



# SCAM-AS-SERVICE EVOLUTION & C2C/3DS ABUSE

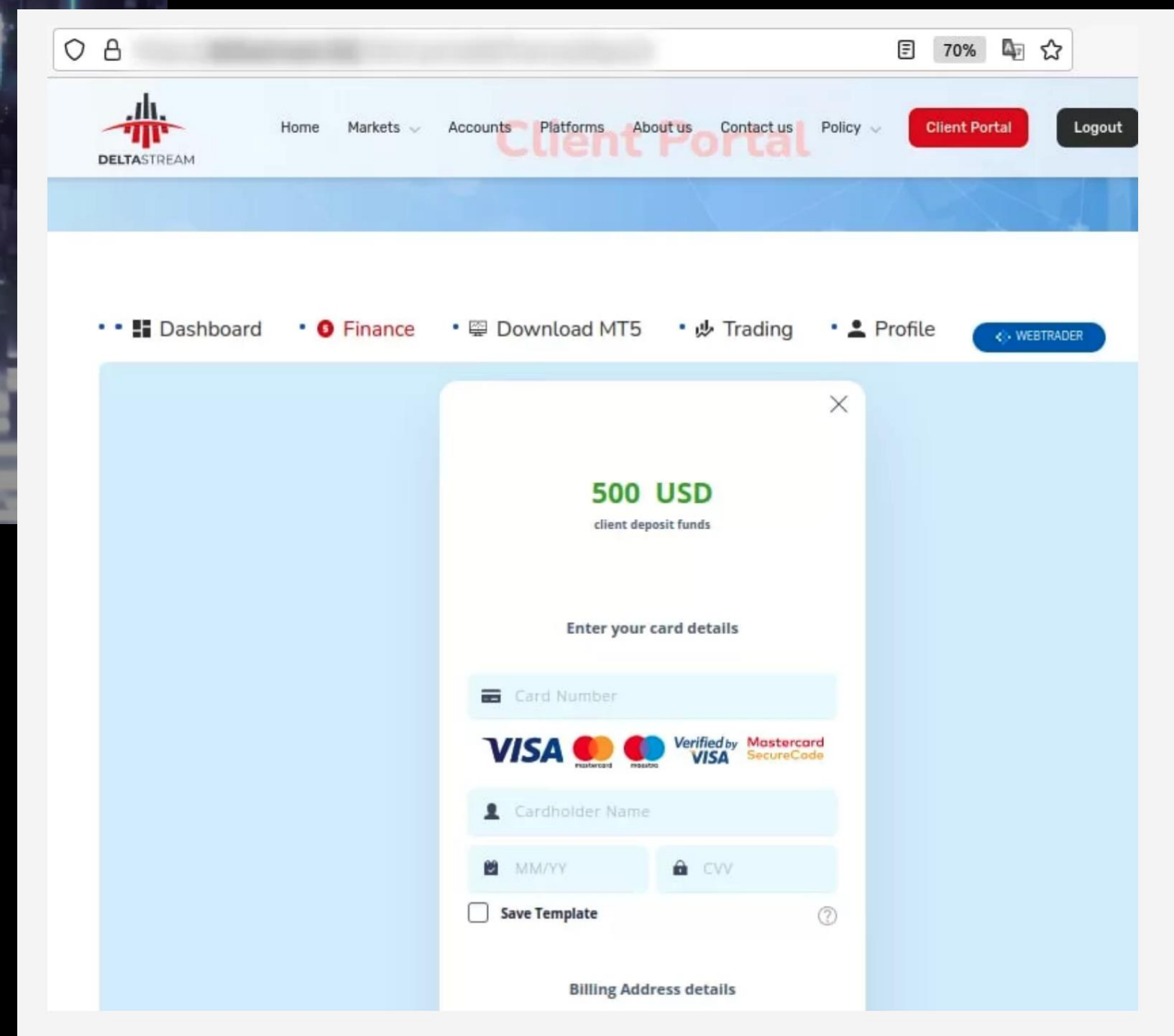
# PHISHING ATTACKS



29.07.2022

## Fake investment scams in Europe

How we almost got rich



# PHISHING ATTACKS



СЗП.ВНДС.Служба.Финансово  
MUTED

https://r2xp7b.ue06septjo.fun/database-search

Найдены все доступные компенсации  
в Ваш адрес на общую сумму  
**270 120 руб. 70 коп.**

Чтобы получить выплату, свяжитесь с нашим юристом. Для этого нажмите кнопку ниже. Он поможет с оформлением и закажет моментальный вывод средств на вашу карту.

**Связаться с юристом для получения выплаты**

**Сумма вашей компенсации: 270120.70 руб.**  
Двести семьдесят тысяч сто двадцать рублей семьдесят копеек

Комментарии граждан о получении компенсации Н.Д.С.:

**Николай Соболев** ● сегодня

Я даже не знал, что вышло официальное постановление о выплате ко за НДС и что теперь я могу забрать свои законные 245000 руб. Я напр соц.сетей об этом узнал, спасибо блогерам что подсказали! Я свою ко проверил и забрал уже. Так что проверяйте и тоже получайте пока ден бюджета выделили.

Юридические услуги  
MUTED

https://r2xp78.qwr2306pay.space/pay?token=ddee54c05bbd9273de48aa1e6481719e&h=02swf8yb\_hamh5ewrfk7

#R2XVIL7720  
Юридические услуги  
К оплате: 372 руб.  
Комиссия: возможна комиссия банка, выдавшего карту

