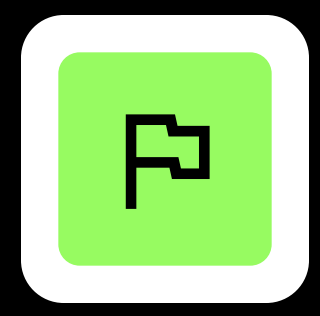


# Business on the dark web

Deals and regulatory mechanisms





# Introduction

Hundreds of deals are made on the dark web every day. Cybercriminals buy and sell data, provide illegal and dubious services to each other, and hire individuals to work in their groups as "employees." Such bargains are from the outset associated with certain risks for all participants, since we are talking about illegal activities. The buyer may not pay for a service or goods, the seller may take the money and disappear. Oftentimes, the same data is sold several times. Even if the ad claims there will be a sole buyer, after a few months the seller may put the data up for sale again or post it on public or private (i.e. accessible only to a certain circle of people, such as authorized forum users) resources. To insure themselves against losses as a result of a dishonest transaction, cybercriminals use various regulatory mechanisms. However, none of these mechanisms guarantee protection against deception for all participants. Moreover, the regulators themselves can also scam the parties of the deal and disappear with the money.

The risks associated with illegal deals may also affect legitimate organizations. For example, a company representative who does not know how the shadow market works may take the initiative and try to buy data or services on the dark web in order to find out about planned or already carried out attacks on the organization.

Or, say, buy out confidential company data that is already up for sale. Since the interaction among cybercriminals has its own features and rules, there is a high chance of not only getting nothing and losing time and money, but also of attracting attackers' interest.

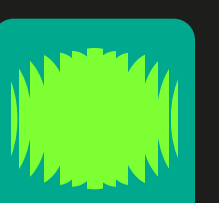
Understanding what kinds of deals there are, how they are made and what roles exist in them plays an important role in searching for information on the dark web and in the subsequent analysis of that information to check for possible threats to companies, government agencies or certain groups of people. It helps information security specialists find information faster and more efficiently without revealing themselves. In addition, this understanding is important in order to take timely measures to counter the threat and eliminate the consequences of fraudulent and malicious activity.

In this article, we will talk about how cybercriminals make deals, what mechanisms they use to control the execution of agreements, and what happens if one of the participants of the arrangement tries to deceive the others.

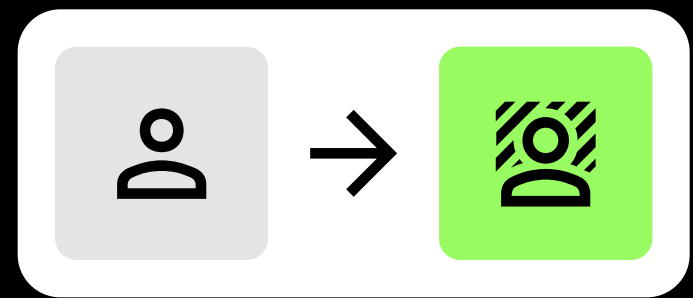
## Types of deals on the dark web

Cybercriminals on the dark web put up for sale both personal data of individuals (for example, scans and photos of documents or bank card data) and information related to various companies (databases with information about employees, partners or customers, documents with corporate information, etc.). In addition, they offer malware under the malware-as-a-service model,

provide access to the infrastructure of companies, and sell various other services, such as collecting confidential information upon request, withdrawing stolen money, denial-of-service attacks (distributed denial-of-service, DDoS) or spam. Finally, cybercriminal groups hire people on the dark web for regular or temporary work.



# Deals via escrow services



To reduce the risks when concluding deals, cybercriminals often resort to the services of intermediaries that are called "escrow agents." The escrow service may be specially organized and supported by a dark web platform, or such services may be provided by a third party who is not interested in the results of the arrangement (also a member of the cybercrime community). Note that the Russian-speaking cybercrime community more commonly uses the term "guarantor" (commonly "garant") to designate both an escrow agent and an escrow service. The principle of making a deal remains the same, only the terminology changes.

**Escrow agents control the deal process and are responsible for such aspects as:**

- Timely provision of data or services in accordance with the declared quality characteristics;
- Timely and full payment for commodities or services;
- Confidentiality of personal and financial information of the deal parties.

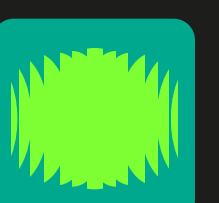
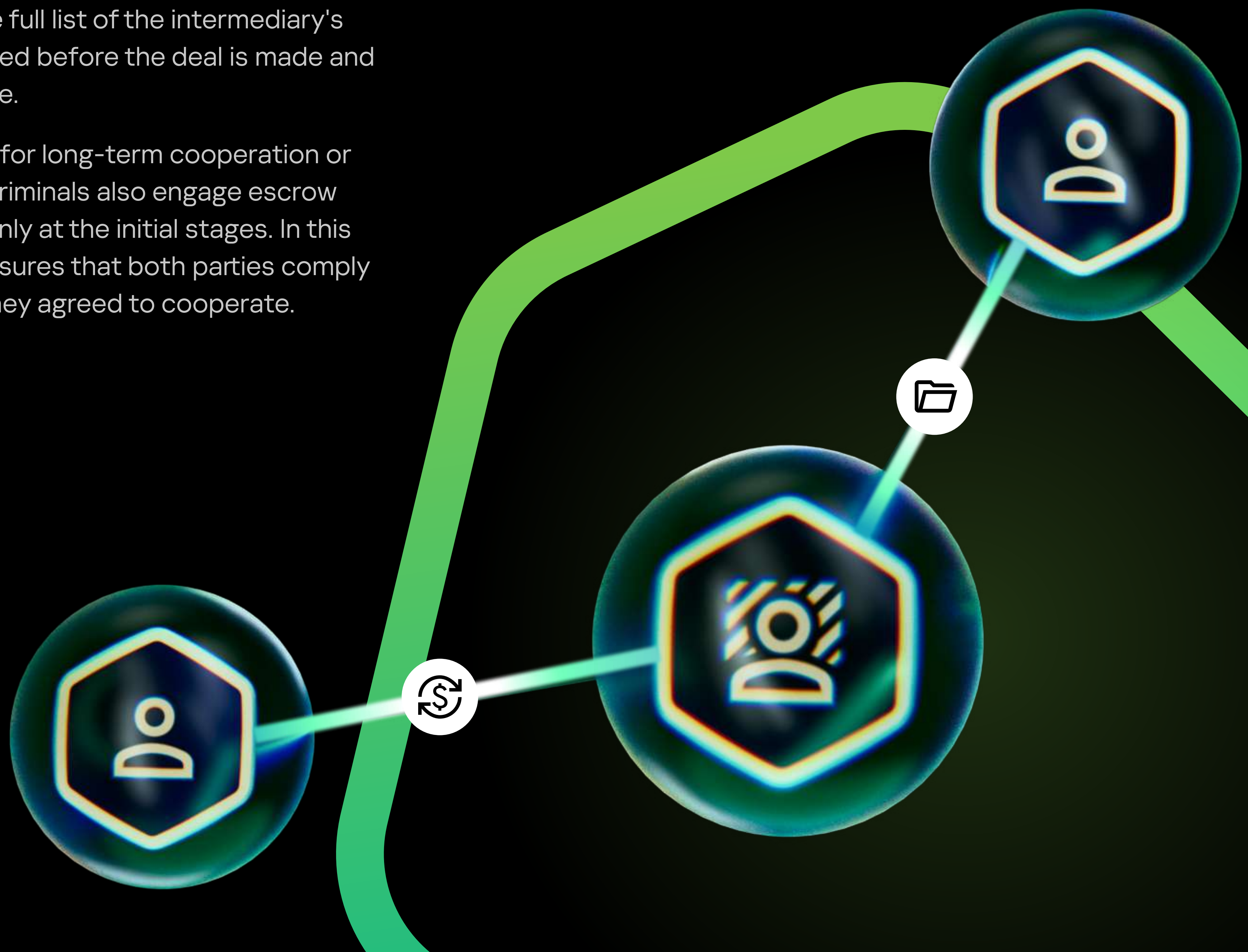
Sometimes the escrow agent also transmits data from the seller to the buyer. The full list of the intermediary's responsibilities is negotiated before the deal is made and may vary from case to case.

