GROUP-IB

DEMYSTIFYING CLASSISCAM

Deep dive into where the scheme started, how it works and evolves

THREAT REPORT

GROUP-IB.COM

Disclaimers

1. The report was written by Group-IB experts without any third-party funding.
2. The report provides information on the tactics, tools, and infrastructure of the various groups. The report's goal is to minimize the risk of the groups committing further illegal acts, suppress any such activity in a timely manner, and raise awareness among readers. The report also contains indicators of compromise that organizations and specialists can use to check their networks for compromise, as well as recommendations on how to protect against future attacks. Technical details about threats are provided solely for information security specialists so that they can familiarize themselves with them, prevent similar incidents from occurring in the future, and minimize potential damage. The technical details about threats outlined in the report are not intended to advocate fraud or other illegal activities in the field of high technologies or any other fields.
3. The report is for information purposes only and is limited in distribution. Readers are not authorized to use it for commercial purposes and any other purposes not related to education or personal non-commercial use. Group-IB grants readers the right to use the report worldwide by downloading, reviewing, and quoting it to the extent justified by legitimate citation, provided that the report itself (including a link to the copyright holder's website on which it is published) is given as the source of the quote.
4. The entire report is subject to copyright and protected by applicable intellectual property law. It is prohibited to copy, distribute (including by placing on websites), or use the information or other content without the right owner's prior written consent.
5. If Group-IB's copyright is violated, Group-IB will have the right to approach a court or other state institution to protect its rights and interests and seek punishment for the perpetrator as provided by law, including recovery of damages.

Table of contents

How the Classiscam scheme emerged

For a long time, the dark side of the Internet has harbored hacker forums that bring together tech-savvy individuals with the skills to cause considerable damage to businesses and governments alike.

As the world evolves, however, the cybercriminal underworld evolves with it. At some point, the abovementioned platforms started attracting less knowledgeable individuals and sometimes even minors looking for a way to earn some extra money online. Most hacker forum users engaged in shady dealings on the Internet that brought them modest profits. On top of that, the forums were chaotic, with no rules or basic moderation in place. Hacker forum communities were incapable of causing serious damage and their activities were local in nature. The incidents attracted little attention from the companies under attack and law enforcement authorities, and they were perceived as a problem for the victim alone, and for them to deal with on their own.

As time passed, the situation began to change. Online communities of low-skill threat actors continued to grow, gathering more and more followers. Forums started developing guidelines and moderating member activity, bringing about a more organized operation of hacker communities and generating higher profits. The desire to make more money prevailed, thereby creating a demand for new earning opportunities and appealing to skilled experts.

At first, the use of social engineering techniques helped hackers compensate for the lack of resources, while the number of operators made up for their low average skill level. The first groups organized on underground forums engaged in nothing more than stealing account data belonging to users of gaming platforms and social media, but their workflow management reached new highs.

From this stage onward, hacker groups would include dedicated organizers who provided anyone interested with links to phishing websites mimicking social media or gaming platform pages. The choice of methods to distribute links and persuade victims to enter their credentials was left entirely to the operators, who were provided with accessible user manuals describing the ins and outs of the scheme. The entry threshold for participating in this type of scam was significantly lowered due to automated tools – scammers started using administrative panels much more often.

Administrative panels

Administrative panels were among the first tools used by workers. Workers are key participants of the Classiscam scam scheme: their goal is to attract traffic to phishing resources. They helped lower the entry threshold for novice scammers willing to take part in this scheme and significantly sped up the creation of phishing pages.

An administrative panel is a website on a dedicated domain or IP address accessed by username/password or a special token received after passing an interview with the project leader.

Users do not need any special technical knowledge to use administrative panels as the interface is accessible and intuitive (Figures 1 to 4).

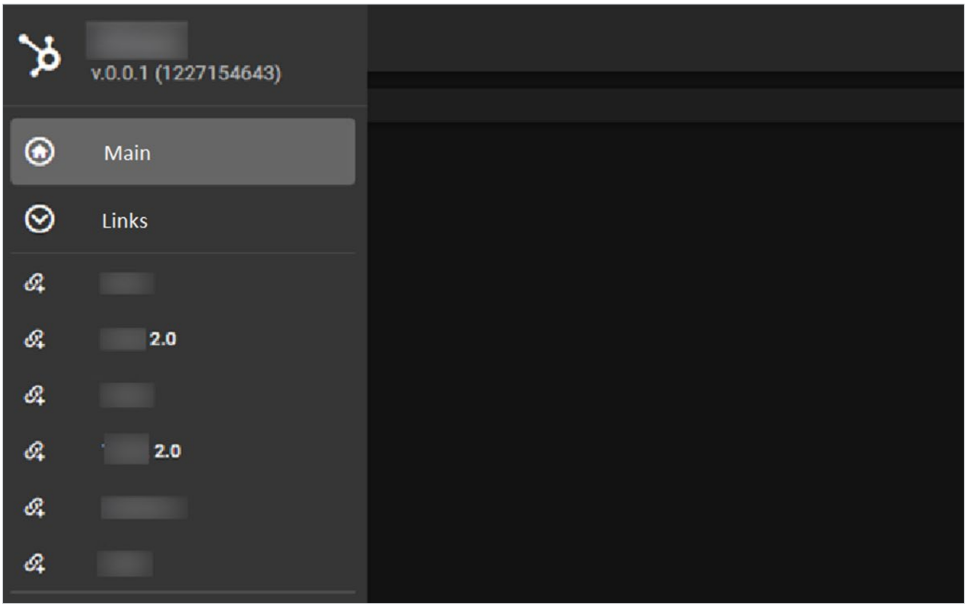


Fig. 1. Example of an administrative panel

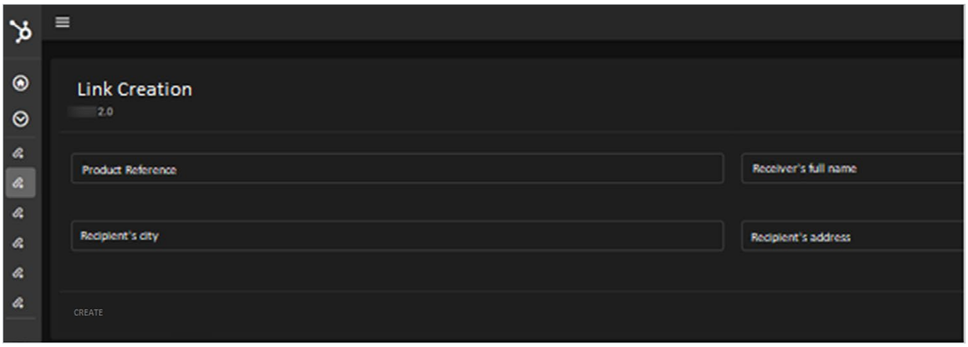
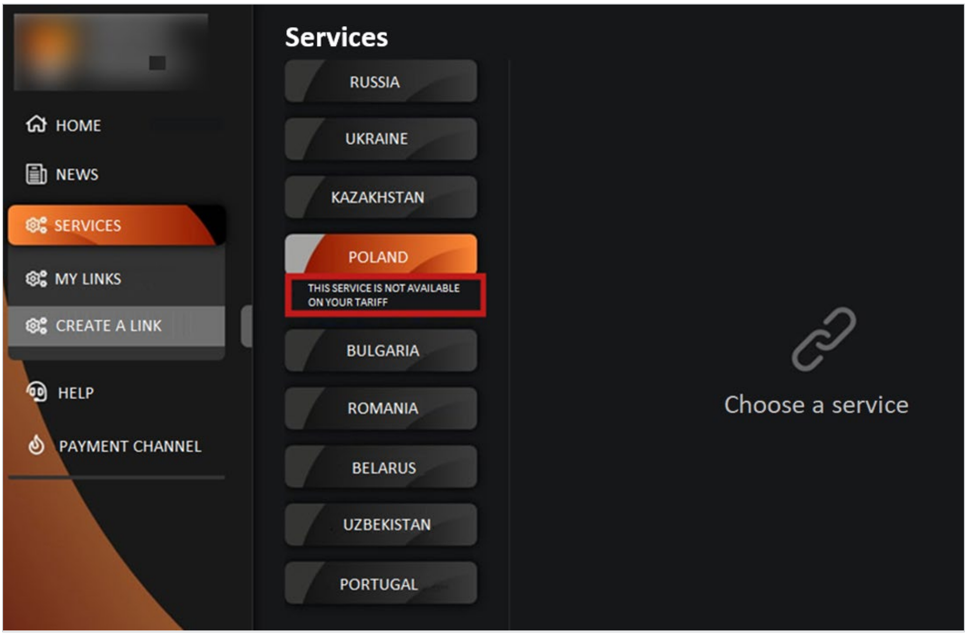
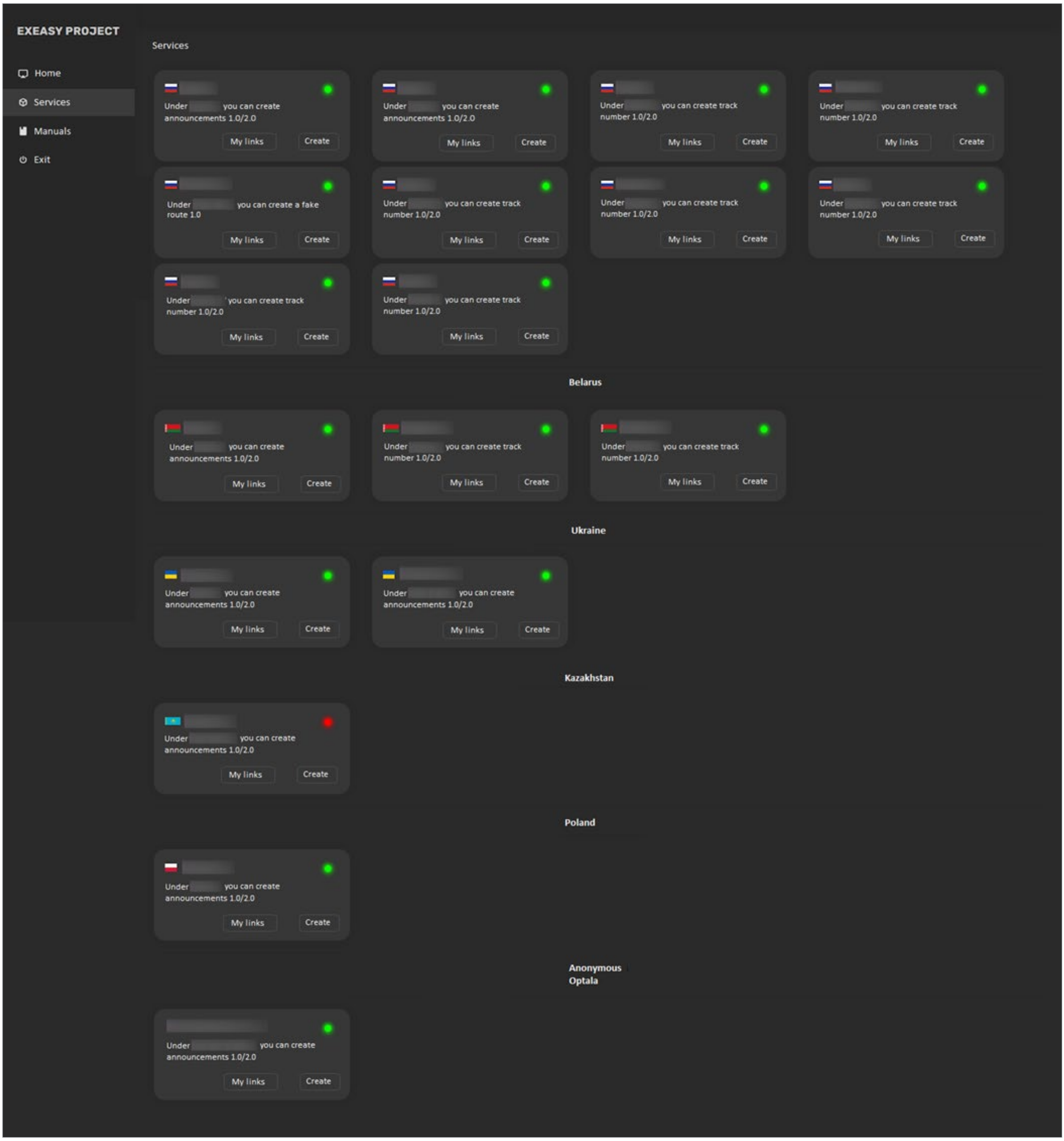


Fig. 2. Example of an administrative panel



THIS SERVICE IS NOT AVAILABLE ON YOUR TARIFF

Fig. 3. Example of an administrative panel



Services

[redacted] Under [redacted] you can create announcements 1.0/2.0

[redacted] Under [redacted] you can create announcements 1.0/2.0

[redacted] Under [redacted] you can create track number 1.0/2.0

[redacted] Under [redacted] you can create track number 1.0/2.0

[redacted] Under [redacted] you can create a fake route 1.0

[redacted] Under [redacted] you can create track number 1.0/2.0

[redacted] Under [redacted] you can create track number 1.0/2.0

[redacted] Under [redacted] you can create track number 1.0/2.0

[redacted] Under [redacted] 'you can create track number 1.0/2.0

[redacted] Under [redacted] you can create track number 1.0/2.0

Belarus

[redacted] Under [redacted] you can create announcements 1.0/2.0

[redacted] Under [redacted] you can create track number 1.0/2.0

[redacted] Under [redacted] you can create track number 1.0/2.0

Ukraine

[redacted] Under [redacted] you can create announcements 1.0/2.0

[redacted] Under [redacted] you can create announcements 1.0/2.0

Kazakhstan

[redacted] Under [redacted] you can create announcements 1.0/2.0

Poland

[redacted] Under [redacted] you can create announcements 1.0/2.0

Anonymous
Optala

[redacted] Under [redacted] you can create announcements 1.0/2.0

Fig. 4. Example of an administrative panel

In addition to a functionality that creates phishing pages, administrative panels often contain a user manual section with instructions to help newcomers.

How the Classiscam scheme evolved

In 2019, Classiscam first appeared on classifieds websites. Scammers did not even use phishing pages: they simply tried to persuade users to transfer money for purchased goods using a bank card or phone number.

Scammers acted as sellers only and used traditional tricks to lure potential buyers: low prices, limited-time offers, and exclusive or hard-to-find items.

Initially, scammers used the following scheme:

Initially, scammers used the following scheme:

1 **Creating or searching for a lure post on a classifieds website**

Threat actors register new accounts or use hacked accounts for various Internet services. They also create their own application or use a third-party application depending on the scheme. For example, they use posts that target various audiences by selling undervalued goods: game consoles, laptops, smartphones, chainsaws, car audio systems, sewing machines, collectibles, fishing fear, sports nutrition, and more.

To find victims more easily, workers use services for tracking ads on the Internet platforms that they plan to attack. The technique helps them carry out mass mailouts to sellers of a specific item or service, thereby improving their chances to find a user that they will be able to trick.

2 **Contacting the victim**

After a user contacts threat actors via an internal chat on the Internet platform, they ask the user to switch to WhatsApp or Viber to continue negotiating the terms of purchase and delivery. Internal chats often notify users about suspicious links and sometimes even delete such links automatically, whereas messengers do not.

3 **Preparing the transaction**

When threat actors communicate with their victims via messaging services, they do their best to look like scrupulous buyers or sellers. They request the victim’s full name, address, and phone number, allegedly to fill in delivery forms on courier service resources. Scammers also describe, or ask victims to describe, the condition of a listed item, demand sales receipts, etc. At this stage, it is difficult to tell a scammers from a legitimate buyer or seller.

4 **Payment through a phishing website**

When negotiations are over, the scammers persuade the victim to follow a pre-created link leading to a phishing resource that fully mimics the legitimate web page of a popular courier service. They provide the victim’s personal data specified at the previous stage to verify that it is legit. The payment is then made on the same resource.

5 **Second deception**

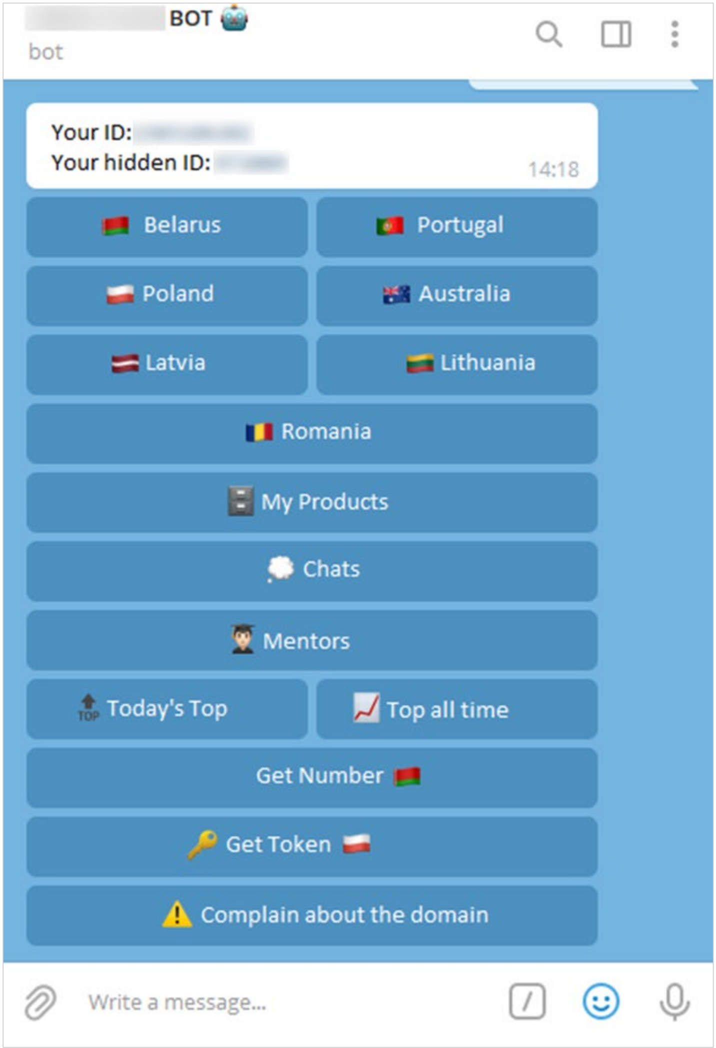
In some cases, scammers manage to trick their victims twice by persuading them to request a refund. After paying for the goods, the buyer is informed that there was an emergency at the post office. The story can take any form: for example, a postal service employee was caught stealing and the ordered goods were seized by the police. As a result, the buyer must request a refund in order to receive their money back. The victim is shown a dedicated web page where they need to provide their bank card data and CVV code, then enter the password received via SMS. Instead of a refund, the same amount is deducted from the card again.

Switch to Telegram bots

Although up to a certain point generating links via an administrative panel took a relatively long time and offered limited functionality compared to modern Telegram bots, the scheme was popular even then.

