Exposed Credentials & Ransomware Operations: Using LLMs to Digest 200K Messages from the Black Basta Chats

By Keegan Keplinger | Aurora Johnson

Published: 2025-04-16 · Archived: 2026-04-06 01:06:11 UTC

We cybercrime analysts tend to get excited when giant collections of ransomware gangs' chat logs are leaked, like the Conti Leaks in 2022 – or, more recently, the year's worth of leaked Matrix chat logs from the Black Basta ransomware group. It's the equivalent of front-row access to something that usually happens behind closed doors, and can shed light on TTPs to help balance the scales for defenders.

Our team dug into the leaked Black Basta chat logs with a particular focus on one of SpyCloud Labs' favorite topics: ***stolen credentials***. Based on our analysis, we learned that:

In this article, we'll highlight what this means for understanding the inner workings of these cybercrime operations and also give insights into the process we used for our research.

We're not telling you anything that's not already well known – ransomware continues to be a global threat affecting every industry vertical. In fact, according to our most recent survey report of over 500 professionals in active enterprise cybersecurity roles, ransomware was cited as the leading cybersecurity threat across industries. Ransomware itself is a billion dollar industry, costing businesses tens of billions of dollars annually when factoring in damage and recovery costs.

There's no doubting it, ransomware has become a central component of the cybercrime economy, with businesses increasingly feeling the impacts since at least 2021. The volumes of attention heaped on ransomware since that year is largely a reflection of the surprising success of the ransomware intrusion model (**Figure 1**).

This model (which today doesn't even require a "ware" to the ransom[1]) represents a peak point in which the underground cybercriminal economy had matured into a self-sustaining market. Skill specialization and role differentiation occurred and a variety of opportunities for monetizing cybercrime emerged.

Ransomware caused a paradigm shift, becoming a central hub into which the wide variety of specialists could contribute to the monetization of network wide intrusions and compromise.

Prior to this model, such large-scale, coordinated network intrusions were only the thing of Hollywood and state-sponsored operations, but ransomware enabled such operations to be monetized, attracting fleets of over-educated, under-employed labor (particularly in Balto-Slavic regions). The model was first "publicly" proofed by the Ryuk ransomware, expanded by the Maze "supergroup" and perfected by Ryuk's evolution into the so-called "Conti" supergroup (aka Trickbot, LLC).

Black Basta's history

In 2022, increased interest from law enforcement and blue teams globally forced the Conti super group to fracture. Amongst the growing popularity of the ransomware model in cybercrime, former Conti members were assessed to be at work in some the newly formed groups, including Black Basta (**Figure 2**). Post-Conti splinters (yellow) represent cases where core members of Conti are assumed to play key roles in newer ransomware brands, whereas Conti-associated (green) may have only circumstantial relationships (such as shared affiliates or initial access brokers, or ad-hoc exchanges of services or access between groups). For example, DEV-0365 was a team within Conti that appeared to prepare and rent Cobalt Strike infrastructure to other ransomware groups.

As researchers quickly discovered, leaked ransomware chats can be a double-edged sword. They are simultaneously a goldmine for new insights *and* an overwhelming firehose of unstructured data. Due to the multi-faceted nature of ransomware operations, a lot of explicit coordination is required. This results in plump chat logs, filled with exact technical specifications, logins, and explicit strategy discussions.

However, reading 180,000 chat logs to extract such details is an insurmountable task for even an average-sized team of analysts. Generative AI – and Large Language Models (LLMs), specifically – offer a unique opportunity to quickly process and extract data, filtering out the keks, smiley faces, and cybercriminal drama to uncover intel of interest.

Prompt engineering

The basic principle for entity and knowledge extraction is to define for the LLM 1) what information you're interested in, 2) what format you want it in, and 3) what rules it should follow. The third criteria, giving the LLM some ground rules, is particularly helpful in countering semantic bias (when the model interprets ambiguous inputs incorrectly).

We parsed the chats into fixed timespans, and then used the LLM to dynamically filter out irrelevant data, keeping only valuable insights. In this case, we divided the chat logs into 24 hour chunks and passed them to the LLM along with variations on the following system prompt:

```
system_prompt = f"The input represents a day of chats from a cybercrime group
specializing in ransomware operations. Extract information about {subject} and return
only a json with the following fields: {fields}. {instructions}"
```

This format was used to run over the Black Basta chats several times, leveraging different fields and focusing on different subjects and instruction sets to help guide the model.

