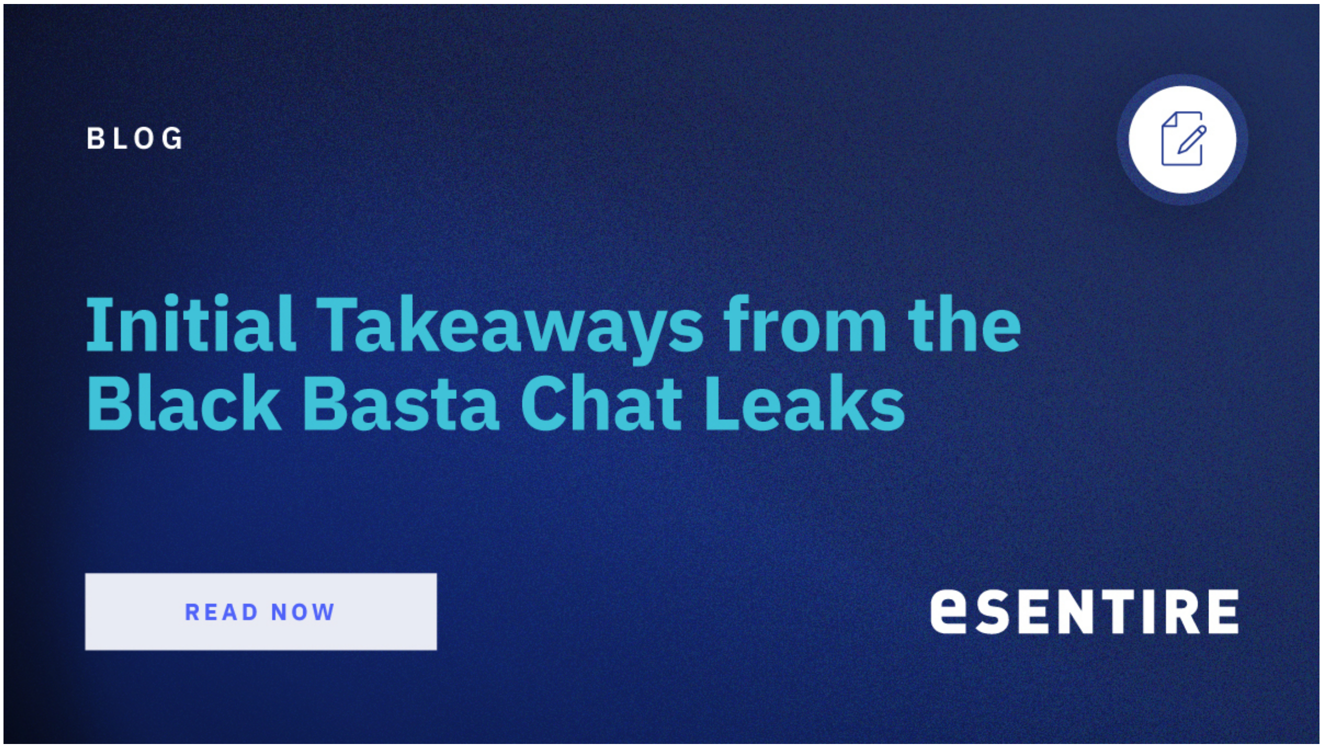
Initial Takeaways from the Black Basta Chat Leaks

esentire.com/blog/initial-takeaways-from-the-black-basta-chat-leaks



Want to learn more on how to achieve Cyber Resilience?

TALK TO AN EXPERT

The Black Basta ransomware group's internal chat logs, leaked on February 11, 2025, consist of nearly 200,000 Russian-language messages spanning September 18, 2023, to September 28, 2024. These logs, exposed by an individual known as "ExploitWhispers", provide a detailed look into the group's operations, internal dynamics, and eventual decline.

The leak is expansive and includes invaluable insight into the group's inner workings, collaborators and payments. It also contains numerous references to business operations and possible entities linked to group members. This blog will focus on several initial takeaways from our analysis of the leak.

Organization Structure of the Black Basta Ransomware Group

Black Basta is a ransomware group that emerged in early 2022 and quickly established itself as a significant cybercriminal operation. It's known for its aggressive double-extortion tactics, where it encrypts victims' data and threatens to leak it unless a ransom is paid. The group primarily targets large organizations across critical sectors like healthcare, manufacturing, government, and financial services, exploiting vulnerabilities in systems or using social engineering to gain access.