When looking for partners for long-term cooperation or hiring "employees", cybercriminals also engage escrow services, but oftentimes only at the initial stages. In this case, the escrow agent ensures that both parties comply with the terms on which they agreed to cooperate.

**In addition to the escrow services, there are several options for insuring the seller from scam in deals that are practiced on the dark web:**

- Full advance payment
- Partial advance payment
- Provision of data in parts with separate payment for each part
- Payment for a deal from a "deposit" – an account on the forum to which the buyer deposits money to confirm their intentions

If the buyer has a good reputation (from the cybercriminals' point of view), payment after delivery is also possible. However, in this article we will focus on arrangements involving an escrow service.



Cybercriminals who are ready to make a deal with the participation of escrow services may note this in their announcements. For example, the author of the announcement on the right is looking for providers of log data from bots (devices infected with botnet-related malware) for cooperation on a regular basis (via a middleman to secure transactions). The author of the announcement below sells his own database for conducting attacks by bruteforcing RDP passwords and agrees to involve an escrow agent.

A sample announcement of an escrow-secured sale of a database for conducting attacks by bruteforcing passwords for RDP services

### Will sell my own developments on bruteforcing RDP. Passwords and ports. 5 years of work. ...

Will sell my own developments on bruteforcing RDP. Passwords and ports. 5 years of work.

Passwords. 22 GB generated solely by myself from different databases. Passwords for services in the USA.

ALL the ideas that could only come to my mind are covered. From staircases [sequences of characters arranged in the form of a staircase on the keyboard] and key combinations to generation with symbols/digits and top words from popular databases. With and without normal distribution.

Ports. Generated ALL possible interesting variations of ports. Mirrored, ladders etc.

The price is 20k. Ready to work through a guarantor 50/50.

 Author1 September 23, 2022



[View a screenshot of the announcement >](#)

A sample announcement about the search for providers of log data from bots (devices infected with malware) for cooperation on a regular basis

### buy fresh logs ...

I'm looking for good vendors who can sell me private new logs every day. I expect mainly US, EU, Japan and other targets, Amazon logs, I look forward to seeing your fresh. private log. My telegram [@]nickname, if you can't accept admin as a middleman to secure transactions please don't contact me, my channel is [https]://t.me/link\_to\_channel

 Author2 December 14, 2022 at 08:12 AM



[View a screenshot of the announcement >](#)

Source – [Kaspersky Digital Footprint Intelligence](#)

It would seem that engaging an escrow agent is an additional expense, and the dedication of a third party to the detailed terms of a deal creates additional threats for cybercriminals. So why are the escrow agents in demand on shadow sites? Having analyzed messages on the dark web, we identified the following key reasons for the prevalence of escrow services when making arrangements:

- Cybercriminals sell information or services via public channels, the entry threshold to which is minimal. Oftentimes, it is enough to create an account on a forum or have a Telegram account. The buyer may have no reputation or experience of cooperation with other cybercriminals who could confirm his credibility and, for example, non-involvement with law enforcement agencies. As for intermediaries, users with a good reputation – by the dark web community standards – are usually invited for that role.
- If it is the sale of unique and expensive data, for example, access to the infrastructure of specific organizations, the potential loss (in case of fraud) can greatly exceed the cost of intermediary services.
- When concluding a deal via an escrow service, the intermediary (escrow agent) assumes part of the responsibility for the result of the deal and the associated risks. Moreover, if the agent is an official representative of the dark web platform, then the forum administration will be responsible for their actions (we will discuss this further in the following sections).



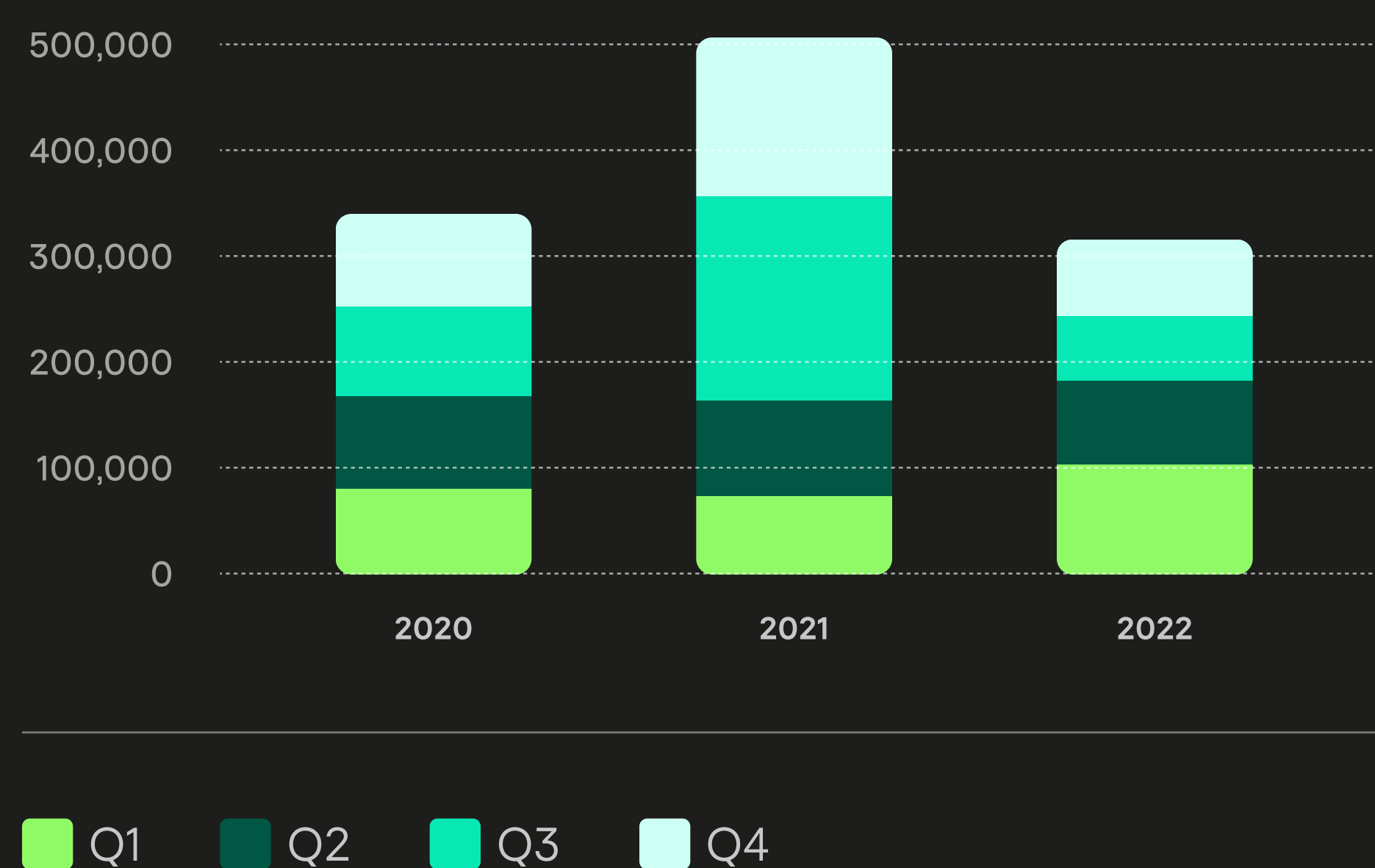
# Statistics on deals via escrow services