The leaders of any criminal group strive to scale up the business and attract as many new members as possible. Considering the favorability of the scheme, it was only a matter of time to solve the problem associated with the limited functionality of the administrative panel. The evolution of Telegram bots helped threat actors find new ways to use the platform to achieve their goals, which gave them the opportunity to bypass restrictions and reach a new level thanks to automation and scaling.

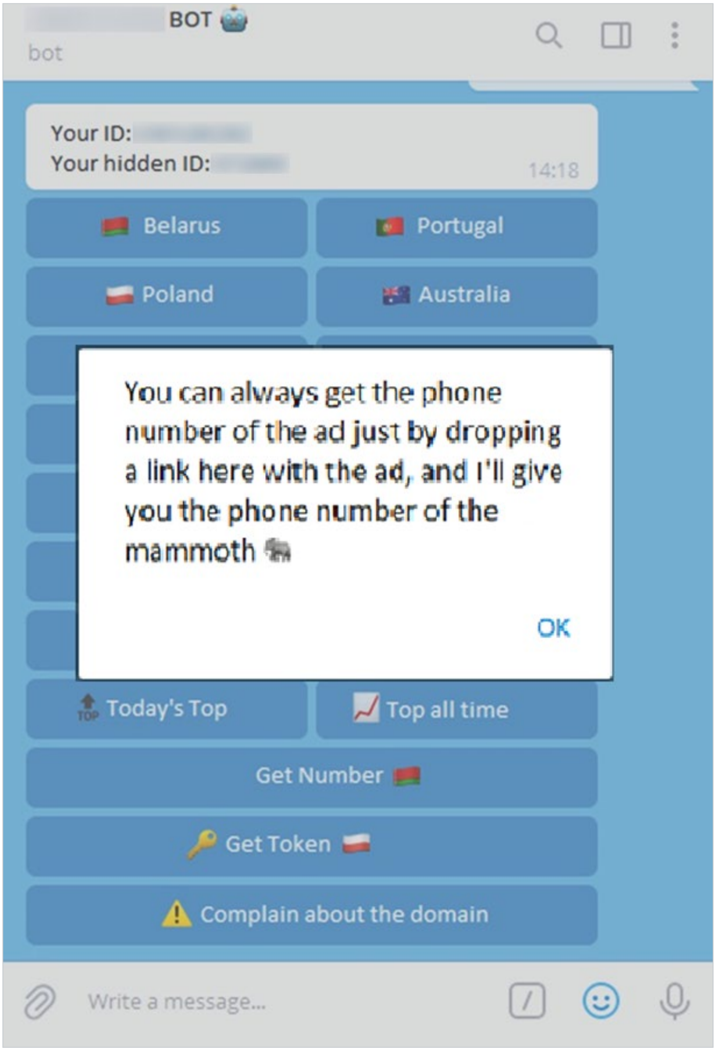
Telegram bots can create links, withdraw money, place job offers, sell all the required tools and instructions, place ads, and even provide legal services. Some examples of Telegram bot interfaces are shown below in Figures 5 to 9.



[redacted] BOT 🤖
bot

Your ID: [redacted]
Your hidden ID: [redacted] 14:18

Fig. 5. Example of a Telegram bot interface

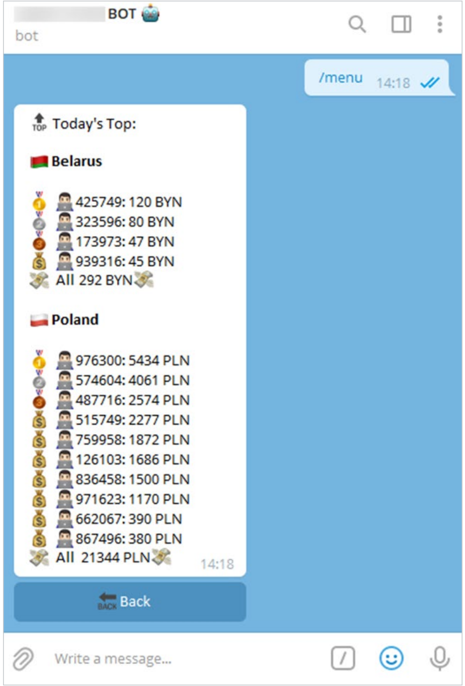


[redacted] BOT 🤖
bot

Your ID: [redacted]
Your hidden ID: [redacted] 14:18

You can always get the phone number of the ad just by dropping a link here with the ad, and I'll give you the phone number of the mammoth 🐘

Fig. 6. Example of a Telegram bot interface



[redacted] BOT 🤖
bot

/menu 14:18 ✓✓

🔝 Today's Top:

🇧🇾 Belarus

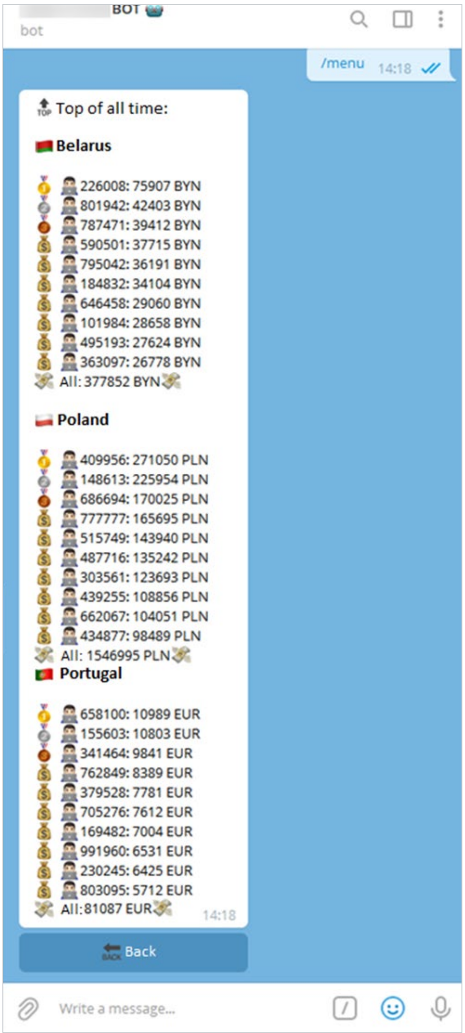
🥇 👨‍💻 425749: 120 BYN
🥈 👨‍💻 323596: 80 BYN
🥉 👨‍💻 173973: 47 BYN
💰 👨‍💻 939316: 45 BYN
💸 All 292 BYN 💸

🇵🇱 Poland

🥇 👨‍💻 976300: 5434 PLN
🥈 👨‍💻 574604: 4061 PLN
🥉 👨‍💻 487716: 2574 PLN
💰 👨‍💻 515749: 2277 PLN
💰 👨‍💻 759958: 1872 PLN
💰 👨‍💻 126103: 1686 PLN
💰 👨‍💻 836458: 1500 PLN
💰 👨‍💻 971623: 1170 PLN
💰 👨‍💻 662067: 390 PLN
💰 👨‍💻 867496: 380 PLN
💸 All 21344 PLN 💸 14:18

🔙 Back

Fig. 7. Example of a Telegram bot interface featuring a Top Workers section



[redacted] BOT 🤖
bot

/menu 14:18 ✓✓

🔝 Top of all time:

🇧🇾 Belarus

🥇 👨‍💻 226008: 75907 BYN
🥈 👨‍💻 801942: 42403 BYN
🥉 👨‍💻 787471: 39412 BYN
💰 👨‍💻 590501: 37715 BYN
💰 👨‍💻 795042: 36191 BYN
💰 👨‍💻 184832: 34104 BYN
💰 👨‍💻 646458: 29060 BYN
💰 👨‍💻 101984: 28658 BYN
💰 👨‍💻 495193: 27624 BYN
💰 👨‍💻 363097: 26778 BYN
💸 All: 377852 BYN 💸

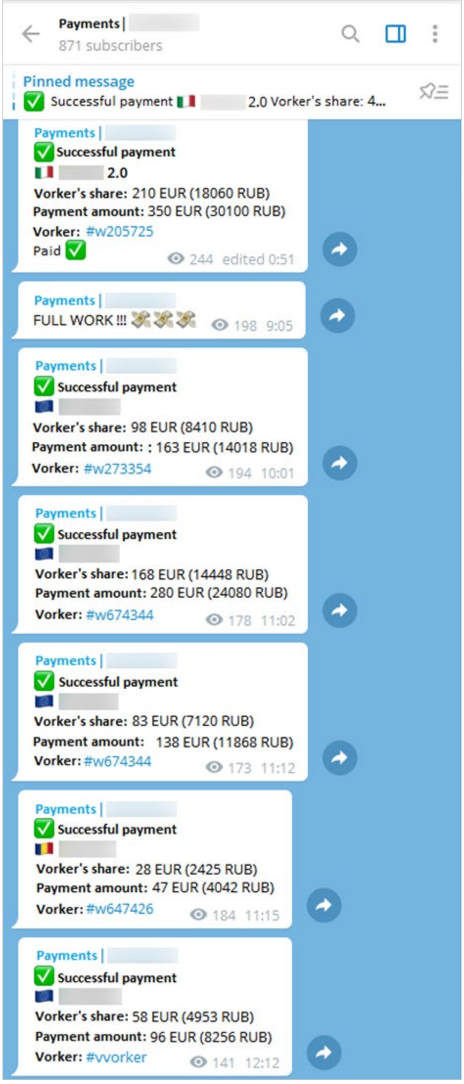
🇵🇱 Poland

🥇 👨‍💻 409956: 271050 PLN
🥈 👨‍💻 148613: 225954 PLN
🥉 👨‍💻 686694: 170025 PLN
💰 👨‍💻 777777: 165695 PLN
💰 👨‍💻 515749: 143940 PLN
💰 👨‍💻 487716: 135242 PLN
💰 👨‍💻 303561: 123693 PLN
💰 👨‍💻 439255: 108856 PLN
💰 👨‍💻 662067: 104051 PLN
💰 👨‍💻 434877: 98489 PLN
💸 All: 1546995 PLN 💸
🇵🇹 Portugal

🥇 👨‍💻 658100: 10989 EUR
🥈 👨‍💻 155603: 10803 EUR
🥉 👨‍💻 341464: 9841 EUR
💰 👨‍💻 762849: 8389 EUR
💰 👨‍💻 379528: 7781 EUR
💰 👨‍💻 705276: 7612 EUR
💰 👨‍💻 169482: 7004 EUR
💰 👨‍💻 991960: 6531 EUR
💰 👨‍💻 230245: 6425 EUR
💰 👨‍💻 803095: 5712 EUR
💸 All:81087 EUR 💸 14:18

🔙 Back

Fig. 8. Example of a Telegram bot interface featuring a Top Workers section



Payments | [redacted]
871 subscribers

Pinned message
✅ Successful payment 🇮🇹 [redacted] 2.0 Vorker's share: 4...

Payments | [redacted]
✅ Successful payment
🇮🇹 [redacted] 2.0
Vorker's share: 210 EUR (18060 RUB)
Payment amount: 350 EUR (30100 RUB)
Vorker: #w205725
Paid ✅
244 edited 0:51

Payments | [redacted]
FULL WORK !!! 💸💸💸 198 9:05

Payments | [redacted]
✅ **Successful payment**
🇪🇺 [redacted]
Vorker's share: 98 EUR (8410 RUB)
Payment amount: : 163 EUR (14018 RUB)
Vorker: #w273354 194 10:01

Payments | [redacted]
✅ **Successful payment**
🇪🇺 [redacted]
Vorker's share: 168 EUR (14448 RUB)
Payment amount: 280 EUR (24080 RUB)
Vorker: #w674344 178 11:02

Payments | [redacted]
✅ **Successful payment**
🇪🇺 [redacted]
Vorker's share: 83 EUR (7120 RUB)
Payment amount: 138 EUR (11868 RUB)
Vorker: #w674344 173 11:12

Payments | [redacted]
✅ **Successful payment**
🇷🇴 [redacted]
Vorker's share: 28 EUR (2425 RUB)
Payment amount: 47 EUR (4042 RUB)
Vorker: #w647426 184 11:15

Payments | [redacted]
✅ **Successful payment**
🇪🇺 [redacted]
Vorker's share: 58 EUR (4953 RUB)
Payment amount: 96 EUR (8256 RUB)
Vorker: #vvorker 141 12:12

Fig. 9. Example of a Telegram channel with worker payouts

Most Telegram bots are developed by third-party specialists who work for fixed fees and do not take part in operating the scheme. Group members are involved in developing Telegram bots on rare occasions only, while the group leader and bot developer are sometimes one and the same person.

Due to the extensive use of various Telegram functionalities, the number of brands involved in the scheme increased **more than 4-fold**. Meanwhile, the geographical footprint of the activities undertaken by the scammers significantly expanded and exceeded its initial range, i.e., CIS countries.

Switching from administrative panels to Telegram bots did not cause any shifts in the composition of scammer groups. The project owner role still belonged to the so-called Topic Starter (TS), but their responsibilities did change significantly.

The distribution scope of the Classiscam scheme is clearly illustrated by the number of participants. Currently, more than **80,000** individuals take part, while the number of domains involved exceeds **5,000**.

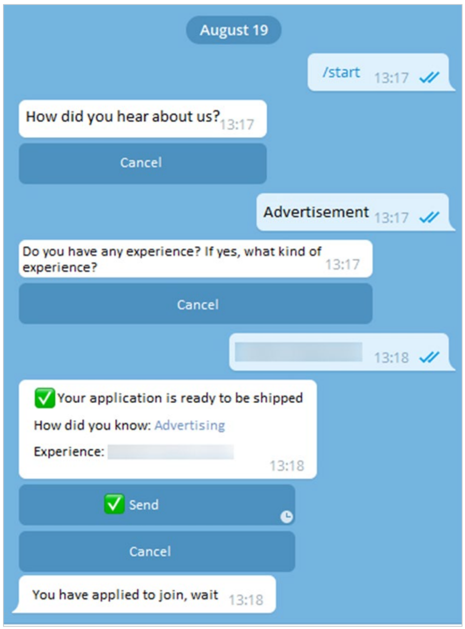
New members are registered via Telegram bots, underground forums, or directly by contacting TSs. Scammers use both public and private chats.

Prospective participants are usually asked about prior engagements in similar projects, their roles, their acquaintances in the project in question, how they found out about the project, underground forum accounts, and proof of successful engagements (Figure 10 below).

After workers have completed the registration procedure, they are given access to three chats:

- General information with current project status, plans for the future and areas for development, scam manuals, etc.
- Worker chats where they communicate with each other, share experiences, and discuss current projects
- Payout chats that conclude the process. Dedicated bots show the usernames of workers who have successfully cheated their victims, how long the operation lasted, the amount they stole, and the brand/platform they used. Often, the chats used for payouts are public – either to attract new participants or to show that the project is ongoing.

The number and composition of chats can differ depending on the group. A tentative scheme is shown in Figure 11 below.



August 19

/start 13:17

How did you hear about us? 13:17

Cancel

Advertisement 13:17

Do you have any experience? If yes, what kind of experience? 13:17

Cancel

[redacted] 13:18

✅ Your application is ready to be shipped

How did you know: Advertising

Experience: [redacted]

13:18

✅ Send

Cancel

You have applied to join, wait 13:18

Fig. 10. Example of an interview with a Telegram bot to become member of a scam group

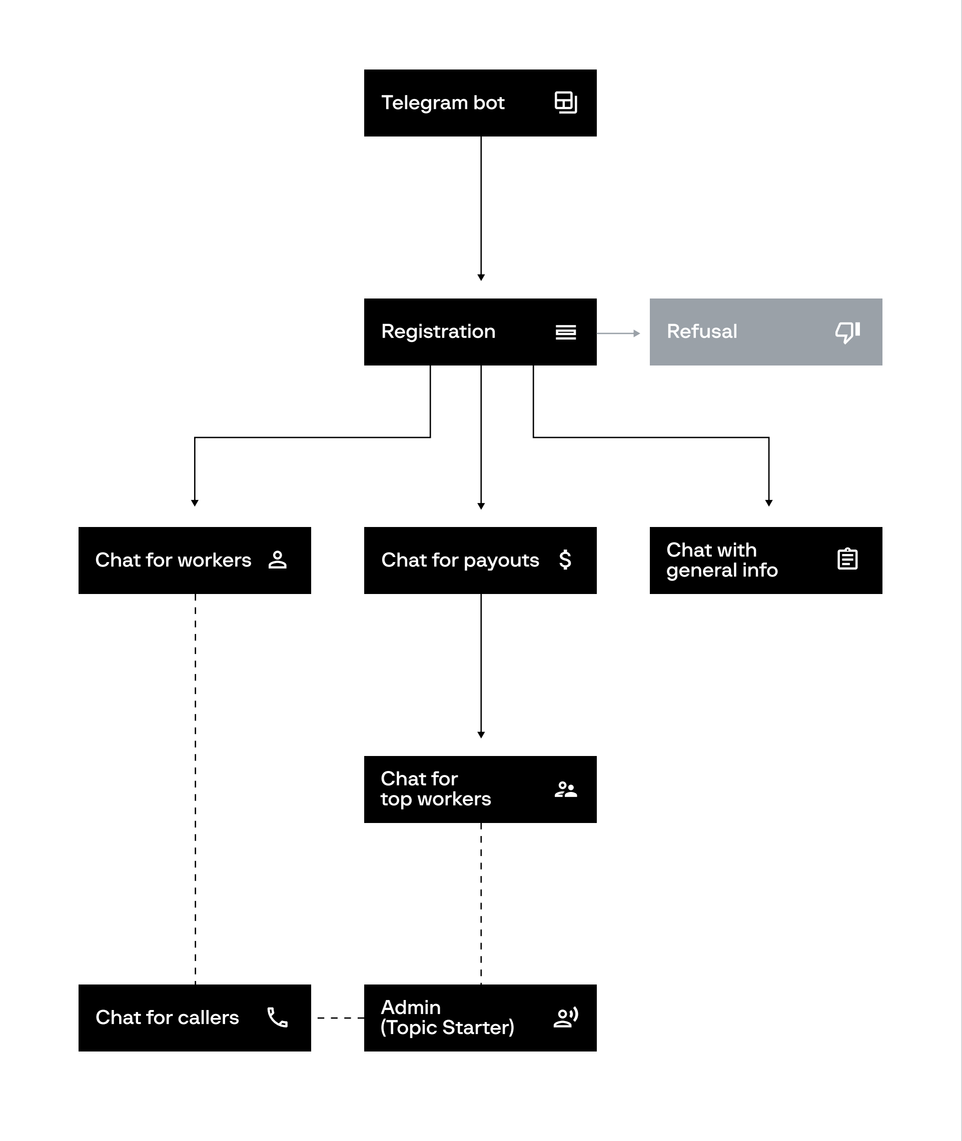
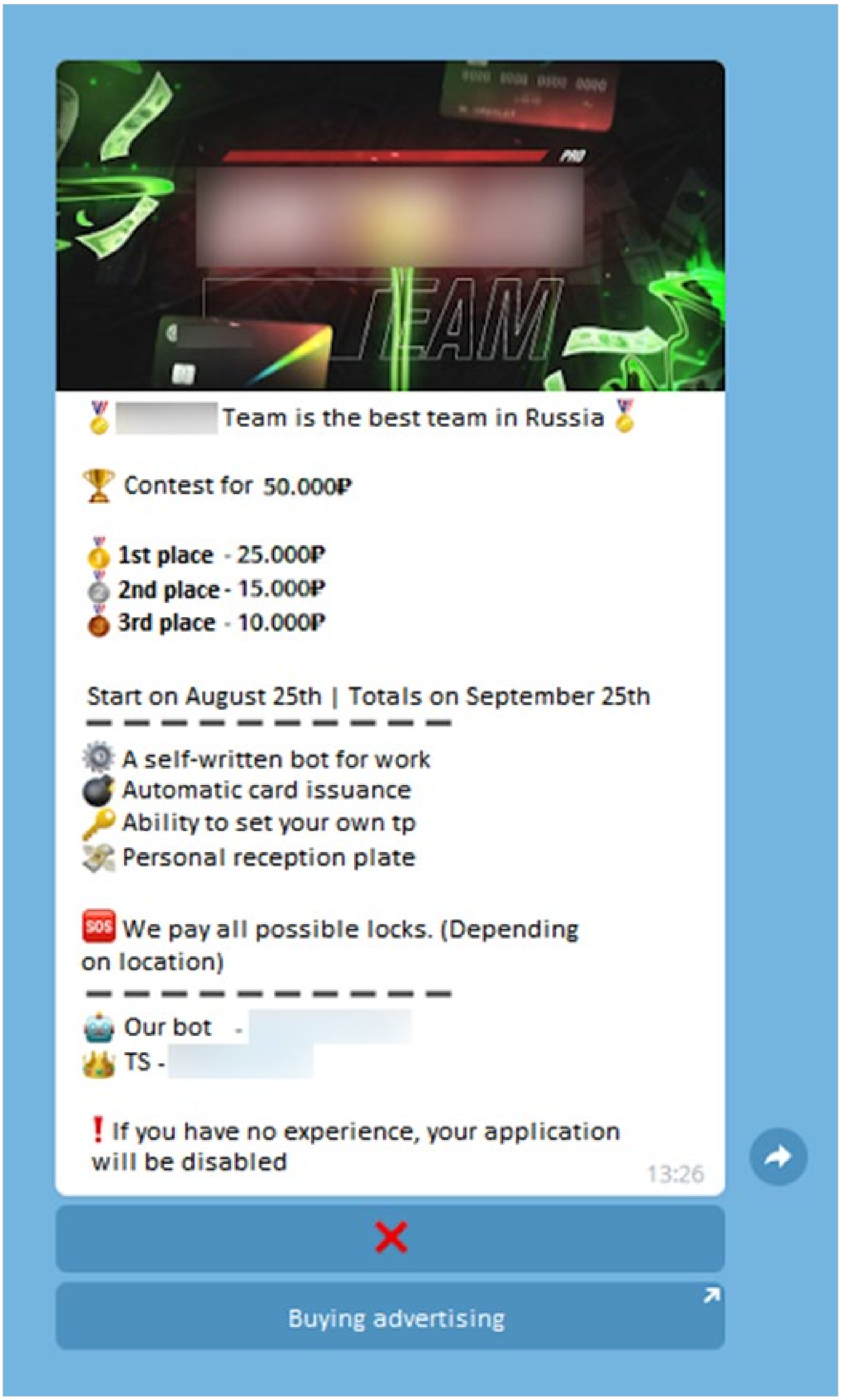