**Сумма выплаты 270 120 руб. 70 коп.**  
Внимание! Принимаются только карты банков РФ.

Номер карты

Действует до:  
Месяц  Год

Имя как на карте

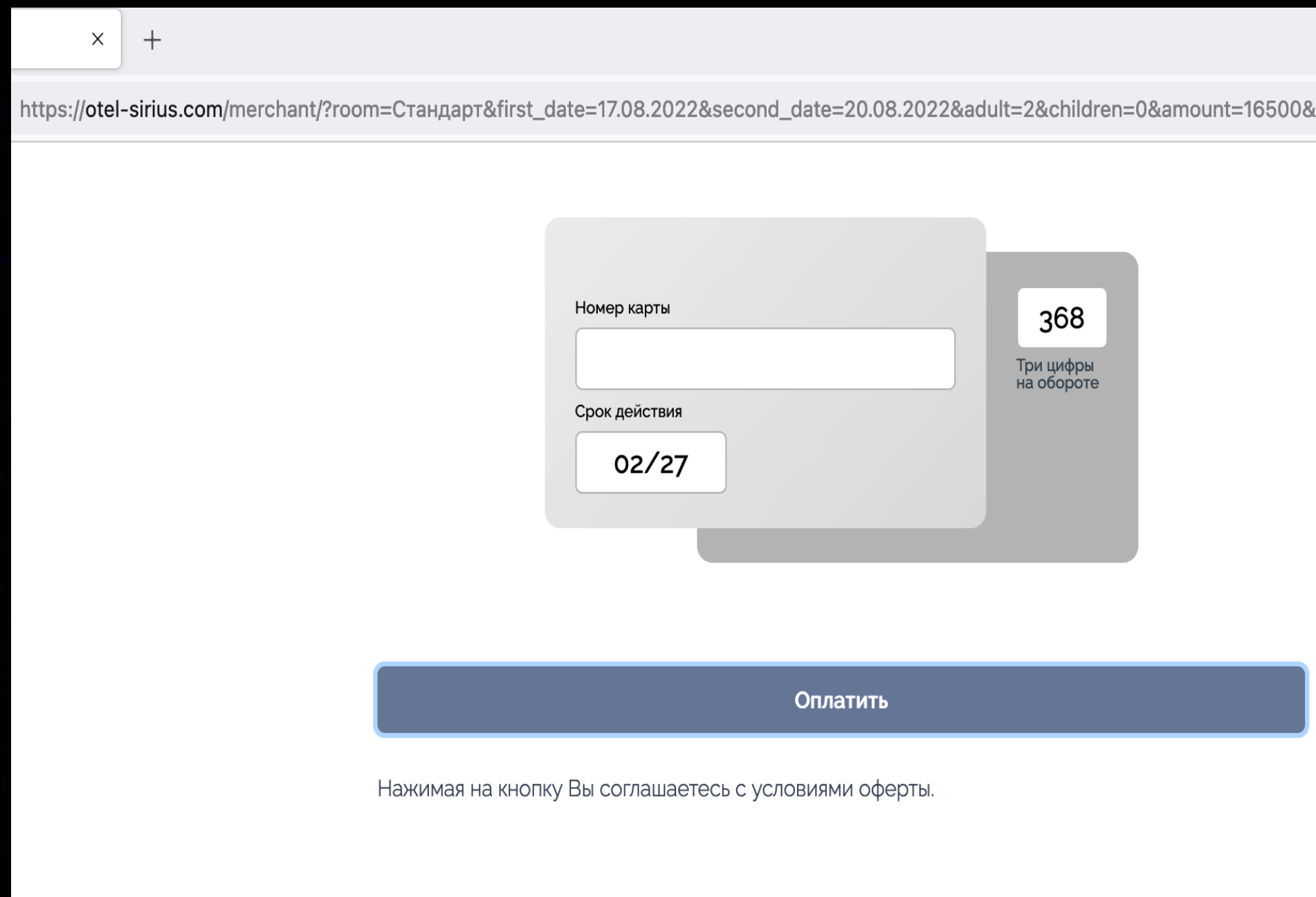
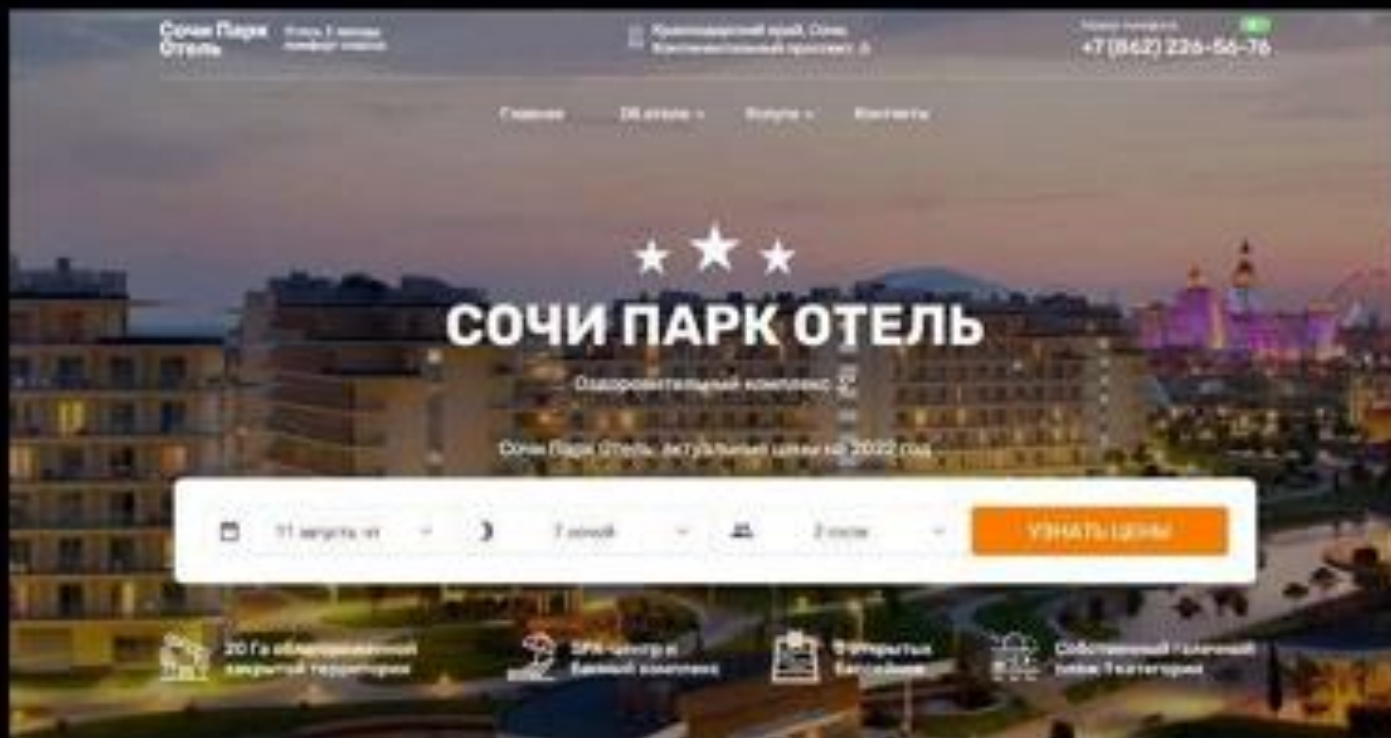
Последние 3 цифры на обороте карты

CVC

**Оплатить**

Введите данные, нажмите Оплатить. После этого введите код из смс.

# PHISHING ATTACKS



# AFFILIATE PROGRAM. SCAM-AS-SERVICE



Admins are responsible for recruiting workers, creating phishing pages, technical support, and communication.

Workers communicate with victims and send them phishing pages. Top workers get access to VIP scripts and target victims from Europe and the US.

If the bot does not support automatic payment through phishing (fake merchant), then Vbiver makes the payment manually on the P2P page of the bank.