This resulted in over 180,000 messages reduced down to daily summaries for particular types of information, including: operational details, personal information, and political intrigue. In some cases – for example, that of *political intrigue* – the 180k messages were reduced down to only a handful of messages. Mentions of relationships with government agencies were not an everyday occurrence in the Black Basta chats, so the resulting extracted messages were sparse.

Of particular interest to SpyCloud's mission of disrupting the credential supply chain leveraged by cybercriminals is the use of infostealers and exposed credentials to facilitate ransomware operations.

Credential exposure starts with a compromise, whether it be from stealer malware, phishing campaigns, or breaches. At this point, only the attackers and the victims can know about the compromise (*Closed Loop* in **Figure 3**). The circle of access expands when this data is sold or traded in the marketplace, or shared in agreements between threat actors. In some cases, the data can be extracted from records of attacker infrastructure. At this point, however, the data isn't widely available (*Semi-Open Loop* in **Figure 3**).

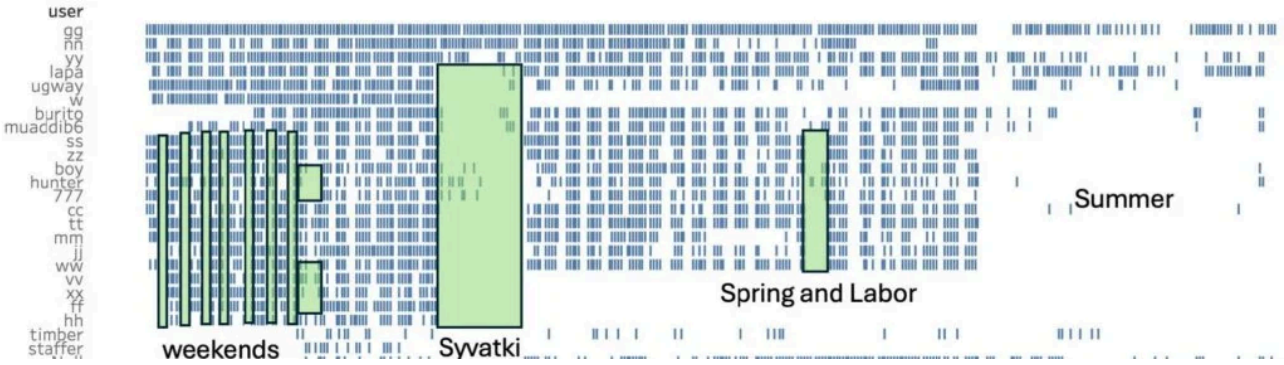
Eventually, most stolen data is made publicly available (*Open Loop* in **Figure 3**) through various public or semi-public channels on the dark web, chat apps, and social media. Actors can choose to "open the loop" for various reasons, including political incidents, depreciation of value, or to establish street-cred.

Once it has been posted publicly, the data is often further split, cross-referenced, and recombined into combolists and password cracking dictionaries that facilitate phishing and brute force attacks. As highlighted below, brute force attacks would eventually take center stage within the Black Basta operation, but that first required desperation…

In the cybersecurity community, 2022 was known for a tidal wave of botnet infections, driven largely by repurposed banking trojans (such as Emotet and Qakbot) that had evolved into generalized loaders. By the end of 2023, the lights of the then-popular botnets like Darkgate and Pikabot – along with the last traces of Qakbot – were barely flickering (**Figure 4**).

Exploitation, phishing, and brute forcing were always part of the Black Basta operation, but brute forcing began to take center stage in early 2024, after the group returned from Syvatki (the period between Orthodox Christmas and the Epiphany, a common holiday in Russia) missing some key members of the botnet team (**Figure 5**). Finally, during that summer, when all that remained was the core leadership of Black Basta, the group purchased 1,000 servers and focused solely on brute forcing.

This change in personnel, infrastructure, and methodology was likely in part facilitated by the group's leader's recent encounters with intelligence agencies, both foreign and domestic.



Throughout the Black Basta operation, combolists, phishing, and stealer logs were leveraged in various ways, but a dominant theme in the implementation of exposed (Open Loop) credentials was brute forcing internet-facing servers (**Figure 6**). At the surface, it might appear surprising that such a simple technique would be so reliably leveraged by a sophisticated ransomware group, but attack surface management is more complicated than it is often given credit for.

