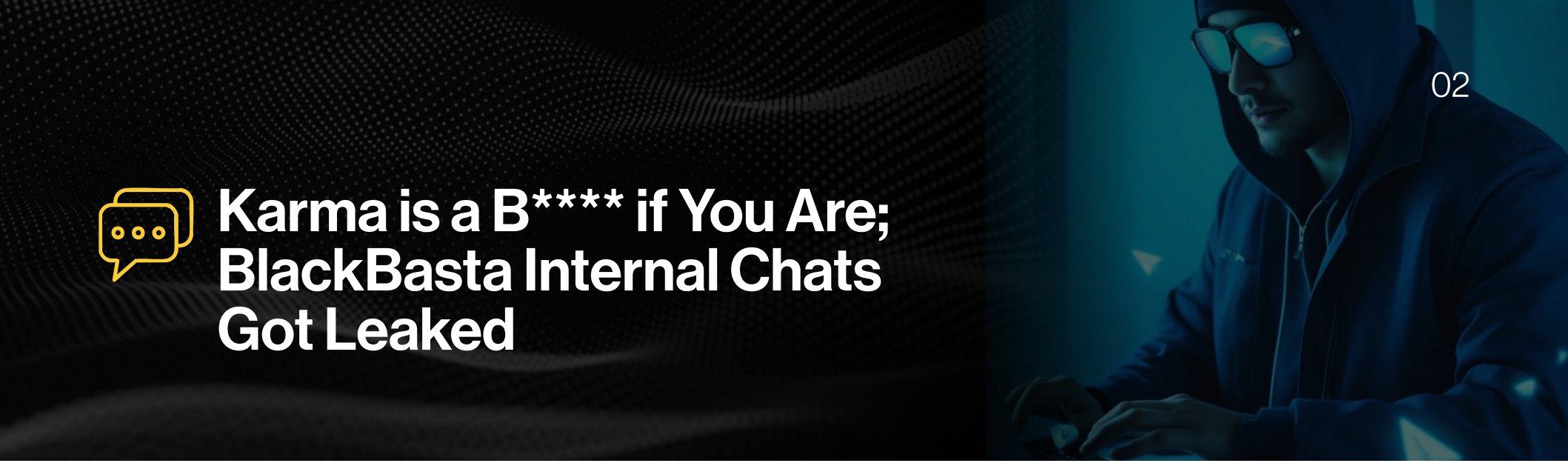
Inside BlackBasta:

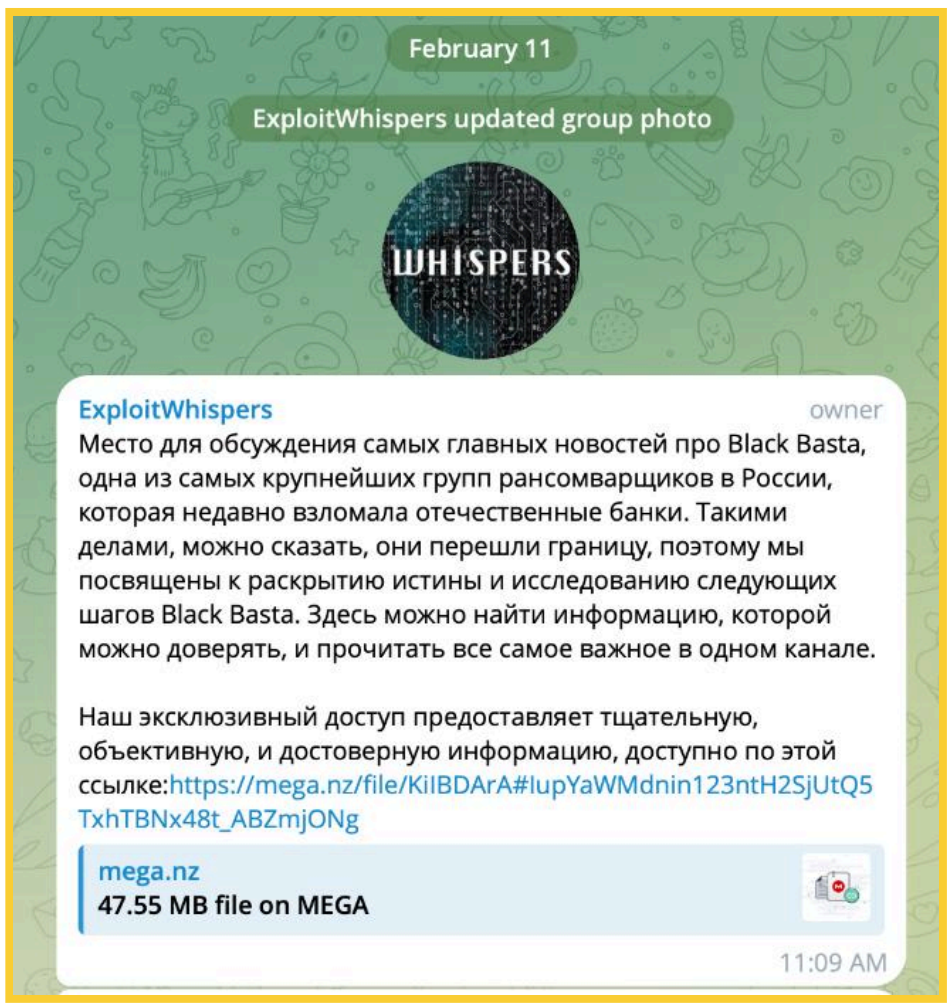
Actor Profiles, Extortion Tactics & Finances

ANALYST1®



Karma is a B**** if You Are; BlackBasta Internal Chats Got Leaked

April 2022. a group of cybercriminals calling themselves **BlackBasta** came together, determined to continue their illicit operations. At its core were former members of Conti, a ransomware group infamous for its high-profile attacks, including the Government of Costa Rica. Conti's downfall came swiftly after the group publicly declared its support for the Russian government following the invasion of Ukraine in February 2022, which became a fatal mistake. Soon after, an individual, seemingly at odds with Conti's political stance, leaked the group's internal chats, exposing their operations to the world and leading to its eventual shutdown in May 2022.
Bad luck seemed to follow former Conti actors again on **February 11, 2025**, when BlackBasta's internal chats were leaked. Using the username **ExploitWhispers** on Telegram, an unknown individual shared a file containing chat logs extracted from the Matrix messenger. The JSON file contains approximately **200,000** messages (the majority in Russian) from **September 18, 2023**, to **September 28, 2024**. In a message accompanying the leak, **ExpertWhisper** claimed that the internal chats were exposed due to an alleged betrayal by **BlackBasta**. According to their statement, the group had crossed a line by targeting Russian banks, ultimately leading to the leak.