PROFIT

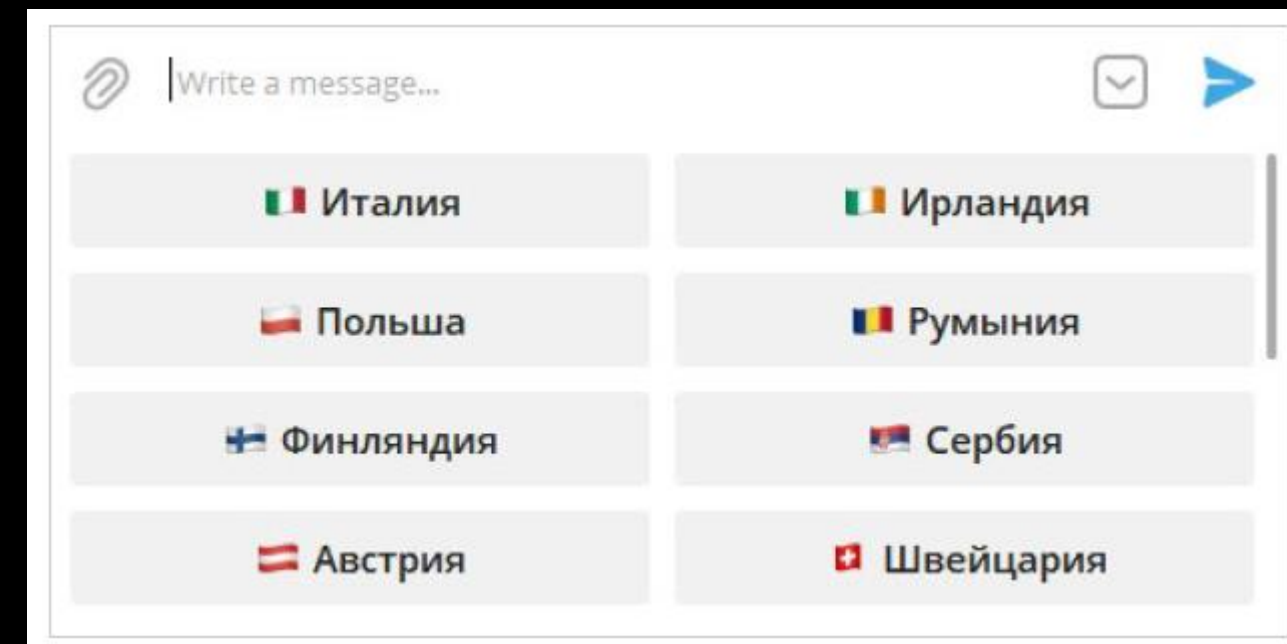
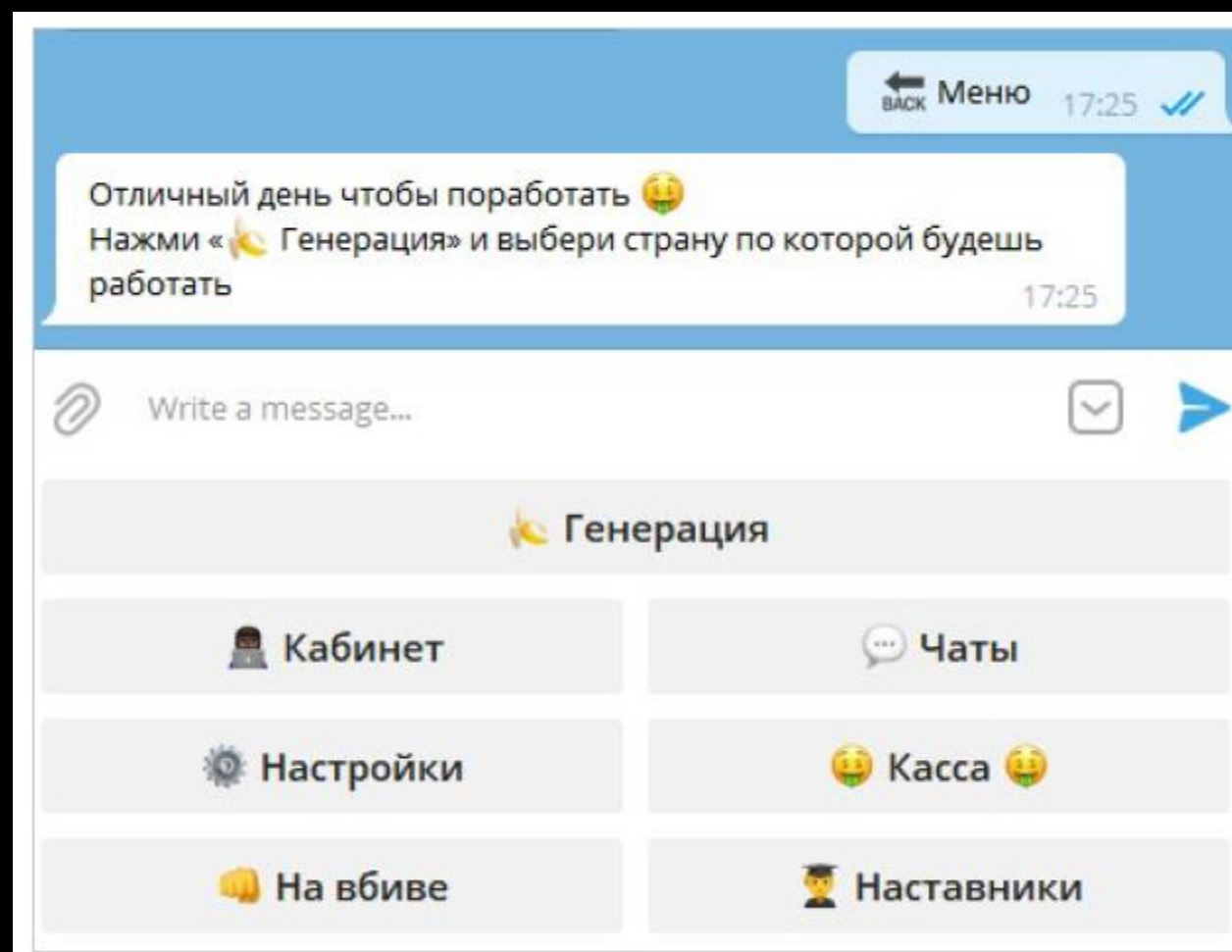
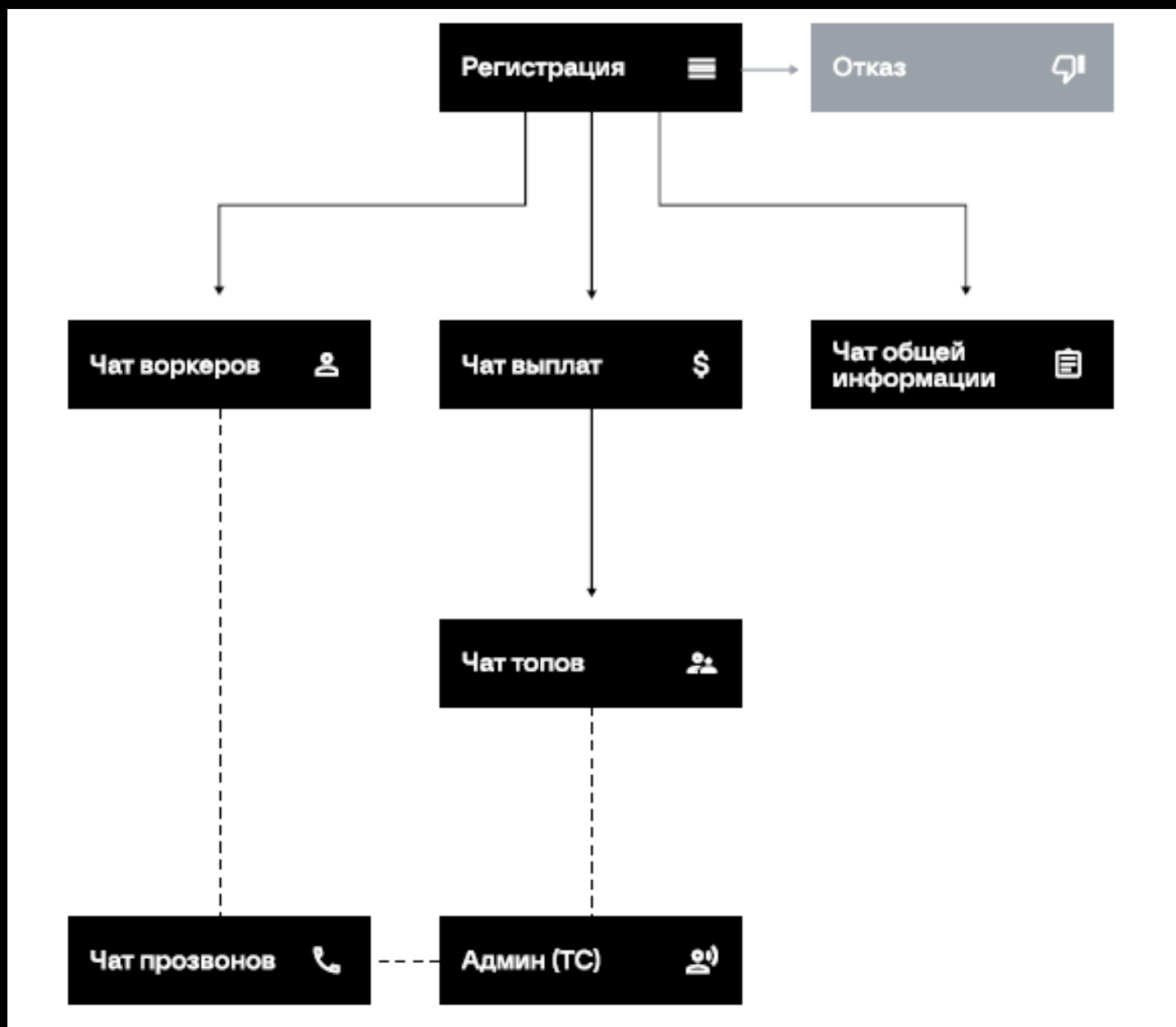
**20-30%**  
of revenue

