ANALYST1

Infrastructure in the Shadows: How Two Leaks Unmasked the Criminal Network of Yalishanda aka Media Land, and BlackBasta

by Anastasia Sentsova

Background:

From BlackBasta to Media Land - The Leak That Triggered the Chain Reaction

The interesting thing about cybercrime is that, sooner or later, the names behind those who commit it are going to come out. Often, unraveling starts from the inside, with actors turning on each other, or someone close enough to do real harm.

In February 2025, an unknown individual under the moniker **ExploitWhispers** emerged on Telegram and leaked BlackBasta's internal chats from the Matrix messenger. The dump came in the form of a JSON file containing roughly 200,000 messages spanning from September 18, 2023, to September 28, 2024. The leak also revealed several names, including **Kirill Zatolokin** (aka Slim Shady).

Amidst the flood of accusations, chat dumps, and exposed actors, another entity came into focus: **Media Land**. Shortly after the first leak, on March 28, 2025, an unknown actor followed up with another data dump, this time revealing a database tied to Media Land's internal operations. The leak contained detailed records including server configurations, client purchase history, user account data, and associated cryptocurrency addresses. That raised the obvious question: what would a "legit" Russian business be doing entangled in cybercrime? The answer was as "shocking" as it was telling — Media Land is tightly connected to the cybercriminal service **Yalishanda**.

Yalishanda, operating since approximately late 2009, is a long-standing bulletproof hosting provider with deep roots in the cybercrime ecosystem. The thing about Russian cybercrime, you know, is that it's deeply interconnected, not just within a specific activity like ransomware, but across the entire infrastructure that supports it. It's a multi-layered structure: protection, cover, infrastructure, fronts that sometimes appear legitimate, all woven into a chaotic web that only begins to make sense when you start pulling the right threads.

These two leaks gave us a rare and extremely useful look into how Russian-speaking ransomware groups work closely with bulletproof hosting providers. The two leaks are connected because Media Land, also known by its underground name Yalishanda, provided the actual infrastructure and support that BlackBasta relied on to run its ransomware operations.

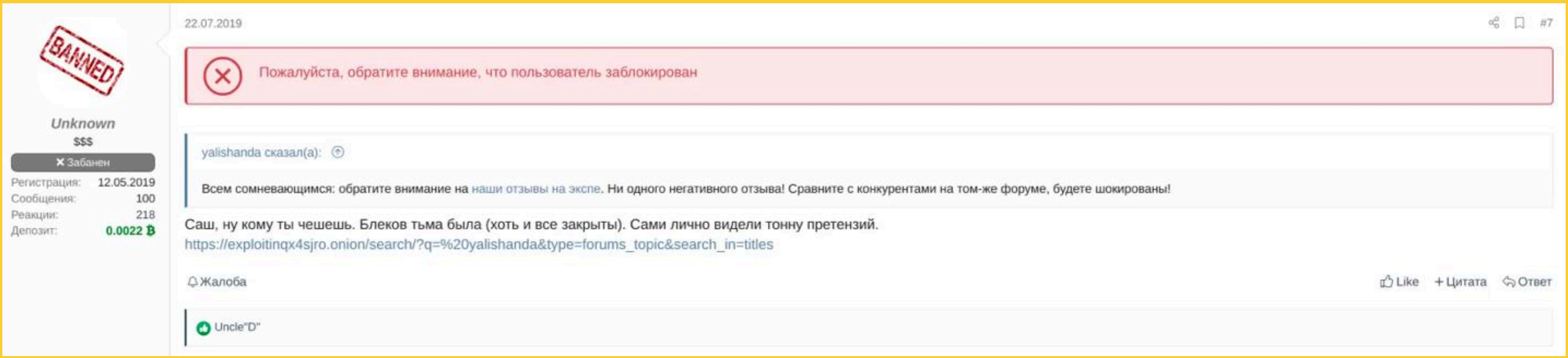
It also created an opportunity for regulatory bodies to take action. On November 19, 2025, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), in coordination with Australia and the United Kingdom, announced sanctions against Media Land and its subsidiary, Data Center Kirishi. Two individuals tied to Media Land were specifically named. One was Aleksandr Volosovik, the company's general director, better known in cybercriminal forums as "Yalishanda," who marketed the company's infrastructure to threat actors. The other, a now-familiar name, was Kirill Zatolokin, who was sanctioned for playing a direct role in Media Land's support of cybercrime operations.
In this research, we'll go back and uncover the actors behind it as well as insights into their operations, tracing all the way through to the movement of cryptocurrency and the payment flows that connect these individuals to broader criminal groups. Behind every alias is a name, and behind every service — a story. Let's dig.

Volosovik & Zatolokin (aka 'Slim Shady') — 'Please Stand Up! The Court Is Now in Session...'

The moment Aleksandr Volosovik's name appeared on international sanctions lists, it probably didn't come as a shock to him. That level of attention was coming for a while. As early as 2019, Brian Krebs publicly named him in an investigation into the Yalishanda infrastructure, calling Volosovik its primary operator. According to Krebs, Volosovik had been in the game for about a decade already by then.

Even in Russian-speaking cybercrime underground circles, Volosovik was occasionally referenced by his real name. **"Sasha, who are you lying to? There's been a lot of arbitration (although they're all closed now). We saw those complaints ourselves,"** wrote a user known as **Unknown**, a prominent REvil member, on July 22, 2019. That kind of callout doesn't happen unless the community knows your name and, more importantly, has history with it.

*Author's Note: Sasha is a diminutive form of Aleksander.



Unknown
$$$
✕ Забанен

Регистрация:	12.05.2019
Сообщения:	100
Реакции:	218
Депозит:	0.0022 Ƀ

22.07.2019 #7

Пожалуйста, обратите внимание, что пользователь заблокирован

yalishanda сказал(а):

Всем сомневающимся: обратите внимание на наши отзывы на экспе. Ни одного негативного отзыва! Сравните с конкурентами на том-же форуме, будете шокированы!

Саш, ну кому ты чешешь. Блеков тьма была (хоть и все закрыты). Сами лично видели тонну претензий.
https://exploitinqx4sjro.onion/search/?q=%20yalishanda&type=forums_topic&search_in=titles

Figure 1: REvil member using the moniker **Unknown** engaged in a conversation with a Yalishanda representative, referring to him by his real name, **Sasha**
Source: XSS Forum

One particularly valuable detail uncovered in Krebs' reporting was a scan of Volosovik's international passport. Not the standard internal passport issued to Russian citizens for domestic use; this was a foreign-travel document, carrying greater weight and reach. But it wasn't just the format that mattered; it was what the passport said.

Volosovik was born on January 30, 1983, and according to the document, his place of birth was listed as Ukraine. We dug further. In the course of our investigation, we found a VKontakte profile strongly believed to belong to him. On it, his hometown is listed as Brovary (Rus: **Бровары**), a city in Kyiv Oblast, northern Ukraine. This alone strongly suggests he was born in Brovary, but at some point, likely in early childhood, he or his family relocated to Russia, where he eventually obtained Russian citizenship.