A message posted by ExploitWhispers on Telegram explains the reason behind their decision to leak BlackBasta's internal chats

Source: Telegram

Full message translated to English: "This is a place for discussions about the most important news related to BlackBasta, one of the largest ransomware groups in Russia, which recently breached domestic banks. By doing this, they have crossed a line, and that is why we are committed to uncovering the truth about their next steps. Here, you can find trustworthy information and read all the key updates in one channel. Our exclusive access provides detailed, objective, and reliable information, available at this link."

These internal conversations offer valuable insights from a researcher's perspective while also revealing the ruthless crimes they commit, which are both intriguing and deeply disturbing. There's a lot to uncover, but in this research, we'll take a brief look at some actors' profiles and then take a deep dive into BlackBasta's inner workings, with a particular focus on their extortion tactics. We'll also look closer at BlackBasta's economy, uncovering the illicit profits generated by actors.

Have you ever wondered what happens behind the scenes when BlackBasta extorts its victims? From manipulating victims to issuing calculated threats, these cybercriminals rely on psychological pressure just as much as technical expertise to get what they want. Let's take a closer look at their own words, straight from the leaked chats.

“tinker,” “gg,” “yy,” & Their Day-to-Day Activities at the Extortion Department

To provide deeper insight into the extortion tactics employed by BlackBasta actors, we first want to briefly introduce some individuals, their day-to-day operations, personal habits, interests, and even their identities, where identifiable in our analysis. Understanding the people behind the attacks helps recognize their behavioral patterns and motivations, which can be crucial when dealing with them.

After years of investigating Russian ransomware, one thing remains clear: actors may change the syndicate name, but the core individuals behind the operations remain the same. This is especially evident in the case of BlackBasta, many of whom are former Conti members who have rebranded into multiple groups.

The analysis of Conti’s leaked chats in 2022 revealed many insights into the group’s inner workings, revealing the key factors behind their success. Initially, the dominant belief was that groups like Conti followed the Ransomware-as-a-Service (RaaS) model, in which affiliates or access brokers breached targets while operators who controlled the ransomware provided their encryption tool. However, the leaks exposed a far more complex reality, painting a picture of a crime syndicate operating much like a traditional business - just one built on cyberattacks and extortion.

This wasn’t just a loose network of cybercriminals; it was a highly organized crime operation, structured into teams with defined roles, hierarchies, and even salaried employees distributed across technical, HR, and other departments. As it was identified, some actors were paid shockingly low wages, barely scraping by as they lived from one illicit paycheck to the next. The familiar image of Russian hackers speeding around in luxurious cars quickly shattered, though, to be fair, this stereotype does hold true for some.

Actor **gg**, identified as a leader in the BlackBasta leaks, appears to be one of them, living a lavish lifestyle and collecting millions of dollars from extorted funds. gg began his journey at Conti, where he was known as a **tramp**, an alias that publicly surfaced through the leaked Conti chats in 2022. His strong technical expertise eventually enabled him to launch his own project, positioning him as a key figure within BlackBasta. Under gg’s careful management, BlackBasta continued operating under the same model established at Conti, integrating wage-based employees alongside a percentage/commission-based structure. This model was applied internally and extended to outside affiliates (access brokers). In some cases, though rare, such arrangements still occurred.

According to a report by Valéry Rieß-Marchive, **Oleg Nefedov**, a 35-year-old Russian citizen, is likely the actor behind gg/tramp personas. Born in the Tatarstan Republic, Russia, Nefedov currently lives in Moscow. An unknown individual who leaked BlackBasta’s chats further reinforced this suspicion. Along with the chats, ExploitWhispers also shared a document containing personal information, including Nefedov’s full name, date of birth, passport details, travel history, businesses, and other sensitive information.

During his visit to Yerevan, Armenia, on **June 21, 2024**, he was arrested, kept under detention, and released later on **June 23, 2024**. According to the official statement, upon Nefedov’s release, he left the courthouse, and **“his whereabouts became unknown.”**

We could be able to track his whereabouts by analyzing the leaked data, which also contained a list of flights Nefedov took, specifying dates and destinations. According to this data, on **June 23, 2024**, Nefedov safely landed at Sheremetyevo Airport in Moscow, making a truly magical escape from Armenia and awaiting justice.

Looking further into the leaked information, we see that Nefedov has an impressively active travel history (for a cybercriminal). If you think it's limited to Russia or former Soviet Union countries like Armenia, you'd be mistaken. Since January 2023, his travels have spanned multiple countries. On January 16, 2023, he flew to the Maldives, then traveled to Dubai, where he stayed for three days before returning to Kazan, Russia, on January 19, 2023. In April 2023, he visited Barcelona and Egypt, followed by a trip to Turkey in June.

An analysis of activity in the leaked chats associated with gg revealed a complete absence of communication between **June 21, 2024**, and **July 2, 2024**, suggesting a possible detainment. gg later commented on his arrest situation in a conversation with another actor operating under the alias "**chuck**". gg speculated that someone had likely given up his information in exchange for the USD 10 million reward announced in May 2022. Reflecting on his escape, gg added: **"I have returned from the other side, from where no one has ever come back."** He then warned chuck not to travel anywhere: **"They showed me my case. They have all the info, on me, on others, our nicknames, and more."**

"Our people picked me up", gg also stated in the **leaked chats**. It remains unclear what powerful figures Nefedov was referring to as the one who protected him from downfall, ultimately allowing him to escape from Armenia. However, his own words from another chat may provide a small hint about the forces at play behind his release. In a TOX conversation, which is not part of the recent BlackBasta chat leaks but was recently disclosed in Valery's report, Nefedov, using the alias "aa," claims that he has been bribing FSB and GRU officials for an extended period of time. **"I have guys from Lubyanka and GRU; I've been paying them off for a long time already."**