Edge devices represent publicly accessible regions of an organization's attack surface. This surface can be exacerbated by misconfigurations in device enrollment, loose security policies, circumvention of security controls, and vulnerability exploitation to remove other security layers, finally leveraging the exposed credentials. As organizations grow, inventory, maintenance, and protection of this attack surface can become weak.

In parallel to this ballooning technological threat surface, the attack surface represented by credential exposure is also growing (**Figure 3** above). Naturally, exposed credentials from this cybercrime data supply chain serve as fuel for brute force engines. And the Black Basta team leaned heavily on this throughout their operation.

The value of stealer logs in constructing combolists

URL:log:pass (ULP) combolists, large lists of credentials consisting of URLs, email/username logins, and passwords that are usually derived from stealer logs, can allow threat actors to construct combolists for brute forcing particular technologies.

On June 12, gg shared several combolists that appear targeted towards different edge devices of interest to Black Basta, including VPN, firewall, and other network security product vendors (**Figure 7**). You can find particular devices and their associated URL formats in internet scanning services like Shodan and Censys. For example, logins for URLs ending in *login.html* and *admin.html* might be good candidates for finding login credentials from ULPs (**Figure 8**).

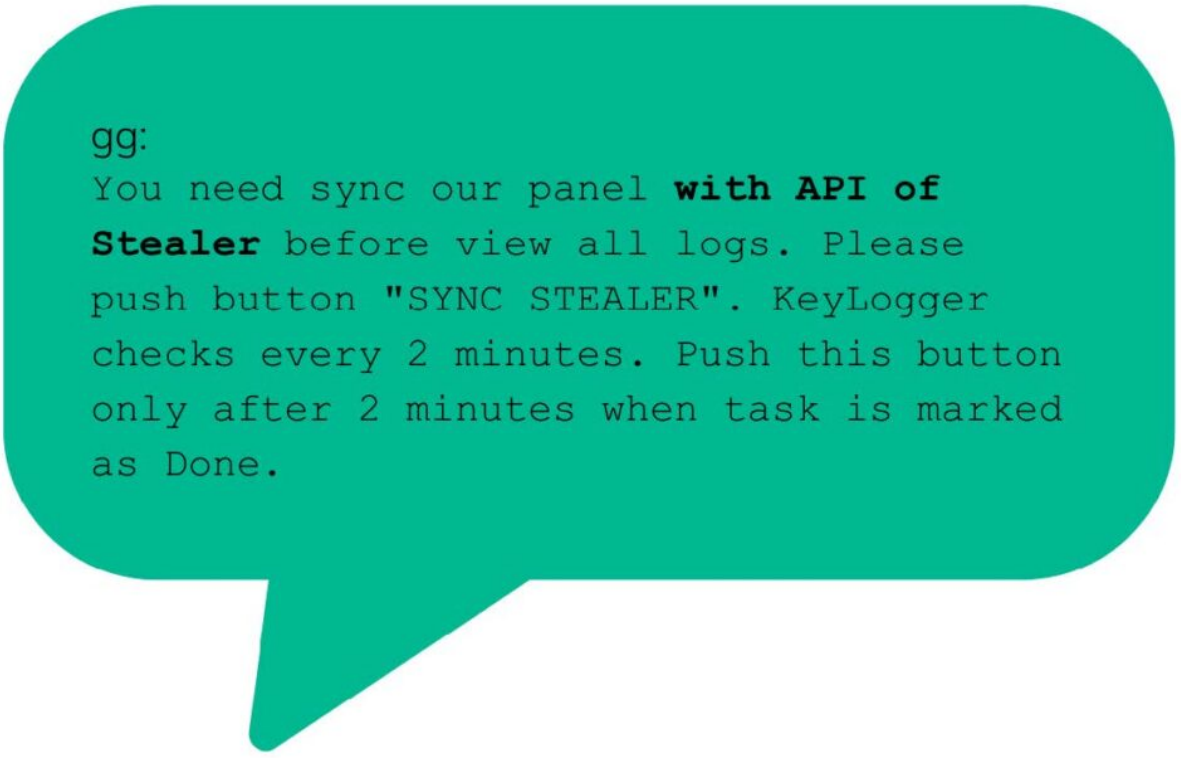
In July 2024, after which it appears that most of the Black Basta team departed (**Figure 5**, Summer), the remaining leadership was conducting the purchase of 1,000 servers for brute forcing on lapa's suggestion. The servers were eventually paid for by gg (**Figure 6**, single red square) in preparation for a massive brute force campaign targeting edge devices.