**70-80%**  
of revenue

**5-10%**  
of revenue



# TELEGRAM INFRASTRUCTURE



# STATISTICS

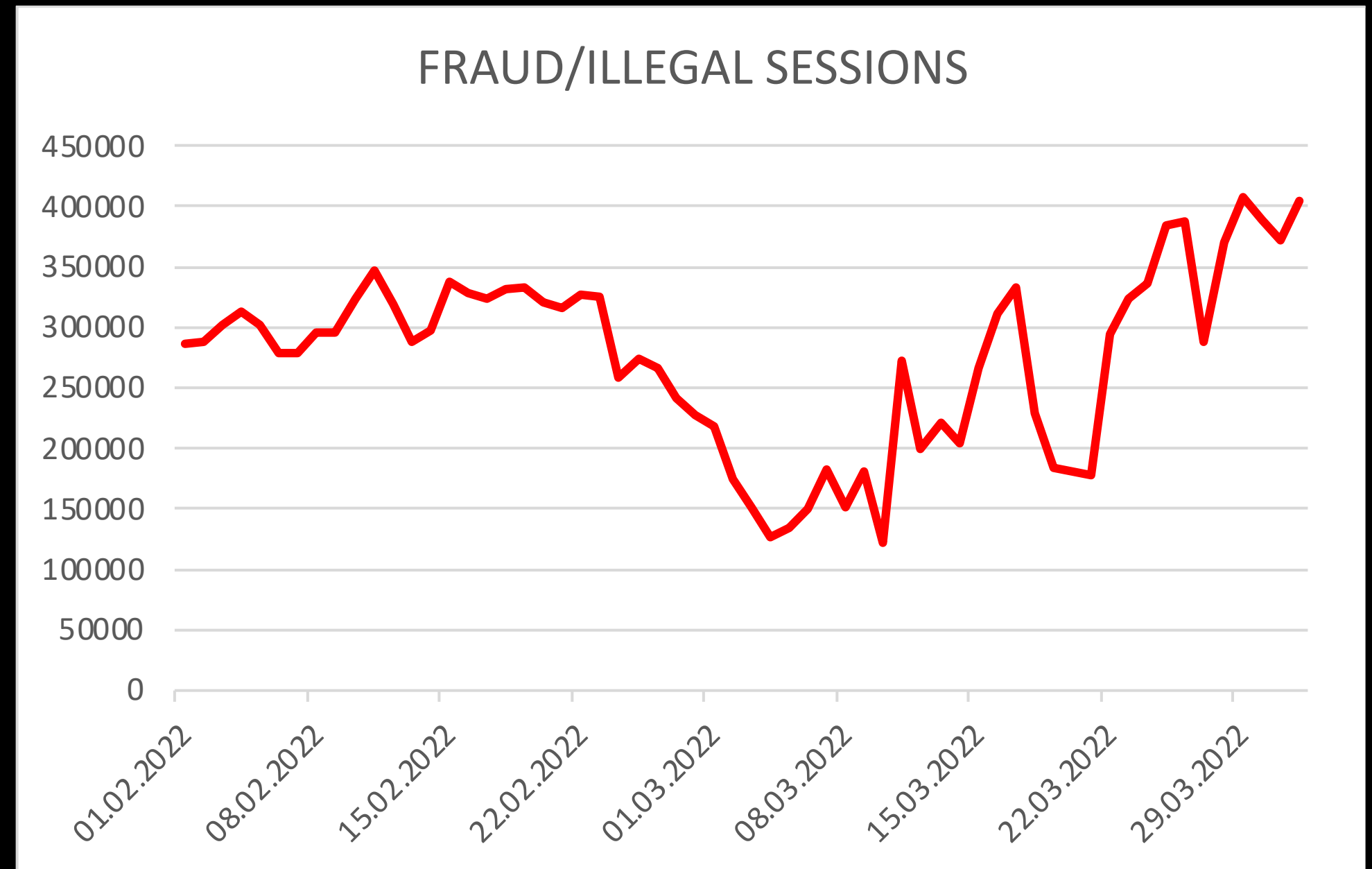


In 2021, the average losses on fraudulent pages amounted to **3,156,230,920** rubles.

