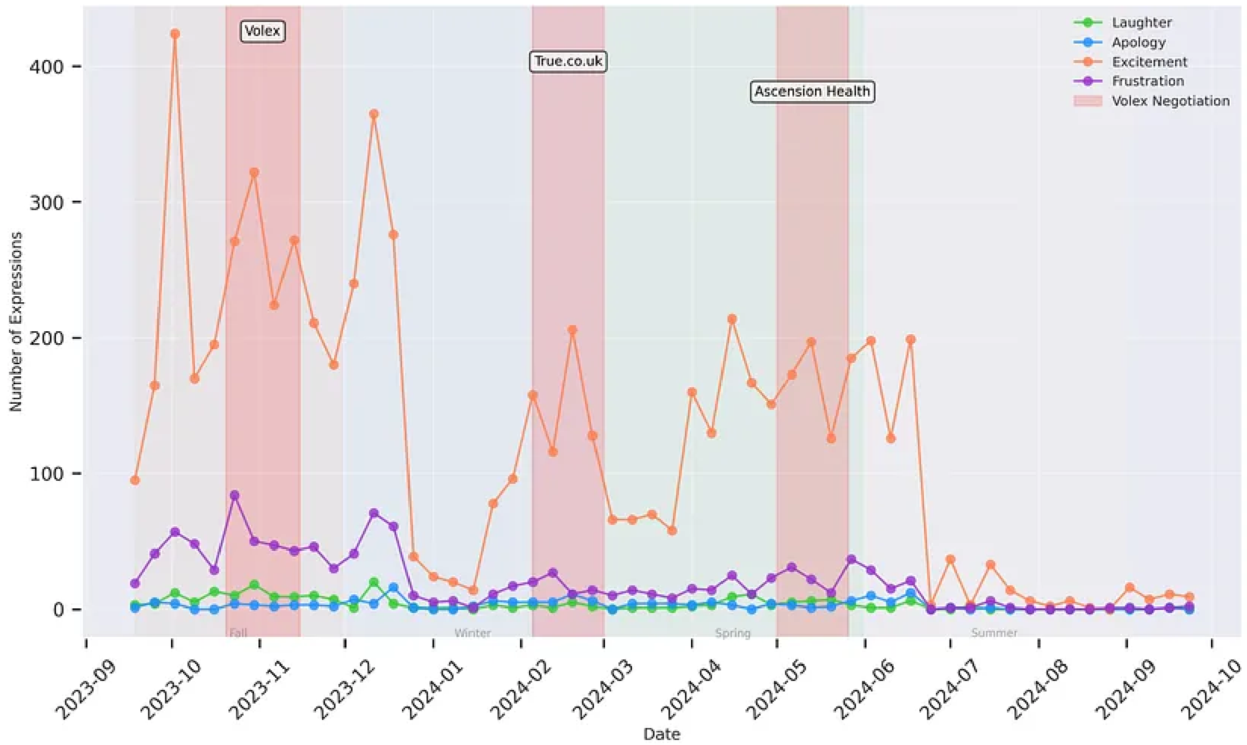
-
-
-

whilst other members only appeared to be related to certain events:

- (Volex)
- (True)
- (Ascension Health)

Communication Changes

Throughout the year, the collective emotions of the group would change depending on the situation they were in.



Graph showing the number of phrases relating to emotions throughout the year in relation to key negotiation events

Excitement was typically expressed in and around major ransomware negotiations, sprinkled with small spikes of frustration.

On average, the longest messages were sent early in the morning at 02:00 whilst the shortest messages were typically sent in the evening 19:00.