Black Basta's phishing campaigns

Phishing campaigns did not appear to take up a large proportion of Black Basta's active campaigns at any given time, but they did appear to often be used in parallel with brute force campaigns on the same technologies.

Infostealers and stealer logs

As demonstrated in our preliminary report, the Black Basta team developed an integration for infostealers in the Black Basta panel. Further reading revealed that the team also manages and deploys stealers throughout their ransomware operations to facilitate tasks like privilege escalation, persistence, and lateral movement. There were also other development efforts towards stealers, such as integrating with hidden virtual network computing (hVNC) and reducing the detectability of LummaC2.



In mentions of infostealer malware (**Figure 11**), Lumma consisted mostly of .exe and .zip filenames following burito's suggestion that they wrap the stealer with a crypter. Stealer logs were also directly shared in the leaked Matrix chats from a handful of stealers with an emphasis on Meduza stealer. Valid credentials have been repeatedly targeted by ransomware groups for initial access, and blue teams often find correlations between accounts found in stealer logs and those leveraged in ransomware incidents.

Here, we see an explicit relationship, including specific tooling in the Black Basta panel to support the integration between stealers and active ransomware operations.

In the case of the Black Basta Matrix chat logs, there is plenty of evidence to affirm the overused – but true – statement that "cybercriminals are constantly evolving." We see their operations as reflective of larger trends in the criminal underground, including:

Role differentiation

Similar to the concept of an assembly line, when threat actors begin to focus and specialize while working with other specialists, each component of an operation gains in quality and efficiency, creating a complex criminal ecosystem where you can basically find anything you're looking for.

Black Basta was a comparatively smaller team than Conti, but had clear roles delineated – such as manager, developers, botnet operators, intrusion specialists, infrastructure management, and EDR R&D.

Adaptiveness

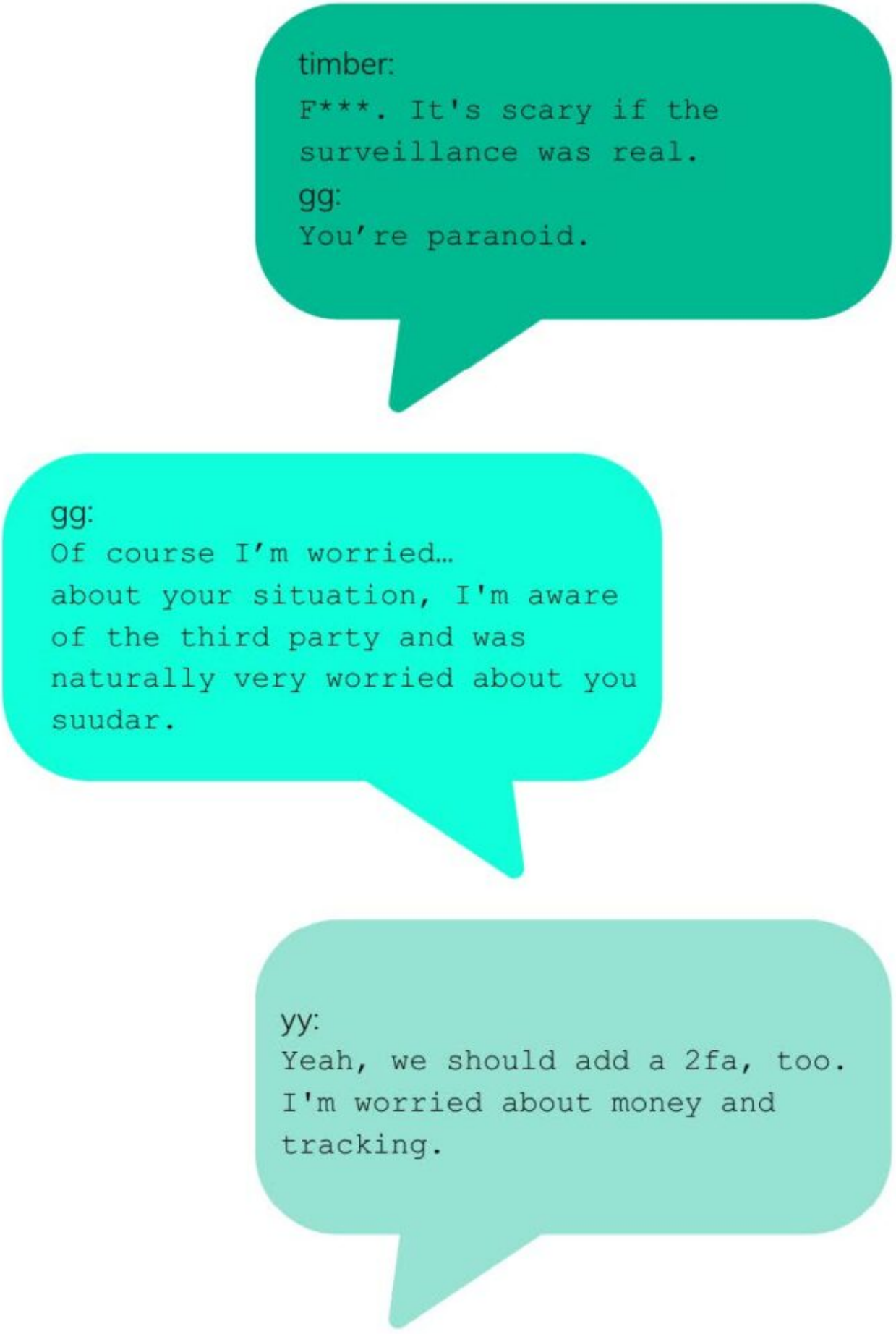
The threat landscape is constantly evolving. There's no rulebook for cybercrime, and cybercriminals are inherently creative problem solvers. For them, obstacles are fun new problems to solve.