The figure on the right shows the statistics of payment attempts from fraudulent and illegal sites for the spring of 2022.

In early February, the number of illegal transactions was about **300K** per day. The drop to **100K** occurred in the first week of March, and then we recorded an increase to **400K** per day.

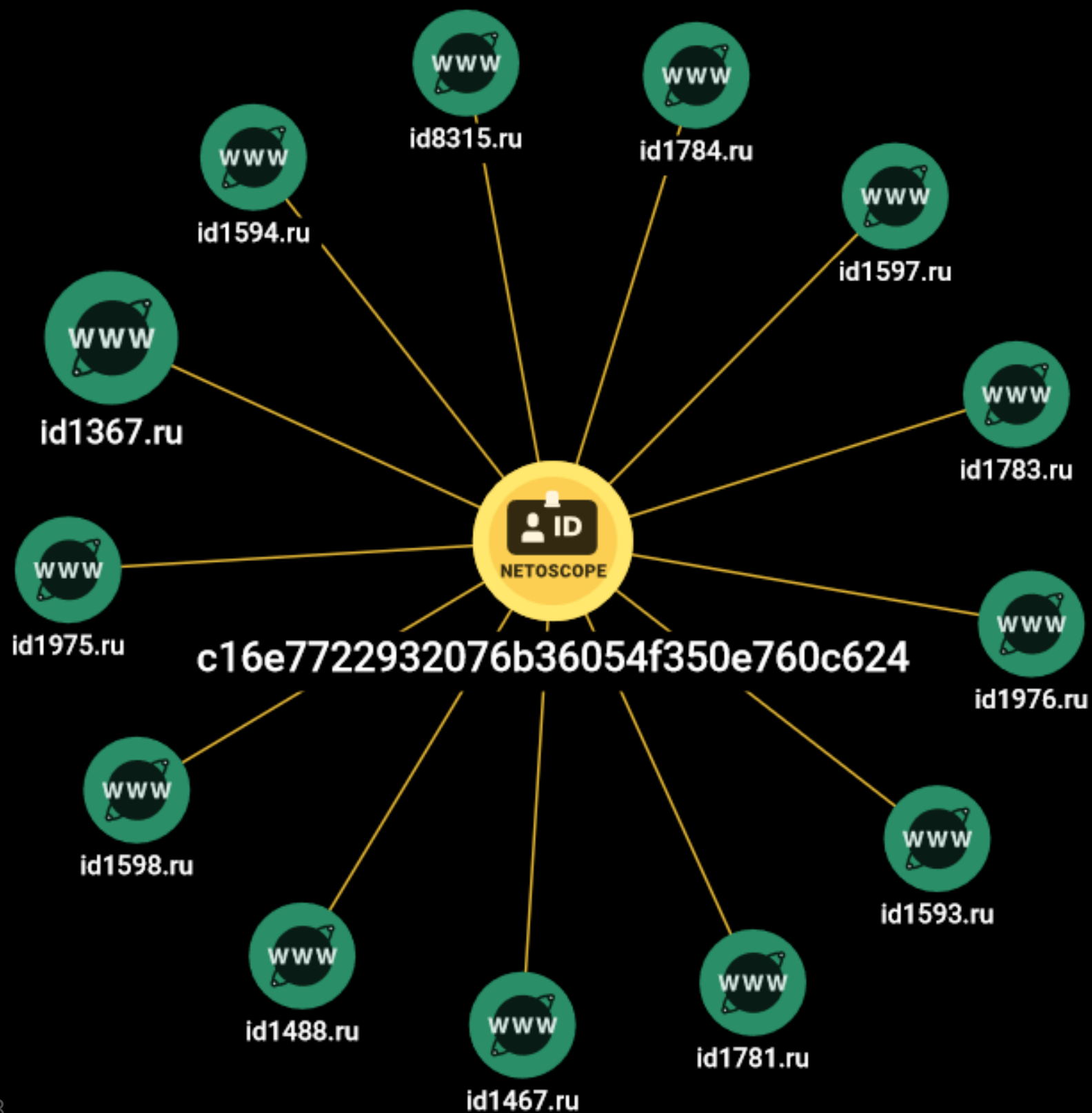
Approximately a **third** of all these sessions are scams using fake payment pages.



The service abuses 169 brands, including postal services, marketplaces, and retailers on more than 64 countries.