We have studied publications on the dark web about deals involving escrow services for the period from January 2020 to December 2022. The sample includes messages from international forums and marketplaces on the dark web, as well as from publicly available Telegram channels used by cybercriminals (a total of 226 forums and 489 channels). The number of messages mentioning the use of an escrow agent in one way or another over the past three years has amounted to more than one million, of which almost 313k messages were published in 2022. About half of the messages for 2022 (150,000) were posted on a platform specializing in cashing out money and services related to this activity.

Messages explicitly mentioning escrow services accounted for 14% of the total number of deal-related messages on various dark web platforms. However, we cannot argue that this percentage really corresponds to the share of arrangements that are concluded via escrow agents, since cybercriminals often discuss detailed terms in person without specifying all the particulars in announcements and offers.

The diagram below shows the total number of messages on shadow sites mentioning escrow agents over the past three years, broken down by quarters.

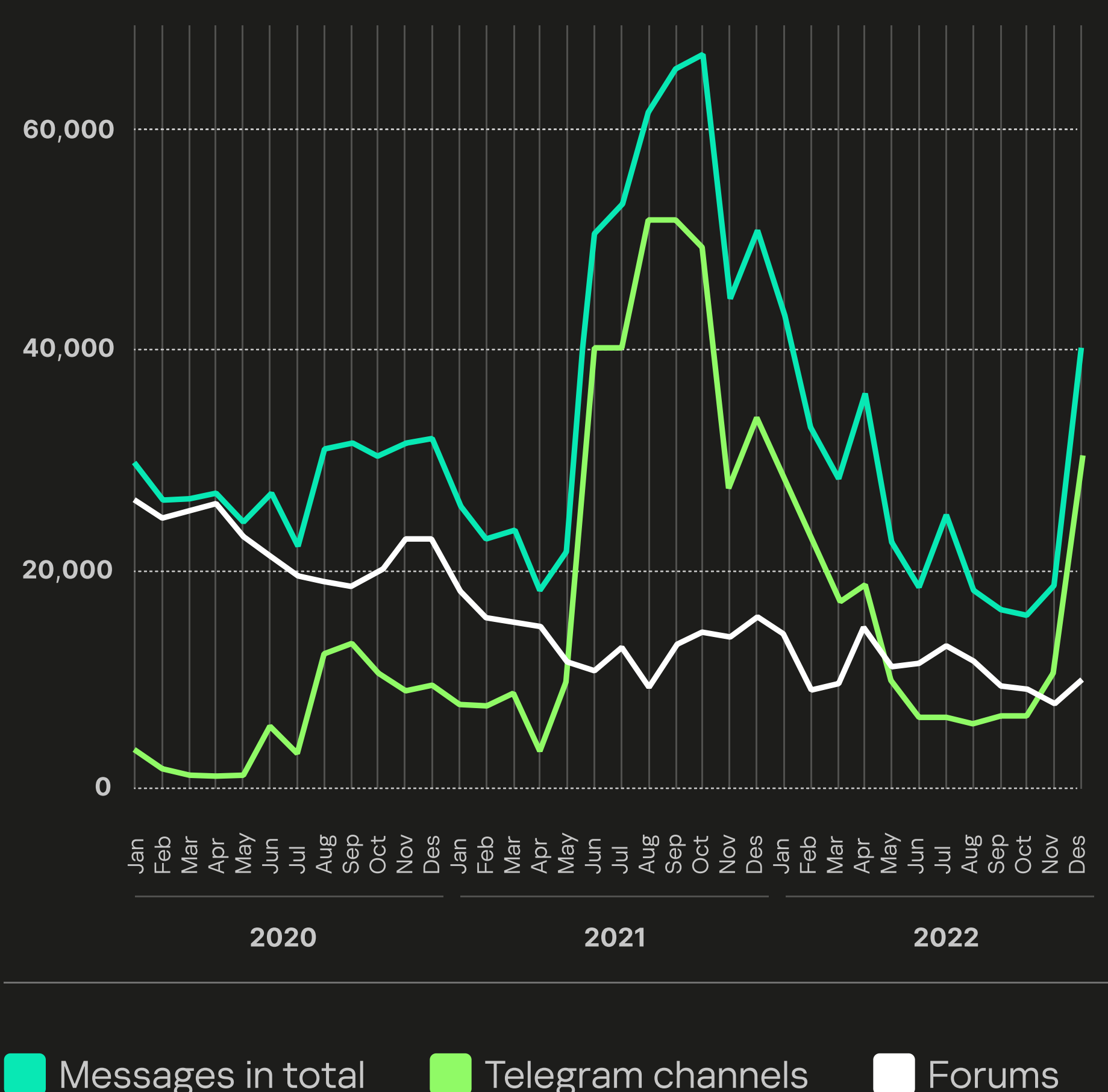
The total number of messages on shadow sites mentioning escrow agents, by quarter, from 2020 to 2022



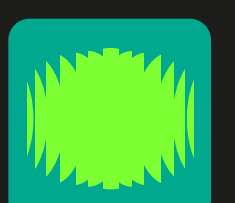
The number of messages in the first half of each of the three years does not differ significantly; the same is true for the first three quarters of 2020 and 2022. The reasons for the increase in their number in the second half of 2021 will be discussed further.