His VK profile also gives us a critical insight into the timing of that move. According to the education history posted there, Volosovik attended School No. 80 in Vladivostok from 1990 to 2000, starting around age 7, consistent with the typical school entry age in Russia. That detail narrows down the window: he must have moved from Ukraine to Russia sometime between 1983 and 1990, most likely with his family. The relocation occurred early enough that he completed his entire formal education in Russia.

After finishing secondary school, Volosovik enrolled in the Far Eastern State Technical University (Rus: ДВГТУ, formerly ДВПИ им. В. В. Куйбышева). He entered the Institute of Mechanics, Automation, and Advanced Technologies, specializing in Automated Production Systems in Mechanical Engineering, and graduated in 2005.

Krebs estimates that Volosovik's criminal involvement began in the late 2000s. If we use 2009 as a benchmark, Volosovik would have been 26 years old, freshly out of university, and at the perfect moment to either enter the professional workforce or, in his case, start his cybercriminal career.

That timing fits. It was a period when the cybercrime economy was professionalizing: Malware-as-a-Service was emerging, ransomware was evolving rapidly, and bulletproof hosting providers were becoming key components of the underground backbone. Volosovik didn't just adapt to this shift; he helped build its foundation.

One revealing detail from Volosovik's VK profile, and a sharp glimpse into his mindset, was his status message, a feature that lets users share whatever's on their mind. At some point, likely around 2023, Volosovik set his status to the following:

"Actions always outweigh words. Someone can yell at you for two hours — and still be there when you need them. Or whisper sweetly for two years — only to betray you."
(Rus: "Поступок всегда важнее слов. Человек способен орать два часа — и помочь. Или два года сюсюкать — и предать.")

What a sentiment. Bitterness. Caution. It reads like something written by someone who's been burned more than once. By that point, Volosovik had likely spent over 15 years inside the cybercriminal ecosystem. A career that long, in a world built on mistrust and money, doesn't just bring status and payouts; it brings pressure, enemies, shifting alliances, and yes, probably plenty of knives in the back.

Another interesting detail appears at the bottom of the passport: the issuing authority listed is the Russian Embassy in China. Why on earth would China be involved in issuing this document to Volosovik? Because China was reportedly a country where he spent considerable time, and because Beijing, home to the Russian Embassy, issued his passport. And that small line turns out to be one of the most important clues in understanding the geography and other connections of Volosovik's activity.

On the surface, it makes sense. The city of Vladivostok, where Volosovik studied and grew up, lies in Russia's Far East, geographically closer to Beijing than to Moscow. Students from Vladivostok frequently participate in cross-border educational exchanges, business trips, or simply travel to China due to the region's logistical convenience and longstanding cultural and economic ties. While we don't know exactly what first brought Volosovik to China, it's clear that by a certain point, traveling there had become routine for him.

Just below is a photo of Volosovik, posted initially on Odnoklassniki, a Russian social media platform. The image is identifiable based on a visible watermark in the bottom corner. It surfaced again later via a VKontakte profile, though not one registered under Volosovik's own name; it was likely the account of a friend or acquaintance. In the image, Volosovik appears to be standing in what looks like a Chinese street market.

Based on the timestamp, the photo was likely taken around 2016. When viewed alongside the passport issuance data dated June 18, 2010, and the embassy location, this image becomes part of a growing trail of indicators suggesting that Volosovik not only traveled to China but may have used it as an operational or logistical hub during that phase of his cybercriminal career.

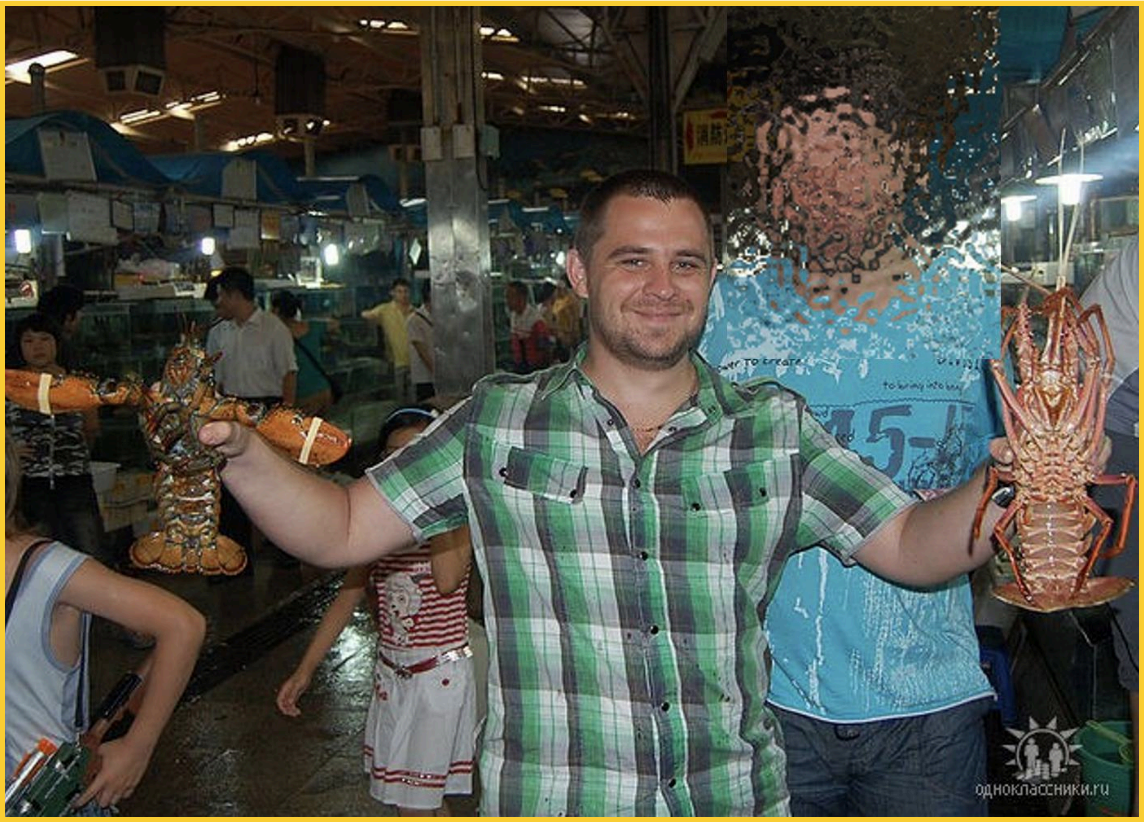


Figure 2: Photo showing Volosovik standing in a Chinese market alongside a person believed to be one of his acquaintances, whose face has been blurred for privacy reasons
Source: VKontakte

China and Vladivostok emerge not just as recurring geographic references in the story of Media Land, aka Yalishanda, but also as the critical intersection where Aleksandr Volosovik and another sanctioned actor, Kirill Zatolokin, appear to have crossed paths.