Fig. 11. Example of a scammer group composition and chat access

In some groups, organizers give awards to the most fruitful workers and add their usernames to a public payout chart (Figure 12). The top gainers are given access to a so-called VIP chat, where participants can influence how the project is developed and use VIP scripts. For example, top workers in one of the groups have exclusive access to operations in Italy and the US, while other scammers do not have this opportunity and are restricted from the VIP chat.



🥇 [redacted] Team is the best team in Russia 🥇

🏆 Contest for 50.000₽

🥇 1st place - 25.000₽
🥈 2nd place - 15.000₽
🥉 3rd place - 10.000₽

Start on August 25th | Totals on September 25th
— — — — — — — — — —
⚙️ A self-written bot for work
💣 Automatic card issuance
🔑 Ability to set your own tp
💸 Personal reception plate

🆘 We pay all possible locks. (Depending on location)
— — — — — — — — — —
🤖 Our bot - [redacted]
👑 TS - [redacted]

❗ If you have no experience, your application will be disabled

13:26

❌

Buying advertising

Fig. 12. Example of an advertisement to hire workers

The modern Classiscam scheme

The current iteration of the Classiscam scheme was created following the evolution of the software interface and functionalities of Telegram bots, which helped scammers move away from websites with administrative panels designed to create phishing pages. Instead they began using Telegram for both communicating and deploying all the tools required for their attacks.

One characteristic feature of the new scheme involving Telegram bots is the high degree of process automation, including the generation of phishing links, payout distribution, worker supervision, and – most importantly – traffic generated manually by regular participants, i.e., workers.

On account of the easy and user-friendly interfaces of Telegram bots and efficient user manuals, participants were no longer required to have high technical skills. The low entry threshold and high payout rate of the scam scheme led to a wide-scale influx of workers in scam groups.

Unlike traditional phishing schemes that rely on semi-automatic attraction of traffic (via spam mailouts, SEO promotion of phishing websites, and creating accounts on social media), as part of this scheme scammers attract traffic manually by manipulating potential victims.

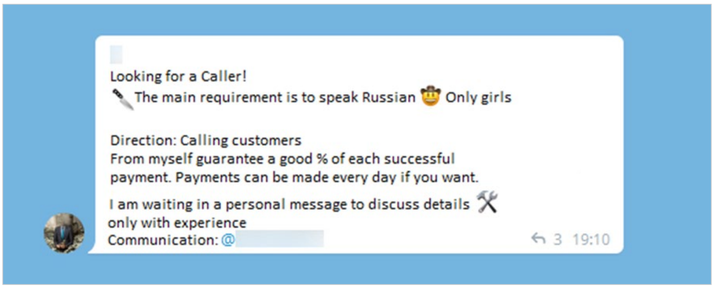
Scam resources do not work on a regular basis. For each individual attempt they generate a new link with a limited lifecycle. The link is deleted manually immediately after a scam attempt, irrespective of its outcome. Failing that, it automatically expires 24 hours after being created.

Additional services and functionalities that help scammers persuade victims

Scammers sometimes employ assistants whose job is to influence victims in order to achieve the desired result. Various methods are used to that end, including:

- **Assistant workers**

  “callers” or “refunders” who masquerade as a platform’s support service team; “bombers” who use dedicated applications for spam SMS mailouts and mass spam phone calls; and scammers who support the operation by manually performing money transactions. If an attack is successful, assistants receive a fixed percentage of the total profit (Figures 13 to 16).

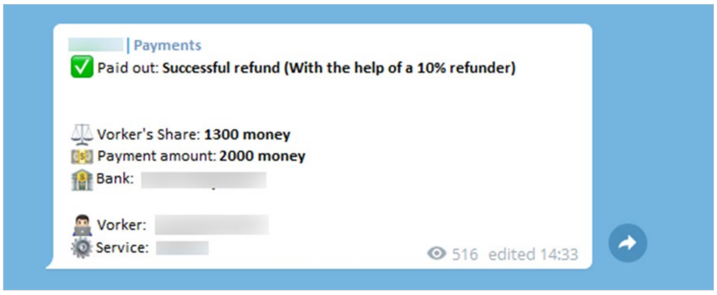


[redacted]
Looking for a Caller!
🔪 The main requirement is to speak Russian 🤠 Only girls

Direction: Calling customers
From myself guarantee a good % of each successful payment. Payments can be made every day if you want.

I am waiting in a personal message to discuss details 🛠
only with experience
Communication: @[redacted]

Fig. 13. Example of an advertisement to hire callers

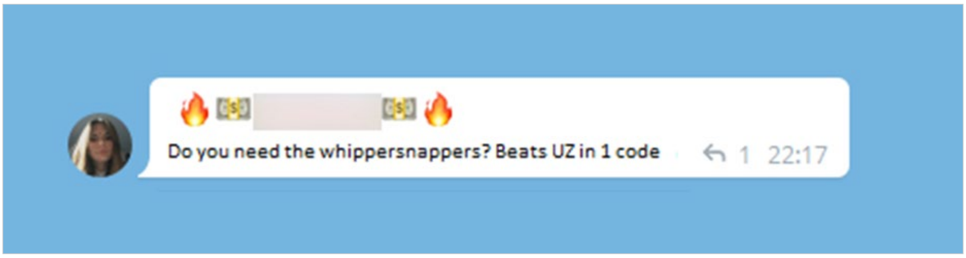


[redacted] | Payments
✅ Paid out: **Successful refund (With the help of a 10% refunder)**

⚖️ Vorker's Share: **1300 money**
💵 Payment amount: **2000 money**
🏦 Bank: [redacted]

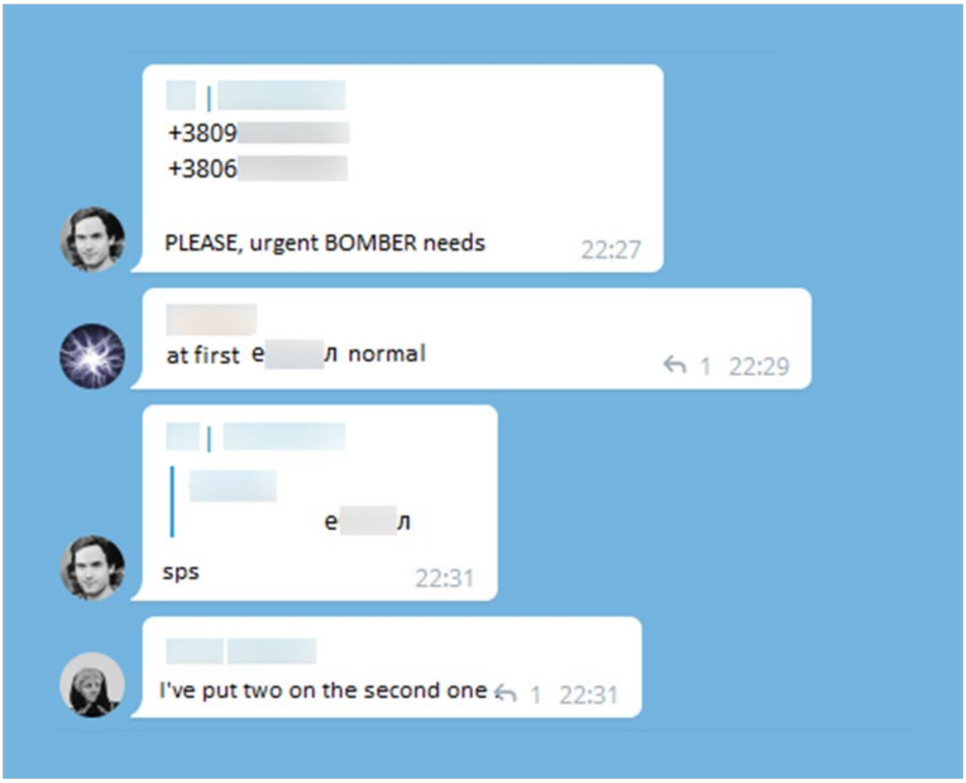
👨‍💻 Vorker: [redacted]
⚙️ Service: [redacted]

Fig. 14. Example of a report on receiving money as part of a refund scheme



🔥💵[redacted]💵🔥
Do you need the whippersnappers? Beats UZ in 1 code

Fig. 15. Advertisement for support services



[redacted] | [redacted]
+3809[redacted]
+3806[redacted]

PLEASE, urgent BOMBER needs 22:27

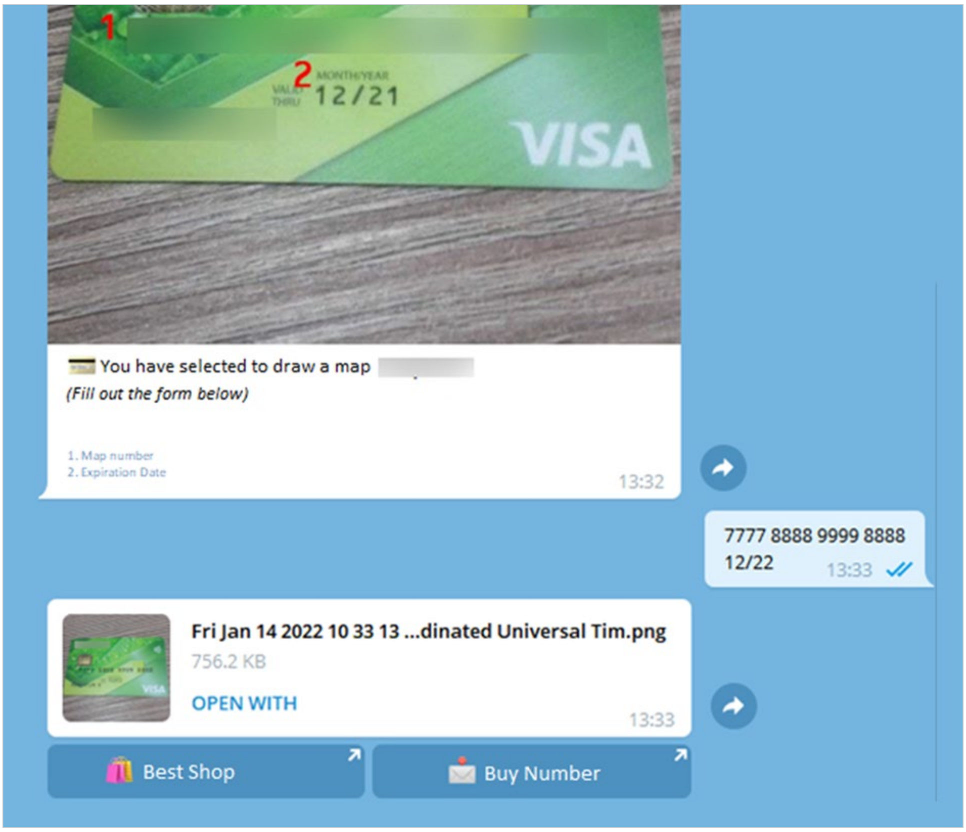
[redacted]
at first e[redacted]л normal ↩ 1 22:29

[redacted] | [redacted]
[redacted]
e[redacted]л
sps 22:31

[redacted]
I've put two on the second one ↩ 1 22:31

Fig. 16. Example of a request to “bomb” a victim

- **Visuals of documents**
  Helps increase the victim’s confidence in the proposed transaction (Figure 17).



You have selected to draw a map [redacted]
(Fill out the form below)

1. Map number
2. Expiration Date

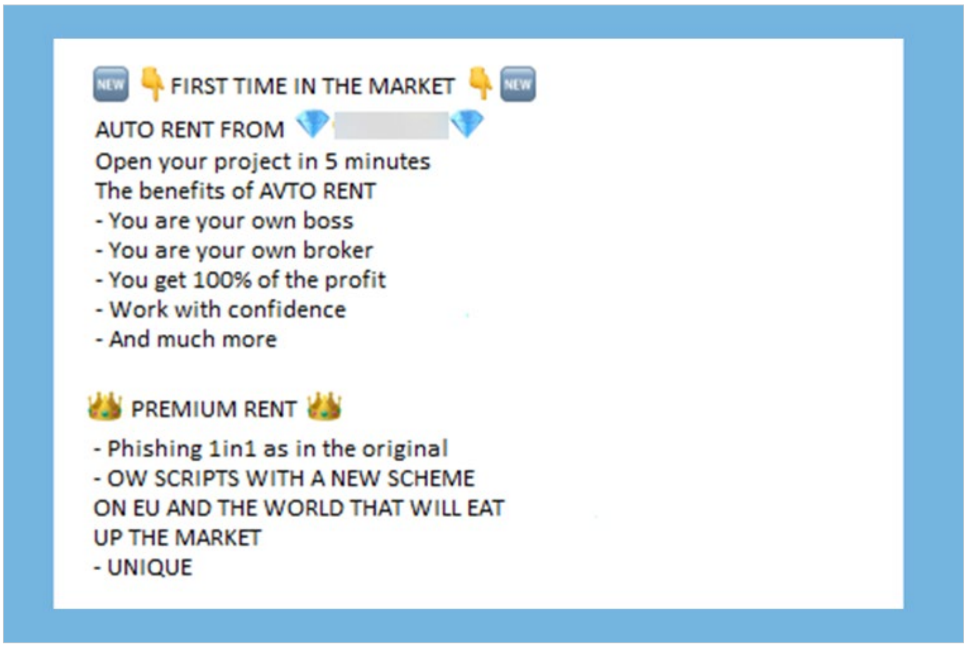
13:32

7777 8888 9999 8888
12/22 13:33

Fri Jan 14 2022 10 33 13 ...dinated Universal Tim.png
756.2 KB
OPEN WITH
13:33

Fig. 17. Example of a visual of a bank card

- **Development and lease of Telegram bots**
  By leasing Telegram bots, threat actors can single-handedly carry out scam attacks and pocket the entire sum received from victims all the while gaining a share of the money stolen by workers who use the rented bot. An advertisement for renting a bot is shown in Figure 18 below.



🆕 👇 FIRST TIME IN THE MARKET 👇 🆕
AUTO RENT FROM 💎[redacted]💎
Open your project in 5 minutes
The benefits of AVTO RENT
- You are your own boss
- You are your own broker
- You get 100% of the profit
- Work with confidence
- And much more

👑 PREMIUM RENT 👑
- Phishing 1in1 as in the original
- OW SCRIPTS WITH A NEW SCHEME
ON EU AND THE WORLD THAT WILL EAT
UP THE MARKET
- UNIQUE

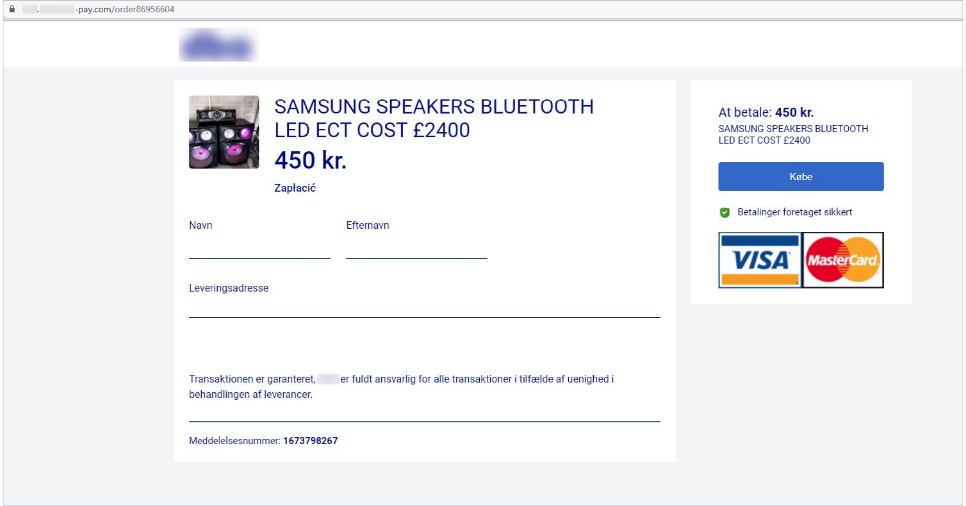
Fig. 18. Example of project rental advertising

Classiscam types

Scammers differentiate their schemes by version: 1.0, 2.0, 3.0, and 4.0.