Dynamics of the number of messages on shadow sites mentioning escrow agents, from 2020 to 2022

Source – [Kaspersky Digital Footprint Intelligence](#)

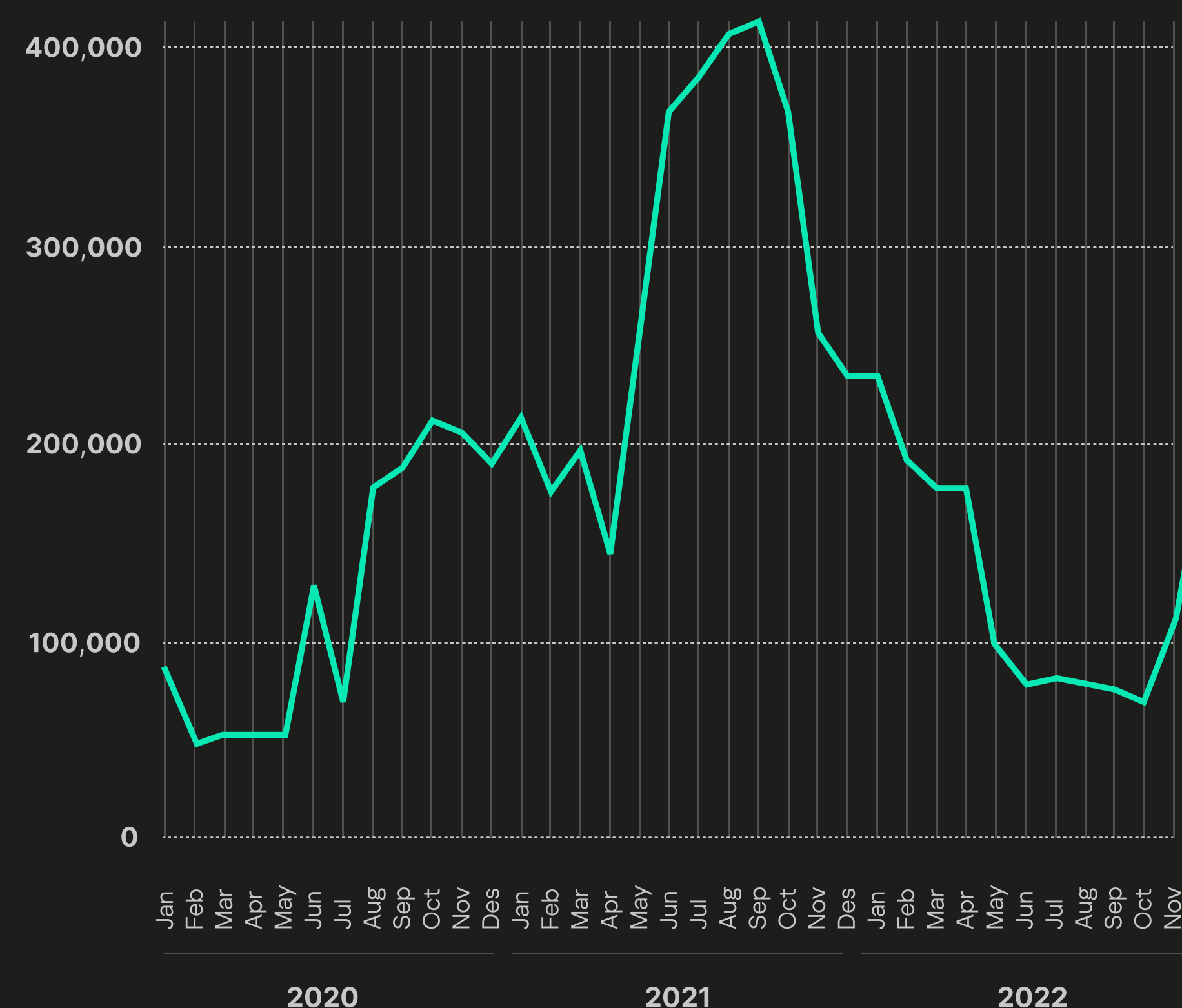


The graph shows that there was a significant surge in the number of messages mentioning escrow agents in the second half of 2021. This surge and the subsequent decline for most of 2022 coincide with the dynamics of escrow-related activity in shadow Telegram channels, while the number of posts on various forums, on the contrary, was steadily decreasing. Let's see how the number of all messages in the shadow Telegram channels from our sample has changed over the past three years.



Dynamics of the number of messages in shadow Telegram channels, from 2020 to 2022

Source – [Kaspersky Digital Footprint Intelligence](#)

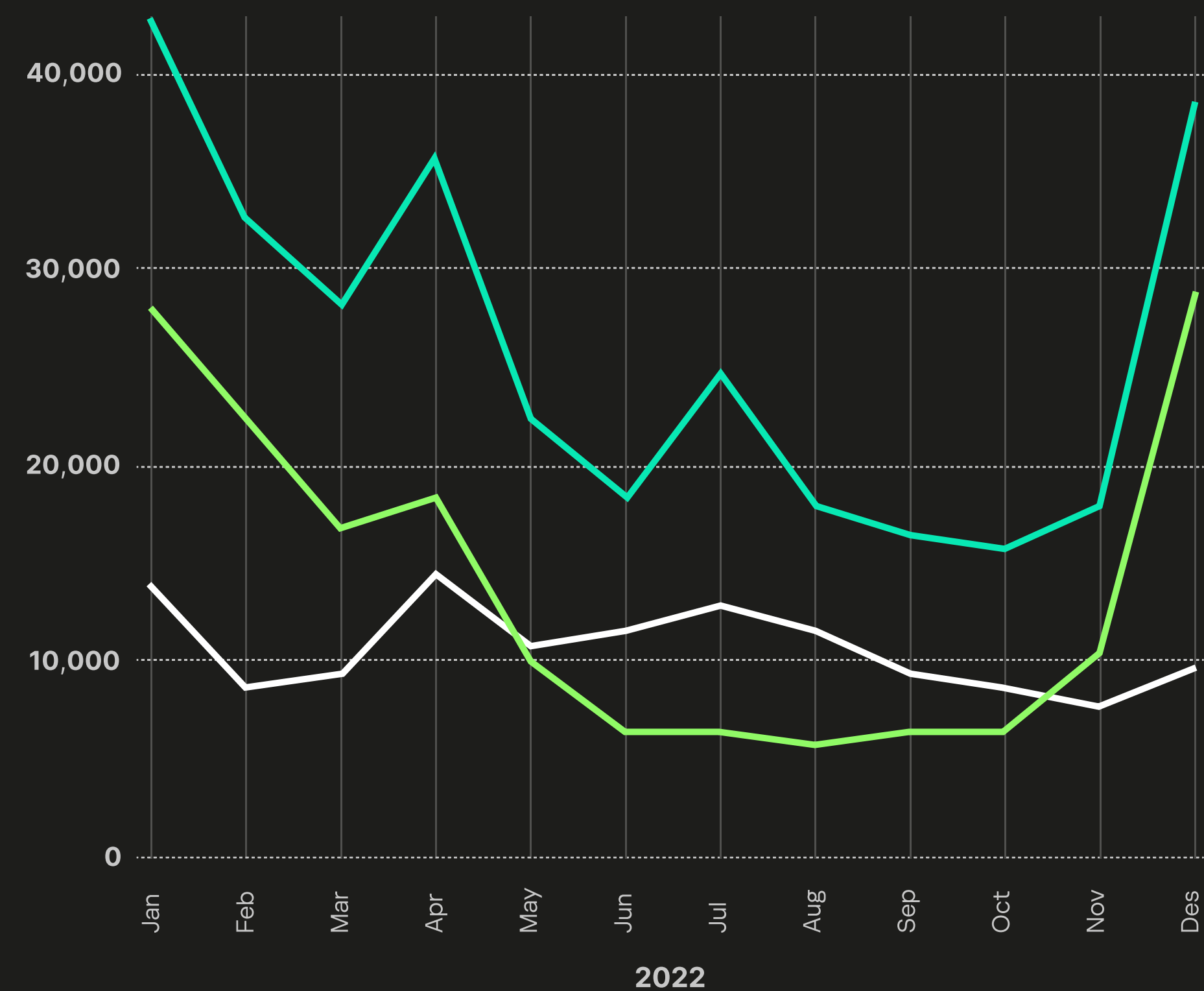


From June to October 2021, not only the number of mentions of escrow services increased, but also the total number of messages in the shadow channels of the messenger. Cybercriminals began to use Telegram more actively as early as in 2020, but it was 2021 when this trend became widespread due to the compromise of several popular Russian-language forums whose administrators reported attacks in the first quarter of the year. In most cases, users' personal data was stolen, including email addresses that could be used to establish the real identities of forum participants. As part of one of the attacks, cybercriminals used a hacked administrator account to steal money from forum participants: they advertised a fraudulent money transfer service on behalf of the site management. One way or another, the likelihood of an attack and the risks for users increased, which undermined the credibility of the forums and provoked the transition to other platforms (in particular, to Telegram).