Notable Members

- “**GG**” (aka “Tramp”): Key figure/leader in the group. Often referred as “boss”; he is consulted on major decisions throughout many aspects of the operation. Likely previously affiliated/connected with Conti ransomware group.
- “**YY**” (aka “Bio”): Possible administrator with the group, can be seen delegating tasks and performing general administrative actions. May have had a role in developing the initial ransomware tools and infrastructure.
- “**Lapa**”: Likely a technical administrator/coordinator of other members/outside vendors.
- “**Tinker**”: Involved with spam/vishing, data preparation, negotiations, and close associate of “GG”. May have also been affiliated with Conti previously. Has connections with other ransomware groups/operators.
- “**Nickolas**”: Close collaborator with “GG” on the “talks.icu” chat. Appears to take part in attacks, may run a separate team. Often provides insights into cybersecurity trends, tooling which “GG” re-iterates back to his crew.
- **“n3auxaxl”:** Remotedeveloper, possibly reported to “YY” or “NN”. In spring of 2024, “GG” circumvented the chain of command and instructed “**n3auxaxl**”to develop an entirely new ransomware for $100,000 up front.
- **“Ugway”:** Technical operators involved with multiple aspects of the operation from deploying attacks, acquiring credentials, malware etc.

Note, this is not an exhaustive list of actors involved with the operation. A broader in-depth study is needed to fully understand the inner workings of the group and affiliates. It’s worth noting that there are chats throughout the leak suggesting some of the core members of the group may work physically in the same office.

Target Selection and Sensitivities

Black Basta prioritized high-value targets, particularly in sectors like finance, manufacturing, and energy. They leveraged open-source intelligence (OSINT) tools such as ZoomInfo, LinkedIn, and RocketReach to profile organizations, assess their revenue, and identify key employees for social engineering attacks. The leaks revealed 380 unique ZoomInfo links, suggesting at least that many companies were targeted during the leak period.

The chat logs also reveal the group is sensitive to certain targets based several factors, including:

1. Countries where legality of ransom payments are a barrier to payment.

2. Industries such as healthcare which might bring political and law enforcement pressure on the group.
3. Russia and “Friendly Countries”.

In March 2024, user Ugway shared a ZoomInfo link for a pharmacy based in France (presumably where he had a foothold). GG, a leader in the group replies with “*We don’t take those into work…. France doesn’t pay”.*

Presumably this is in reference to specific laws or barriers to getting payments in a prompt manner, thus they appear to avoid those targets (Black Basta had listed several victims based in France prior to this).

In May 2024, group members panicked following widespread media attention of the attack on Ascension. Members were quick to portray the attack as a mistake and frame their subsequent actions (decrypting systems, etc.) as the morally right thing to do.

Does this mean Black Basta avoids any target in the healthcare industry? Likely not.

In one negotiation with a healthcare provider, they explicitly stated the goal was not service disruption, but data extortion:

“We are aware of the current disruptions, from diverted ambulances to cancelled surgery appointments. This wasn't our goal. Our goal was data, which you did not protect and which you will need to pay for.”

Additionally, in the lead up to the Ascension attack in November 2023, GG was presented with access to an associated Catholic healthcare facility and asked, “*Doesn’t it bother you that it’s a church?”* to which he replied “*No*”.

Candid chats between certain members also made it clear leaders and senior members such as GG and Tinker are aware of political fallout from high profile attacks that could bring affect their ability to earn.

A long message from Tinker on May 9th following the Ascension attack highlights this sensitivity, effectively suggesting the attack could bring retaliatory attacks from American authorities which could knock out their systems. He also warned that they could be sanctioned and thus be unable to receive ransom payments.

Then there is the concern with local authorities. A March 2024 conversation between Tinker and GG spells out this concern and the group’s fears of Russian authorities such as the Federal Security Service (FSB).

Tinker: A friend from the second team, who knows I work for you, told me that an agency is looking for you. They have questions about your targeting of ‘friendly countries.’ I’ve known him since around 2021, so I figured it’s better to pass this on to you, just in case. Because times are really restless now, and honestly, because of the Navalny kids, they’re tearing shit up....

And you know yourself – as soon as political shit starts moving, they come to Conti, it was like that before the war already.

The warning alludes to the ongoing political environment in Russian surrounding the death of Alexei Navalny in captivity the month prior. The reference to GG’s knowledge of Conti is also notable. The second team in question is BlackSuit/Royal:

Tinker: The second team is BlackSuit, Royal. The guy is one of their pentesters. I know him as ‘Alpha,’ seems like he’s also ‘Forest.’

The conversation continues, with Tinker revealing the FSB was probing ransomware actors involved in a domestic ransomware attack:

GG: …we don’t target friendly countries at all. We might probe China sometimes but not set it up.
Tinker: He didn’t elaborate much – said ‘we f*** up a friendly country with a locker’ – verbatim.
GG: We don’t touch anyone from friendly countries
Tinker: The agency is the FSB. I know we don’t touch them, if we actually did – I wouldn’t be talking to you about this right now)

These candid conversations demonstrate the awareness core members have with respect to the political environment. It also demonstrates the nexus between the Russian ransomware space and the Russian intelligence services keeping tabs on the Russian ransomware groups.

Mature operators perhaps recognize the key to survival in the ransomware space is a balancing act: on one end maintaining a fearsome reputation with victims and on the other avoiding scrutiny from domestic & foreign authorities. Nobody it seems wants to be the head of the snake. It’s this political awareness that likely led GG to seek a rebranding/rebuild following the attack against Ascension.