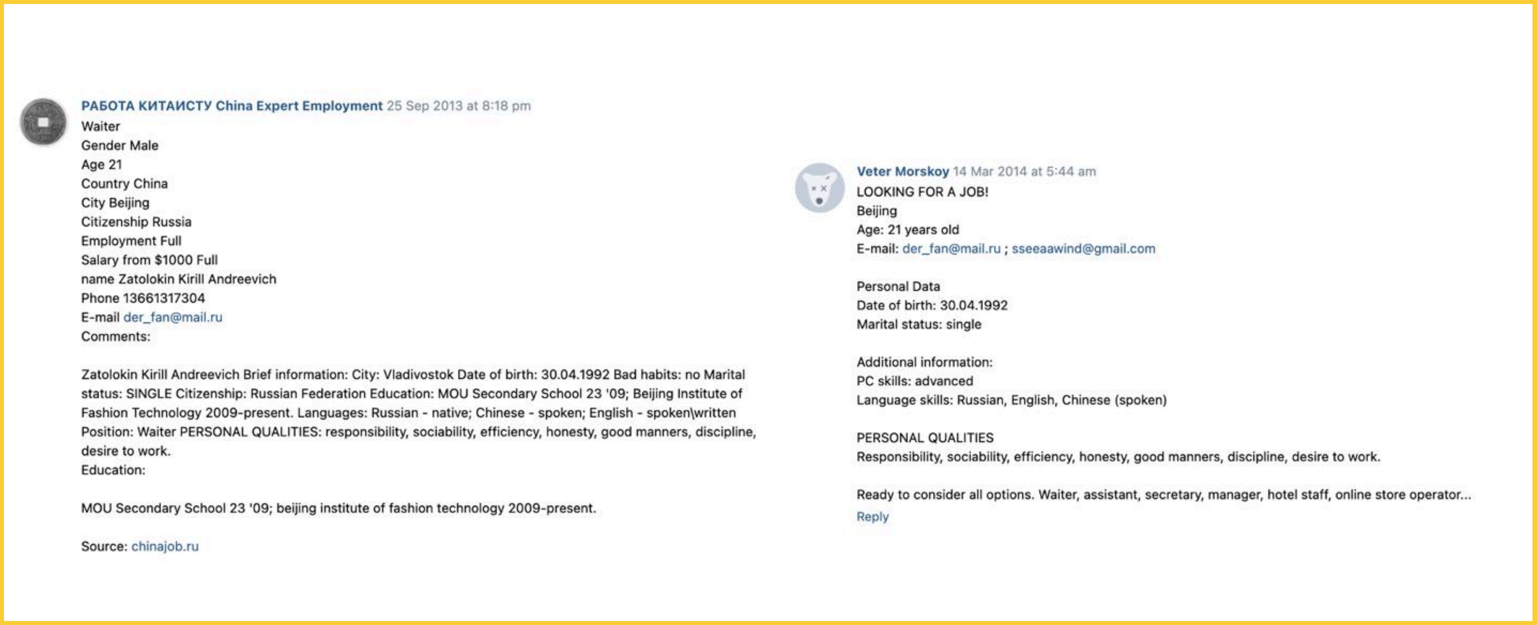
Unlike Volosovik, whose name was exposed through major investigative reporting, Zatolokin remained in the shadows until recently. But while their roles and visibility differ, the trail reveals several compelling links between them.

Both men lived in Vladivostok, and both spent time in Beijing, China, a rare overlap that suggests a potential meeting point. While the exact moment Zatolokin entered Volosovik's orbit remains unclear, investigative findings indicate it likely occurred no earlier than May 2014.

According to the investigation, Kirill Zatolokin posted on VKontakte on September 25, 2013, responding to job board threads for those seeking work in China. In that message, he stated he was looking for a waiter position and openly listed a surprising amount of personal information: his full name (Kirill Andreevich Zatolokin), his age at the time (21), his email address (der_fan@mail[.]ru), and even a China-based phone number (13661317304) and education history. He also described his language abilities, noting that in addition to his native Russian, he spoke conversational Chinese and conversational/written English.

Zatolokin's timeline lines up clearly. He graduated from School No. 23 (Rus: МОУ СОШ 23) in Vladivostok in 2009 and immediately enrolled in the Beijing Institute of Fashion Technology, listing his enrollment as ongoing from 2009 to the present. By 2013, four years into his stay, he was actively seeking work locally. Taken together, the post leaves little room for doubt: Zatolokin was physically in Beijing, actively looking for employment, engaged in day-to-day local life, not simply a student enrolled on paper or someone passing through.

Then, on March 14, 2014, he resurfaced in another post, this time revealing even more personal details. He included his full date of birth, April 30, 1992, and used the same email from the previous post (der_fan@mail[.]ru), while also adding a new one sseeaawind@gmail[.]com. In the description of a job he was looking for, he stated his flexibility: "Ready to consider all options including waiter, assistant, secretary, manager, hotel staff, online store operator."



РАБОТА КИТАИСТУ China Expert Employment 25 Sep 2013 at 8:18 pm
Waiter
Gender Male
Age 21
Country China
City Beijing
Citizenship Russia
Employment Full
Salary from $1000 Full
name Zatolokin Kirill Andreevich
Phone 13661317304
E-mail der_fan@mail.ru
Comments:

Zatolokin Kirill Andreevich Brief information: City: Vladivostok Date of birth: 30.04.1992 Bad habits: no Marital status: SINGLE Citizenship: Russian Federation Education: MOU Secondary School 23 '09; Beijing Institute of Fashion Technology 2009-present. Languages: Russian - native; Chinese - spoken; English - spoken\written Position: Waiter PERSONAL QUALITIES: responsibility, sociability, efficiency, honesty, good manners, discipline, desire to work.
Education:

MOU Secondary School 23 '09; beijing institute of fashion technology 2009-present.

Source: chinajob.ru

Veter Morskoy 14 Mar 2014 at 5:44 am
LOOKING FOR A JOB!
Beijing
Age: 21 years old
E-mail: der_fan@mail.ru ; sseeaawind@gmail.com

Personal Data
Date of birth: 30.04.1992
Marital status: single

Additional information:
PC skills: advanced
Language skills: Russian, English, Chinese (spoken)

PERSONAL QUALITIES
Responsibility, sociability, efficiency, honesty, good manners, discipline, desire to work.

Ready to consider all options. Waiter, assistant, secretary, manager, hotel staff, online store operator...
Reply

Figure 3: Job ads posted by Zatolokin on VKontakte seeking work in China, in which he provided personal information
Source: VKontakte

That last line, "online store operator," stands out. Because that's precisely the kind of role Zatolokin would go on to fill inside Media Land, aka Yalishanda, the so-called infrastructure front that was anything but innocent. Yalishanda wasn't just a hosting service. It was a storefront, polished enough to pass for legitimate, durable enough to shelter ransomware syndicates like BlackBasta. And behind that counter? It wasn't just Volosovik running the show. This is where Zatolokin, who turned himself into "Slim Shady", stepped into position, handling infrastructure and quietly keeping the criminal machine humming along.

We will further explore Zatolokin's role in BlackBasta's operations, but first, a quick tour through Media Land, aka Yalishanda's life in the underground.

Media Land, aka Yalishanda: Hosting You Can’t Complain About (Literally)

The history of Yalishanda and its whitewashed shell, Media Land, is one of the more compelling case studies in Russian-speaking cybercrime. The deeper you dig, the more obvious it becomes that running a “legit” business makes perfect sense, especially when the underground one is scaling like Yalishanda was.