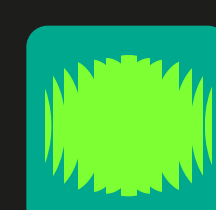
For most of 2022, we saw some decline in activity, including escrow-related activity, on shadow sites in general. This may be a consequence of the escalated geopolitical situation – the global crisis has motivated many cybercriminals to temporarily or completely cease their illegal activities and move to new places using the accumulated capital. Nevertheless, at the end of 2022, we again see an increase in the number of mentions of escrow agents, primarily in shadow Telegram channels. The activity associated with the escrow agents returned to the figures of the beginning of the year, which is due (among other things) to the recovery of cybercriminal activity after a significant decline that we observed for almost the entire year.

Dynamics of the number of messages on shadow sites mentioning escrow services, 2022

Source – [Kaspersky Digital Footprint Intelligence](#)



Messages in total Telegram channels Forums

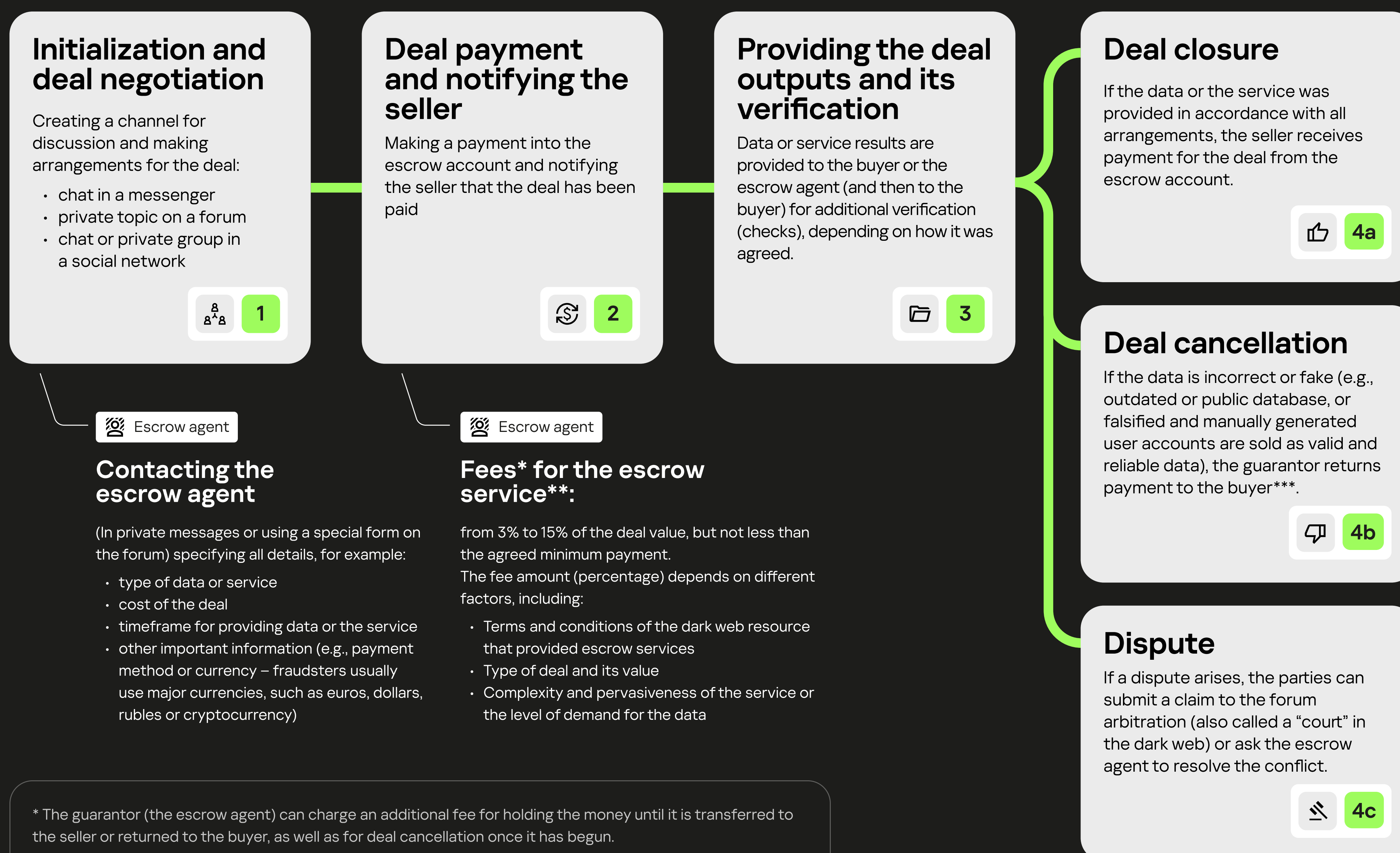


# Operation scheme of an escrow service

Many popular forums on the dark web have their own official escrow services. Most often, administrators choose one or more experienced forum participants who already have a reputation as reliable intermediaries. There are also independent escrow agents in the dark web community. However, according to our observations, cybercriminals who talk about such matters publicly prefer to contact the official agents of various popular sites. This is due to the fact that such escrow services are verified, and in case of possible problems, the participants of the transaction can initiate an arbitration procedure to protect their interests (we will talk about arbitration a bit later).

We have found and analyzed the operation rules of the escrow services of more than ten popular sites. Independent agents rarely publish this information, so we did not take them into account in our analysis. We've found out that the rules and procedures for concluding transactions with escrow services on various shadow platforms are almost the same. The typical scheme of a transaction involving an escrow service is as follows.

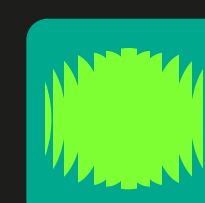
## The typical scheme of a deal that involves an escrow agent



\* The guarantor (the escrow agent) can charge an additional fee for holding the money until it is transferred to the seller or returned to the buyer, as well as for deal cancellation once it has begun.

\*\* The fee for escrow service is paid by either party (seller or buyer) depending on the agreed terms and the parties' interest in using of guarantor's services.

\*\*\* In case of deal cancellation, the guarantor's fee is not refundable.