Ascension Incident, Backroom Deals and Planned Rebranding

In early May 2024, Ascension suffered a major attack that resulted in disruptions to healthcare services across their network. Media reports, quoting sources briefed on the investigation, tied the attack to the Black Basta group. The leaked chats showed panic among members surrounding the attack, with members worried about repercussions and attention from authorities following reports by CNN and Bleeping Computer.

The incident can possibly be traced to November 2023, when user SS identified an exposed remote access point at an affiliated hospital (based on the naming convention this appears to be a development endpoint left exposed with default credentials). Despite knowing the target was a hospital with religious affiliations, GG pressed forward and enumerated several hundred domain trusts linked to the target.

Based on messages shared, it appears a Kerberoasting attack was used to acquire credential hashes which were then shared back to the group in text files.

Following media publications in May 2024, GG (likely the group's leader) revealed how the team reacted to the attack, including a meeting in "the office" with other group members.

GG:
We set it up before the weekend, accidentally hit healthcare.
There's going to be a hell of an analysis now
I gave them the decryptor yesterday for free and want them to recover faster
I don't want people to suffer
We're pentesters, not murderers
If kids or cancer patients suffer, how am I supposed to live with that!?
No money is worth this
That's why I just held a meeting in the office

They further go on to explain the operational security implications, further showing how concerned the group was with repercussions following such a high-profile attack.

GG:
Said that we're changing everything…
SIM cards
VPS
VPNs
All the servers for work
YY is walking around sad

These revelations were discussed seemingly in private between GG and another individual, @n3auxaxl on the collectionofmanager[.]space Matrix chat. GG went on to propose creating an entirely new operation behind the back of other members, using @n3auxaxl to develop the code:

GG: I have a proposal for you…here's a priority task…Write software…From scratch.
@n3auxaxl: What kind?
GG: But only two people should know about this…You…And…I. No one else. Can't tell anyone.
@n3auxaxl: Yes of course.
GG: Well, you get what kind of software I'm talking about. But take Conti's source code as a basis. BlackBasta will run in parallel, but we'll create new software together.
@n3auxaxl: Got it, understood the task

GG then clarifies this development work will include a leak site (blog), admin panel, chat and builder for the encryption/decryption software. They specifically request the builder be separate from the main server, likely to protect the software from rogue affiliates and law enforcement.

He instructs @n3auxaxl to put aside his other work and focus only on this task. GG then reveals the working conditions:

```
GG: You’ll get a percentage from each of our payouts right away. We’ll start with 5%
of each amount + $100,000 bonus for the software right off the first payout
```

GG then reveals the working conditions with YY, saying *“My YY is getting 10% now, but he’s been with us for 3 years and bought an apartment, a car, launched a few businesses.”*

GG re-iterates this project must not be shared with anyone, including NN (“*Don’t blab to anyone…..NN - don’t say anything*”). Despite the request for secrecy, GG then takes to a chat on the bestflowers247[.]online Matrix chat to inform others of his plan:

```
GG: I talked to the programmer, we’re going to do a rebranding. YY doesn’t need to
know this, the programmer there is much stronger and will make us some badass
software. We need to come up with a name. Basta will keep working for now in
parallel. But after such a f****-up, we need to do a rebranding, or they’ll grab us
by the ***.
```

The incident and subsequent discussions in the leak reveal how GG, a politically savvy and experienced ransomware operator undercut his fellow Black Basta members to advance his interests in the face of possible outside threats from domestic security services.

It’s also a positive sign that law enforcement efforts to disrupt these groups is breeding distrust and paranoia amongst group members forcing them to expend more calories and undermine each other.

Extortion and Negotiation Tactics

Black Basta is a double extortion group, meaning they encrypt systems and steal data, effectively threatening to leak it if extortion payments aren’t made. The leaked chats reveal the group’s call script, used to contact the affected business and pressure them into payment.

The script is in English, with comments in Russian for how to handle specific scenarios (bolded and translated below):

Hello, my name is Eric,

I am calling from the BlackBasta group regarding the recent cybersecurity incident taking place in your company. Can you connect me with your management?

If they connect me:

Our name is BlackBasta Syndicate, and we are the largest, most advanced, and most prolific organized group currently existing. We are the ultimate cyber tradecraft with a credential record of taking down the most advanced, high-profile, and defended companies one can ever imagine. You can Google us later; what you need to know now is that we are business people just like you.

We have your data and encrypted your files, but in less than an hour, we can put things back on track: if you pay for our recovery services, you get a decryptor, the data will be deleted from all of our systems and returned to you, and we will give you a security report explaining how we got you.

We have been trying to get in contact with your team, but I need to talk to the management directly. This is urgent and is about the critical data that we took. Do you know that there is a data breach taking place?