When Media Land LLC was officially registered in October 2015 by Aleksandr Volosovik, the Yalishanda empire was already flourishing, and its brand was well-known across cybercriminal forums. Starting operations as early as 2009, Yalishanda quickly became a go-to service in the criminal ecosystem. Bulletproof hosting (BPH) providers like Yalishanda thrive on one core promise: we don’t care who complains. Yalishanda didn’t just offer server space; it provided a full-stack service for cybercriminals: hosting, technical support, domain registration, and abuse resistance all in one. That makes them ideal for ransomware operators, info stealers, and initial access brokers (IABs).

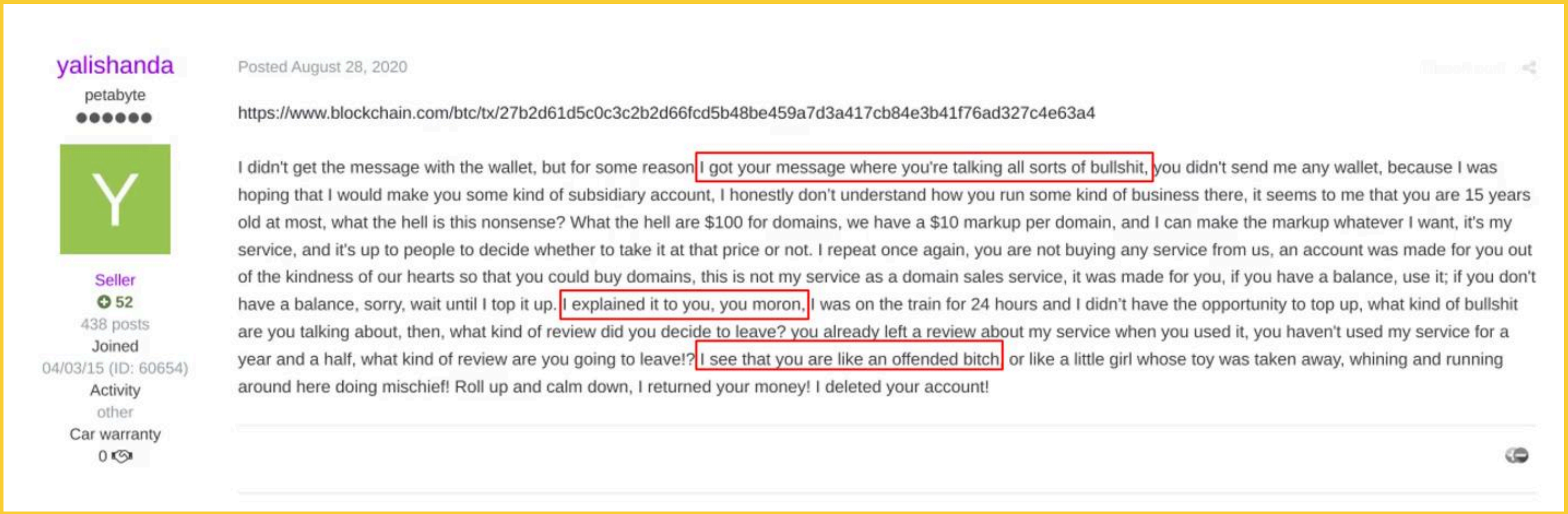
So... where do you find the clients for a service like Yalishanda? Well, of course, on the usual hangouts: shady Dark Web forums like **Exploit** or **XSS**. That’s where Yalishanda set up shop, pitching itself as the “seller,” complete with promises of reliability and protection.

Offering first-class services, the customer support was handled, how to say it, in a **wery roossian styel**, blunt and direct. One time, when someone dared to complain, in what is known in cybercrime forums as “arbitrage”, things got spicy.

On **August 27, 2020**, a user named Loadbaks filed a complaint claiming Yalishanda didn’t deliver the service he paid for. He even dropped a BTC address **1PY4JX82rhKTSyP7ywhJgiYeVvTcpcaW8d** and asked for a refund of **$222.89**, to be exact.

Yalishanda refunded him. But not with a soft apology and thank-you-for-your-patience. No. They dropped a cold blockchain receipt, transaction hash **27b2d61d5c0c3c2b2d66fcd5b48be459a7d3a417cb84e3b41f76ad327c4e63a4** and followed it up with a message that could be paraphrased as: “No service? Fine. Here’s your money back. Now shut up.”

No charm. No smoothing things over. Just raw, post-Soviet tech support energy. For investigators, though? It was a goldmine. These moments offer behavioral fingerprints, wallet addresses, and above all, insight into how these underground businesses operate when they think no one’s watching.



yalishanda
petabyte
●●●●●●

Seller
52
438 posts
Joined
04/03/15 (ID: 60654)
Activity
other
Car warranty
0

Posted August 28, 2020

https://www.blockchain.com/btc/tx/27b2d61d5c0c3c2b2d66fcd5b48be459a7d3a417cb84e3b41f76ad327c4e63a4

I didn't get the message with the wallet, but for some reason I got your message where you're talking all sorts of bullshit, you didn't send me any wallet, because I was hoping that I would make you some kind of subsidiary account, I honestly don't understand how you run some kind of business there, it seems to me that you are 15 years old at most, what the hell is this nonsense? What the hell are $100 for domains, we have a $10 markup per domain, and I can make the markup whatever I want, it's my service, and it's up to people to decide whether to take it at that price or not. I repeat once again, you are not buying any service from us, an account was made for you out of the kindness of our hearts so that you could buy domains, this is not my service as a domain sales service, it was made for you, if you have a balance, use it; if you don't have a balance, sorry, wait until I top it up. I explained it to you, you moron, I was on the train for 24 hours and I didn't have the opportunity to top up, what kind of bullshit are you talking about, then, what kind of review did you decide to leave? you already left a review about my service when you used it, you haven't used my service for a year and a half, what kind of review are you going to leave!? I see that you are like an offended bitch or like a little girl whose toy was taken away, whining and running around here doing mischief! Roll up and calm down, I returned your money! I deleted your account!

Figure 4: A Yalishanda actor responded directly to a service complaint filed by a user, offering insight into how the organization handled customer support disputes in underground forums
Source: Exploit Forum

Opening a legitimate company was likely a strategic move to gain surface-level credibility, the kind of legitimacy a ".onion" address simply can't provide. Interestingly, the company was incorporated in St. Petersburg, suggesting that Aleksandr Volosovik relocated from Vladivostok at some point, possibly to scale operations or establish closer ties with hosting providers, financial intermediaries, and infrastructure partners. A registered entity like Media Land allowed them to conduct various activities that require at least a façade of legitimacy, from signing contracts and leasing IP ranges to launching spin-off ventures such as Data Center Kirishi, which was registered in July 2022 and later sanctioned as part of the same criminal infrastructure network.

Having a legit company also lets you give employees a sense of protection, like, "Hey, it's just hosting, nothing shady here." That's what made it possible for employees like **Kirill Zatolokin**, aka Slim Shady, to step in. In the official sanctions announcement, an image appears to show Zatolokin standing in what looks like a Media Land office, wearing a company T-shirt with the logo front and center. A truly special moment in the research, when you finally get to put a face to the moniker.