Automated escrow service for deals on the dark web

### Automated Escrow Service – Never get scammed again on the forum or anywhere else! ...

We have seen quite a few topics/posts relating to wanting some form of middleman service so I would like to introduce you all to EscrowService

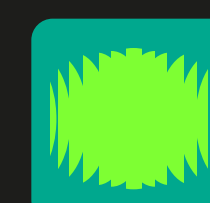
- Automated Escrow
- 1% Fees (no MM/service can match)
- Private 1-2-1 Trades
- Public Listings for Vendors
- XMR Payment/Deposits
- Client-side PGP Encryption

Author October 20, 2020 at 03:59 PM



[View a screenshot of the announcement](#) >

Some shadow forums are developing their automatic escrow systems to speed up and simplify relatively typical deals between cybercriminals. For expensive or untypical cases, they still engage a human intermediary. Automated escrow services work according to the same scheme as a human agent, but allow to conduct typical transactions faster, provided that both parties comply with all conditions and agreements.





# Why a deal may fail

So, all the details of a deal have been discussed and agreed upon by all parties. Why might it fail? If we disregard the situation where the seller or buyer, for whatever reason, change their mind about bringing the matter to an end and cancel the deal, the main reason for a deal break will be foul play. Despite the fact that there are certain rules of communication between cybercriminals on the forums and something like "dark web etiquette", no escrow service protects against cheating. Both the seller and the buyer, as well as the escrow agent, can violate the deal arrangements, especially when it comes to large sums, e.g., several million dollars.

The seller may provide incorrect or outdated and public data under the guise of up-to-date information or not fulfill the service promised. For example, a dark web forum user offering more than 600 bank cards for sale in an auction format, judging by the comments of another user, sold them fabricated information (in another discussion on the same forum).


A topic example with an offer to sell bank card data to a sole buyer

**610 CC usa name+cvv+cc num+address+exp date + snn valid 80-90%** ...

Fresh base '615 cc USA'  
Full info + snn  
Valid 80-90%

Start 1000  
Step 200  
Blitz 4000

Auction lasts 5 hours  
Escrow service +++ (Do not offer weekly payments! Escrow !!  
+ partial check of 10-20 cards)


 Author August 07, 2022 at 16:52



[View a screenshot of the announcement >](#)

Reviews indicating that the post's author provided fake data

You're a professional at scamming. Same day that you stole 1000 usd from me you stole from other user of this forum. ( / topic/210157/ ). I sent the report to [@]admin directly to his pm and did not bother to open arbitration. This was not 1 month ago. This was last week. You already scammed enough with this account. Go ahead and keep working with your new accounts.

 Accuser August 07, 2022 at 23:28




[@]User1 [@]User2 [@]User3 if you want proof that Author is scammer, send me PM. I will provide videos and screenshots.

 Accuser August 07, 2022 at 23:28

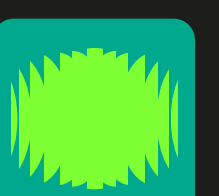


thx @Accuser

 User3 August 07, 2022 at 23:30



[View a screenshot of the reviews >](#)



The buyer, in turn, can claim the results of the seller's work do not meet the agreed conditions and leave without paying. For example, the author of the post in the screenshot below ordered services for making payments (banking transactions) to their banking accounts from various legal entities (as stated in the text of the post, "for verification" of the registered firms), but have not paid for these services. As a result of the complaints, their account was blocked.

A sample review indicating non-payment for services by the buyer

**Work for firm registrars** ...

Hi everyone.

Need payments from an LLC or a private entrepreneur

The payments are needed for verification. Continue using the firms for whatever you may need them for, they live forever after my manipulations

Need more than 1,000 per month  
Contact me via Telegram

Author September 20, 2022 at 14:01

[View a screenshot of the announcement >](#)

Did not pay for 7 companies. He has two user accounts.

I will provide proof

If I receive the payment, I will delete the comment  
If not, I'll begin arbitration to sort it out

User September 28, 2022 at 20:35

[View a screenshot of the review >](#)

Finally, the escrow agent may simply disappear with the money (and sometimes with the goods). For instance, a member of the dark web community, chosen as the official guarantor of two shadow forums (including one of the most popular forums), discredited themselves by not paying a total of 170,000 dollars in four deals.

A claim against the official escrow agent (guarantor) of the site in connection with non-fulfillment of financial obligations

**Escrow Agent, 160k\$, Agent's contacts on the forum** ...

I am suing the guarantor of the forum. I ask, on the basis of the rules of the forum, to bring the administration of said forum to financial responsibility, in view of the rules. Quote (guarantor's contacts): icq jb (otr/pgp) forum profile. As evidence that Escrow Agent is the official guarantor of the forum \*\*\*, I tag the administration of the forum – in particular, the forum admins.

Quote

Amount claimed, USD:

1. \$100,000 – deal with \*\*\* (disrupted by the fault of the guarantor)
2. \$50,000 – deal with \*\*\* (morpher C)
3. \$15,000 – deal with \*\*\* (writing a PowerShell morpher)
4. \$5000 – deal with \*\*\* (writing reflective DLL)

The total amount of the claim is \$170,000 (one hundred and seventy thousand US dollars). The guarantor received the money, as there are corresponding confirmations

– The essence of the claim –

Several deals were concluded with ... for the execution of works. The works are underway and will be completed soon.

After my confirmation of the money transfer to the seller, the guarantor's exchange service got locked. The seller did not receive any money. Every day the seller and I asked about the status of the money, to which we received an answer – "it got locked. Have requested docs, working on it." For one week, the money was hanging on the guarantor's end, which of course led to the buyer's legitimate bewilderment and the deal break. After that, I asked for my money back. Every day I asked how things were going, to which the answer was the same – "I am working on this." 03/16/2020 my patience ran out, and I asked to set a deadline for payment. After that, I canceled the previously appointed deals, due to this attitude and an absolutely unbusinesslike approach (the deal was disrupted by the fault of the guarantor, and I don't want my future ones to fail as well), therefore I decided to withdraw the funds and transfer them to another guarantor – the forum admin. I understand that all the money is stuck on the exchange, and I still have not received a clear and intelligible answer on when I will receive the money within 2 weeks. Moreover, he told me 'I am a neutral guarantor, no one is responsible for me.' This is absolutely unacceptable.

Summarizing the above, I came to the conclusion of making a claim. This is absolutely not an appropriate behavior of a guarantor. I beg your pardon – this led to the deal termination, as well as the fact that a large sum of money is now hanging God knows where. And I am not receiving answers on when I get it back specifically.

Considering the above, I ASK TO:

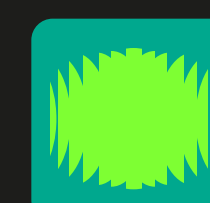
1. Permanently remove this person from deals as a guarantor on any forum
2. Set the exact date of payment of the entire amount (\$160,000) or in parts (I remind you, it has already been a total of 2 weeks)
3. In case of refusal or impossibility to satisfy this condition – publicly display the corresponding status
4. If the conditions of paragraph 3 are fulfilled, bring the guarantor to financial responsibility (since he was the official guarantor of the forum) in the amount of \$160,000
5. If it is impossible to fulfill paragraph 4 – assign the corresponding status to the forum, as well as directly to its administrator with mandatory disclosure of previous nicknames

Edited on 03/18/2020. Logs and other sensitive info have been removed. I will share these details with the interested parties via Jabber with the permission of the arbiter.

Chronology: 03/18/2020 – 10k returned. 160k left.