Versions vary in what actions a worker takes and whether they masquerade as a buyer, a seller, a renter, or an owner.

1.0 — Seller scam. A typical scam scheme: a buyer receives a generated phishing payment link and is defrauded of their money.



[redacted].[redacted]-pay.com/order86956604

[redacted]

SAMSUNG SPEAKERS BLUETOOTH LED ECT COST £2400
450 kr.
Zapłacić

Navn

Efternavn

Leveringsadresse

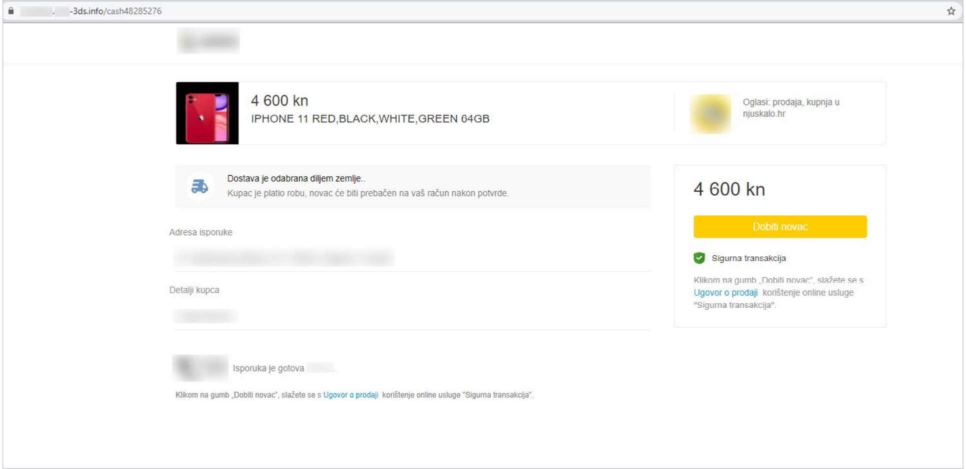
Transaktionen er garanteret, [redacted] er fuldt ansvarlig for alle transaktioner i tilfælde af uenighed i behandlingen af leverancer.

Meddelelsesnummer: **1673798267**

At betale: **450 kr.**
SAMSUNG SPEAKERS BLUETOOTH LED ECT COST £2400

Fig. 19. Example of a phishing page to pay for a purchase

2.0 Buyer scam. Scammers find sellers on classifieds websites and ask to have the listed item sent via a delivery service. The attackers then generate a phishing page and send it to the seller, allegedly for verification. The seller enters their bank card details, but instead of receiving money ends up with the sum deducted from their account.



[redacted]-3ds.info/cash48285276

4 600 kn
IPHONE 11 RED,BLACK,WHITE,GREEN 64GB

Oglasi: prodaja, kupnja u njuskalo.hr

Dostava je odabrana diljem zemlje..
Kupac je platio robu, novac će biti prebačen na vaš račun nakon potvrde.

Adresa isporuke
[redacted]

Detalji kupca
[redacted]

Isporuka je gotova [redacted].

Klikom na gumb „Dobiti novac", slažete se s Ugovor o prodaji korištenje online usluge "Sigurna transakcija".

4 600 kn

Sigurna transakcija

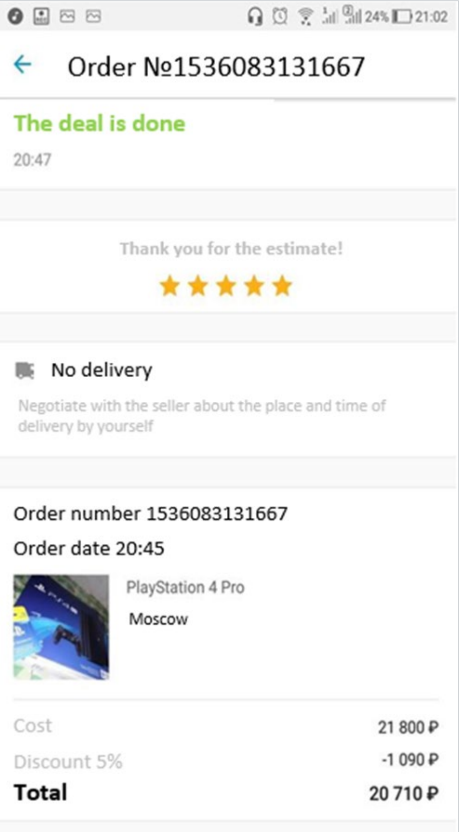
Klikom na gumb „Dobiti novac", slažete se s Ugovor o prodaji korištenje online usluge "Sigurna transakcija".

Fig. 20. A phishing page used to receive money for the item for sale

3.0 A seller publishes an advertisement with preactivated delivery included. When a buyer pays for the item, the scammers sends a screenshot with a message from the service admins asking for a verification code.

Using this code, the seller gains access to the user's account and ticks the box that confirms receipt of the purchased item.

As a result, the buyer gets defrauded of both the item and their money.



24% 21:02

Order №1536083131667

The deal is done
20:47

Thank you for the estimate!
★★★★★

No delivery
Negotiate with the seller about the place and time of delivery by yourself

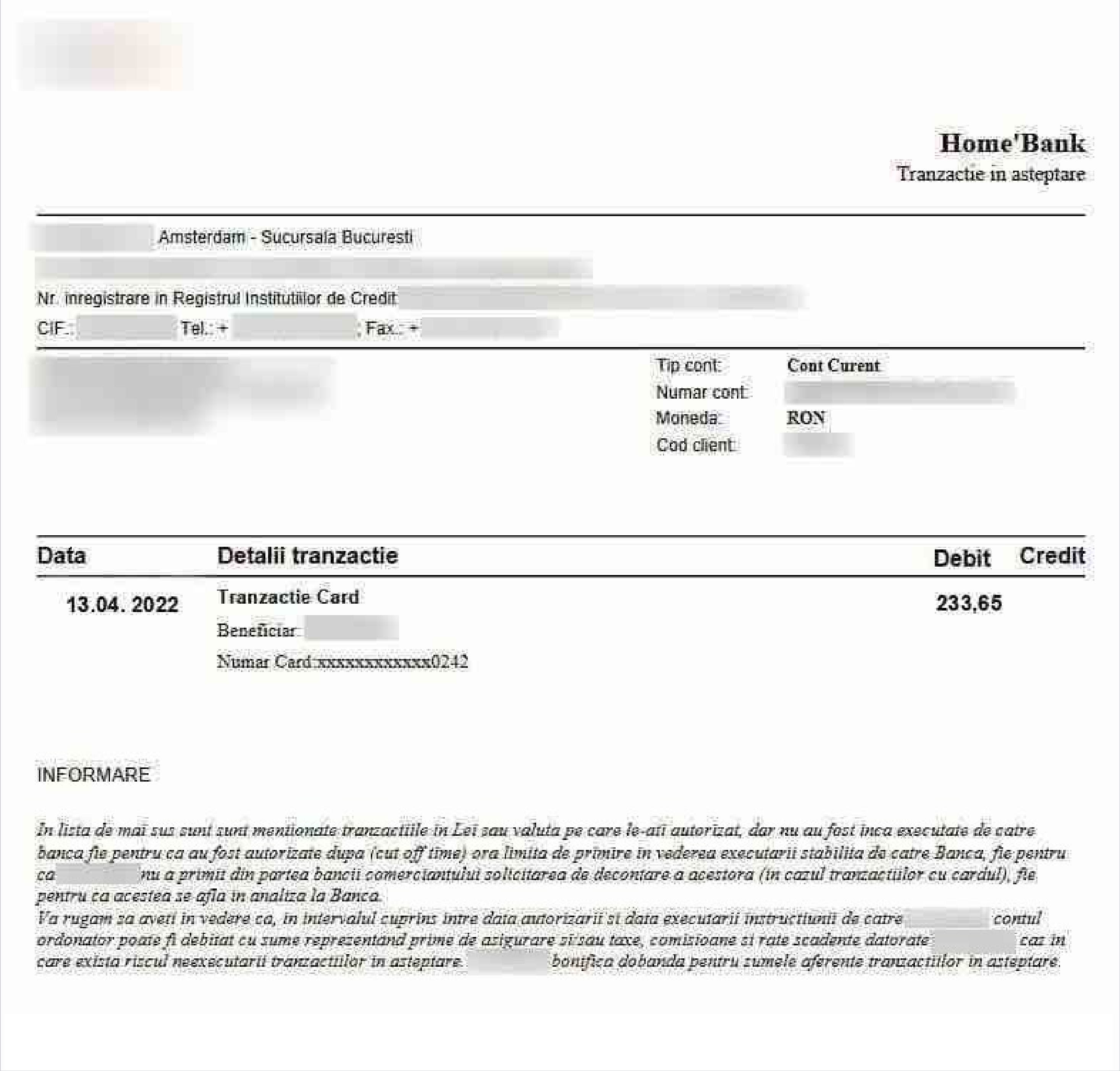
Order number 1536083131667
Order date 20:45

PlayStation 4 Pro
Moscow

Cost	21 800 ₽
Discount 5%	-1 090 ₽
Total	20 710 ₽

Fig. 21. Confirmation of receipt of goods by a scammer

4.0 The buyer pretends to have paid for the product and sends a fake check. After a few minutes, the buyer messages the seller saying that they prefer another seller's item and asks for their money back. Often, scammers say something like, "Please give me my money back. You are not a scammer, are you?". The seller returns the money, unknowingly making a dent in their own savings since no payment was made.



[redacted]

Home'Bank
Tranzactie in asteptare

[redacted] Amsterdam - Sucursala Bucuresti
[redacted]
Nr. inregistrare in Registrul Institutiilor de Credit [redacted]
CIF.: [redacted] Tel.: + [redacted] ; Fax.: + [redacted]

[redacted]

Tip cont:	Cont Curent
Numar cont:	[redacted]
Moneda:	RON
Cod client:	[redacted]

Data	Detalii tranzactie	Debit	Credit
13.04. 2022	Tranzactie Card Beneficiar: [redacted] Numar Card:xxxxxxxxxxxx0242	233,65	

INFORMARE

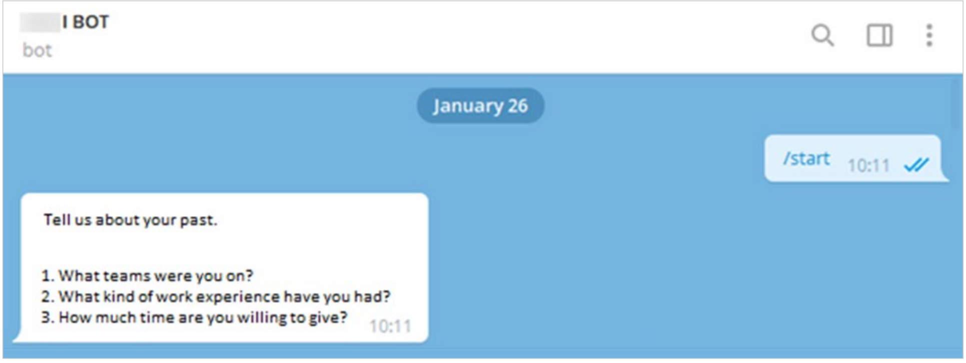
In lista de mai sus sunt sunt mentionate tranzactiile in Lei sau valuta pe care le-ati autorizat, dar nu au fost inca executate de catre banca fie pentru ca au fost autorizate dupa (cut off time) ora limita de primire in vederea executarii stabilita de catre Banca, fie pentru ca [redacted] *nu a primit din partea bancii comerciantului solicitarea de decontare a acestora (in cazul tranzactiilor cu cardul), fie pentru ca acestea se afla in analiza la Banca.*
Va rugam sa aveti in vedere ca, in intervalul cuprins intre data autorizarii si data executarii instructiunii de catre [redacted] *contul ordonator poate fi debitat cu sume reprezentand prime de asigurare si/sau taxe, comisioane si rate scadente datorate* [redacted] *caz in care exista riscul neexecutarii tranzactiilor in asteptare.* [redacted] *bonifica dobanda pentru sumele aferente tranzactiilor in asteptare.*

Fig. 22. Example of a fake payment receipt

Joining scam groups and creating phishing pages using Telegram bots

Joining scam groups

To generate phishing links using a Telegram bot that belongs to a scam group, a candidate must first be interviewed by the group admins (Figure 23). As part of the process, they must launch a dedicated bot and then press a confirmation button when required.



[redacted] I BOT
bot

January 26

/start 10:11

Tell us about your past.

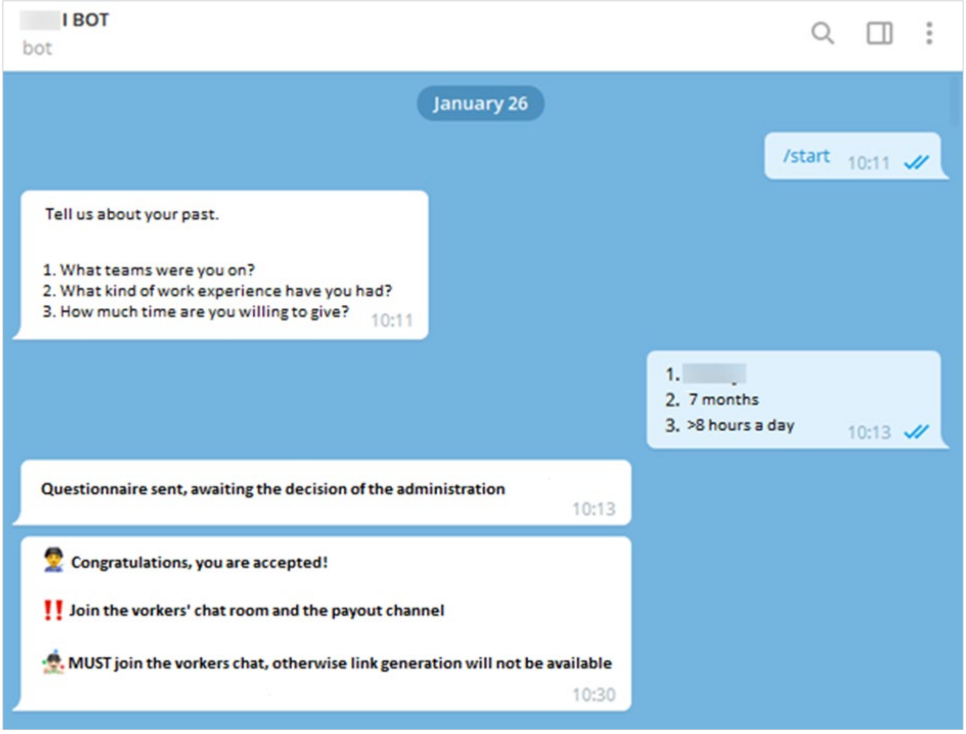
1. What teams were you on?
2. What kind of work experience have you had?
3. How much time are you willing to give? 10:11

Fig. 23. Examples of questions asked by admins to aspiring scam group members

Candidates must answer several questions designed to help admins assess their experience with the type of scam scheme in question (Figure 24). Often, candidates are asked to name:

- **Scam groups** that they used to work for or still work for
- **Online platforms** with which they have experience
- **The amount of time** that they plan to dedicate to scam activities

Candidates are also often asked for a **screenshot** with their **payouts** and the **account ID** of the worker who invited them to the project.



[redacted] I BOT
bot

January 26

/start 10:11

Tell us about your past.

1. What teams were you on?
2. What kind of work experience have you had?
3. How much time are you willing to give? 10:11

1. [redacted]
2. 7 months
3. >8 hours a day 10:13

Questionnaire sent, awaiting the decision of the administration 10:13

Congratulations, you are accepted!

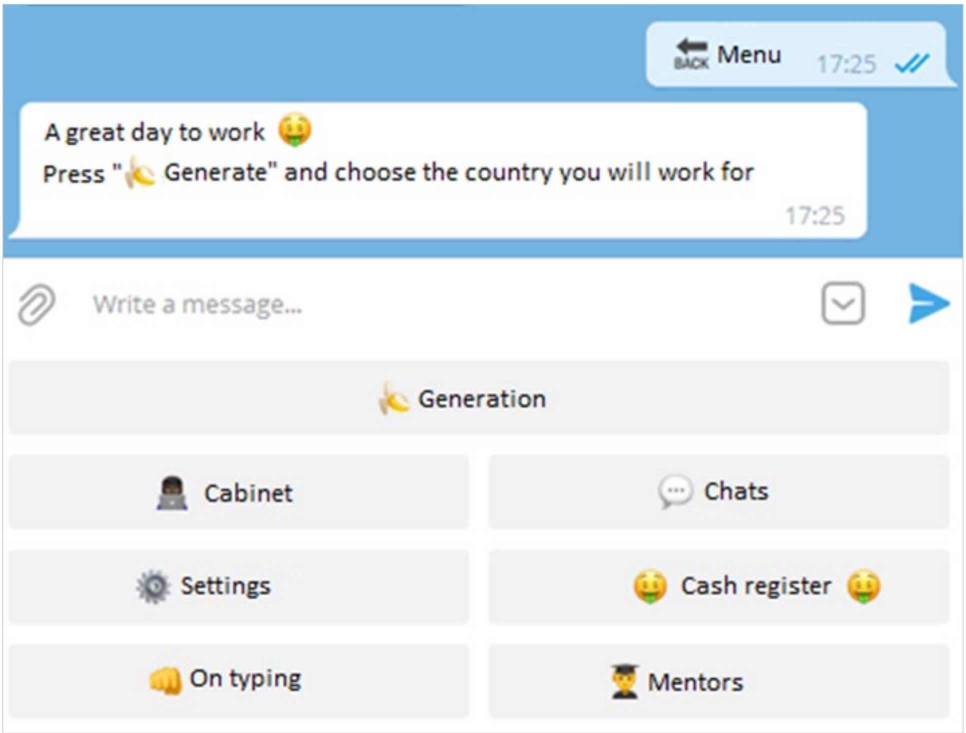
‼ Join the vorkers' chat room and the payout channel

MUST join the vorkers chat, otherwise link generation will not be available 10:30

Fig. 24. Example of a successful application to a scam group

Creating phishing links

Telegram bots have a dedicated section for creating phishing links that can be opened from the main menu (Figure 25). The section can have different names: “brands”, “link generation”, “create a link/tracking number” (depending on a platform type), etc.



🔙 Menu 17:25

A great day to work 🤑
Press "🍌 Generate" and choose the country you will work for
17:25

Fig. 25. Example of a bot menu

Next, the worker must choose a country/brand as a template to generate a phishing link (Figure 26).