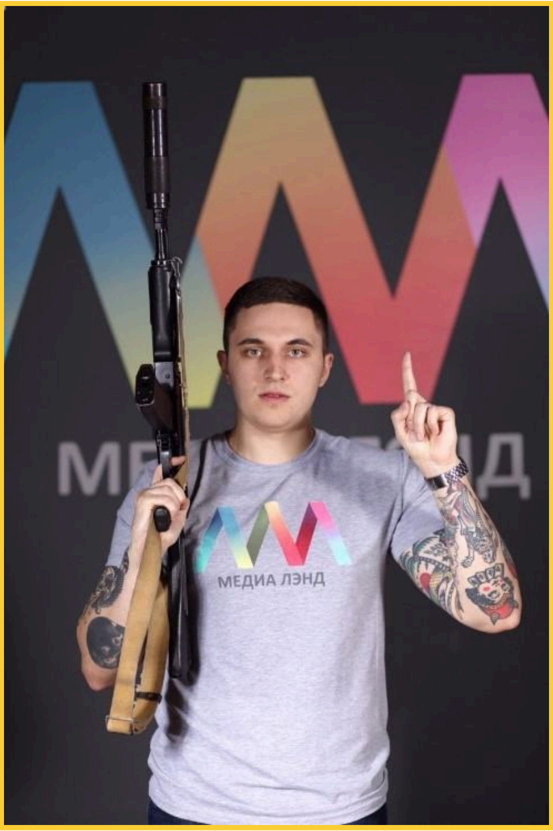
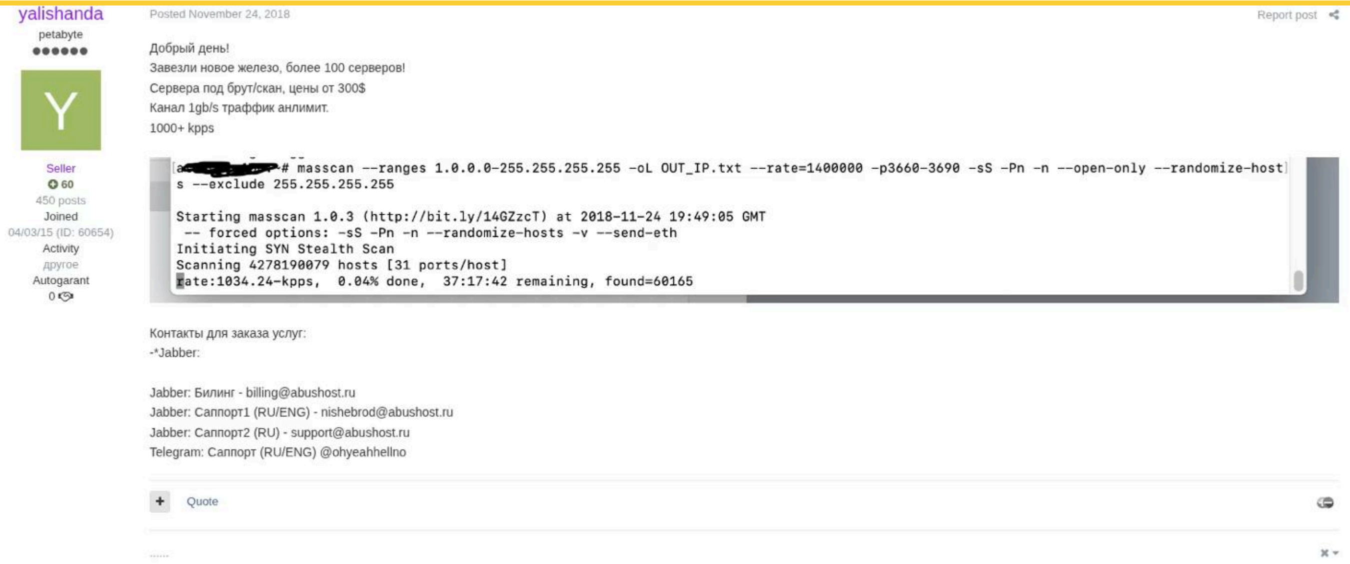


Figure 5: A photo of Kirill Zatolokin, posted alongside the sanctions announcement, shows him standing in what appears to be a Media Land corporate office
Source: DOJ

While busy with his day job, Zatolokin stayed even busier with his second: running customer support operations under Yalishanda's shadow infrastructure brand. Over the years, Yalishanda used multiple communication accounts to support clients, but one Telegram account, **@ohyehhellno**, was used directly by Zatolokin. This account, alongside the usual Jabber contacts, was repeatedly listed in Yalishanda's advertisements and forum posts across cybercriminal marketplaces such as **XSS** and **Exploit**.



Posted November 24, 2018

Добрый день!
Завезли новое железо, более 100 серверов!
Сервера под брут/скан, цены от 300$
Канал 1gb/s траффик анлимит.
1000+ kpps

```
[a[redacted]# masscan --ranges 1.0.0.0-255.255.255.255 -oL OUT_IP.txt --rate=1400000 -p3660-3690 -sS -Pn -n --open-only --randomize-host]
s --exclude 255.255.255.255

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2018-11-24 19:49:05 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 4278190079 hosts [31 ports/host]
rate:1034.24-kpps,  0.04% done,  37:17:42 remaining, found=60165
```

Контакты для заказа услуг:
-*Jabber:

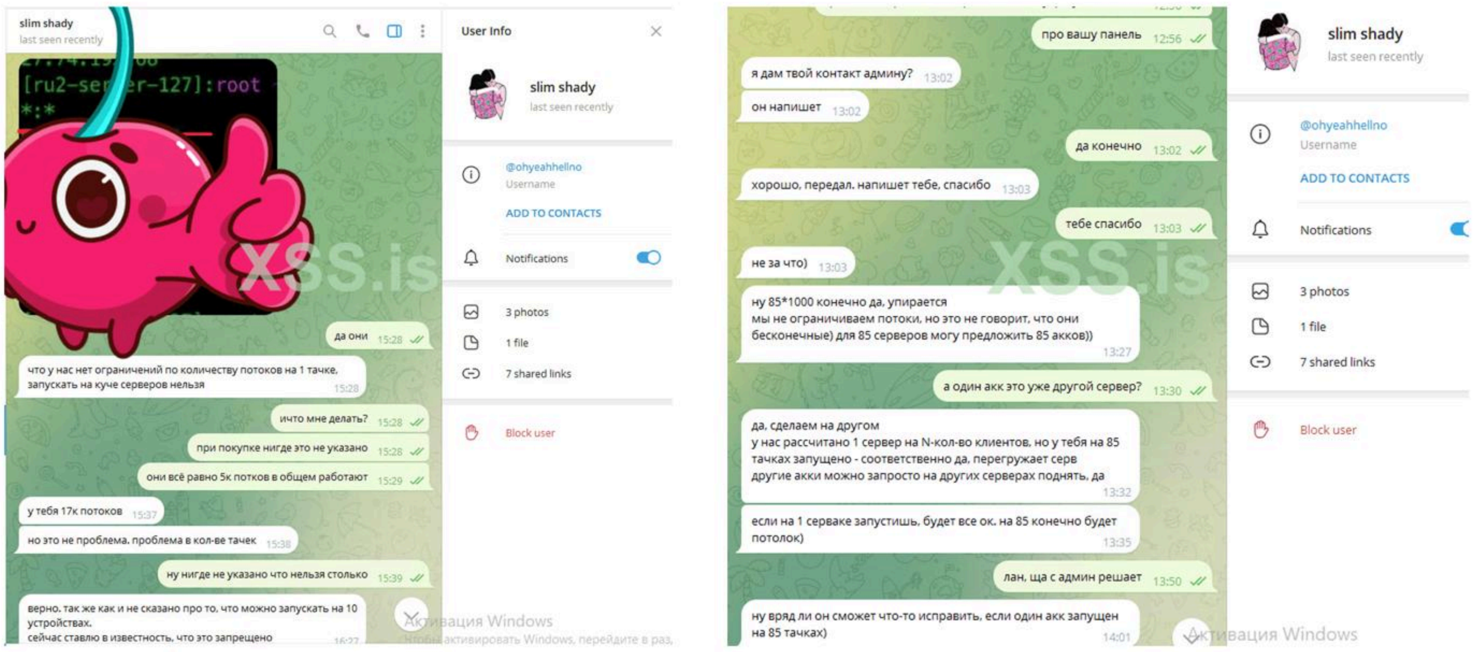
Jabber: Билинг - billing@abushost.ru
Jabber: Саппорт1 (RU/ENG) - nishebrod@abushost.ru
Jabber: Саппорт2 (RU) - support@abushost.ru
Telegram: Саппорт (RU/ENG) @ohyeahhellno