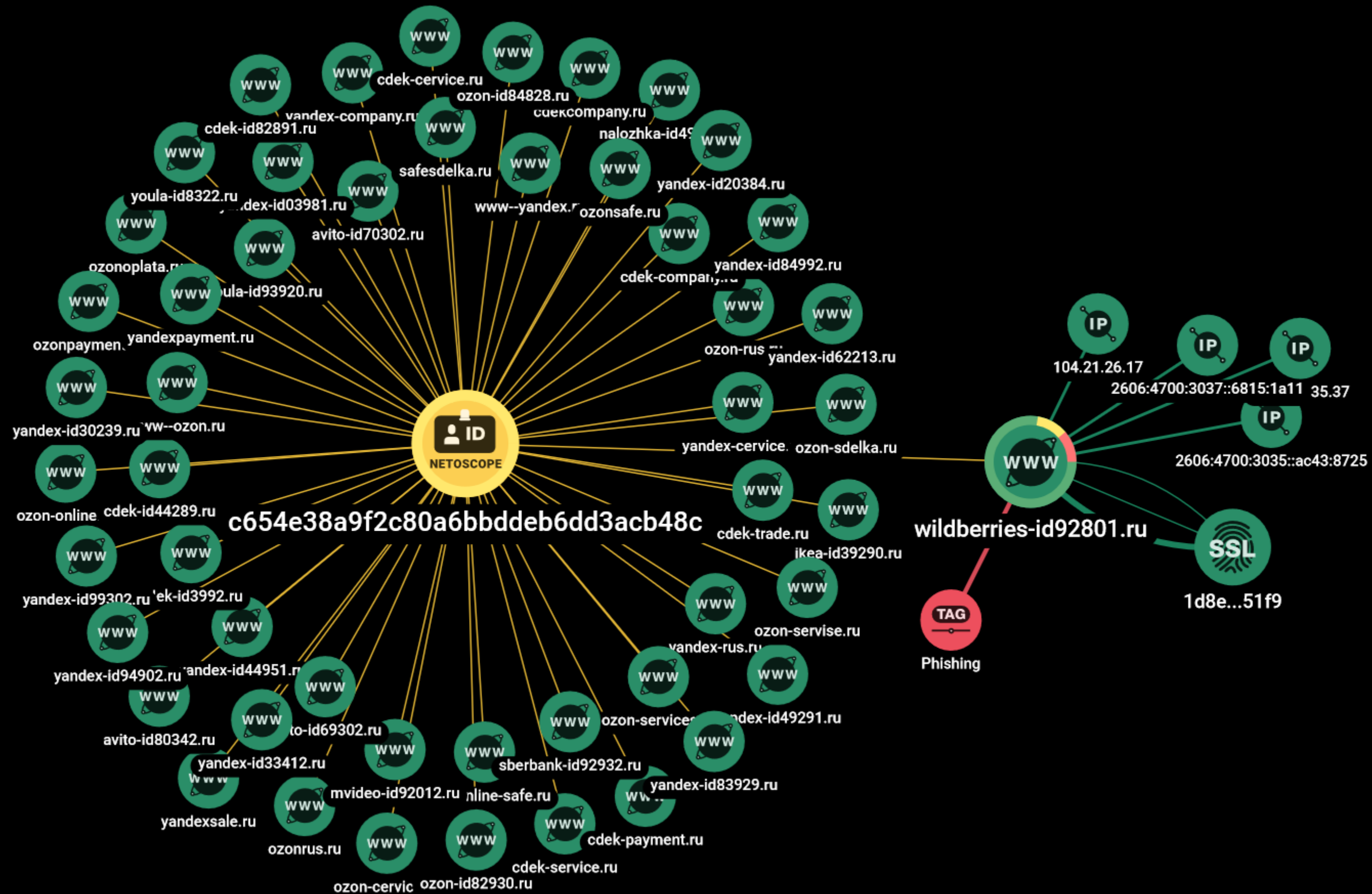


# PHISHING INFRASTRUCTURE. GRAPH

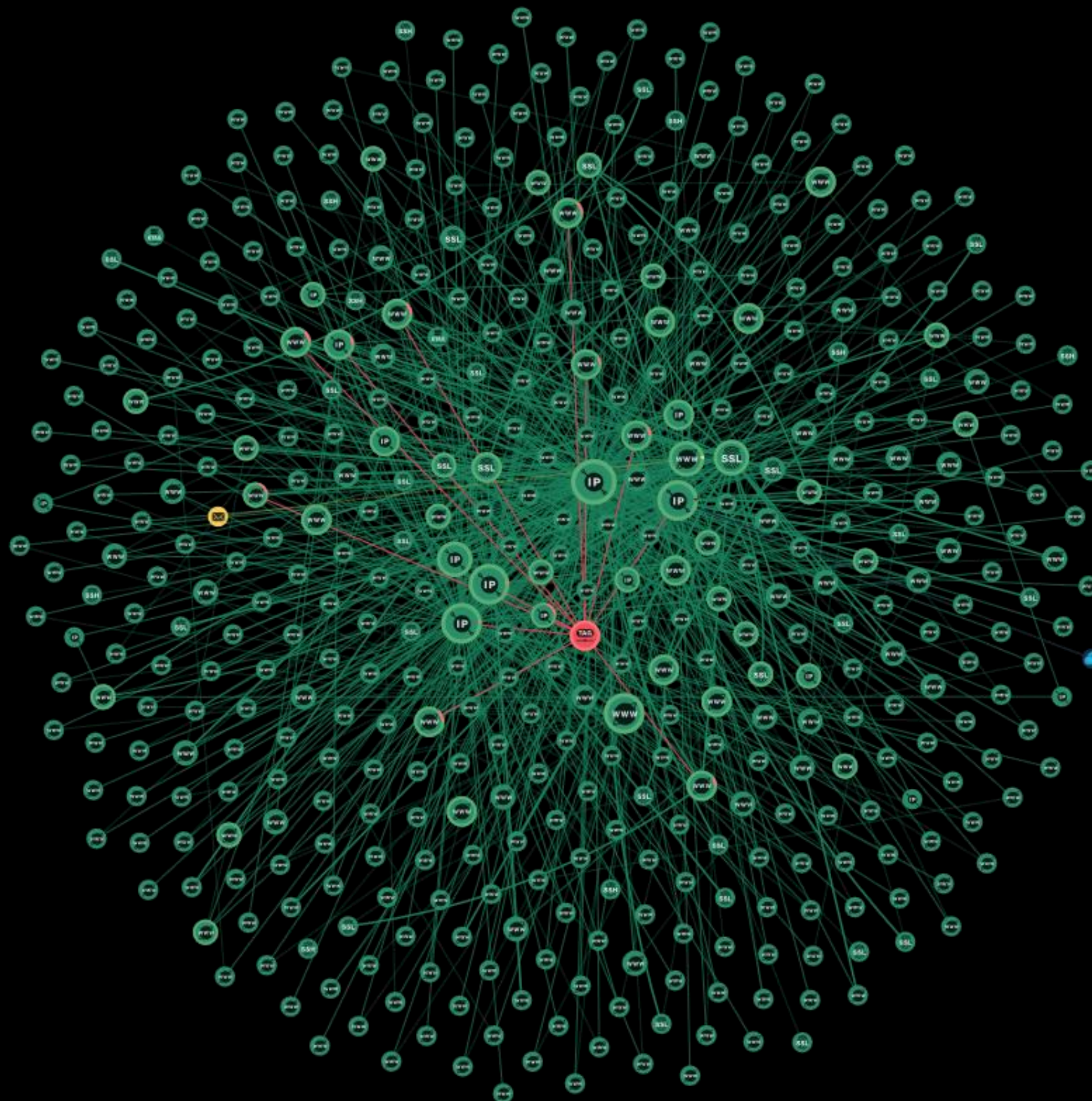


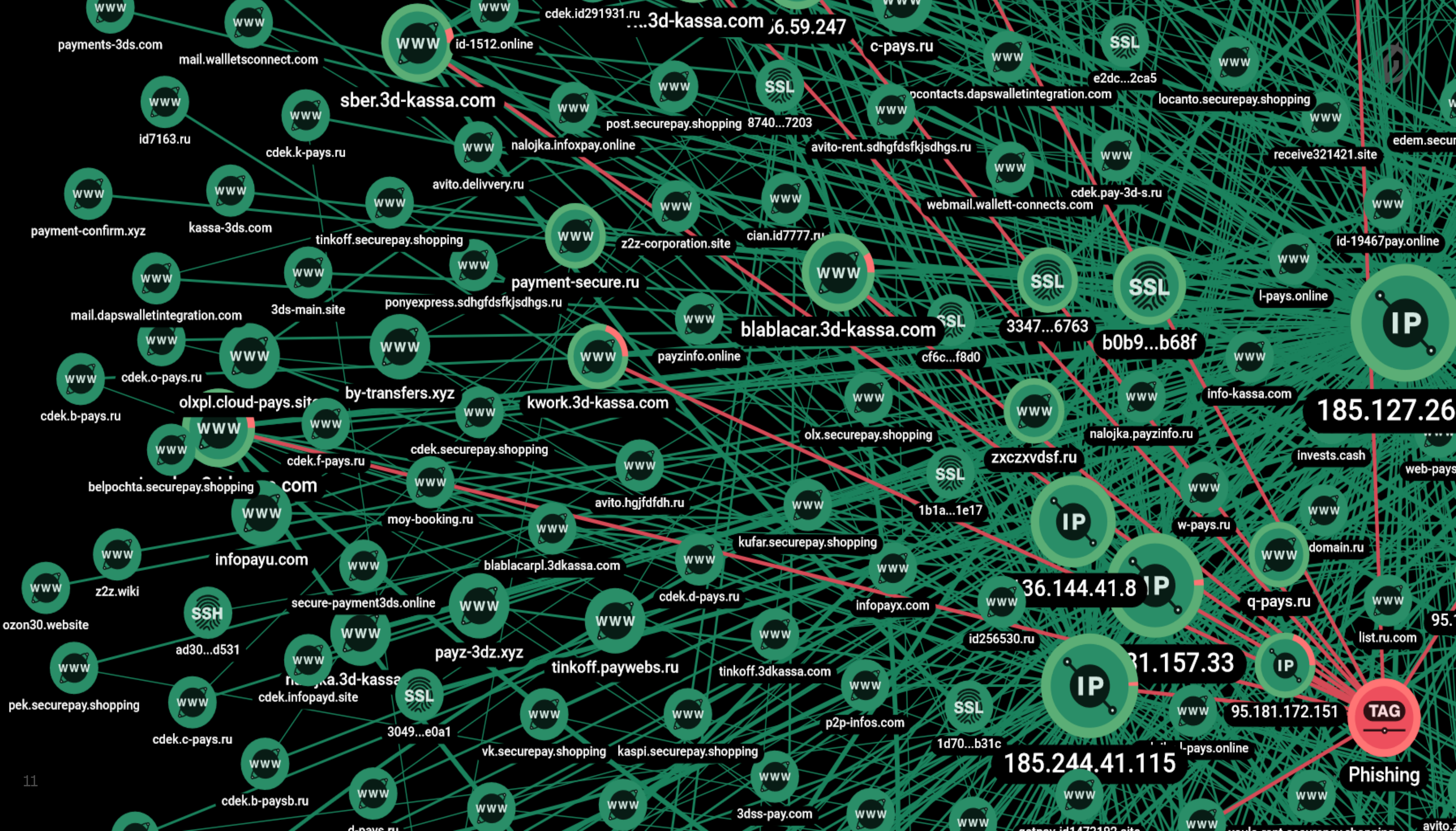


# PHISHING INFRASTRUCTURE. GRAPH

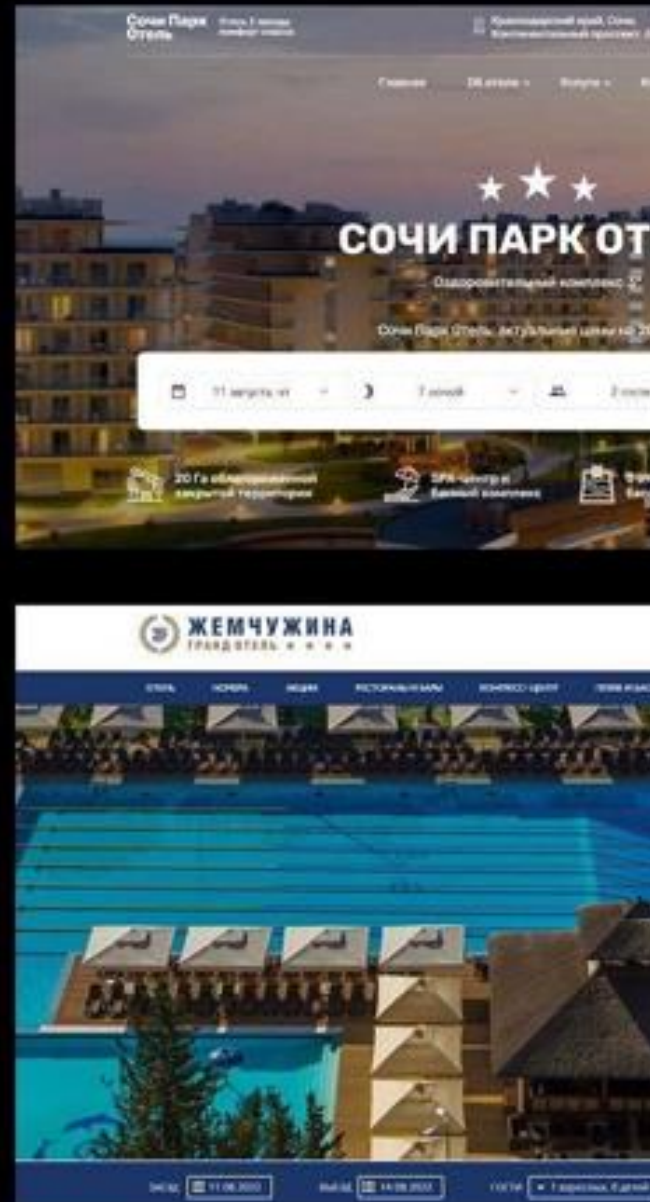



# PHISHING INFRASTRUCTURE. GRAPH





# PHISHING ATTACKS WITH 3DS





### Введите Ваш код

Магазин: SIRIUS HOTELS  
Сумма: 16500 RUB  
Дата: 17.08.2022  
Номер карты: \*\*\*\* \* 0107  
Личное приветствие: None

Одноразовый код был направлен на Ваш номер телефона.  
Пожалуйста, проверьте реквизиты транзакции и введите одноразовый код.

22&second\_date=20.08.2022&adult=2&children=0&amount=16500&d

Три цифры на обороте

зетесь с условиями оферты.