If yes:

If we publish your data, we will not only expose all the ongoing customer and business operations which you are obligated to keep private, but most likely get you under a class action lawsuit yourself. This is why it is important for me to talk to you directly, as we hope that the management will be able to have enough proficiency to address these risks.

If they don’t connect me to management, demand IT or finance instead. As in any scenario, be sure to ask for or note down the name of the person on the other end if they introduce themselves.

If they argue that they can’t connect me:

Your management is the best suited to handle this. If you are not connecting me to them, I will be calling them directly. We have your finance director’s home and personal numbers. We will be calling him and other managers until they respond, and I will make sure to tell them your name and that you were the one who did not connect me to them in a civilized, formal way.

If they say they don’t know about the breach:

We have your data and are ready to publish it. All of it - financial documents, client data, ongoing cases. We began a proper conversation in the designated chat, but you led this to nowhere. I want to reiterate that we have enough files on you to force the firm to dissolve in case we publish the data.

Finally, the call script outlines a series of instructions mixed with threats ranging from legal action to financial penalties.

```
Now I need to convey to you the following seven points:
1. Go back to the chat and begin a proper conversation with us.
2. Do NOT tell us that you cannot pay. We saw your financial records. You CAN pay.
You will need to make sacrifices, but it is more than possible. You know this as you
handle the records.
3. Stop taking this situation as a joke and delegating it to a hired negotiator -
bring yourself or other partners to the chat. This chat is a simple Firefox-based
messenger. The only skill you need to use it is basic English literacy. There is no
reason some random hired person is doing the talks for you.
4. If you keep ignoring us, we will be calling you and your colleagues directly. We
will be calling the supreme council. We will be using personal data against you. This
is not a threat; my management just asked me to inform you of the course of action.
5. We have other means of pressure. Ask your hired negotiators, or do it yourself.
6. There is no way you can shield yourself out of this - you are already in it. Time
to recognize this.
7. My management says that they are not trying to threaten or frighten you. This
applied pressure is only a result of you - not you specifically, but as a company -
trying to abstain from this situation and bringing a hired person to the negotiations
table. They want an honest and equal discussion based on mutual respect. This is why
when you disrespect us and downgrade the level of discussion, we will do the same.
```

The goal of the call script is to identify a direct line to management, and where possible avoid 3rd party IR or ransom negotiators. The statement about using financial records to determine ransom amount is backed up by other internal chats.

For example, in a January 2024 conversation regarding an ongoing extortion negotiation, GG instructs Tinker to analyze the victim’s financial data and drop it in the negotiation chat. GG emphasizes that “*Everything needs to be backed up with solid arguments and clarity”* before instructing Tinker to demand a multi-million-dollar ransom from them.

The chats also show internal deliberations about ransom payment negotiations. The group appears flexible and willing to extend deadlines and negotiate payments.

For victims, having a clear understanding of the scope of the intrusion and subsequent data theft is crucial and provide an upper hand in negotiations. Notably, chat logs show GG has the final say on negotiations, further cementing him as a leader within the group.

Interest in Commercial Cybersecurity and Threat Intelligence Services

The leaked chats show immense interest in testing capabilities of cybersecurity tools, in particular Endpoint Detection and Response products. Group members can be seen discussing “EDR Killers” or bypasses, often linking to Exploit or XSS forum posts for these services. There are also internal discussions about the effectiveness of these bypasses in lab tests, indicating the group had contracted or developed these capabilities.

Group member GG can be seen talking extensively in another chat (talks.icu) with user @Nickolas about a lab environment for testing and training. GG expresses interest in acquiring trial licenses for “*Sentinel, Crowd, Sophos, Cisco, Trend Micro”* using stolen identities.

It’s clear that @Nickolas is someone with cybersecurity industry knowledge of defensive tools and threat intelligence/dark web monitoring services (the pair discuss buying enterprise licenses from one service to augment their credential stuffing attacks).

He can be seen coaching GG on evolving cybersecurity trends such as Multi-Factor Authentication (MFA) adoption, EDR and Managed Detection and Response services telling GG “*MDR is basically the future trend of the cybersecurity industry*… *For small and medium businesses, it’s the only way to protect against attacks."* @Nickolas then suggests exploiting compromised credentials to access networks using remote access services such as VPN.

Elsewhere in the chat, members can be seen sharing leaked credentials from infostealers for threat intelligence services such as VirusTotal and Censys, indicating interest in monitoring their exposure in such tools.

Evolving Initial Access Methods Were a Focus, and Headache

Identification and containment of early-stage ransomware activity is critical to preventing follow-on attacks. The chats show the group would cast a wide net with their campaigns, then sift through footholds looking for high-value targets. This offers defenders a time window to clean up infected endpoints, compromised accounts etc. before they are activated.

Overall, the chats reveal a multitude of initial access methods in line with observed trends throughout the timespan of the leak. These include known exploits, credential stuffing attacks, phishing (including QR code phishing), vishing (via Microsoft Teams and Zoho voice), email bombing, malicious search advertisements, signed installers, etc.