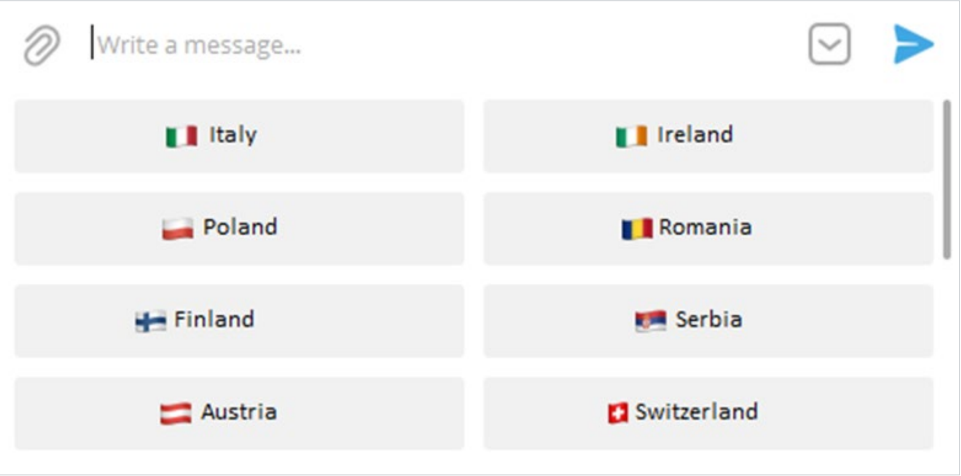
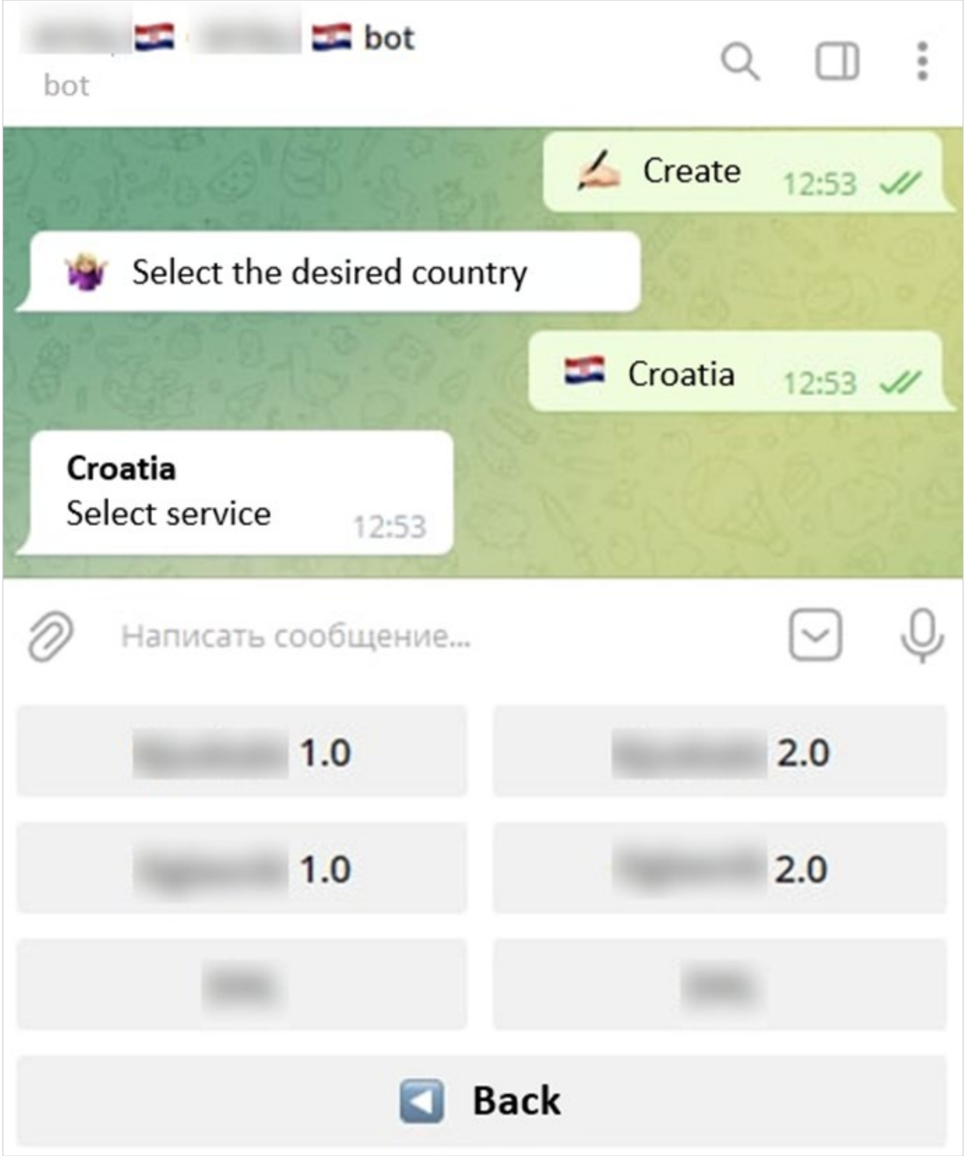


Fig. 26. Choosing a country



bot

bot

✍️ Create 12:53

Select the desired country

Croatia 12:53

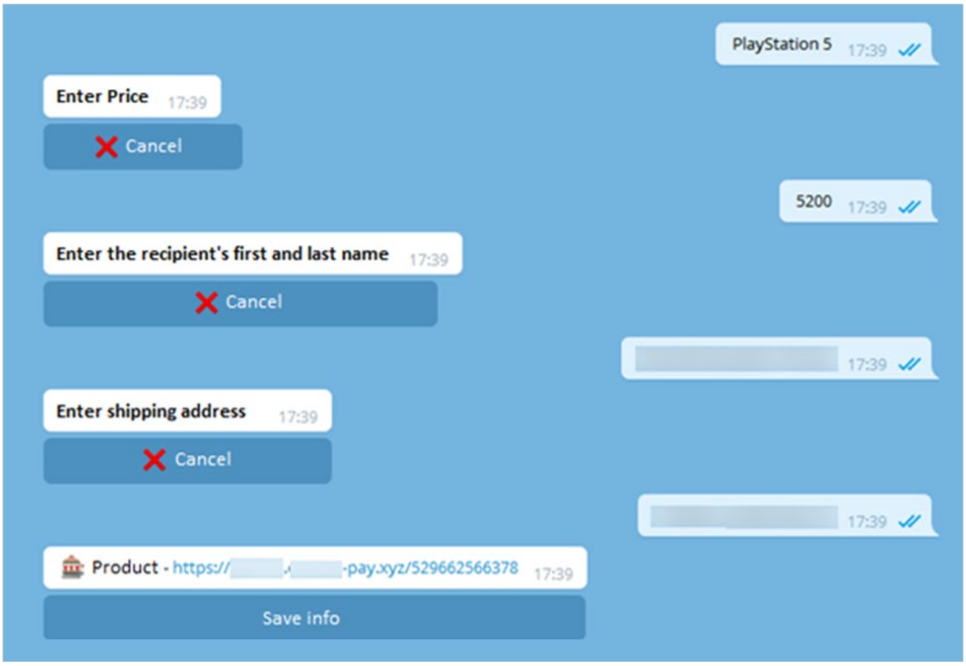
Croatia
Select service 12:53

Fig. 27. Classiscam versions

Some bots inform users in advance what Classiscam version (Figure 27) will be used to generate a phishing link. In other cases, users can choose the version after setting the link generation parameters.

After the scammer has chosen the brand to attack, they must fill out the key parameters that their phishing page will be based on (Figure 28). They usually provide the following information:

- Name of goods/services
- Price
- Photos of goods/services
- Name of the recipient
- Mobile phone number of the recipient
- Address of the recipient



PlayStation 5 17:39

Enter Price 17:39

5200 17:39

Enter the recipient's first and last name 17:39

[redacted] 17:39

Enter shipping address 17:39

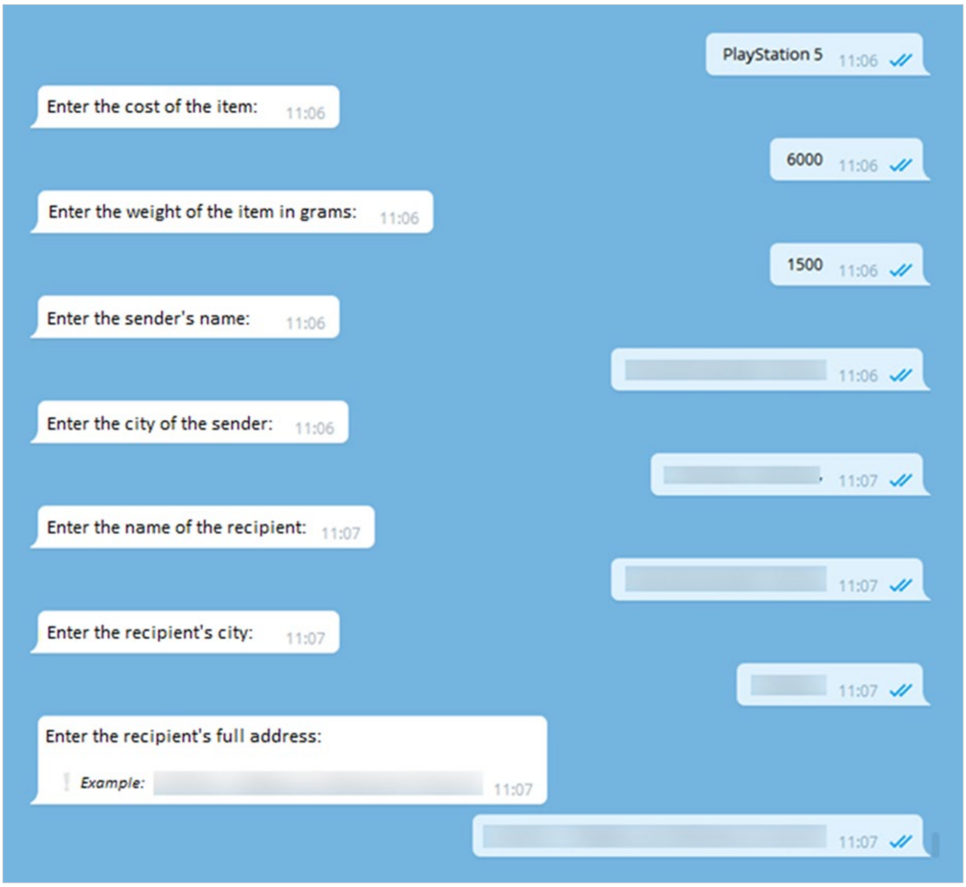
[redacted] 17:39

Product - https://[redacted].[redacted]-pay.xyz/529662566378 17:39

Fig. 28. The choice of key parameters required to generate a phishing link

If a worker plans to create a phishing page supposedly belonging to a logistics company, they also need to enter the name and city of the sender, the weight of the package, and the date when it was sent/received (Figure 29).

In some cases, they only need to provide a link to a listed item leading to the legitimate website that will be used to create a phishing link with the same data.



PlayStation 5 11:06

Enter the cost of the item: 11:06

6000 11:06

Enter the weight of the item in grams: 11:06

1500 11:06

Enter the sender's name: 11:06

[redacted] 11:06

Enter the city of the sender: 11:06

[redacted] 11:07

Enter the name of the recipient: 11:07

[redacted] 11:07

Enter the recipient's city: 11:07

[redacted] 11:07

Enter the recipient's full address:

Example: [redacted] 11:07

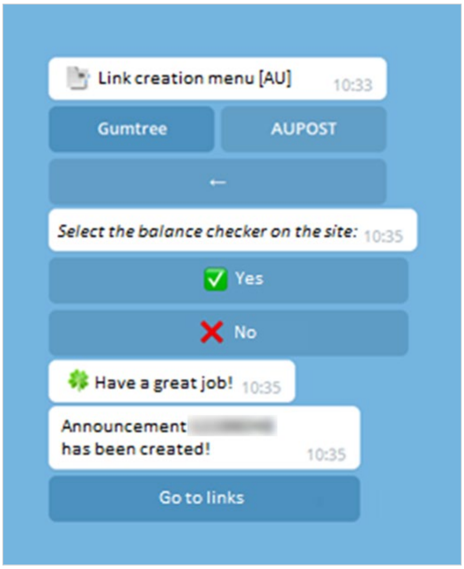
[redacted] 11:07

Fig. 29. Creating a phishing page supposedly belonging to a logistics company

After a worker has entered all the abovementioned data, a bot can request to enable a functionality that will check the victim's account balance. If this functionality is enabled, a form to enter the bank card account balance will be embedded into the newly generated phishing page. This is done so that the scammer can withdraw all the money from the victim's account.

After that, the Telegram bot generates a phishing link (or several links depending on the version of the scam scheme). Some types of bots generate links to several brands in one go.

An example of a phishing page is shown in Figure 31 below.



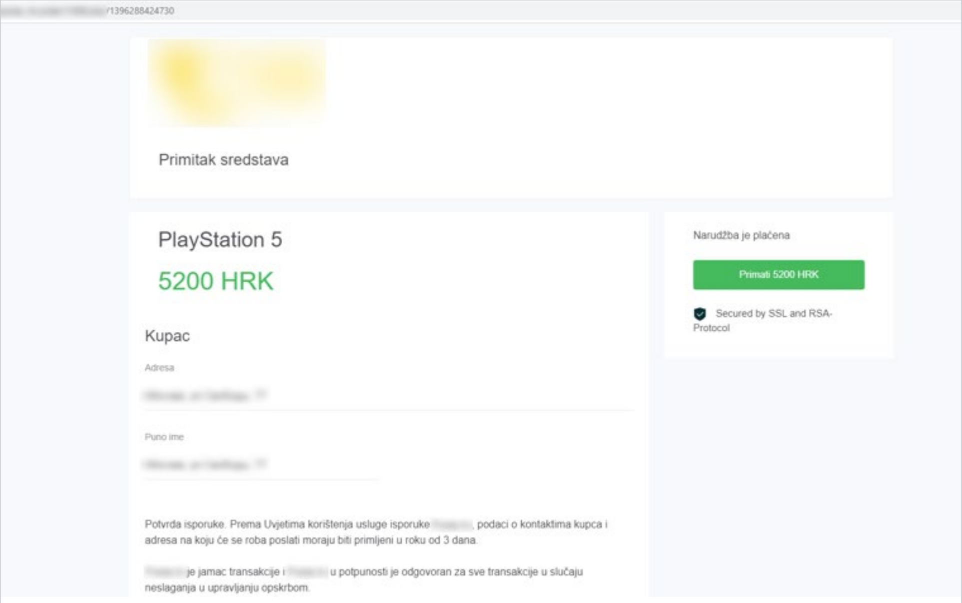
Link creation menu [AU] 10:33

Select the balance checker on the site: 10:35

🍀 Have a great job! 10:35

Announcement [redacted] has been created! 10:35

Fig. 30. Example of creating a phishing link



[redacted]/1396288424730

Primitak sredstava

PlayStation 5

5200 HRK

Kupac

Adresa

[redacted]

Puno ime

[redacted]

Potvrda isporuke. Prema Uvjetima korištenja usluge isporuke [redacted], podaci o kontaktima kupca i adresa na koju će se roba poslati moraju biti primljeni u roku od 3 dana.

[redacted] je jamac transakcije i [redacted] u potpunosti je odgovoran za sve transakcije u slučaju neslaganja u upravljanju opskrbom.

Narudžba je plaćena

Secured by SSL and RSA-Protocol

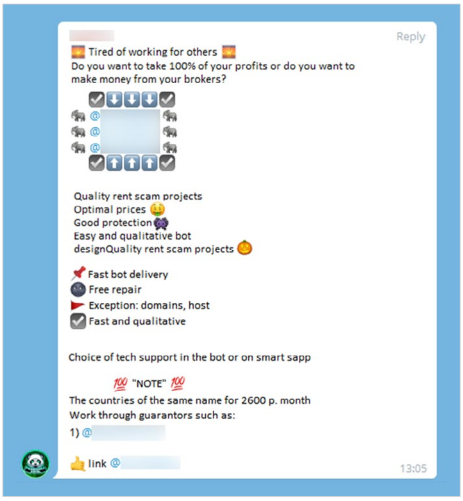
Fig. 31. Example of a phishing page

Shift to affiliate programs

After 2019, the role of Topic Starters became similar to one of mid-level managers supervised by organizers, developers, and administrators. Some TSs were allowed to register phishing domains, while others could only supervise payouts and worker activities.

Topic Starters became significantly less important. They went from being individual facilitators to mere cells within larger organizations.

The new role of TSs led to changes in the community's organization structure and to a shift to an affiliate model (Figure 32).



[redacted]

🌅 Tired of working for others 🌅
Do you want to take 100% of your profits or do you want to make money from your brokers?

☑⬇⬇⬇☑
🐘 @[redacted] 🐘
🐘 @ 🐘
🐘 @ 🐘
☑⬆⬆⬆☑

Quality rent scam projects
Optimal prices 🤑
Good protection 👾
Easy and qualitative bot
designQuality rent scam projects 🎃

📌 Fast bot delivery
🌑 Free repair
🚩 Exception: domains, host
☑ Fast and qualitative

Choice of tech support in the bot or on smart sapp

💯 "NOTE" 💯
The countries of the same name for 2600 p. month
Work through guarantors such as:
1) @[redacted]

🤙 link @[redacted]

13:05

Fig. 32. Example of an advertisement for an affiliate program

An affiliate program is based on the cooperative effort between the organizer and TSs that they are familiar with. In turn, TSs build their own teams and create forum topics while using rented Telegram bots with phishing domains. A server containing a script to generate phishing pages is shared between TSs and their teams that take part in the affiliate program.

To become a Topic Starter, a worker must have extensive experience and a history of generating large profits. A TS must understand the intricacies of the scam scheme, be able to enlist and engage workers, and conduct training sessions for newcomers. TSs receive a small share of the profits after each successful theft committed by the members of their team, with around 80% going to the workers and 10 to 15% going to the organizers of the affiliate program.

The exact composition of affiliate program participants has not been established. The fact that such organizations are formed can be seen by the general domain and server infrastructure as well as the messages posted on thematic forums. Affiliates often comment on each other's profiles on underground forums to rate how reliable and trustworthy someone is.

Role of workers

The role of the largest category of scheme participants, the workers, did not change when the scheme evolved.

Workers are frontline staff who communicate with potential victims and try to persuade them to follow the phishing link and disclose their personal data.