Figure 6: Post shows early promotion of Yalishanda services on a dark web forum. This is where the first mentions of the Telegram handle @ohyehhellno, used by Zatolokin, were observed.
Source: Explot Forum

Mentions of the Telegram account **@ohyehhellno** go back as far as November 2018, which suggests that **Kirill Zatolokin** may have been active in Yalishanda's operations from at least that date. Dark-web forum observations give us a glimpse into his role. Compared with previously observed Yalishanda account behavior, the support provided under this handle appears significantly more professional and hands-on.

In one case, a screenshot of a support chat was shared on the forum XSS by a user. It shows a frustrated customer complaining about performance issues: the customer was running 17,000 threads across 85 machines, which overwhelmed the backend.

ohyehhellno (Zatolokin) responded by clarifying that although there was no strict limit on threads per machine, spreading operations over so many servers violated internal policy, even if that policy had never been clearly documented for clients. His proposed solution was either to move the workload to another server or to divide it across multiple accounts.



slim shady — @ohyeahhellno — Username

да они 15:28
что у нас нет ограничений по количеству потоков на 1 тачке, запускать на куче серверов нельзя 15:28
ичто мне делать? 15:28
при покупке нигде это не указано 15:28
они всё равно 5к потков в общем работают 15:29
у тебя 17к потоков 15:37
но это не проблема. проблема в кол-ве тачек 15:38
ну нигде не указано что нельзя столько 15:39
верно. так же как и не сказано про то, что можно запускать на 10 устройствах.
сейчас ставлю в известность, что это запрещено 16:27

про вашу панель 12:56
я дам твой контакт админу? 13:02
он напишет 13:02
да конечно 13:02
хорошо, передал. напишет тебе, спасибо 13:03
тебе спасибо 13:03
не за что) 13:03
ну 85*1000 конечно да, упирается
мы не ограничиваем потоки, но это не говорит, что они бесконечные) для 85 серверов могу предложить 85 акков)) 13:27
а один акк это уже другой сервер? 13:30
да, сделаем на другом
у нас рассчитано 1 сервер на N-кол-во клиентов, но у тебя на 85 тачках запущено - соответственно да, перегружает серв
другие акки можно запросто на других серверах поднять, да 13:32
если на 1 серваке запустишь, будет все ок. на 85 конечно будет потолок) 13:35
лан, ща с админ решает 13:50
ну вряд ли он сможет что-то исправить, если один акк запущен на 85 тачках) 14:01

Figure 7: Screenshots shared by a forum user show a message exchange with Yalishanda's customer service, handled by Zatolokin via his Telegram account.
Source: XSS

The screenshot clearly displayed both the Telegram handle @ohyehhellno and the account name "Slim Shady." This matches the alias used by the anonymous source who leaked the BlackBasta chats, where the Slim Shady moniker also appeared frequently.

Zatolokin, or SlimShady, played a dual role: he not only provided customer support for Yalishanda's infrastructure services, but also acted as a key bridge between Media Land and BlackBasta, one of the most active ransomware syndicates operating at the time.

We'll break down that connection in the next section. It wasn't just a collaboration; it was a full-blown infrastructure fusion, a match made in ransomware heaven... or more accurately, infrastructure hell.

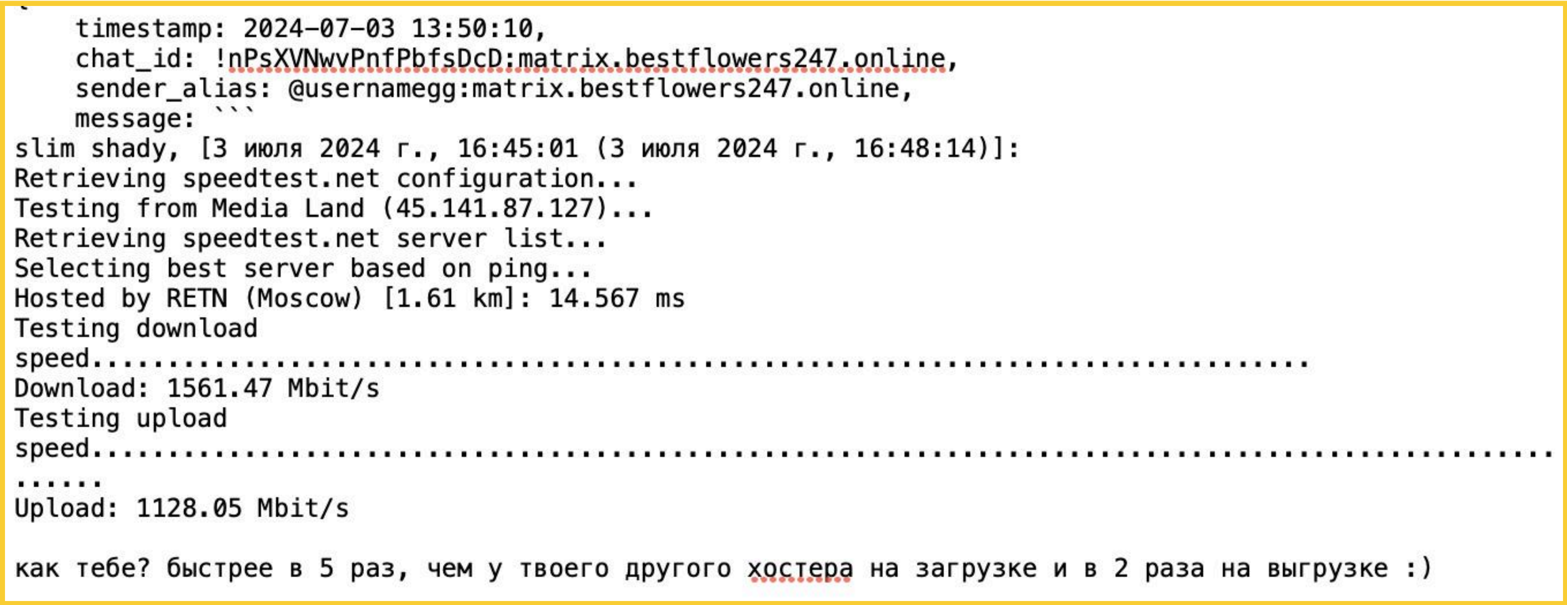
Media Land aka Yalishanda & BlackBasta: A Match Made in Infrastructure Hell

The Slim Shady moniker appeared quite frequently in the leaked BlackBasta chats. Although he did not participate directly in the group discussions, he was often referred to by “gg,” one of BlackBasta’s core operators (likely an alias for Oleg Nefedov, as examined earlier research).