There is also evidence of acquiring access from access brokers, which presents more opportunity to identify and contain before the keys exchange hands.

Our analysis did not find expansive use of sophisticated TTPs or exploits. However, there is evidence of the group sought and exploited 0day and Nday vulnerabilities. For example, in June 2024, Symantec published research describing Black Basta exploiting an elevation of privilege (EoP) vulnerability (CVE-2024-26169) in Windows Error Reporting (WER) Service patched by Microsoft in March 2024. Their analysis identified variants of the exploit tool dating back to February 2024 and December 2023. The leak provides some clues to the group using variants of a WER EoP dating back to November 2023:

1. On November 10, 2023, user YY shared file “WER_Research_07062023.exe” followed by discussion on privilege elevation. It isn’t clear if YY created the file or acquired it.
2. On December 6, 2023, the file is brought up again in reference to an LPE (Local Privilege Escalation).
3. On February 20 2024, user “Chuck” asks GG about his exploit for "Windows win32kbase.sys insecure call to werkernel.sys elevation of privileges vulnerability” and whether he got it from “vulns-rock”.
4. In May 2024 when CVE-2024-26169 was disclosed by Microsoft, YY links the MSRC page in refence to file "WER_Kernel.exe" and tells the group “*It operates the same way as other WER_FAULT vulnerabilities (we had two other similar ones)”. GG clarifies to YY the exploit was created by the “same programmer” (likely referring to a WER EoP exploit already in their possession).*

Elsewhere in the leak, members such as GG commonly shared exploit listings from a correspondent “zdays”, such as this Ivanti Connect Secure RCE listing priced at $200,000:

```
[11:59:39] zdays: __All questions should have the most detailed answers__



# Item name and vulnerable versions list:

Ivanti Connect Secure SSL-VPN Server Pre-Auth RCE

Vulnerable Versions Tested: Latest (22.3R1) + 9.1R12 + 9.1R11 + 9.1R8 + 9.1R7
and probably older

# Webpage of vulnerable item:

https://www.ivanti.com/products/connect-secure-vpn

# Price: 200к
# Affected OS:
# Does this exploit affect the current target version?
Yes
# Targets can be found with google dork/shodan/censys?
Yes. Below shodan query:

http.html:"<script src=\"/dana-na/\""

https://www.shodan.io/search?query=http.html%3A%22%3Cscript+src%3D%5C%22%2Fdana-
na%2F%5C%22%22
# Exploit Type (select all that apply)

[X] Remote code execution

[ ] Privilege escalation
```

The listing appears similar to those shared on 0day [.]today exploit market. It’s not clear whether the group purchased the exploit in this case, however it’s one example of multiple such listings shared in the chat.

This collaboration between group members and outside advisors/vendors is often what allowed the group to adapt to the changing landscape and operationalize emerging tradecraft and exploits sold on forums or shared publicly by offensive security researchers.

One example of this evolution can be found with the groups use of Microsoft Teams. In the fall of 2023, the group began exploring the use of Teams for phishing, specifically delivering payloads such as DarkGate.

They quickly operationalized the idea using TeamsPhisher and TeamsEnum to identify and target accounts. In spring 2024 the tactic evolves to focus on vishing, perhaps inspired by user @nickolas, a collaborator often used by GG in the talks[.]icu chat.

@nickolas: … I was looking yesterday - looking, probably Teams is a pretty good vector for phishing and vishing. You can call and message almost all of them in Teams, but there’s just one problem, if the contact is external, they need to accept it.
GG: I worked Teams a year ago. I was spamming them too. But I didn’t call.
@nickolas: Try it. With Teams, you can also create an account like an IT admin. An admin calls him… And starts loading him up

The group also appeared to have invested heavily into vishing operations in early 2024, likely focused on email bombing. Email bombing is a technique in which a target is bombarded with spam emails then contacted via phone call by a threat actor impersonating IT staff.