(Note: "Lubyanka" is commonly used to refer to the FSB. It refers to the Lubyanka Building in Moscow, which historically served as the headquarters of the KGB (the Soviet Union's security agency). After the dissolution of the KGB in 1991, the building became the headquarters of its successor agency, the FSB (Federal Security Service of Russia)

```
2022-11-14  14:15:15    AA  у менять есть с лубянки и гру ребята , кормлю давно их
2022-11-14  14:15:40    AA  они возьмут только на работу к себе
2022-11-14  14:15:49    AA  о сроках и тд речи даже идти не будет
2022-11-14  14:16:17    AA  просто будешь ходить как на белую работу каждый денб к 8 утра
и уходить в 18
2022-11-14  14:20:18    dd  это лучше
2022-11-14  14:20:22    dd  чем там быть
2022-11-14  14:20:26    dd  одназначно
```

The screenshot shows a conversation between gg (referred to as AA in the chats) and another actor, where gg discusses his acquaintances within Russian special services.

Source: Valéry Rieß-Marchive

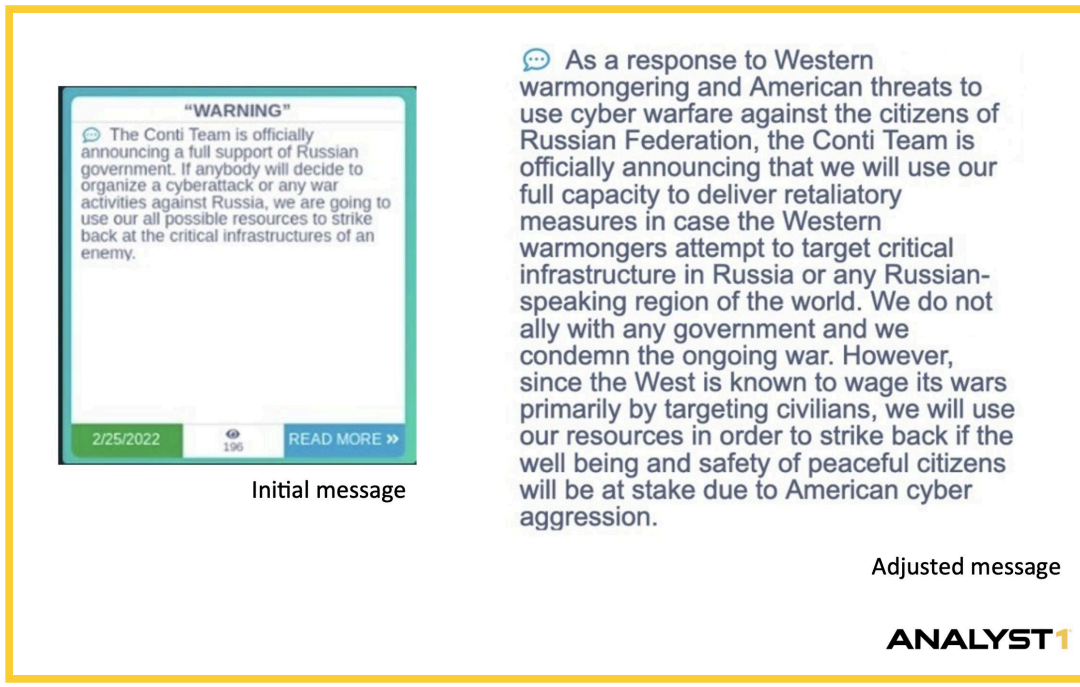
These special privileges perhaps also allowed gg to maintain a physical office in Moscow, where some actors met and worked together in person regularly. In January 2024, BlackBasta secured a new office. **"Do you want to come and see the new location?" gg** messaged **yy**, another suspected former Conti member. According to chat analysis, yy's role at BlackBasta involved coding and managing the syndicate's infrastructure, including the admin panel and data leak sites.

Over the years, it became evident that gg and yy had formed a close working relationship, with yy proving to be a valuable asset. yy's growing influence within BlackBasta earned him a high-ranking position, which was also reflected in the profits they received, a topic we will explore further in this report. However, despite yy's status, the hierarchical structure remained evident, with gg acting as the main boss. While gg was responsible for giving orders and setting the strategic direction for their illicit business, he also had a strong concern for maintaining order in their physical office. **"You left your socks, toilet paper, and towels all over the place,"** gg said to yy. **"You see everything is clean around here, so please make sure you keep it this way,"** he added.

Another actor, operating under the alias **tinker**, identified in the leaked chats, was also a former Conti member. tinker's "official" role at BlackBasta is that of a "data analyst" responsible for investigating victims, analyzing stolen data to identify the most sensitive information, and engaging in negotiations with victims. He carried out the same tasks in Conti, working alongside a team of callers and spammers engaging in triple extortion efforts, a tactic that was also retained in BlackBasta.

"We were making such an impact that we became regulars, dominating media headlines," tinker recalls nostalgically about his time in Conti. Based on chat logs, around May 2024, tinker was working with former Conti actors who were part of Team 2. Team 2 eventually rebranded into **Royal** and then into **BlackSuit**, a fact also confirmed by the leaked BlackBasta chats through the actors' own confessions. **"I also work for BlackSuit, but I think it's time for me to leave,"** tinker told gg on May 20, 2024.

Interestingly enough, tinker was the one who re-crafted that fatal Conti's announcement of support for the Russian government: **"When a "jumper" from Team2 posted on the blog saying, "We are for Russia," I wrote to Hors about it. He immediately gave me access, and I replaced it with a proper message in the style of "We are for peace." It didn't really help, though. But my point is that I had a strong understanding of how to shape the message and manage public relations effectively."**



The image displays Conti's initial message on the left, which was later replaced with the "adjusted" version on the right.

Source: Analyst1

As part of the extortion trio, gg, yy, and tinker appeared to form a highly effective team. Each played a crucial role in BlackBasta's operations, combining their expertise in technical execution and victim negotiations. But what tactics did they use to pressure their victims into compliance, and more importantly, how did they choose their targets in the first place? Let's take a closer look in the next section.