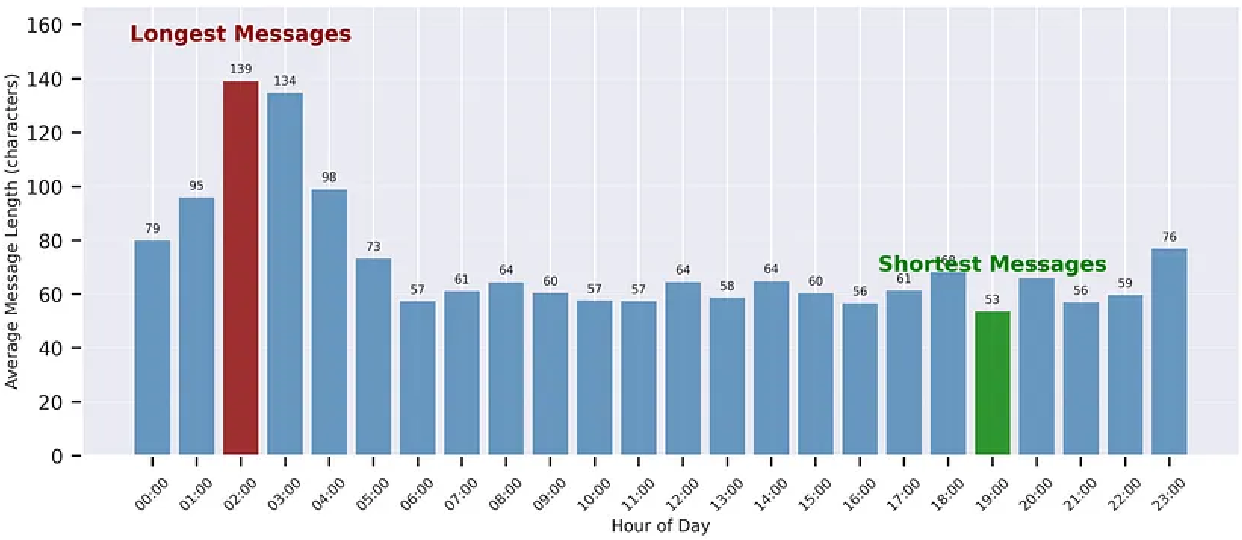
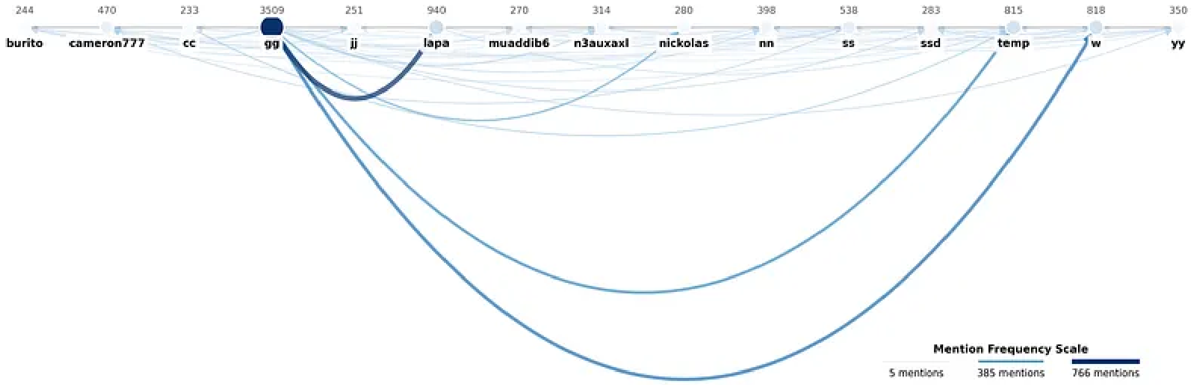


Chart showing the average message length over the average day

Relationships

The number of times Black Basta members make reference to other group members gives an idea of the potential links within the group.



Graph showing the number of times each Black Basta member mentioned each other

The high number of connections highlighted the amount of communication that took place within the group.

Connections of note include:

- GG → lapa
- GG → W
- SS → cameron777
- W → SSD
- burito → n3auxaxl

Conclusion

The Black Basta leak lays bare a year of ransomware operations, revealing distinct patterns in activity, communication, and group dynamics.

Structured working hours and heightened exchanges during negotiations paints a picture of an organized effort shaped by key contributors and shifting priorities.