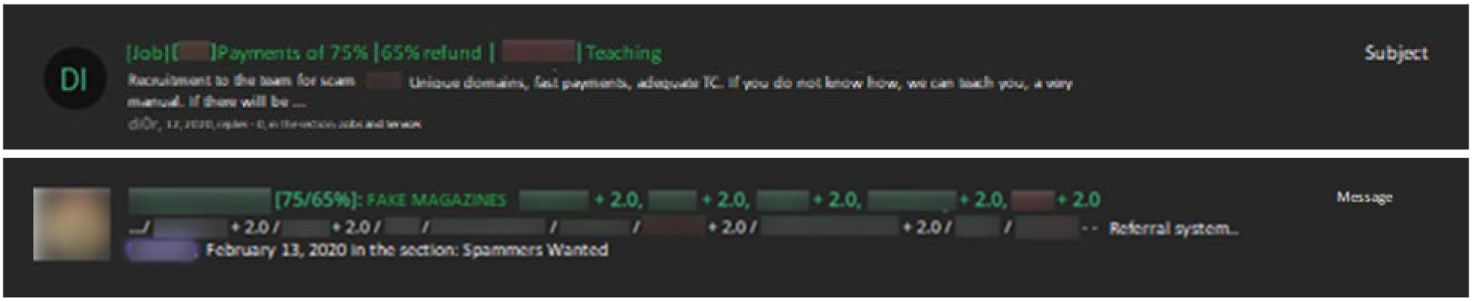
Workers are divided by specialization depending on the tasks they undertake:

- **Callers** talk to victims on the phone masquerading as support staff and help other scheme participants, jumping on any role depending on the scheme.
- **Refunders** pose as website technical support staff and communicate with victims via a chat window usually displayed at the bottom of a phishing page or a dedicated message service. Their role is to help victims supposedly arrange a refund, when in fact the same sum is once again deducted from the victim's account.
- **Supporters** are participants who manually handle payments if a victim struggles to make a payment to the scammers.
- **Bombers** carry out mass spam attacks via SMS messages and calls. Threat actors rarely resort to this practice, but usually the purpose is to intimidate victims or take revenge for an unsuccessful scam attempt.

International expansion

For a long time, Classiscam threat actors limited their attacks to brands based in CIS countries. The scam scheme has been around for a while, however, which has made it much more difficult than before to successfully attack Russian-language resources. Brands conduct advertising campaigns to inform their customers about scam schemes and to ensure security by deleting phishing resources.

In mid-February 2020 the scammers first used underground forums to post advertisements for freebie Telegram bots that users could use to generate phishing forms for the Ukrainian version of a free classifieds platform called OLX (Figures 33 to 35).



DI [Job][[redacted]]Payments of 75% |65% refund | [redacted] | Teaching

Subject

Recruitment to the team for scam [redacted] Unique domains, fast payments, adequate TC. If you do not know how, we can teach you, a very manual. If there will be ...

di0r, 12, 2020, replies - 0, in the section Jobs and [illegible]

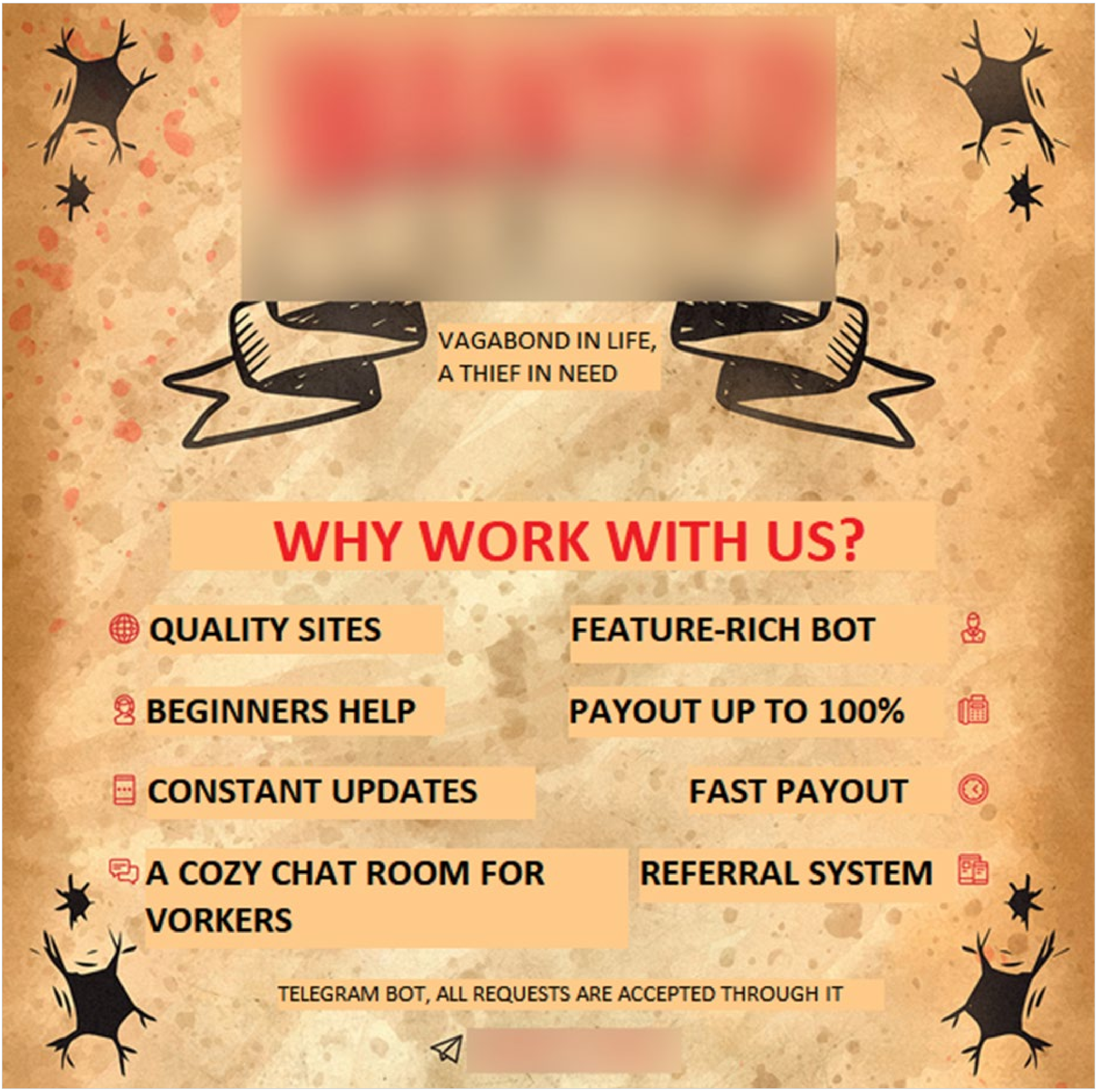
[redacted] [redacted] [75/65%]: FAKE MAGAZINES [redacted] + 2.0, [redacted] + 2.0, [redacted] + 2.0, [redacted] + 2.0, [redacted] + 2.0

../ [redacted] + 2.0 / [redacted] + 2.0 / [redacted] / [redacted] / [redacted] / [redacted] + 2.0 / [redacted] + 2.0 / [redacted] / [redacted] -- Referral system..

[redacted] February 13, 2020 in the section: Spammers Wanted

Message

Fig. 33. Advertisements for scam groups on underground forums



[redacted]

VAGABOND IN LIFE,
A THIEF IN NEED

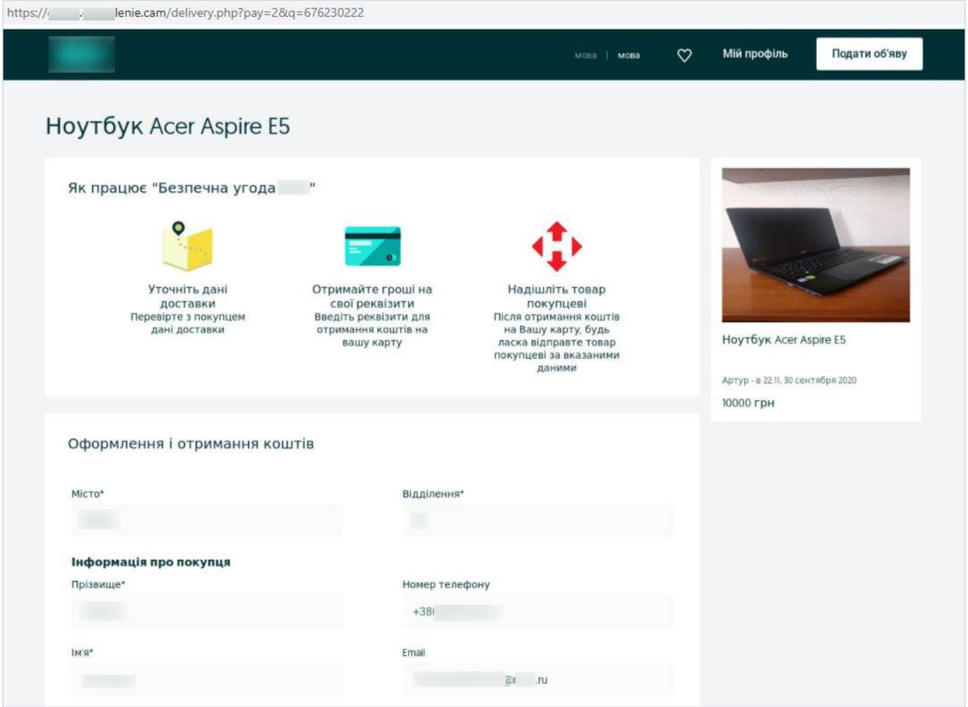
WHY WORK WITH US?

- QUALITY SITES
- FEATURE-RICH BOT
- BEGINNERS HELP
- PAYOUT UP TO 100%
- CONSTANT UPDATES
- FAST PAYOUT
- A COZY CHAT ROOM FOR VORKERS
- REFERRAL SYSTEM

TELEGRAM BOT, ALL REQUESTS ARE ACCEPTED THROUGH IT

[redacted]

Fig. 34. Advertisement for a scam group



https://[redacted].[redacted]lenie.cam/delivery.php?pay=2&q=676230222

Ноутбук Acer Aspire E5

Як працює "Безпечна угода [redacted]"

Уточніть дані доставки
Перевірте з покупцем дані доставки

Отримайте гроші на свої реквізити
Введіть реквізити для отримання коштів на вашу карту

Надішліть товар покупцеві
Після отримання коштів на Вашу карту, будь ласка відправте товар покупцеві за вказаними даними

Ноутбук Acer Aspire E5
Артур - в 22:11, 30 сентября 2020
10000 грн

Оформлення і отримання коштів

Місто* [redacted]

Відділення* [redacted]

Інформація про покупця

Прізвище* [redacted]

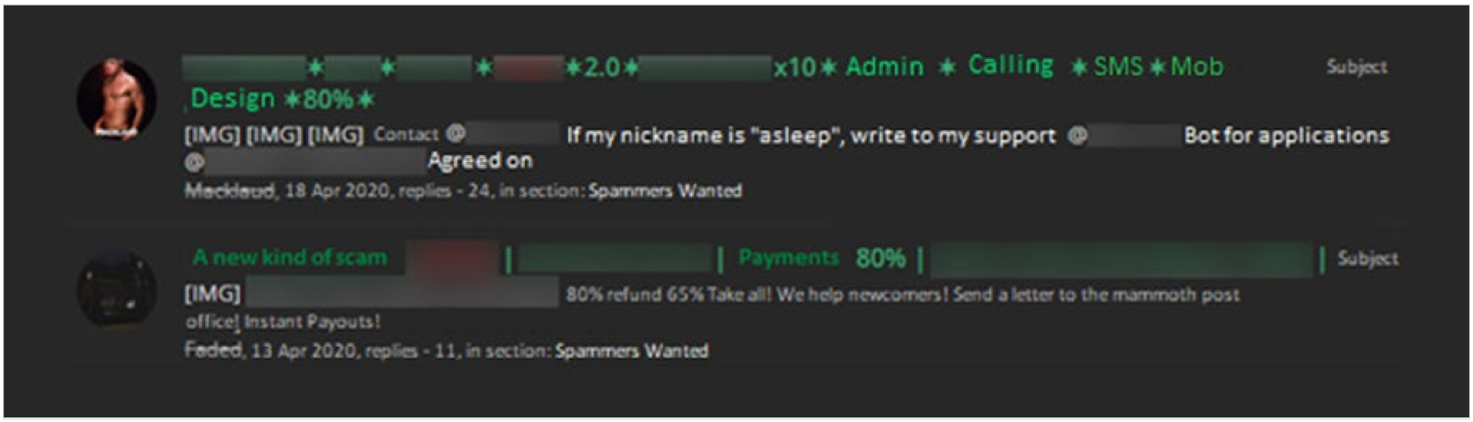
Номер телефону +38[redacted]

Ім'я* [redacted]

Email [redacted]@[redacted].ru

Fig. 35. Example of a phishing resource that uses OLX (Ukraine)

In early April, a new scam scheme was first advertised on underground forums. It focused on Kufar, a Belarusian free classifieds platform (Figure 37).



[redacted]✱[redacted]✱[redacted]✱[redacted]✱2.0✱[redacted]x10✱ Admin ✱ Calling ✱SMS✱Mob Design ✱80%✱ Subject

[IMG] [IMG] [IMG] Contact @[redacted] If my nickname is "asleep", write to my support @[redacted] Bot for applications @[redacted] Agreed on

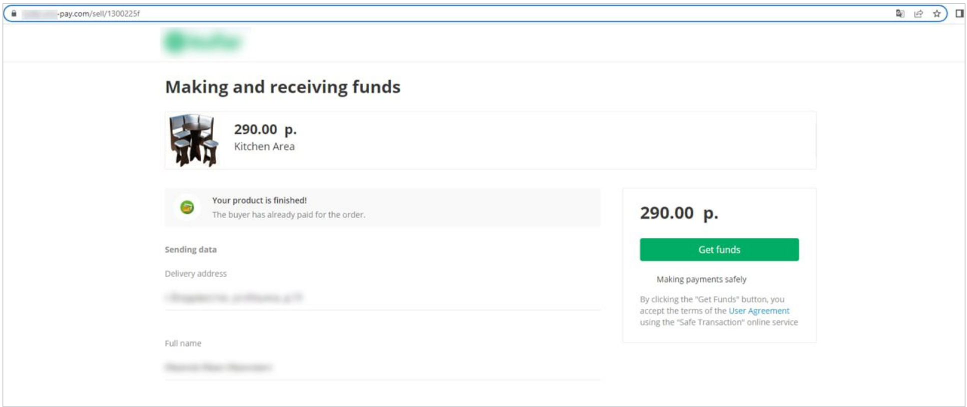
~~Mackdaud~~, 18 Apr 2020, replies - 24, in section: Spammers Wanted

A new kind of scam [redacted] | [redacted] | Payments 80% | [redacted] | Subject

[IMG] [redacted] 80% refund 65% Take all! We help newcomers! Send a letter to the mammoth post office! Instant Payouts!

~~Faded~~, 13 Apr 2020, replies - 11, in section: Spammers Wanted

Fig. 36. Advertisements for scam groups that focus on attacking users of a Belarusian free classifieds website



[redacted]-pay.com/sell/1300225f

Making and receiving funds

290.00 p.
Kitchen Area

Your product is finished!
The buyer has already paid for the order.

Sending data

Delivery address [redacted]

Full name [redacted]

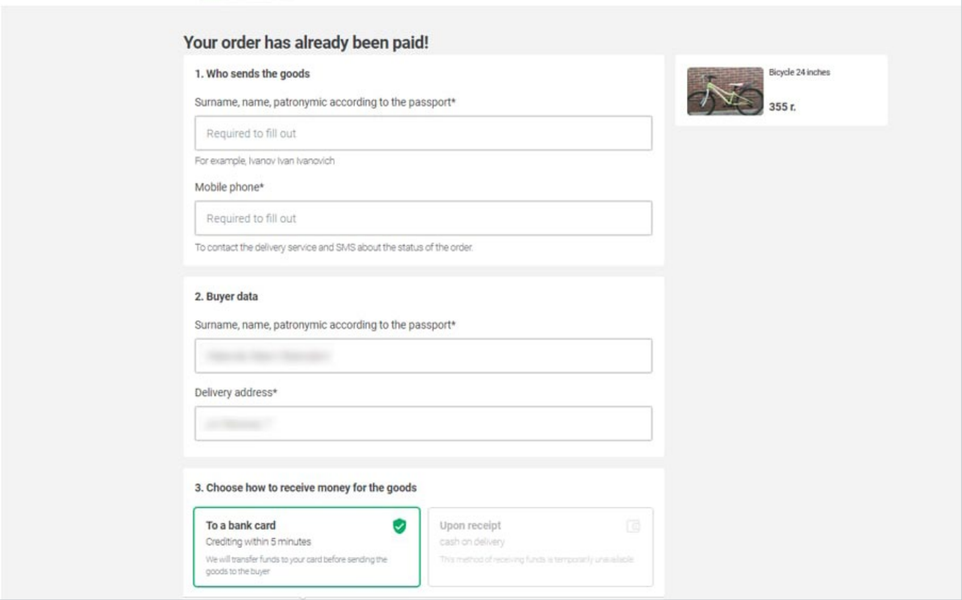
290.00 p.

Making payments safely

By clicking the "Get Funds" button, you accept the terms of the User Agreement using the "Safe Transaction" online service

Fig. 37. Example of a phishing resource that uses Kufar

Belarusian logistics companies were also exposed to such attacks. Shortly after targeting Kufar, the threat actors also targeted the Belarusian branches of CDEK (Figure 38) and Belposhta (Figure 39).



Your order has already been paid!

1. Who sends the goods

Surname, name, patronymic according to the passport*

Required to fill out

For example, Ivanov Ivan Ivanovich

Mobile phone*

Required to fill out

To contact the delivery service and SMS about the status of the order.

2. Buyer data

Surname, name, patronymic according to the passport*

[redacted]

Delivery address*

[redacted]

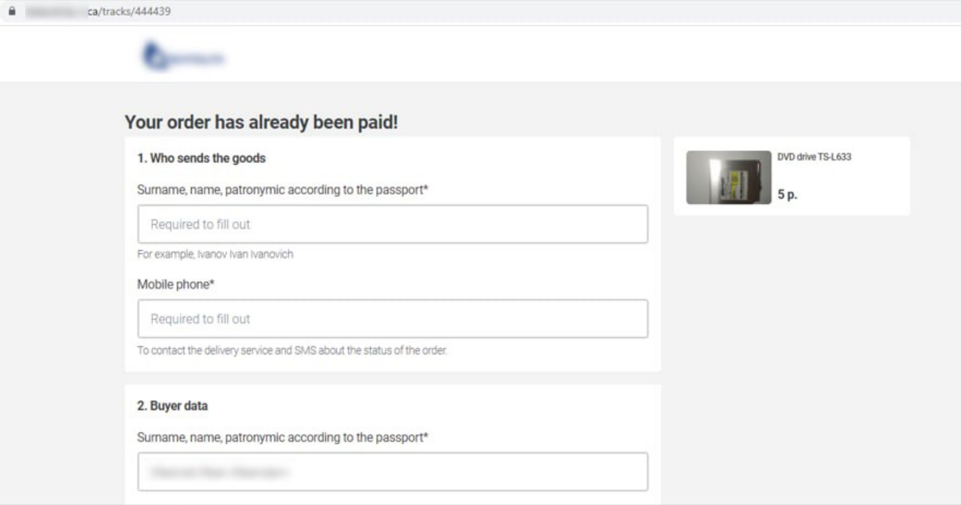
3. Choose how to receive money for the goods

To a bank card ✓
Crediting within 5 minutes
We will transfer funds to your card before sending the goods to the buyer

Upon receipt
cash on delivery
This method of receiving funds is temporarily unavailable

Bicycle 24 inches
355 r.