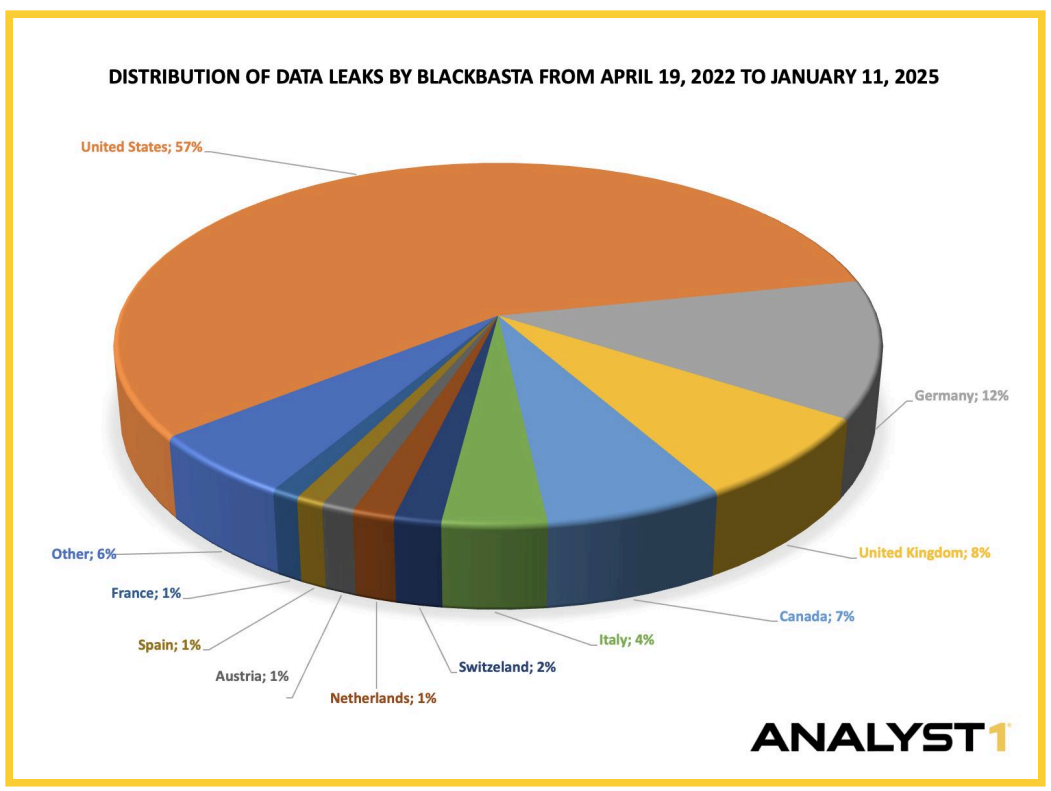
Choosing a Victim

BlackBasta's actors are opportunistic, but they don't attack just any entity at random. Instead, their **target selection** follows a set of rules, which, broadly speaking, are dictated by three main characteristics: **country, industry**, and **revenue**. On top of that, BlackBasta's actors closely monitor **political dynamics** to minimize risks from specific geopolitical or law enforcement actions.

BlackBasta operates as a Big Game Hunting (BGH) ransomware group, a strategy in which cybercriminals focus on high-value entities. The goal is to maximize ransom payouts by targeting large organizations with high revenue, knowing they can demand substantial ransoms.

However, according to internal communications between actors, not all high-revenue companies are considered profitable. Among the most payable (compliant) targets, the U.S. and Germany were explicitly highlighted as the regions most likely to pay. As a result, these entities are targeted the most.

This actor's statement aligns with the activity observed on the BlackBasta data leak site. During its operation, from **April 19, 2022**, to **January 11, 2025**, the **United States** accounted for **57%** of reported victims, followed by **Germany** at **12%**. The complete list of claimed victims includes entities from multiple countries, such as the United States, Germany, United Kingdom, Canada, Italy, Switzerland, Netherlands, Austria, France, Spain, Denmark, Belgium, Australia, Sweden, India, Brazil, Liechtenstein, Finland, Jamaica, Puerto Rico, Israel, Japan, New Zealand, Turkey, Poland, and the Czech Republic. (Source: ecrime.ch)



The graph illustrates the distribution of BlackBasta's victims across different regions

Source: Analyst1 through ecrime.ch

Despite the wide range of regions BlackBasta targets, certain nations are deliberately excluded from their operations. Countries that are off-limits are those referred to in their own words as **"friendly countries"** (Rus: дружественные страны). This exclusion is not limited to former CIS countries, which are typically avoided in accordance with the unspoken rule of the Russia-aligned cybercriminal underground. Notably, China is also included in the list of these so-called friendly countries, further emphasizing the group's geopolitical considerations in their target selection process.

BlackBasta actors appear to have no restrictions on selecting target sectors. Among the attacked sectors discussed in chats and posted on the BlackBasta data leak site are **Finance, Legal, Construction, Manufacturing, Real Estate, Retail, Healthcare**, and others.

However, the current political climate, in some cases, might affect their choice of sector and region. The leaked chats reveal a strong emphasis on carefully choosing targets based on geopolitical dynamics, a focus that has intensified with the ongoing war in Ukraine. An interesting case demonstrating actors' political concerns emerged during the Ascension Health attack, a high-profile entity that fell victim to BlackBasta, who reported a breach on **May 9, 2024**. While the entity was undoubtedly a valuable target, and actors deliberately went after it, discussions within the group revealed mixed feelings about the attack. The hesitation stemmed from the critical nature of the healthcare sector and the broader political climate, which could lead to significant backlash.

This concern became evident in a conversation between gg and tinker. While gg viewed the attack purely as a business opportunity by saying: **"I knew what I was doing and approved it"**, tinker acknowledged the ethical dilemmas and potential consequences of targeting such a high-profile victim. On **May 10, 2024**, tinker expressed concerns about the risks involved: **"If someone, God forbid, dies and we already know that emergency services are blocked, first, we are 100% not getting paid, and second, we'll bring serious problems upon ourselves. This will be classified as a terrorist attack, and there will be no more payouts from the U.S."**

Tinker elaborated further, drawing a parallel to past geopolitical events and ransomware-related international negotiations: **"Moreover, when it comes to politics, Russians** (author's note: Russians referred to as Russian government) **have a tendency to react. When the Colonial Pipeline was hacked in 2021, the ransomware issue made it onto the agenda of the Putin-Biden summit. As a result, after that summit, ransomware groups in Russia faced severe crackdowns. Now, the geopolitical climate is different, but I'm sure negotiations between them are ongoing. I wouldn't be surprised if, during the next round of talks, the U.S. says something like, 'Instead of giving Ukraine 10 long-range missiles, we'll send only five, and in return, you hand over those responsible for killing our patient."**

This conversation highlights the internal divisions among BlackBasta actors, where some prioritize financial gain while others express concerns about the geopolitical consequences their actions might provoke. However, despite these concerns raised by actors like tinker, the hierarchical structure remains firmly in place, with decisions and the overall "business" approach ultimately dictated by leadership. The same applies to extortion tactics, which we will explore in more detail in the next section.