User March 18, 2020

[View a screenshot of the announcement >](#)







Forum administrators conducted their own investigation, as a result of which the escrow agent was blocked and promised to pay the entire amount of deals within a few months. The agent did return the money in four months, but despite this, their reputation was irreversibly damaged, and the administration of the forums refused to cooperate with them in the future.

#### Announcements of the forum administration on termination of cooperation with the escrow agent in connection with violations and unethical behavior

Dear Forum Members,

We inform you that the alternative guarantor has a number of outstanding financial obligations for a large amount. While the details and reasons for this situation are being clarified, please refrain from making deals via \*\*\*\* as a guarantor. Once the issue is resolved (positively or negatively), we will definitely notify you.

Their account on the forum is temporarily banned until he resolves all the issues that have arisen. We will not jump to conclusions, but we will be waiting for clarification. We apologize for this inconvenience.

 Forum Administration March 18, 2020   

[View a screenshot of the announcement >](#)

The debt has been fully repaid to the User





Nonetheless, we have to consider several important factors. One of them is inappropriate behavior that we have all seen.

The guarantor was endowed with serious reputational powers, which he used the wrong way, thereby discrediting 2 forums, breaking trust in the forum Administration and making some confusion. The fact that he returned the money is good, but, frankly speaking, he acted badly.

Due to the loss of trust, their status will not be changed. Whether to continue working with him or not is at everyone's personal discretion, but the team of our forum and I are not responsible for deals with him. I don't want to worry every time I deal with 100k+ amounts thinking what could happen.

Regarding the status, this is my personal decision, I do not believe that a person with such powers and status can behave like that, and for me it is beyond understanding.

The discussion on this topic is closed.

 Forum Administration June 20, 2020   

[View a screenshot of the announcement >](#)

In general, on the dark web, even a forum administration can solve the situation in their own favor to the detriment of other interested parties. At the same time, in addition to the participants of the deals themselves, third parties can disrupt it as well. For instance, on third-party sites and messengers, cybercriminals register fake accounts and impersonate popular independent escrow services, official escrow agents of well-known forums, administrators and other trusted persons. On large shadow platforms, it is often explicitly noted that all participants of a deal should be carefully checked when communicating outside the forum before passing something to them. The forum administration can post warnings in the sections addressing the rules of work and communication with other forum members, on the main page, in automatically generated messages under each new post about a deal, or, alternatively, in the form of a fixed line at the top of the forum web page.

#### An example warning about the need for additional checks when interacting with regard to deals in messengers

**Admin** 



User1 and User 2, we wait Admin

I don't have any contact, ONLY PM on the forum

Forum moderator does not sell or buy.

Forum escrow service and forum administration do not have telegram channels, chats, etc.

Anyone who says this is RIPPER

 Moderator August 21, 2022 at 10:08 PM   

[View a screenshot of the warning >](#)

#### An example warning about the unavailability of the forum's escrow service on third-party services and messengers

The Escrow Service communicates only through the Forum's DMs. No Telegram or other services

[View a screenshot of the warning >](#)



# How disputes are resolved

As we mentioned above, if one of the parties of the deal is caught on cheating, cybercriminals file a claim or complaint, and attract (sometimes for an additional fee) the forum's arbitration system or an experienced member of the cybercriminal community who performs the functions of arbitration and has the appropriate reputation (they are called arbiters). Having analyzed various messages and posts on this topic, we have noticed that the form of a claim or application for consideration in arbitration is standardized on large shadow resources. The form includes information about the parties of the deal, the amount, a brief description of the situation with evidence, which is usually not published in the discussion, but sent directly to the chosen arbiter, as well as expectations for the decision.





The screenshot below shows an example of a claim against the operator of a cash-out service. In the text of the claim itself, the essence is indicated as briefly as possible. Detailed information about the arrangements is provided by the escrow agent in the following message, which also confirms the fact of concluding the deal.

An example of a claim to the operator of a cash-out service (theft of money)

**[Claim] Refund from the forum member** ...

[Claim] Refund from forum member

1. Transaction via the Guarantor Service in the amount of 500,000 RUB. Stiffed me on 702,000 RUB. His share was 12%. The amount to be paid is 617,700 RUB.
2. Can send proof (a video with the dialogue) to the arbiter on Telegram

 Claimant June 07, 2022 at 10:21 PM   

[View a screenshot of the announcement](#) >

Source – [Kaspersky Digital Footprint Intelligence](#)

Description of the essence of the deal and confirmation from the escrow service (to continue the claim shown in the previous screenshot)

## **[Claim] Refund from the forum member** ...

I confirm the fact of the deal

1. Provide a link to your profile on the forum: [hidden link]
2. Specify your Telegram accounts for communication: [hidden link]
3. Specify the link to the seller's profile on the forum: [hidden link]
4. Deal amount (specify the nominal value and currency, for example, 100 USD): 500,000 rubles
5. Payment method: Cash in
6. Who pays the guarantor's commission: [hidden link]
7. Description of the product or service. Transmission method, quality assessment criteria: Working to cash money out for citizens of the Russian Federation under the conditions described below, with my own stuff, (I charge 12% of the cashing out amount for the stuff). All withdrawal fees are on me, the buyer pays the commission for the exchange into cryptocurrency. I am responsible for any possible blockings.

In case of fraud on my part or if I violate this agreement, I undertake to transfer to him money from this guarantor in the amount of losses.

In case of the following problems with the stuff, I am financially responsible:

1. In case of fraud by the drop, I reimburse all the funds that the drop stole.
2. I will reimburse all funds if I give the wrong set of stuff for work, namely:
  - \*. There are no documents that are needed to call the call center.
  - \*. Missing or inactive SIM card.
  - \*. Missing code word.
  - \*. Missing or incorrect PIN.
  - \*. The drop is arrested, had negative credit score, bailiffs, microloans, any similar situations.
  - \*. Issued incorrect or blocked banking details.

I assist in removing blockings, the drop visits the bank.

1. I reimburse all funds if I cannot provide screenshots, videos, access to the personal area and a call to the call center. And anything that interferes with finding out the reason for blocking the card.
2. I reimburse all funds if a loss of funds occurs due to my human factor (inattention, fatigue, confusion, wrongdoing etc.).
3. I am a sane person and I understand in what field I work. In case of problems with law enforcement agencies, I have no questions to the buyer, and if I did not have time to transfer the proper funds to him, I undertake to transfer them from this guarantor. If you don't hear from me for two weeks, then the funds from this guarantor are transferred to the buyer.





I can withdraw funds from the guarantor if the buyer does not give me any work for 14 days in a row, does not respond for more than 14 days in a row, or if I want to stop working with the buyer and he/she has no claims against me.

If my work does not satisfy the buyer, he/she can insist on stopping working with me and returning me the money from the guarantor.

The arrangement is concluded until 08/01/2022.

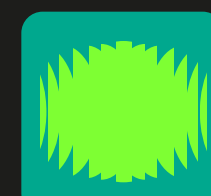
The arrangement can be extended by agreement of both parties.

Each party may terminate the arrangement unilaterally at its own request, if the other party has no claims.

 Escrow agent June 07, 2022 at 10:26 PM   

[View a screenshot of the announcement](#) >

Source – [Kaspersky Digital Footprint Intelligence](#)



So, we see that an agreement was concluded between the forum members as part of the cash-out service, but for some reason the contractor did not fulfill their obligations, although they were transferred money and an additional 12% of the total amount to pay for "consumables." The difference between the initial amount of the deal and the amount that the buyer is asking to refund is caused by the fact that the arrangement was concluded not for a certain amount, but for a certain period of time (in the example given, until August 01, 2022) with the possibility of extension.