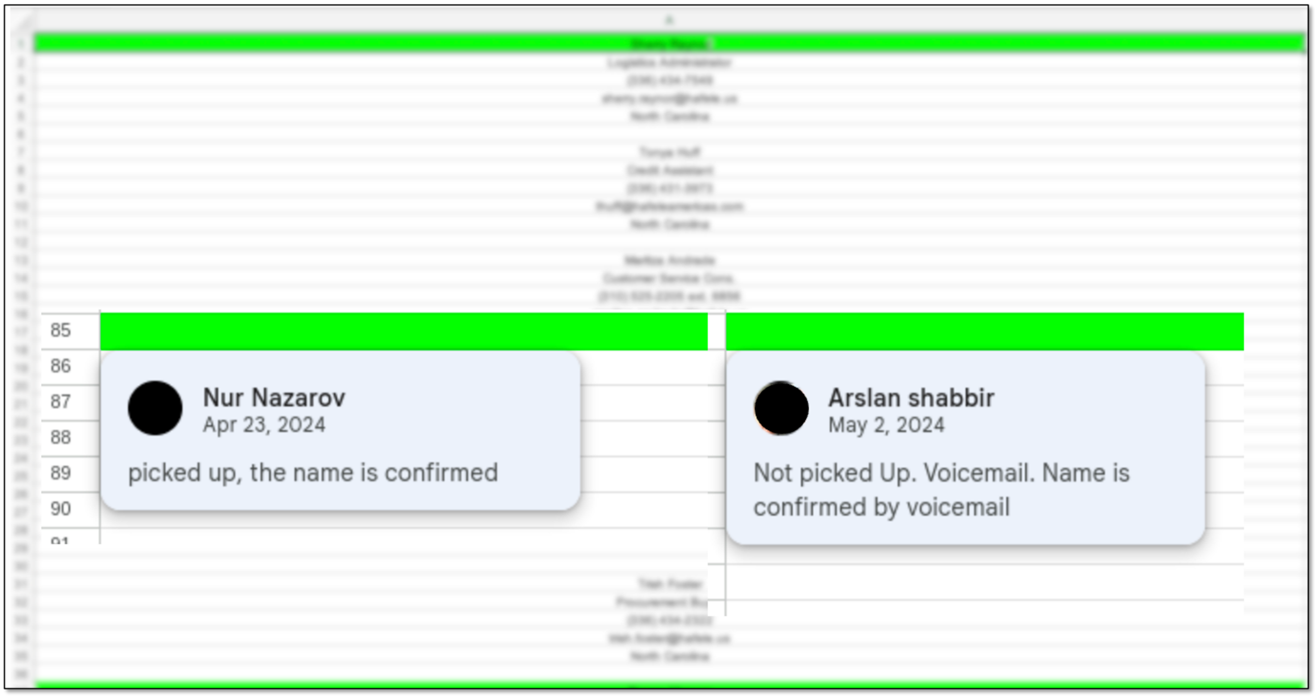
The victim is subsequently coerced into installing remote access software effectively turning their system into a beach head. In May 2024 GG shared Rapid 7’s analysis of Black Basta’s email bombing campaigns and regrettably acknowledged their work had been identified already.

Outsourcing Call Operations

The matrix chat “colorado[.]su” (see Urlscan.io report) included in the leaks offers a glimpse into how the vishing attacks were operationalized. Calls were outsourced to at least two individuals who were instructed to work through a call sheet and impersonate IT staff for 50 cents a call using VOIP services such as Zoho Voice:

Manager361: The first block contains information about the company. The second block lists IT specialists who work there, and you are calling on behalf of one of them. I'll send whom to call now. You didn't call this company, right?
Nurnazarov: No, I haven't called them.
Manager361: *redacted company info*
Manager361: I'll tell you when to call.
Nurnazarov: Ok.
Manager361: Call the first one at 25 minutes.
Nurnazarov: Got it.
Manager361: Call.
Nurnazarov: K*** hung up.
Manager880: Unavailable?
Nurnazarov: "No, I talked to her. After asking about the computer, whether everything was working fine. She hung up, saying 'no'.
Manager880: We heard it. Well, that happens.
Nurnazarov: I was supposed to introduce myself as an employee of ******** right?
Manager361: Yes. IT department.

The handlers provided targets using Google sheets and instructed to record the outcome of the call using an inline comment while following a call script provided by their handlers.



[redacted]

85
86
87
88
89
90

Nur Nazarov
Apr 23, 2024

picked up, the name is confirmed

Arslan shabbir
May 2, 2024

Not picked Up. Voicemail. Name is confirmed by voicemail

The goal of these phone calls isn’t fully clear, but it was likely done to validate active phone numbers and in certain cases conduct social engineering scams in furtherance of email bombing and similar techniques designed to install remote access tools.

Besides outsourcing labor-intensive efforts like vishing, the group made use of contacts and underground service for maintaining operational agility and efficacy.

Underground Connections: Build vs. Buy

The leaked chats make it clear Black Basta operators routinely use or were inspired by cybercrime-as-a-service offerings on underground forums and Telegram. Members can be seen sharing various underground services from malware, loaders, exploits, credential lists, spam lists and initial access auctions. It’s clear underground buys went through GG, who did some basic vetting and testing of samples before authorizing any deals.

Analysis of the chats shows several Malware-as-a-Service (MaaS) families were employed by the group, including DarkGate, PikaBot, Meduza, Lumma and others. For example, in October 2023 GG discusses operationalizing RastaFarEye’s DarkGate loader:

```
GG:
There’s a very cool loader for targeted loading
It’s DarkGate
We’ve got a license paid for 3 months
```

Later, in November 2023 “W” approaches GG with a new stealer they found on Exploit:

```
W: Looks like I found a new stealer.
GG: Which one?
W: hxxps://forum[.]exploit[.]in/topic/226619/?tab=comments#comment-1400316 (Meduza
Stealer). Lifetime $1199.
GG: Good, then take payment details and we’ll start the work.
```

In other cases, group members can be seen debating whether to purchase services vs build their own. In late 2023, group members debated paying the steep cost of BatLoader or FakeBat’s monthly rental (~$5000) for signed loaders, and considered how they could acquire certificates and do it themselves (“*Maybe we should test it [FakeBat]”*).