BlackBasta's Extortion Playbook

Setting a Ransom Payment

With BlackBasta being a Big Game Hunter, as previously mentioned, the revenue aspect plays a significant role in choosing a victim. It is also identified as a starting point for setting ransom demands, as the amount demanded is directly tied to a percentage of the victim's annual revenue. Actors typically aim to set initial ransom demands at around 1 to 3% of the company's annual revenue, which they estimate using data sources like ZoomInfo.

From negotiation observations, the initial ransom is usually set high, followed by discounts offered by actors as part of the negotiation process. This tactic appears to be a deliberate strategy used to create psychological pressure on victims, making the eventual "discounted" amount seem more reasonable and increasing the likelihood of payment.

To secure a ransom payout, BlackBasta strategically targets its victims' most vulnerable points, applying pressure in two critical ways to force a response. The first blow comes from encrypting the victim's systems, which results in operational disruptions and massive financial losses. The second layer of attack involves exfiltrating sensitive data, which is then used as leverage in the extortion process.

By analyzing sensitive financial information, including insurance information extracted from stolen data, they gain insights into their victim's position and ability to pay. Preserving all of the knowledge accumulated over the years, tinker, a negotiator and "data analyst," plays a crucial role in identifying financial documents stolen from victims. He also faces significant pressure from gg, the boss, who has the final say on the ransom amount. In one chat with tinker on **March 1, 2024**, gg emphasized the importance of leveraging financial data during negotiations:
"Go analyze their financial data and send the documents directly into the chat. I need a data analyst who will corner them with the information we have."

In one such case handled by tinker and gg, the victim was a Canadian real estate company with an annual revenue of approximately USD 103 million. After negotiations, the victim agreed to pay USD 400,000. During a chat between gg and tinker, tinker appeared to justify the USD 400,000 amount, demonstrating a detailed analysis of their victim's finances: **"They are offering 400K, and overall, judging by their finances, that seems to be their absolute limit. Don't forget that annual revenue often includes contracts signed that year for their entire duration. So, for example, if they signed a $1 million supply contract with Company A for five years, that entire $1 million would be counted as revenue for a single year.**

This means that a high reported revenue doesn't always translate into large available funds. For a company of their size, a $500K investment is likely their upper limit, even considering all debt funding options." Despite tinker's assessment, gg pushed to demand USD 500,000, aiming to **"push them to the limit"** and get a higher ransom.

Interestingly enough, such ransom amounts under USD 1 million were observed by tinker to have a higher chance of payout and be easier to secure, an observation they shared in a chat with gg on March 13, 2024:
"I actually noticed a long time ago that if you keep the ransom just slightly under $1 million, it significantly reduces the psychological shock and helps victims convince their banks or offices to approve emergency funding. In many financial transactions, there are clear limits; anything below $1 million is processed more easily, while amounts above that trigger more scrutiny."

Double & Triple Extortion Tactics

In the **double** and **triple** extortion model, exfiltrated data is the primary leverage to pressure victims into compliance. The larger the volume of stolen data and the more sensitive its contents, the stronger BlackBasta's position during negotiations.

Double extortion tactics involve threatening victims with publishing their stolen data on BlackBasta's data leak site. Since the data leak site is one of the main pressure points during negotiations, actors aim to make it as intimidating as possible to maximize fear and urgency among victims. On **December 12, 2023**, gg messaged another actor, emphasizing the need to enhance the fear factor of their leak site: **"We need a scary blog with high-profile victims. The reaction from people who visit our data leak site should be: 'What a fucking tiger these guys are??'"** This statement underscores BlackBasta's strategic use of psychological pressure, ensuring that their data leak site not only exposes victims but also serves as a warning to future targets, reinforcing the fear of non-compliance.

From the observed chat logs, the process leading to posting a victim's data and the final publication follows multiple stages. While specific actions may vary, the general sequence typically unfolds as follows:

1. **Initial Contact with the Victim**

   Actors contact the victim, providing them with a chat ID for negotiations. If the victim responds quickly, negotiations begin.

2. **Applying Pressure through Threats**

   Data Leak Threat: If the victim does not engage in negotiations or communication stagnates, actors escalate by sending them a link to their "test" data leak post. This post is not yet public but is intended to be published if the victim refuses to comply. The goal is to apply psychological pressure, making the victim feel that time is running out.

   If negotiations continue to stall, actors take it further by publicly posting the victim's name on their data leak site. Internally, they refer to this as "highlight" (Rus: подсветить). This move serves as an additional pressure tactic, signaling to the victim that this is their last chance to negotiate before full exposure.

   According to the observed chat logs and data leak site activity, actors delete the victim's name from the data leak site if the ransom is paid.

   Demonstrating the Knowledge of Stolen Data: To increase pressure on victims, BlackBasta actors often demonstrate their knowledge of the victim's financial situation, using details obtained from exfiltrated data. By providing insight into the company's cash flow, liquidity, and funding capabilities, they attempt to counter resistance and steer negotiations toward a payout.

   An example of such a message sent to a victim reads: **"So it's better for you to drop this 'if we don't pay, we both lose' thing right away! Once and for all. Instead, let's focus on resolving it the easy way. First, you have around $700K-$800K in cumulative end-of-the-year cash flow. You can enact some emergency funding to raise this to, let's say, another $400K in cash. This gives you $1.2 million in total."**

   Supply Chain Attack Threat: To apply additional pressure, BlackBasta actors have, in some cases, threatened victims with supply chain attacks, claiming they have ongoing access to the victim's network. This threat of a supply chain attack reinforces the idea that not paying the ransom could result in further breaches, not just affecting the victim's company but also its partners, clients, and customers. This strategy aims to create urgency and increase the likelihood of payment.