An example of an arbitration process on a complaint against a service provider who was supposed to open a bank account (the deal was carried out through an escrow service)

### Arbitration initiated by user User1 against user User2 ...

User1 created a new arbitration

Arbitration: Arbitration link

Claimant: User1

Defendant: User2

Amount: 4,000 RUB

Additional information:

VIA.GARANT: yes

Details: The situation is as follows, the seller is waiting for an additional payment of 4K for opening a banking account for User2. I sent him 3K, he promised he would do it in 15 minutes, but he did not fulfill these obligations, and an hour later he wrote, "Let's work via the escrow service." So I said let's do it.

Published on September 02, 2022 by Arbiter bot

The arbitration process has begun in case no. \*\*\*\* between user User1 and user User2

Published on September 02, 2022 by User1 (the topic author)

This seller repeatedly failed to fulfill his obligations, constantly demanded prepayment, plus offered his scammy escrow agents, 2 times he slandered the forum. This user is new on the forum and he is a straight-out scammer, his prices for these services are not reasonable, you can immediately see that the guy is short on brains. Anyway, he stiffed me on 3,000 rubles, please take action. Please, decent people, send him a DM on Telegram, if he doesn't change his nickname or delete his Telegram before that moment.

[View a screenshot of the announcement >](#)

As a result of filing a claim, complaint or appeal, the arbitration service will organize a kind of court for cases of cheating on the dark web. Large forums include a separate thread on this topic, in which users discuss complaints and publish decisions.

After a decision is made, the participants of dark web forums, if they do not agree with the actions of the arbiter, may try to appeal the decision with the involvement of another judge or, if permitted by the rules of the site, the administrators of the forum, because the arbiter may also be biased or interested in a particular outcome.

An example announcement of an appeal of an arbitration decision on a cybercrime forum

### Action appellation of staff – Moderator Appelation+1 User1 Yesterday, at 09:52 2 ... 2 User2 Yesterday, at 11:07

I would like to appeal the decision of the moderator - content deletion - my message in thread

Login or register to view links.

My reasons: Its not so much to explain there , I just need a person that would do that for me , its just simple thing , in telegram he explains me everything he can do and he can get in the team or get rejected that's all.

User1 November 09, 2022 at 09:52 AM

[View a screenshot of the announcement >](#)

Source – [Kaspersky Digital Footprint Intelligence](#)

If you look at the decisions of the arbitrations, the proceedings (logically) end with a demand to compensate for the damage, or the accusation is recognized as untenable. If the participants found guilty do not return the money within the time limit set by the arbiter, they are blocked and added to the list of unreliable members of the cybercrime community ("blacklist" or "fraudsters" list), indicating not only the nickname on the forum and the reason for the ban, but also other identifying information, such as the crypto or electronic wallets used, and nicknames on other sites. Punishment may follow, even if the perpetrator tried to appeal the decision of the arbitrator.



# Reputation is most important

As we can see, depending on the circumstances, up to five parties can be involved in a deal: the seller, the buyer, the escrow agent, the arbiter, and the administration of the dark web resource – it is the forum administrators who monitor the execution of the arbitration decision or apply final sanctions to fraudsters. At the same time, regardless of the role in the deal, the main motivation for cybercriminals to play fair is reputation. It is the reputation of the cybercriminals that determines the number of deals with them and their profit from illegal activities. This is due to the fact that, despite there are ads on popular forums, word-of-mouth and reviews from other users remain the main ways to get information about "verified" members of the cybercrime community, whether it is a data or service provider, an escrow agent or an arbiter.

The screenshot of announcement from a dark web forum about finding a reliable arbiter is on the right. Only candidates who have already earned the appropriate good reputation are considered for the position.

The administration of shadow sites approaches the choice of escrow agents and arbiters with very special care. And this is justified, since they become official representatives of the dark web resource. If they act deceitfully or incompetently, the site will have to take full responsibility, meaning that its reputation may suffer.

Cybercriminals who do not perform the functions of escrow agents and arbiters also take their reputation in the dark web community seriously. For instance, in threads with public arbitrations on popular shadow forums, in 2022 alone, we found more than 50 discussions related to protecting the reputation of community members. As follows from the situation description in these discussions, they were created in response to negative comments on posts, slander, false accusations, blocking or deleting accounts without serious violations or evidence of such violations.

Announcement of the search for a reliable arbiter to join a forum team

## Recruitment for the position of "Arbiter"

I am always humble in victory or defeat

It was decided to recruit an arbitrator.

All responses should be sent in this thread (using the following template), there is no need to refer to anyone.

There are several criteria:

1. You must be registered no later than 01/01/2020;
2. Adequacy and stress tolerance;
3. Ability to assimilate information;
4. You must not have serious violations;
5. You must have at least 500 posts and 200 likes;
6. You need to have an account in [Please login or register to view links] and Telegram (specify in the job response form).

Administrator may reject your response without explanation. We don't charge deposits from potential employees. Do not be fooled.

[Hidden content. You need to be registered to see it. Click to expand...]

Hides are not needed.

Flood / questions in the thread – penalty points.  
Responses not made by the rules – penalty points

There is no exact deadline for closing the thread, good luck!

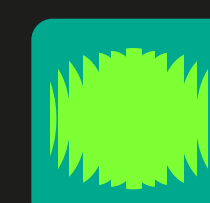
Referring to anyone is not required!

13 forum members like this.

Forum administration June 19, 2021 at 8:32 PM

[View a screenshot of the announcement](#) >

Source – [Kaspersky Digital Footprint Intelligence](#)



# Takeaways

The dark web has long been a multi-purposed platform, on which not only announcements and offers are placed, but also many deals are carried out, partnership agreements are concluded and various services are provided (usually illegal). The shadow market is growing, and various sites on the dark web are developing and automating services to support deals and resolve disputes between community members, including escrow services and the arbitration system. These mechanisms allow the community to reduce the risks of fraud when concluding deals in exchange for some complication of the interaction between cybercriminals. The automation of some escrow services accelerates the execution of typical arrangements, provided that the parties comply with all agreements. Escrow agents and arbiters also create some kind of "legal framework" in the dark web community, in which the reputation of cybercriminals, services, marketplaces and other resources plays an important role. However, despite the existence of these mechanisms, the risk that any party of the deal can cheat – from the seller and the buyer to the administration of the forum – does not disappear completely. Anyone can succumb to the temptation to embezzle other people's money, especially when it comes to large amounts.

Since the dark web community becomes more complex, structured, and develops self-regulation systems as it grows, for effective protection against cybercriminals it is worth understanding how it operates, how cybercriminals interact with each other, where and what information they can publish. It is necessary to conduct regular monitoring of the dark web for various cyberthreats – both planned attacks (these may be indicated with announcements about finding a partner or specific data for implementing a targeted attack) and incidents that have already occurred (these may be indicated, for example, with announcements about the sale of databases belonging to an enterprise or of credentials for access to its infrastructure).

To inquire about threat monitoring services for your organization, please contact us at

[dfi@kaspersky.com](mailto:dfi@kaspersky.com)