References to Slim Shady regularly surfaced in gg’s chats with the actor known as lapa, who was identified as being responsible for managing key parts of BlackBasta’s infrastructure. Some of lapa’s specific activities will be examined later in this section. Although the anonymous source behind the leak mentioned his possible real identity, we have chosen not to publish it pending further confirmation from official law enforcement channels.

Judging by the tone and frequency of those references, Slim Shady served as a technical and logistical point of contact, relaying backend updates and infrastructure metrics, including bandwidth performance from Media Land servers.

In one conversation, gg forwards a message from Slim Shady showing a speed test result for IP 45.141.87.127, part of Media Land’s network. Slim Shady boasts in the message: “How’s that? 5x faster than your other hoster on downloads and 2x faster on uploads :)”



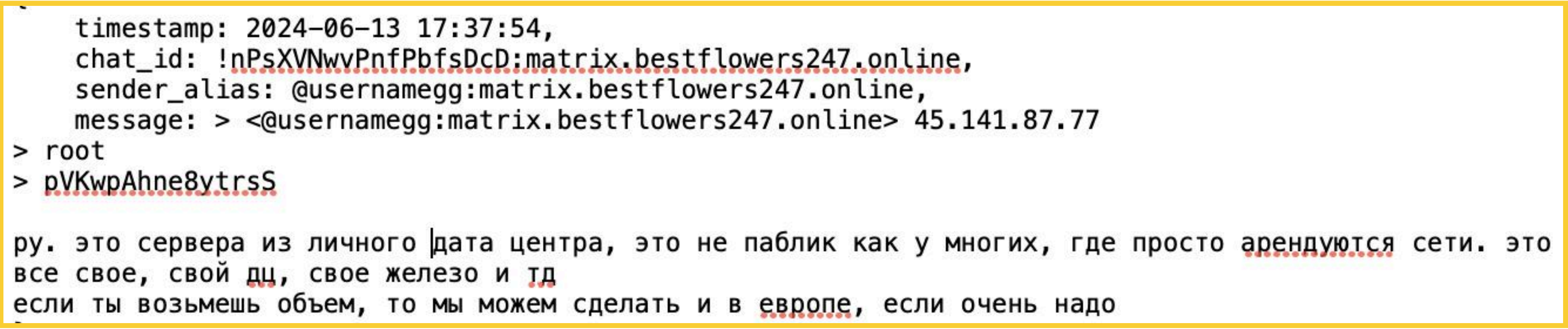
````
    timestamp: 2024-07-03 13:50:10,
    chat_id: !nPsXVNwvPnfPbfsDcD:matrix.bestflowers247.online,
    sender_alias: @usernamegg:matrix.bestflowers247.online,
    message: ```
slim shady, [3 июля 2024 г., 16:45:01 (3 июля 2024 г., 16:48:14)]:
Retrieving speedtest.net configuration...
Testing from Media Land (45.141.87.127)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by RETN (Moscow) [1.61 km]: 14.567 ms
Testing download
speed................................................................................
Download: 1561.47 Mbit/s
Testing upload
speed................................................................................................
......
Upload: 1128.05 Mbit/s

как тебе? быстрее в 5 раз, чем у твоего другого хостера на загрузке и в 2 раза на выгрузке :)
````

Figure 8: The actor gg shared a message from Slim Shady with fellow operator lapa, showing the results of a speed test performed from Media Land’s infrastructure on servers purchased by BlackBasta
Source: Leaked BlackBasta chats

The tone aside, the technical context revealed real infrastructure usage patterns. BlackBasta appeared to be heavily reliant on Media Land's hosting capabilities. In a discussion dated July 22, 2024, Slim Shady outlined that a 200-server deployment for BlackBasta was consuming between 17–20 Gbps of bandwidth, with plans to increase to 50 Gbps. However, this level of usage was neither anticipated nor contractually defined at setup, and Slim Shady warned that it was unsustainable under the existing pricing scheme.

He clarified that Media Land's standard plan included 20 Gbps per 100 servers. Anything beyond that required an additional payment, calculated at $4,000 per 10 Gbps. To illustrate the scale, he compared the client's usage to that of a neighboring datacenter with 1,400 racks and only a 300 Gbps uplink. Slim Shady urged the client to find a "middle ground," either by consolidating server usage or increasing their budget, to avoid saturating bandwidth and degrading performance.

Besides the sheer volume of infrastructure BlackBasta acquired through Media Land, there's a strong indication that they were treated as VIP clients. In one conversation, Slim Shady makes this clear: "RU. These are servers from a private data center, not public ones like many others use, where networks are simply rented. This is all our own: our own data center, our own hardware, etc. If you take volume, we can also deploy in Europe, if needed."



```
    timestamp: 2024-06-13 17:37:54,
    chat_id: !nPsXVNwvPnfPbfsDcD:matrix.bestflowers247.online,
    sender_alias: @usernamegg:matrix.bestflowers247.online,
    message: > <@usernamegg:matrix.bestflowers247.online> 45.141.87.77
> root
> pVKwpAhne8ytrsS

ру. это сервера из личного дата центра, это не паблик как у многих, где просто арендуются сети. это
все свое, свой дц, свое железо и тд
если ты возьмешь объем, то мы можем сделать и в европе, если очень надо
```