Examples of such messages are as follows:
"In case you do not pay, this data exposure and our own efforts will lead to other bad entities being able to connect to your network and end up attacking you and your customers. The price to resolve this situation is $28,720,000 USD. In case of successful negotiations, we guarantee you will get"

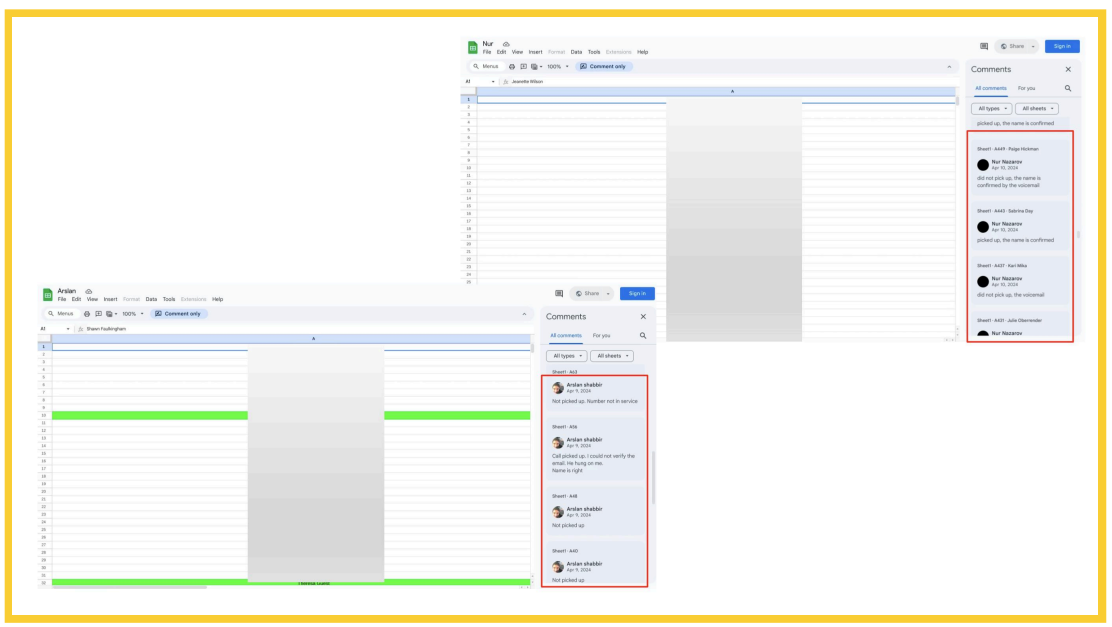
“We will use our spam engine, the one we used to infect you in the first place, sending a neat, nicely written message - "Hello, this is (name of the company removed by author) - we are sending a follow up to the recent email on disclosing a data breach (because i am sure you sent one to your clients as you are obligated by the law to do so). In the attached document, you can see further information about the breach, and an audit of exposure." And guess what - the file will be our payload! We send this to all your clients!

3. Escalation and Final Steps

If the victim continues to refuse negotiations, their data is fully published on the BlackBasta leak site. This move is meant to punish non-compliance and serve as a warning to future victims. Based on actors' chat logs, the stolen data is available for sale to anyone who might be interested.

The **triple extortion** tactic is also key to BlackBasta’s extortion playbook. This method involves direct harassment of victims, executives, and employees associated with the targeted victim. This triple extortion approach ensures that victims feel pressure from multiple directions, encrypted systems, data exposure threats, and direct intimidation, increasing the likelihood of ransom payment.

Two members of the group, operating under the aliases **"iamnurnazarov"** and **"arslanshabbirmalik”**, were identified as low-level, salaried individuals assigned to the role of "callers" managed by the actor under the alias **“manager361”**. Both individuals were given access to Google Sheets containing a list of targeted victims and were instructed to make calls to pressure them into complying with ransom demands. In the screenshot below, you can see actors commenting on their calls with the victim, providing updates on the status of the conversation, and reporting their progress in the extortion process.



The screenshot shows Google sheets shared with each caller; the names of the companies are blurred

Source: Analyst1

Both "iamnurnazarov" and "arslanshabbirmalik" serve as perfect examples of the hierarchical structure within BlackBasta and the stark differences in earnings among its members. While top-tier actors like gg and yy were raking in six- and seven-figure profits, these low-level "callers" were grinding away for what can only be described as cybercrime's version of minimum wage. According to chat logs, the approximate payment for each successful call, meaning the victim picked up and a conversation took place, was a whopping USD 5 per call. On a good day, these actors could make anywhere from USD 20 to USD 50.

If cybercrime had a corporate ladder, these guys would be stuck on the bottom rung, cold-calling victims for a few bucks while their bosses were moving millions. In the next section, let’s take a closer look at the real profits being made by higher-ranking actors and how BlackBasta's economy truly works. Spoiler alert: it’s not evenly distributed.

Inside BlackBasta's Finances: Who Earns What?

When investigating BlackBasta's operations or any other ransomware groups, following the money is crucial in identifying patterns and behaviors at both the group and individual actor levels. This approach can potentially lead to asset seizures and arrest opportunities. In this section, we will provide insights to uncover the financial operations of BlackBasta actors, specifically focusing on yy, gg, and tinker.