This is weighed against the cost of extended validation certificates GG purchased from an unnamed source (“*2 from SSL (cloud ones), 1 from Global in a file”*) for 4 or 5 thousand dollars each. In another situation, group members were frustrated with a credential list they were using for attacks. They discussed building a database and spending time to improve the quality of the list before deciding to purchase a new dataset from an underground forum for several thousand dollars.

Group members were keenly aware of the latest trends and capabilities and re-invested extorted funds into R&D or capabilities from cybercrime-as-a-service vendors. The table below contains a non-exhaustive list of these mentions.

Notable Underground Forum and Telegram Mentions

Thread	Title	Note
xss[.]is/threads/111413/	Sentinel One Neutralizer and more	EDR bypass.
xss[.]is/threads/104180/	Domain Admin, USA, ~1k hosts via AD	Access Broker Auction
xss[.]is/threads/107819/	Virustotal enterprise (VT)	Selling access to enterprise Threat Intelligence platform.
xss[.]is/threads/115537/	Domains from $1 In one click! | Auto-connection SSL (CloudFlare) | Monitoring on CT	Infrastructure services.
exploit[.]in/topic/165990/	Bulletproof Servers for a wide range of tasks	Infrastructure Services.

exploit[.]in/topic/202662/	Windows Secure-Websocket HVNC	HVNC product from RastaFarEye (DarkGate).
exploit[.]in/topic/205970/?	Loader for Google/Bing Ads, in .EXE or .MSIX format with Smart Screen/Windows Defender/Chrome bypass + Trojan DanaBot HVNC, Stealer.	BatLoader main thread by Afron.
exploit[.]in/topic/217478/	[RENT] Loader v2.0 - bypass WinDef and Google Alerts + RunPE Nativ\ [RENT] Loader - bypasses WinDef and Google Alerts	FakeBat main thread by EugenFest.
exploit[.]in/topic/220755/	LummaC2 - Stealer, 75-80% knockout, tool for professionals	LummaC2 stealer thread by Shamel.
exploit[.]in/topic/226619/	Meduza Stealer	Meduza Stealer thread by MeduzaCorp
exploit[.]in/topic/230608/	Matanbuchus [SERVICE] Private crypt + private droppers + exe conversion.	Matanbuchus thread by BelialDemon.
exploit[.]in/topic/232123/	Canada RDP corp 20.2$M insurance	Access Auction.
t[.]me/evtokens	N/A	RastaFarEye (DarkGate)
t[.]me/Crypt4U_bot t[.]me/Mavr_MMM	N/A	D3F@ck Loader related Telegram channels/bots.
t[.]me/payk_w t[.]me/spektr234	N/A	FakeBat related Telegram channels.

t[.]me/werbeergroup	N/A	Mail/pass combo list for sale.
t[.]me/evil_proxy	N/A	EvilProxy PhaaS

It’s worth noting that the group extensively shared open-source projects, tools and proof-of-concept code available on sources such as GitHub. In several instances members were chastised for purchasing capabilities from underground forums which were simply wrappers around publicly available exploit PoC or offensive tools.

The takeaway is this: offensive capacities in the public sphere/underground will be adapted by adversaries. As defenders we need to be more agile than our adversaries in operationalizing countermeasures to limit the success of our adversaries.

Black Basta's AI Experiment: Interest, Frustration, and Practical Application

Black Basta members displayed a notable interest in leveraging AI tools for malicious activities, as revealed in their discussions within the chat logs. Initial conversations involved exploring "WormGPT," an uncensored alternative to ChatGPT, with NN expressing a desire to access it. Members like GG actively shared links related to ChatGPT and its applications, including articles about WormGPT, such as the one from `vc[.]ru` (*hxxps://vc[.]ru/chatgpt/761733-wormgpt-alternativa-chatgpt-bez-eticheskih-granic-i-ogranicheniy*), and also suggested searching on forums to find ways to acquire it.

Furthermore, Ugway shared resources related to phishing using ChatGPT and the "hackergpt[.]chat" platform (hxxps://www[.]hackergpt[.]chat/ru). Member Lapa also highlighted ChatGPT's search popularity (hxxps://explodingtopics[.]com/blog/top-google-searches), indicating a general awareness of its widespread use and potential.

Elsewhere in May of 2024, member Tinker explains to GG that he uses LinkedIn to gather targets for spam and vishing. He indicates he’ll use it to automate the process at some point using ChatGPT:

```
Tinker: LinkedIn…the main one. Plus, all the other databases I got for spam…from
other affiliate networks. And then I cross-check via LinkedIn. With the new GPT, it
all gets automated through their open API.
```

Despite exploring these tools, their practical adoption appears varied. While NN sought advice on PowerShell scripts, they also expressed frustration with ChatGPT access suggesting challenges or obstacles in utilizing the AI for some tasks.