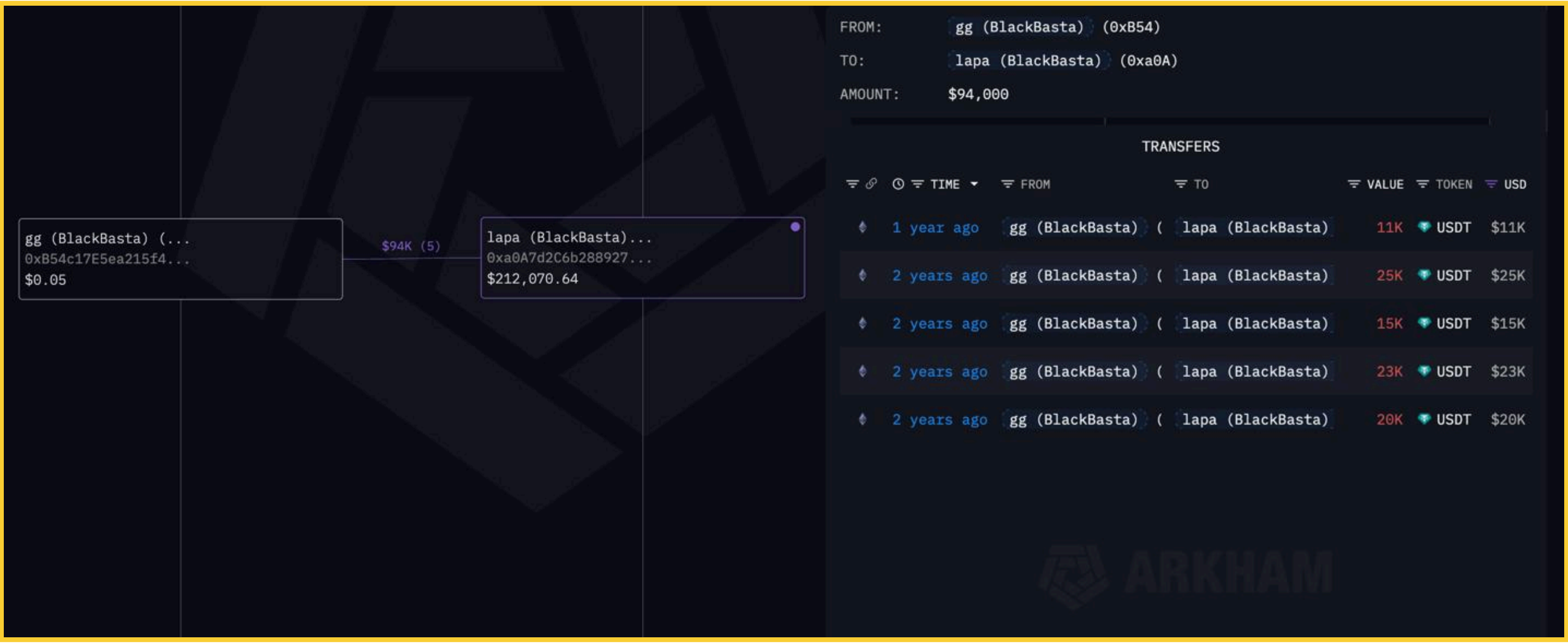
Figure 9: gg shared a message from Slim Shady (Zatolokin) with lapa regarding an offer of servers hosted in a "personal" data center, emphasizing the elevated status of BlackBasta as a VIP client
Source: BlackBasta leaked chats

While not a central figure like Slim Shady or gg, the actor known as lapa played a critical role in infrastructure maintenance. One of lapa's tasks was purchasing SOCKS proxies, a common evasion tool for ransomware operators. These proxies were layered over Media Land's servers used by BlackBasta to anonymize operations, bypass detection, and obscure traffic patterns.

We identified two transactions that appear to serve as evidence of SOCKS-proxy payments from gg to addresses provided by lapa:

- On **April 1, 2024**, gg made a transaction of **BTC 0.01163** (≈ US 829.25 at the time) to address **bc1qn0z8etys62cljzwjxl80k9y5nag7pq42s9lyes**, which was given by lapa to gg as a proxy service payment address. The sending address **bc1qsvtxaheucztkgg27k4zs439um4559jy63p37cqft4rr4la7rvwvq87zdxp** has been attributed to gg; transaction hash: **aa4d8e9e8eb5de54659c20b62021fde1b114c396ab6bb9cb7acd99140c7a6e2e**
- Also on **April 1, 2024**, gg sent another **BTC 0.01019** (≈ US 726.57) to a different address provided by lapa - **bc1qvwntvw5sxtsavaya85up958pjn2eysaqcflffe**
  The funds came from address **bc1qv0hkpnml79pjefdmzve4wg5tr5a2sxmhmda35z4v8r57gclvvc0qptr007**, again attributed to gg; transaction hash: **0c4ef055c67cd6351a691f88398845239c01a87a6b6b2e63d3d4fd098a53db12**

Lapa's operational role was not only tactical but also well-compensated. Through further analysis, we've identified a personal USDT address used by lapa **0xa0A7d2C6b288927cf73a5cf59970373262ea73c6** that received multiple payments totaling **$94,000 USD**. These transfers were made from address **0xB54c17E5ea215f45A61E8790cf546AD175Af2Cf0**, which was later attributed to gg based on the context surrounding the chats. See the complete list of transactions in the table below.



FROM: gg (BlackBasta) (0xB54)
TO: lapa (BlackBasta) (0xa0A)
AMOUNT: $94,000

TRANSFERS

TIME	FROM	TO	VALUE	TOKEN	USD
1 year ago	gg (BlackBasta) (	lapa (BlackBasta)	11K	USDT	$11K
2 years ago	gg (BlackBasta) (	lapa (BlackBasta)	25K	USDT	$25K
2 years ago	gg (BlackBasta) (	lapa (BlackBasta)	15K	USDT	$15K
2 years ago	gg (BlackBasta) (	lapa (BlackBasta)	23K	USDT	$23K
2 years ago	gg (BlackBasta) (	lapa (BlackBasta)	20K	USDT	$20K

Figure 10: The graph displays multiple payments made by gg to lapa's personal cryptocurrency address, identified in the leaked chats. These transactions appear to represent salary disbursements for lapa's infrastructure support work.
Source: Graph made with Arkham

Transaction Hash	Amount	Date
0xb77e237067282cb497cc5246c3c047ce36de2c2d6a3a15e395808a696a84cb34	20,000 USD	February 13, 2024
0x321dc9d6d2110a47ce9000d9e0fc983987fe59a318d5d889623ed08e1c0f42e2	23,000 USD	February 23, 2024
0x792f1533ba55c3059520ba39e29e9b1b0e8f43da3a7208b417b1d443959ec0a9	15,000 USD	March 7, 2024
0x1988652a17c8cd3f5f7a14d83cf6162c0943bf9b9cd96d4756d5f7c52214a1ff	25,000 USD	March 27, 2024
0xa5eca747fdc92a81693d166e24c942501c581be063e858620891c9b709acb36a	11,000 USD	May 30, 2024

What stands out in the payment trail is the use of USDT (Tether). While BTC remains the primary currency for receiving ransomware payments, actors frequently convert and transact in USDT after laundering funds. The stablecoin provides liquidity, predictable value, and ease of use across dark OTC markets and crypto services. This matches comments made by gg in chats, where he explained that funds used to pay for services like SOCKS procurement or salary for lapa came from money that had already been "cleaned" by his internal laundering operation. In short, Lapa was part of the laundering-to-logistics pipeline.

Conclusion

The leaks of BlackBasta's internal chats and Media Land gave us something rare: a clear look into how ransomware groups actually operate and who helps them do it. Together, the leaks gave investigators, analysts, and defenders an unprecedented opportunity to map the evolution of modern cybercriminal infrastructure into a professionalized, scalable, and compartmentalized system. Names became faces. And yet, the story isn't over.

Even after being named or sanctioned, many of the people involved, such as Volosovik and Zatolokin, remain active. Their infrastructure is built to survive. They rotate domains, change wallets, and use new Telegram handles. They adapt. That's what makes fighting this ecosystem so hard.

But thanks to these leaks, defenders now know much more about where to look, what to track, and how this underground economy actually works. It's a huge step forward, but only one. They shift, rebrand, and build again.

If ransomware is the business, infrastructure is the backbone. Let's keep cracking it.

ANALYST1