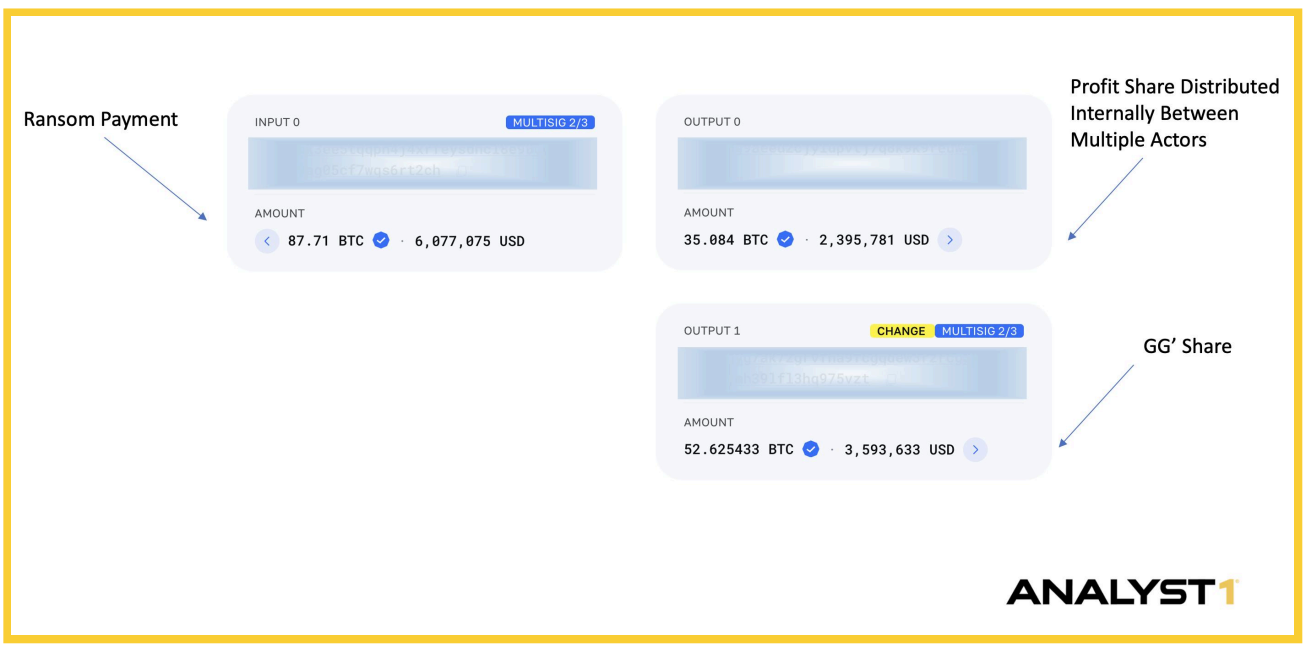
When investigating leaked chats, it is important to remember that not every cryptocurrency address mentioned can be directly attributed to BlackBasta actors. Among the observed cryptocurrency transactions, we identified different types of payments, including ransom payments and distributed salaries/percentages/commissions. We also observed so-called "working addresses" for payments made for goods and services to outside entities separate from BlackBasta's operations. In addition, some transactions also include crypto-to-cash exchanges and laundering requests (favors) between actors.

The starting point for our on-chain investigation revolves around gg, who appears to be the central figure in BlackBasta's financial operations. As the boss, gg seemingly receives the largest share of profits. He acts as the primary operator, responsible for providing cryptocurrency addresses to receive ransom payments before redistributing funds through salaries and commissions to other BlackBasta actors.

Below are examples of different payments that we observed in the leaked BlackBasta chats, showcasing various transaction types and purposes within the group's financial operations:

Two scenarios of ransom distribution exist within BlackBasta's operations. The first occurs when actors who are members of the group obtain access to the victim's network, allowing the ransom to be distributed internally. The second follows a traditional RaaS model, where BlackBasta collaborates with outside access brokers (affiliates) and shares a portion of the profit.

One ransom payment of nearly **USD 6 million** was identified as having been paid to them on **May 28, 2024**. Almost **USD 2.4 million** (approximately **40%**) was shared by gg with another actor for further distribution among the rest of the BlackBasta actors who played a role in the attack.

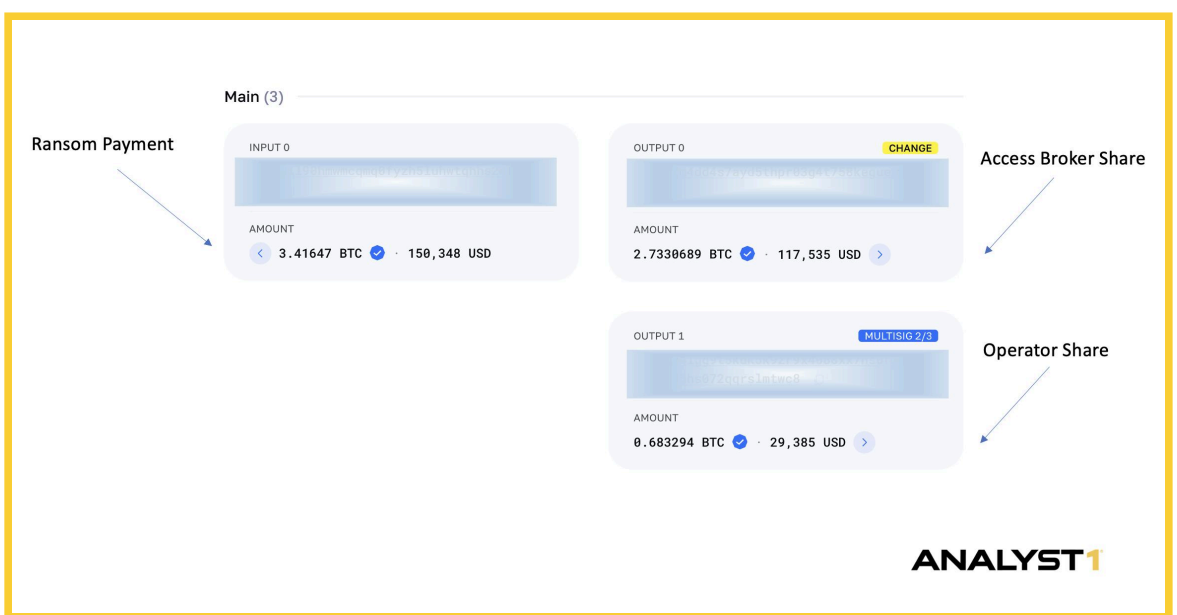


The image displays the distribution of ransom proceeds between gg and other actors, showing that nearly 40% of the total ransom was shared with other actors involved in the attack

Source: Analyst1 through blockchair.com

In three cases where an outside affiliate was involved, gg was not the primary recipient of the ransom payment. Instead, he would receive a 20% share as an operator. The affiliate BlackBasta collaborated with in these cases is an external "partner" who also worked with other ransomware groups. Three notable cases illustrate this pattern, where gg received approximately 20% of the ransom amount:

- **USD 151,323** from **USD 756,624** (~20%)
- **USD 29,385** from **USD 149,715.54** (~20%)
- **USD 20,677** from **USD 98,320** (~20%)



The graph shows the distribution of ransom between BlackBasta Operator and Access Broker in a percentage share of 20%

Source: Analyst1 through blockchair.com

Actor gg is also the one distributing payments for salaries and commissions. From the analysis of cryptocurrency addresses attributed to **tinker**, along with chat logs, they likely receive a salary-based payment in addition to **1%** of each successful extortion, calculated based on the ransom amount received. Based on the investigation, tinker received multiple payments of different amounts. As such, it was identified that on **June 10, 2024**, a payment of **BTC 0.04568111** (equivalent to **USD 3,200.69** at the time of the transaction) was made from the BTC address, which was subsequently attributed to actor **gg**. Another payment of **BTC 0.18682** (equivalent to **USD 8,158.22** at the time of the transaction) was made on **December 20, 2023**, from the BTC address, subsequently attributed to actor gg.

Based on observations of payments received by **yy**, it is likely that the actor operates on a percentage-based compensation model rather than receiving a fixed salary. Various large payments and cryptocurrency addresses associated with yy were identified, with differing amounts and no clear payment schedule. The exact profit share yy receives remains unclear, as payments vary across transactions. In one instance, yy's share was approximately **10%** of the total ransom amount, while in another case, the percentage increased to around **15%**.

According to the investigation, it was identified that on **June 10, 2024**, a payment of **BTC 1.8682** (equivalent to **USD 79,633** at the time of the transaction) was made from the BTC address, which was subsequently attributed to actor **gg**. Another payment was made on **January 15, 2024**, a transfer of **BTC 3.1216** (equivalent to **USD 132,702.64** at the time of the transaction) was made from a BTC address attributed to gg. This payment to yy was identified as ransom proceeds from a ransom payment of **BTC 31.21607443** (equivalent to **USD 1,302,720.14** at the time of the transaction) that a victim made on **January 14, 2024**. The address appeared in chat logs, where **gg** shared it with **tinker** for the purpose of receiving ransom payments from victims. The percentage yy seems to receive as their share of profit is approximately **10%** of the total ransom amount.

In addition to distributing payments, gg was observed assisting other actors with money laundering and cash-out efforts. On **January 2, 2024**, actor **yy** asked **gg** if they could help launder 1 Bitcoin through a mixer. **gg** agreed and provided the BTC address for the transfer, which was to be completed the next day. According to the investigation, it was identified that a payment of **BTC 1**(equivalent to **USD 42,845.23** at the time of the transaction) of cleaned BTC was made on **January 3, 2024**, from the BTC address attributed to gg.

```
timestamp: "2024-01-02 19:50:32",
chat_id: "!kJVcUcyUsQhwBCuIPD:matrix.bestflowers247.online",
sender_alias: "@usernameyy:matrix.bestflowers247.online",
message : "can you help me mix black bitcoin to white bitcoin or white xmr?"


timestamp: "2024-01-02 19:50:54",
chat_id: "!kJVcUcyUsQhwBCuIPD:matrix.bestflowers247.online",
sender_alias: "@usernameyy:matrix.bestflowers247.online",
message : "1 btc I want to clear"


timestamp: "2024-01-03 06:27:37",
chat_id: "!kJVcUcyUsQhwBCuIPD:matrix.bestflowers247.online",
sender_alias: "@usernamegg:matrix.bestflowers247.online",
message : "can be done"
```

The image displays a conversation between yy and gg, where yy requests gg's assistance in laundering BTC through a mixer, to which gg agrees.

Source: Analyst1

Another case involving gg's assistance in cashing out ransom proceeds took place. On **November 30, 2023**, actor **timber** asked gg if they could assist in cashing out 12 million rubles, to which gg agreed. On the same day, timber transferred **BTC 3.4** (equivalent to **USD 128,261.46** at the time of the transaction) to the address provided by gg. The cash-out of ransom proceeds was likely arranged by gg through local illicit services specializing in converting cryptocurrency into cash. In this scheme, cryptocurrency funds would be sent to an exchanger, which often included illicit and darknet market exchanges, for a percentage fee and then delivered to the recipient in hard cash. According to chat logs, at that time, gg exchanged cryptocurrency totaling 50 million rubles, with nearly 12 million rubles to be received by timber.

```
timestamp: "2023-11-30 12:39:52",
chat_id: "!nxLqijVxVyYVFjslfv:matrix.bestflowers247.online",
sender_alias: "@timber:matrix.bestflowers247.online",
message : "Hi. Can you help me exchange bitcoins for cash? While my friend in Moscow will bring some on the weekend"


timestamp: "2023-11-30 12:40:01",
chat_id: "!nxLqijVxVyYVFjslfv:matrix.bestflowers247.online",
sender_alias: "@timber:matrix.bestflowers247.online",
message: "12кк"


timestamp: "2023-11-30 16:05:26",
chat_id: "!nxLqijVxVyYVFjslfv:matrix.bestflowers247.online",
sender_alias: "@usernamegg:matrix.bestflowers247.online",
message : "the courier will bring me 50,000,000 now"


timestamp: "2023-11-30 16:08:51",
chat_id: "!nxLqijVxVyYVFjslfv:matrix.bestflowers247.online",
sender_alias: "@usernamegg:matrix.bestflowers247.online",
message : "11,330,000 rubles to be given to you"
```

The image shows a conversation between gg and timber, where timber requests gg's assistance in cashing out 12 million Rubles, which gg agrees

Source: Analyst1

Conclusion

The leaked BlackBasta chats gave us valuable insights into the group's operations, revealing how they carry out attacks, extort victims, and manage their finances. The leaks exposed key details about how they distribute ransom payments, launder money, and maintain their hierarchy. As the investigation continues, identifying and exposing key actors is crucial to disrupting their operations. Revealing their real identities puts pressure on them, making it harder for them to operate undetected and increasing the chances of arrests and asset seizures.

For now, the BlackBasta data leak site is down, but history shows this won't last long. They still have their resources, hungry for money, and will find new ways to continue their operations. Whether it's under a new name or through alliances with other groups, they are likely to be back. Analyst1 continues tracking BlackBasta and its affiliates and monitoring their activity.


ANALYST1®