Block weak and exposed passwords at the source

More and more, cybercriminal operations are adapting the same business model legitimate corporations use.

What does the future hold for Black Basta?

The cybercriminal lifestyle is filled with paranoia and anxiety – a sentiment often explicitly expressed by threat actors in leaked chats – which is why pressure from law enforcement and defenders can help reduce cybercriminal presence. It is expected that some portion of Black Basta members will retire while others will simply rebrand or contribute their skills to another operation.


timber:
F***. It's scary if the surveillance was real.
gg:
You're paranoid.
gg:
Of course I'm worried... about your situation, I'm aware of the third party and was naturally very worried about you suudar.
yy:
Yeah, we should add a 2fa, too. I'm worried about money and tracking.

Since there is no rulebook for cybercrime, there's no rulebook for defending, but the closest thing we have is "best practices." To protect against the use of valid breached, leaked, and stolen credentials to attack your organization, we recommend the following:

01

Reduce risk of infostealer infections

Individuals and organizations should take steps to avoid infostealer infections to minimize the potential for follow-on cyberattacks.

02

Use password managers

Organizations should offer employees access to a master password tool, and individuals should use a master password keeper instead of storing passwords in the browser. Stealers often steal passwords, credit card information, and other personal data stored in your browser. If you don't save your passwords using your browser's built-in password manager, then it's less likely an infostealer infection will be able to get your passwords.

03

Don't reuse passwords

SpyCloud research shows 70% of users reuse old passwords that have been exposed on the dark web. Users can use a password manager to generate a new, unique password for each account and keep them organized. Organizations can look to NIST guidelines to create and enforce good and manageable password hygiene through proper password policies.

You can check if any of your passwords are exposed on the dark web with SpyCloud's free Password Checker.

04

Use multi-factor authentication (MFA).

MFA renders a stolen password useless without a registered authenticating device or a sophisticated bypass.

05

Monitor for exposed credentials and identity data

There are both consumer-facing and enterprise services to monitor credentials that have been leaked on the darknet due to breaches, malware, or phishing. Users and organizations can get started by using our free Check Your Exposure tool to check your corporate email address to understand if your identity data is circulating in the criminal underground.

Sign up to get the latest cybercrime research, insights, and best practices in your inbox

[1] Ransomware actors are increasingly removing as much malware from their attack flows as possible, sometimes even the ransomware itself, and relying only on the exfiltrated data for extortion. This works well for targets who are sensitive to data exposure and helps reduce the risk of harming, for example, patients in hospitals (which can lead to indictments, litigated ransom payments, and

---