Fig. 38. Example of a phishing resource that uses CDEK (Belarus)



[redacted]ca/tracks/444439

Your order has already been paid!

1. Who sends the goods

Surname, name, patronymic according to the passport*

Required to fill out

For example, Ivanov Ivan Ivanovich

Mobile phone*

Required to fill out

To contact the delivery service and SMS about the status of the order.

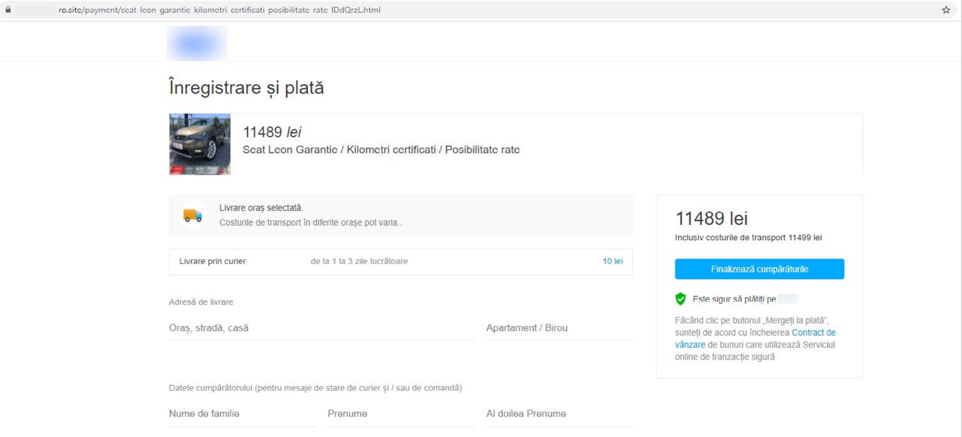
2. Buyer data

Surname, name, patronymic according to the passport*

[redacted]

DVD drive TS-L633
5 p.

Fig. 39. Example of a phishing resource that uses Belposhta



[redacted]ro.site/payment/seat leon garantie kilometri certificati posibilitate rate IDdQrzL.html

Înregistrare și plată

11489 *lei*
Seat Leon Garantie / Kilometri certificati / Posibilitate rate

Livrare oraș selectată.
Costurile de transport în diferite orașe pot varia..

Livrare prin curier — de la 1 la 3 zile lucrătoare — 10 lei

Adresă de livrare

Oraș, stradă, casă

Apartament / Birou

Datele cumpărătorului (pentru mesaje de stare de curier și / sau de comandă)

Nume de familie

Prenume

Al doilea Prenume

11489 lei

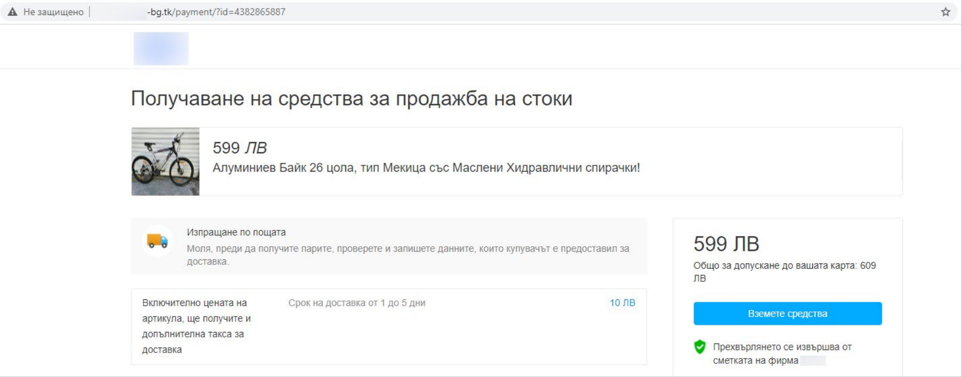
Inclusiv costurile de transport 11499 lei

Este sigur să plătiți pe [redacted]

Făcând clic pe butonul „Mergeți la plată", sunteți de acord cu încheierea Contract de vânzare de bunuri care utilizează Serviciul online de tranzacție sigură

Fig. 40. Example of a phishing resource in Romanian that uses OLX

As early as the beginning of August, public Telegram channels were used for a scam scheme targeting the Bulgarian (Figure 41) and Kazakh (Figure 42) versions of OLX.



Не защищено | -bg.tk/payment/?id=4382865887

Получаване на средства за продажба на стоки

599 *ЛВ*
Алуминиев Байк 26 цола, тип Мекица със Маслени Хидравлични спирачки!

Изпращане по пощата
Моля, преди да получите парите, проверете и запишете данните, които купувачът е предоставил за доставка.

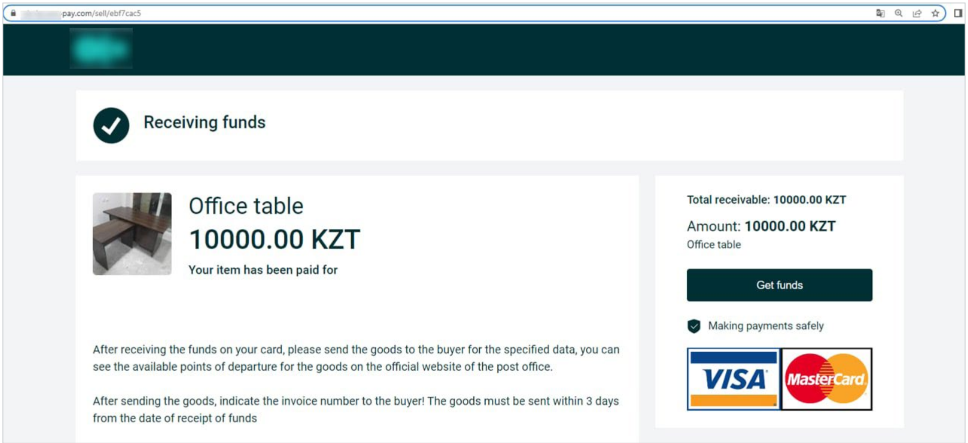
Включително цената на артикула, ще получите и допълнителна такса за доставка | Срок на доставка от 1 до 5 дни | 10 ЛВ

599 ЛВ
Общо за допускане до вашата карта: 609 ЛВ

Вземете средства

Прехвърлянето се извършва от сметката на фирма

Fig. 41. Example of a phishing resource in Bulgarian that uses OLX



pay.com/sell/ebf7cac5

Receiving funds

Office table
10000.00 KZT
Your item has been paid for

After receiving the funds on your card, please send the goods to the buyer for the specified data, you can see the available points of departure for the goods on the official website of the post office.

After sending the goods, indicate the invoice number to the buyer! The goods must be sent within 3 days from the date of receipt of funds

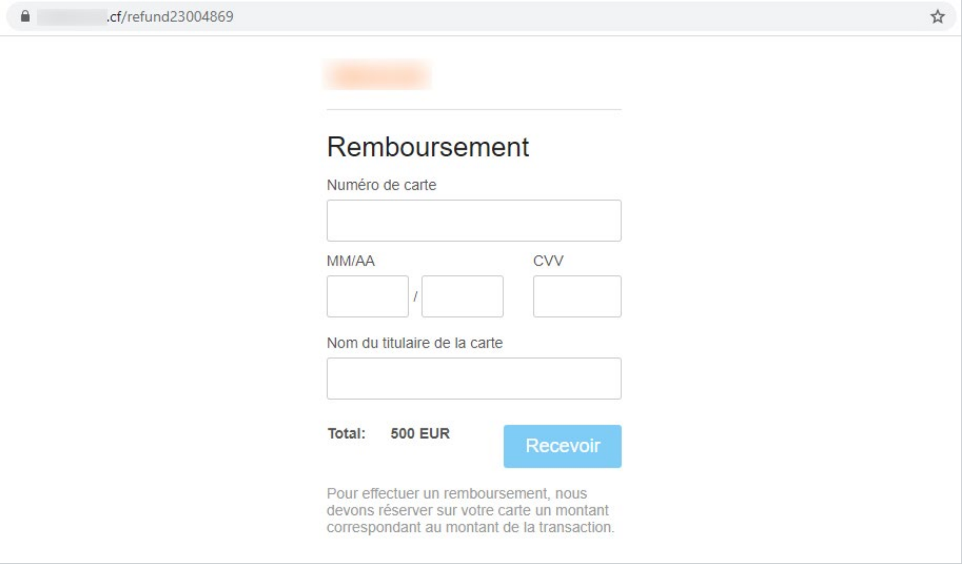
Total receivable: **10000.00 KZT**
Amount: **10000.00 KZT**
Office table

Get funds

Making payments safely

Fig. 42. Example of a phishing resource with Kazakh currency that uses OLX

Scammers did not limit the expansion of the scheme to CIS countries. In late August, popular Telegram bots were used to spread advertisements of a scam project targeting a French free classifieds website called Leboncoin (Figure 43).



.cf/refund23004869

Remboursement

Numéro de carte

MM/AA /

CVV

Nom du titulaire de la carte

Total: 500 EUR

Recevoir

Pour effectuer un remboursement, nous devons réserver sur votre carte un montant correspondant au montant de la transaction.

Fig. 43. Example of a phishing resource that uses Leboncoin

A few attacks on foreign brands had already been carried out before 2020, but these were isolated cases. Software tools for generating phishing pages were available only for experienced scammers in closed forums. The evolution of the Classiscam scheme and the expansion of the hacker community both made the scheme spread faster worldwide.

Using European brands for scamming purposes is more complex technology-wise. Scammers sometimes experience difficulties when verifying accounts on websites and resort to buying stolen credentials and phone numbers via underground forums and communities.

Topic Starters now face the issue of linking foreign-currency bank cards to Telegram bots. This problem can be resolved by using the services of experienced mules (proxies who receive and withdraw money for a fixed percentage of the profits).

For each brand, enthusiast scammers create scam manuals to help novices log onto foreign platforms and communicate with victims.

Scope of attacks

While researching the scam scheme, Group-IB investigators found more than 384 Telegram bots. Currently, no less than 90 are still active, but this number is constantly changing. A bot can stop working at any moment for various reasons, in which case the whole team is disbanded or switches to another bot.

The Classiscam scheme is currently popular in **64** countries in Europe, the CIS region, and the Middle East. The scheme uses **169** brands including classifieds, delivery services, marketplaces and service platforms, banks, and local businesses such as cinemas.

For the most recent reporting period, from **April 2020** to **February 2022,** scammers who practiced this scheme made at least **$29,500,000** in total, while the average theft amount was about $83.

In total, investigators found about **2,000 topics** on more than **60** specialized forums where threat actors were looking for workers to participate in phishing affiliate programs.

Web pages created by scammers are difficult to identify using proactive methods due to their short lifespan, which is sometimes limited to only a few hours.

The most popular national domains used for the Classiscam phishing scheme are broken down by currency as shown below in Figure 44.

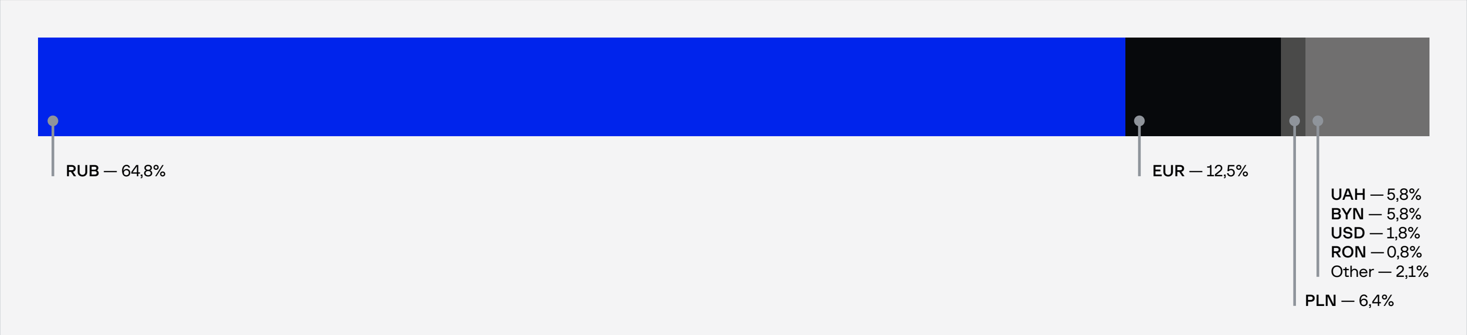


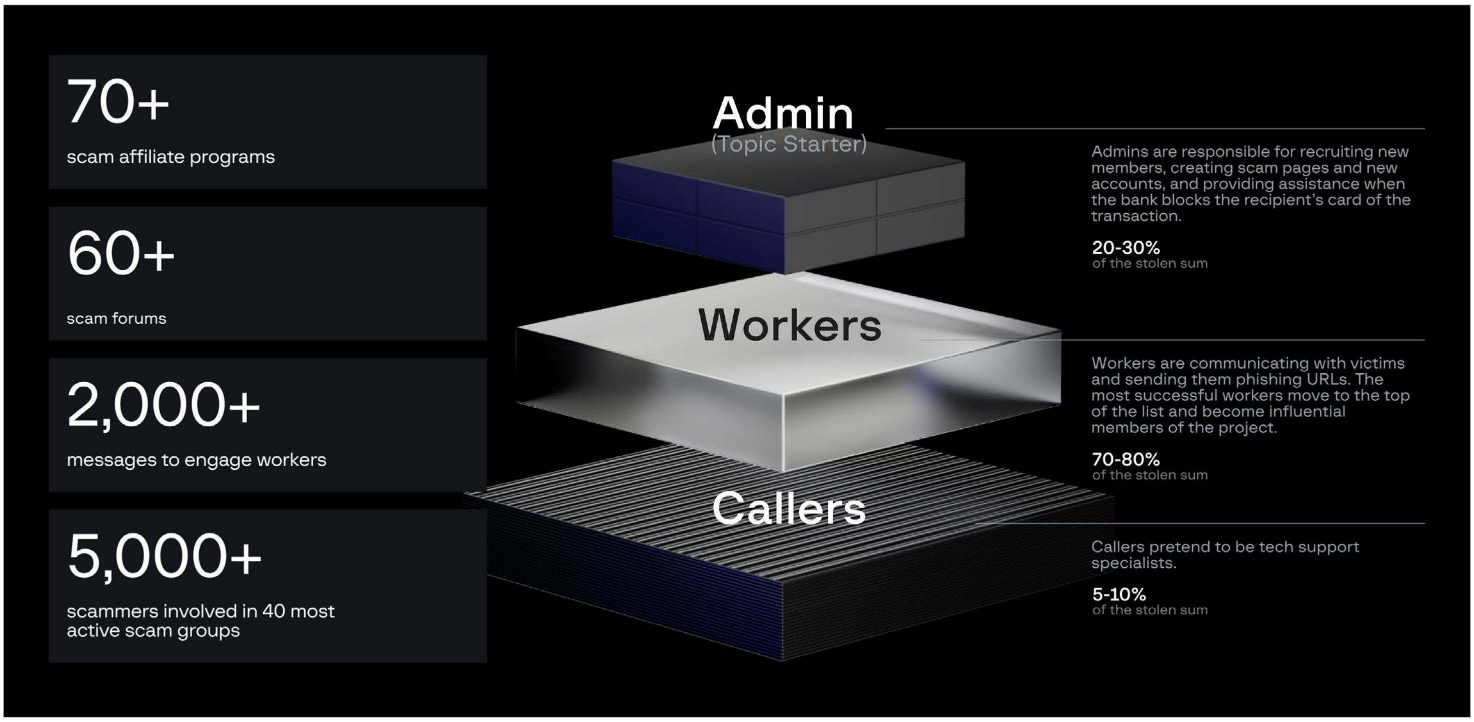
Fig. 44. Distribution of cash amounts by currency

Increase in abuse-resistant hosting offers

The need for abuse-resistant hosting has engendered a multitude of offers. A few large outfits dominated this niche before 2020, but many new players appeared in just one year. They do not provide a particularly high-quality service, lacking intricacies in routing and possessing only a rudimentary handling of IP ranges for intercepting victim complaints. The presence of such hosting providers on the market therefore hinders efforts to counteract fraudulent activity. Ultimately, this affects both cybercrime in general as well as information security.

SaaS as the way forward

Given that Classiscam has a hierarchy of roles, reuses previously created templates and methodologies, and grows thanks to a low entry threshold for new participants, it can be said that the scheme is designed according to the SaaS (software/scam as a service) principle. In this case, the software involved is a link-building toolkit and the users are ordinary workers who create links and directly communicate with victims. Profits are distributed proportionally among participants based on their role (Figures 45 to 46).



70+
scam affiliate programs

60+
scam forums

2,000+
messages to engage workers

5,000+
scammers involved in 40 most active scam groups

Admin
(Topic Starter)

Admins are responsible for recruiting new members, creating scam pages and new accounts, and providing assistance when the bank blocks the recipient's card of the transaction.

20-30%
of the stolen sum

Workers

Workers are communicating with victims and sending them phishing URLs. The most successful workers move to the top of the list and become influential members of the project.

70-80%
of the stolen sum

Callers

Callers pretend to be tech support specialists.