In line with this, Ugway also noted GPTchat went crazy in one conversation. However, there is a notable instance of practical application: NN successfully used ChatGPT to quickly generate a plausible "fake letter" after accidentally opening a chat on a connected computer, effectively calming the panicked individual with the AI-generated technical jargon.

This highlights the potential for AI to be used for social engineering and deception within their operations. The chat logs suggest a strategic interest in integrating AI into their toolkit, but the extent of their usage is influenced by factors such as access, knowledge, and the availability of alternative methods.

Closing Thoughts and Recommendations from eSentire's Threat Response Unit (TRU)

The leaked Black Basta chats offer a rare glimpse into the inner workings of a major ransomware operation. This blog scratches the surface, there are still many insights and leads for researchers and law enforcement to dig into.

But how should we think about this as network defenders? One of the biggest takeaways from the leak is the agility with which the group operationalizes new tradecraft.

Members are actively scouring forums and open-source cybersecurity research for new techniques before adopting it themselves or purchasing the capability from partners/vendors.

By and large, the group appeared to exploit low-hanging fruit risks and increasingly focused on social engineering techniques towards the end of the leak.

In eSentire's 2024 Year in Review, 2025 Threat Outlook Report, we highlighted many of these same trends observed across the threat landscape, how we disrupted them and key recommendations for reducing risk. An excerpt of these recommendations can be found below.

Defending Against Initial Access Vectors

- **Phishing and Security Awareness Training (PSAT):** Adopt a PSAT program around browser-based attacks, including social engineering tactics. The training should include exposure to real-world examples, such as:
  - Pikabot– Malvertising, Especially with Google Ads
  - RATS and Infostealers – Free Software / Software Bundles
  - Advanced Persistent Threats - Fake Job Postings
- **Endpoint Coverage:** Ensure good endpoint coverage with Endpoint Detection and Response (EDR) tools to catch User Execution before initial access malware evolves into an intrusion foothold.
- **Network Coverages:** Ensure good network coverage with Network Detection and Response (NDR) solutions to cover Remote Exploitation.

- **Log Coverage:** Exploitation of services run on http servers (like Windows IIS and SSL VPNs) can only be detected with proper logging of the relevant server software.
- **Patch Prioritization:** Know your inventory and prioritize actively exploited vulnerabilities that overlap with your tech stack with a comprehensive Managed Vulnerability Service program.

Defending Against Intrusion Actions

- **Zero Trust:** Practice zero trust using an internal fire wall to impair Lateral Movement. To maintain productivity, make applying for and getting access opened between machines easy.
- **Minimum Permissions:** To impair Privilege Escalation, start all users with the lowest privileges and require access requests as needed. Ensure an expiration method for access and ensure old accounts are being cleaned up.
- **Endpoint Coverage:** To impair Defense Evasion, ensure endpoint coverage on domain controllers, workstations, and servers – anything that can be used as a staging ground for hands-on intruders. Intruders will intentionally use out-of-scope endpoints as staging grounds.
- **Network Coverage:** Ensure internal-to-internal traffic is monitored and configured to alert on signs of lateral movement, credential collection, and command & control beaconing.
- **Log Coverage:** Attackers are more frequently practicing BYOVM – Bring Your Own Virtual Machine in which they register their own machine on the network leveraging valid credentials and hiding in the VPN pool. Because VPN software does not support endpoint monitoring agents, detection and investigation require VPN logging.

Recommendations to Build Resilience Against Ransomware Attacks

- **Anticipate:** Ensure you are continuously assessing, and understanding, your risk exposure and remaining vigilant against sophisticated ransomware threats. Be aware of the risk of cyberattacks, hands-on intruders, and the capability of ransomware groups to lock down systems and leverage stolen data for extortion.
- **Withstand:** Be able to quickly investigate – and react to – an ongoing intrusion, leveraging security telemetry to minimize damage. You should also have alternate processes in place in case critical systems are down.
- **Recover:** Have backups for critical and sensitive systems, processes in place to gracefully transition off backup systems, and keep backup systems in a ready state. Be ready to rebuild domain controllers and servers.
- **Adapt**: Monitor the threat landscape, understand how risks evolve with technology, and reduce unnecessary risks.

To learn how eSentire Next Level MDR can help you build resilience against sophisticated ransomware threats, connect with an eSentire Security Specialist now.

Spence Hutchinson Staff Threat Intelligence Researcher

Spence is a Staff Threat Intelligence Researcher with the Threat Intelligence team. As part of the broader Threat Response Unit, TI is responsible for monitoring the threat landscape and working with fellow TRU members to respond to ongoing threats. Spence graduated with an advanced diploma in Computer Security and Forensics prior to joining eSentire as an analyst in 2013 and has held various analytical, training and leadership roles since.