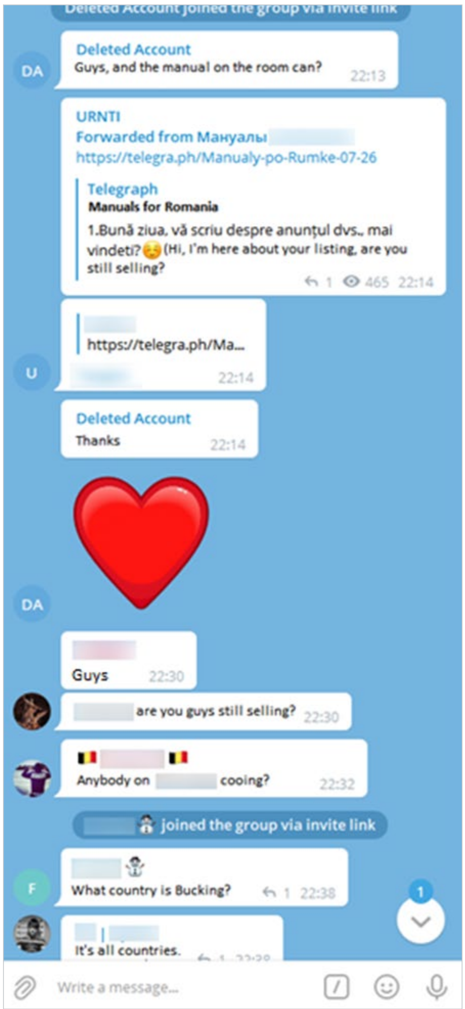
5-10%
of the stolen sum

Fig. 45. Hierarchy of criminal groups

In chats, workers receive support and obtain various deception tools in order to:

- Specify a particular domain name for the resource
- Send emails and SMS messages from the chosen resources
- Generate fake screenshots with support service messages
- Obtain user manuals with playbooks (some of them paid)
- Buy databases for mass mailouts, accounts, phone numbers, and various services

Screenshots showing the process of creating links, domains, and user manuals



Deleted Account joined the group via invite link

Deleted Account
Guys, and the manual on the room can? 22:13

URNTI
Forwarded from Мануалы [redacted]
https://telegra.ph/Manualy-po-Rumke-07-26
Telegraph
Manuals for Romania
1.Bună ziua, vă scriu despre anunțul dvs., mai vindeti?😣(Hi, I'm here about your listing, are you still selling?
1 465 22:14

[redacted]
https://telegra.ph/Ma...
[redacted] 22:14

Deleted Account
Thanks 22:14

❤️

[redacted]
Guys 22:30

[redacted] are you guys still selling? 22:30

🇧🇪[redacted]🇧🇪
Anybody on [redacted] cooing? 22:32

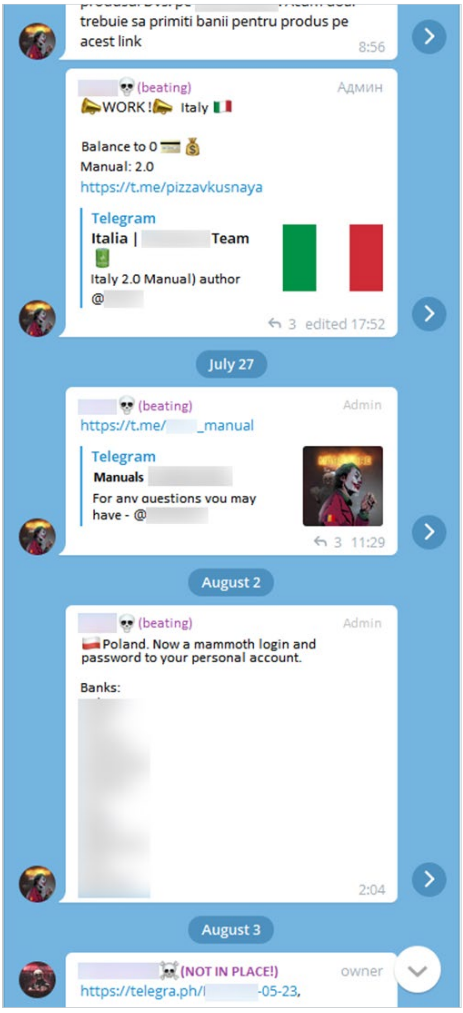
[redacted] joined the group via invite link

[redacted]
What country is Bucking? 1 22:38

[redacted] | [redacted]
It's all countries.

Write a message...

Fig. 46. Example of a mailout of a user manual in a scam group dedicated to attacks on Romanian online services



[redacted]
trebuie sa primiti banii pentru produs pe acest link 8:56

[redacted] 💀 (beating) Админ
📣WORK !📣 Italy 🇮🇹

Balance to 0 💳 💰
Manual: 2.0
https://t.me/pizzavkusnaya
Telegram
Italia | [redacted] Team
Italy 2.0 Manual) author
@[redacted]
3 edited 17:52

July 27

[redacted] 💀 (beating) Admin
https://t.me/[redacted]_manual
Telegram
Manuals [redacted]
For anv questions vou may have - @[redacted]
3 11:29

August 2

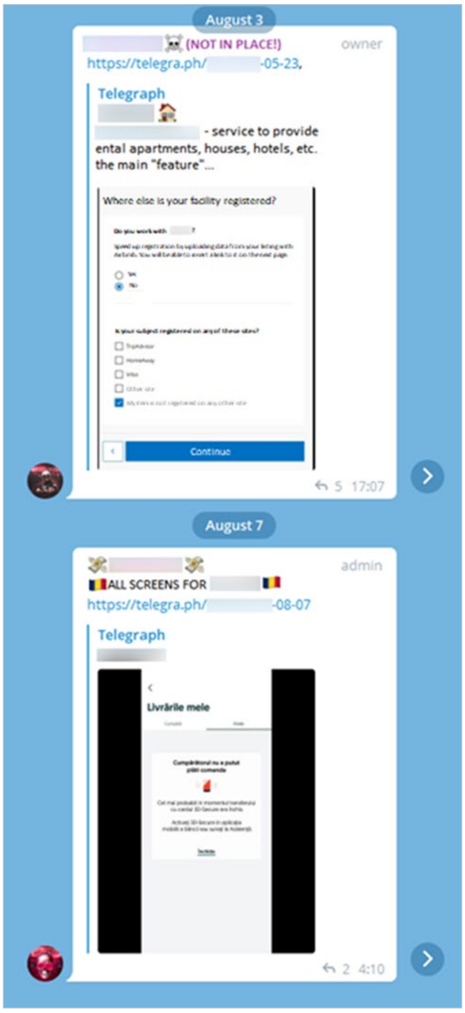
[redacted] 💀 (beating) Admin
Poland. Now a mammoth login and password to your personal account.

Banks:
[redacted]
2:04

August 3

[redacted] ☠️ (NOT IN PLACE!) owner
https://telegra.ph/[redacted]-05-23,

Fig. 47. Example of a mailout of a user manual in a scam group dedicated to attacks on Italian online services



August 3

[redacted] ☠️ (NOT IN PLACE!) owner
https://telegra.ph/[redacted]-05-23,
Telegraph
[redacted] 🏠
[redacted] - service to provide
ental apartments, houses, hotels, etc.
the main "feature"...

Where else is your facility registered?

☐ ☐ ☐ ☐ ☑

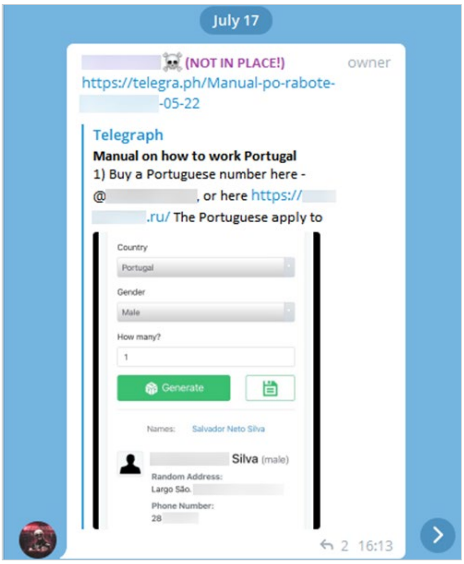
5 17:07

August 7

[redacted] admin
ALL SCREENS FOR [redacted]
https://telegra.ph/[redacted]-08-07
Telegraph
[redacted]

2 4:10

Fig. 48. Example of a mailout of fake materials in a scam group. The materials will be used for attacks on Romanian online services



July 17

[redacted] ☠️ (NOT IN PLACE!) owner
https://telegra.ph/Manual-po-rabote-[redacted]-05-22
Telegraph
Manual on how to work Portugal
1) Buy a Portuguese number here - @[redacted], or here https://[redacted].ru/ The Portuguese apply to

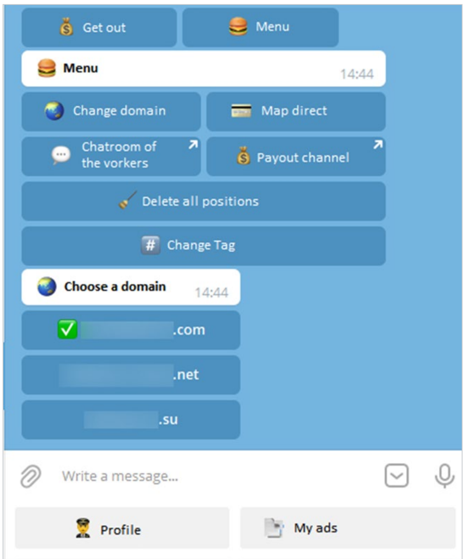
Country
Portugal
Gender
Male
How many?
1

Names: Salvador Neto Silva

[redacted] Silva (male)
Random Address:
Largo São [redacted]
Phone Number:
28[redacted]

2 16:13

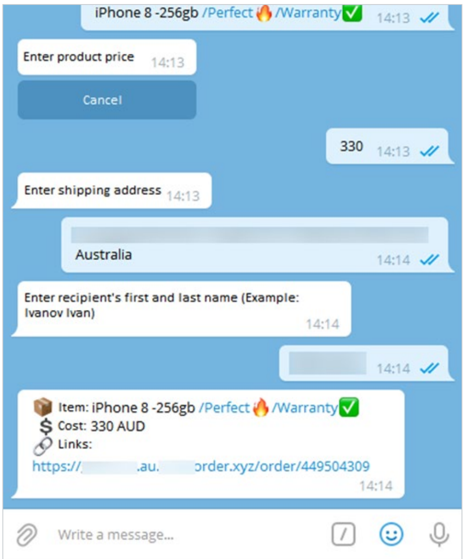
Fig. 49. Example of a manual sent to scam group members to attack Portuguese online services



🍔 **Menu** 14:44

🌍 **Choose a domain** 14:44

Fig. 50. Example of how scammers choose a domain to generate phishing links



iPhone 8 -256gb /Perfect 🔥 /Warranty✅ 14:13

Enter product price 14:13

330 14:13

Enter shipping address 14:13

[redacted]
Australia 14:14

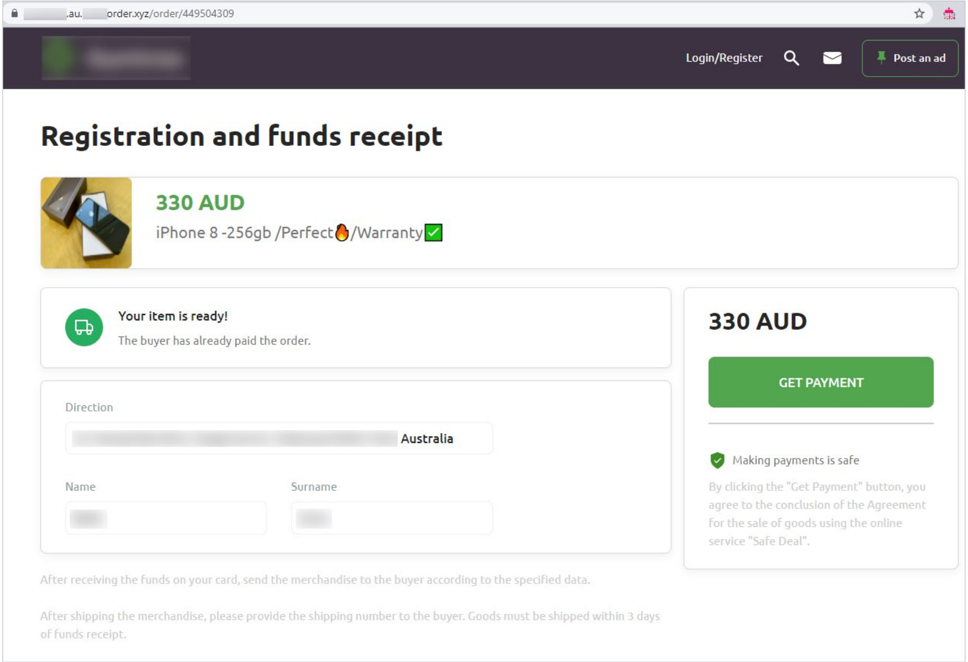
Enter recipient's first and last name (Example: Ivanov Ivan) 14:14

[redacted] 14:14

📦 Item: iPhone 8 -256gb /Perfect 🔥 /Warranty✅
$ Cost: 330 AUD
🔗 Links:
https://[redacted].au.[redacted]order.xyz/order/449504309
14:14

Write a message...

Fig. 51. Example of a phishing page creation process



[redacted].au.[redacted]order.xyz/order/449504309

Registration and funds receipt

330 AUD

iPhone 8 -256gb /Perfect🔥/Warranty✅

Your item is ready!

The buyer has already paid the order.

330 AUD

GET PAYMENT

Direction: [redacted] Australia

Name: [redacted]

Surname: [redacted]

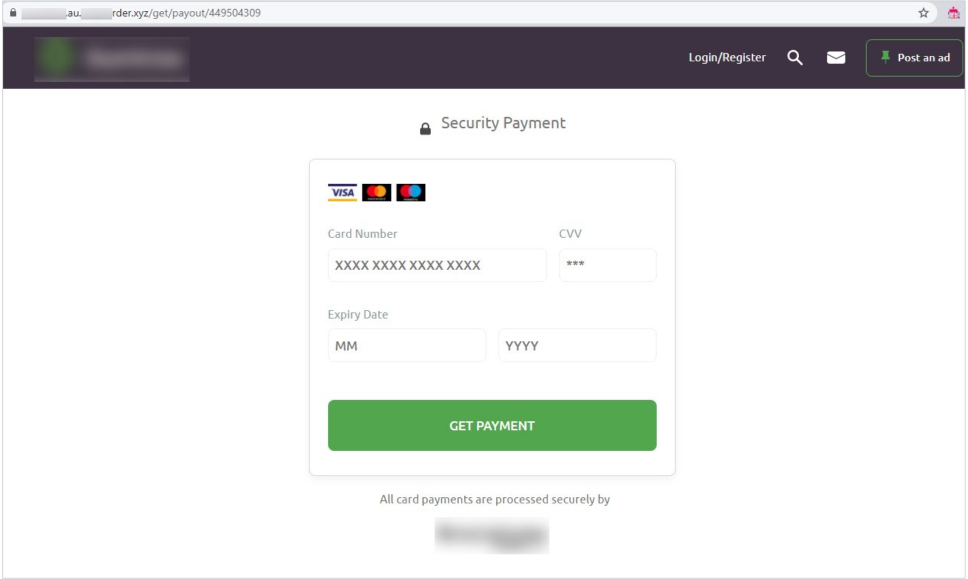
Making payments is safe

By clicking the "Get Payment" button, you agree to the conclusion of the Agreement for the sale of goods using the online service "Safe Deal".

After receiving the funds on your card, send the merchandise to the buyer according to the specified data.

After shipping the merchandise, please provide the shipping number to the buyer. Goods must be shipped within 3 days of funds receipt.

Fig. 53. Example of a phishing page



[redacted].au.[redacted]rder.xyz/get/payout/449504309

Security Payment

Card Number: XXXX XXXX XXXX XXXX

CVV: ***

Expiry Date: MM YYYY

GET PAYMENT

All card payments are processed securely by [redacted]

Fig. 54. Example of a phishing payment form

New role of administrative panels

As a result of how the scheme evolved and expanded, Classiscam scammers started involving more and more brands and countries in their activities. The amount of information became so significant that it became difficult to store it in a Telegram bot. In the second half of 2021, Group-IB specialists intercepted advertisements for ready-to-use comprehensive scam toolkits. Such toolkits help buyers perform all the necessary operations unassisted, without a team — they become a TS, a worker, a supporter, and a refunder all in one.

To experienced scammers, such toolkits are much more valuable than Telegram bots. In order to promptly obtain access to scam tools, a scammer can simply deploy an administrative panel.

Key findings

The Classiscam scheme has been around for a long time and has significantly evolved since it first appeared. Switching from administrative panels to Telegram bots helped scammer simplify communications between themselves and speed up the process of creating phishing pages. Successful attacks on popular Russian-language services spurred threat actors into increasing their attack footprint by involving various new brands, from lesser-known Russian-language businesses to foreign companies.

In total, more than **384 scam groups** were found to be taking part in the scheme and using **169 brands** as part of their operations. The geographical scope of the attacks includes **64 countries** in Europe, the CIS region, and the Middle East.

Thorough research into the data relating to the scam groups revealed that there are significantly fewer of them than previously believed because many are not separate entities, as is customary among traditional cybercriminal outfits. Workers often participate in several groups at once.

This sphere is divided among a narrow circle of individuals who form small groups. Instead of project leaders there are Topic Starters, who are ordinary hired workers and who receive either a share of the total profits or a fixed wage plus a share. In this report, such scam projects are called affiliate programs.

This understanding of the scheme determined the methods used to handle such groups and the ways that their capabilities were assessed all the while leading to changes in counteraction and tracking methods. The idea emerged that an intelligence-driven approach would produce much better results than the traditional method of blocking endpoint websites.

For instance, the intelligence-driven method was used to detect the whole range of IPs bought by a certain group, their own NS servers, and techniques to withdraw stolen funds.

The findings helped track all the changes to how the scheme worked and what the groups involved did. They also helped resolve issues when they first emerged and struck hard at all attack vectors, from bots to fund withdrawal.

Based on this information, it became possible to inflict irrecoverable damage to such groups by persecuting their leaders.

When affiliates turned to Telegram, they all used the same infrastructure – domains, dedicated servers, payment gateways, phishing kits – which simplified the process of merging groups into affiliate programs.

With time, the SaaS scheme was elevated to a completely new level. The top of the food chain was represented not by managers of supergroups (individuals who owned several groups), but by the individuals who provided similar services to supergroup owners.

As a result, anyone could join the scheme and register their own scam bot. All technical issues were solved for them, up to the point when the funds were withdrawn. Managers only had to engage workers and distribute profits.

Group-IB DRP specialists recommend that businesses actively counteract scam. For the Classiscam scheme, they provide recommendations and an example of attribution and an IoC.

Group-IB's mission: Fight against cybercrime

Group-IB is a leading provider of innovations and solutions for detecting and preventing cyberattacks, eliminating fraud, and protecting brands from digital risks worldwide.

19 years of hands-on experience

1.300+ cybercrime investigations worldwide

70.000+ hours of incident response

600+ world-class cybersecurity experts

Active partner in global investigations

INTERPOL

Europol

Recognized by top industry experts

FORRESTER®

kuppingercole ANALYSTS

Gartner®

IDC

FROST & SULLIVAN

Technologies and innovations

Cybersecurity

- Threat intelligence
- Attack surface management
- Email protection
- Network traffic analysis
- Malware detonation
- EDR
- XDR

Anti-fraud

- Client-side anti-fraud
- Adaptive authentication
- Bot prevention
- Fraud intelligence
- User and entity behavior analysis

Brand protection

- Anti-phishing
- Anti-piracy
- Anti-scam
- Anti-counterfeit
- Protection from data leaks
- VIP protection

Intelligence-driven services

Audit & Consulting

- Security Assessment
- Penetration Testing
- Red Teaming
- Compliance & Consulting

Education & Training

- For technical specialists
- For wider audiences

DFIR

- Incident Response
- Incident Response Retainer
- Incident Response Readiness Assessment
- Compromise Assessment
- Digital Forensics
- eDiscovery

Managed Services

- Managed Detection
- Managed Threat Hunting
- Managed Response

High-Tech Crime Investigation

- Cyber Investigation
- Investigation Subscription

GROUP-IB

Preventing and investigating cybercrime since 2003

FIGHT AGAINST CYBERCRIME	GROUP-IB.COM INFO@GROUP-IB.COM	APAC +65 3159 3798	EU & NA +31 20 226 90 90	MEA +971 4 508 1605