# P2P (C2C)

Card-to-card transfers (aka p2p, card2card, c2c) is a way to transfer money online using bank card details. To make a c2c money transfer, you need to have a bank card and know the recipient's card number.

The screenshot displays the Tinkoff website's interface for card-to-card transfers. At the top, the Tinkoff logo and navigation menu are visible. The main heading is "Перевод с карты на карту" (Transfer from card to card), with a subtitle "Мгновенный перевод денег между любыми картами любых банков" (Instant money transfer between any cards of any banks). Below this, there are two tabs: "По номеру карты" (By card number) and "По номеру договора" (By contract number). The "По номеру карты" tab is active. The interface is divided into two main sections: "С карты" (From card) and "На карту" (To card). The "С карты" section is highlighted in blue and contains a form for entering card details: "Открытие" (Opening), "Номер \*7263" (Number \*7263), "Срок" (Term), "CVC 000" (CVC 000), and a card type selector (MasterCard). Below the form, there is a note: "Введите срок действия карты. На карте он указан рядом с именем владельца" (Enter the card validity period. On the card, it is indicated next to the owner's name). The "На карту" section is highlighted in light blue and contains a form for entering the recipient's card number: "Любого банка" (Any bank), "Номер карты" (Card number), and a toggle switch. At the bottom, there is a field for "Сумма, ₽" (Amount, RUB) and a question mark icon. A footer note states: "Размер комиссии будет уточнен после ввода реквизитов платежа" (The commission amount will be clarified after entering the payment details).

# 3-D SECURE

**3D-Secure (Three-Domain Secure) is a protocol used as an additional level of protection for user authorization in CNP operations (without the presence of a card).**

Three domains are involved in the operation:

- 1) Issuer: the bank that issued the card to the client and is responsible for withdrawing funds and transferring them to the acquirer
- 2) Acquirer: a bank that provides services to the online store and accepts payment from the issuer
- 3) Domain of the payment system that provides the technical side of the transaction

How it works: you enter the card number to pay for the goods. At this moment, a certain amount is deducted from the account and frozen for a while on the payment system domain, waiting for confirmation via SMS. If the verification code has not been entered, the money is returned to the card holder's account after some time, without reaching the store address.

Bankamatik Mastercard SecureCode

KART NUMARANIZ: XXXX - XXXX - XXXX - 3317

199,00 TL DSM GRUP DANISMANLIK 16.09.2022 - 11:14

Online alışverişinizin ödemesini tamamlamak için, 54579\*\*\*99 numaralı cep telefonunuza SMS ile gelen ya da İşCep'e Anlık Mesaj olarak iletilen doğrulama kodunu girerek onaylayınız.

Doğrulama Kodu

ONAYLA

Tekrar Gönder

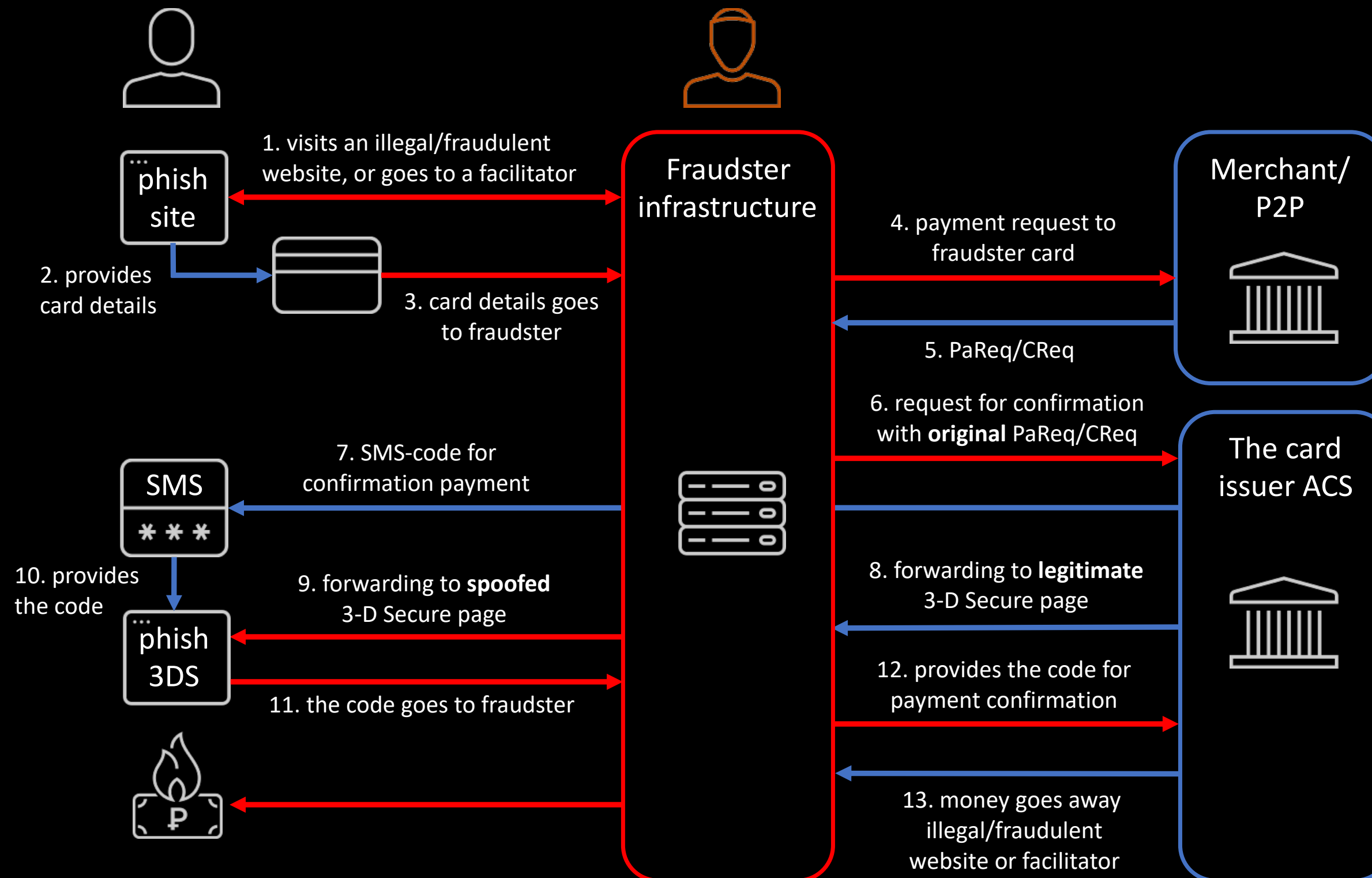
[İşlemi İptal Et](#) [Yardım](#)

172

KART BİLGİLERİNİZ İŞYERİ İLE KESİNLİKLE PAYLAŞILMAMAKTADIR.

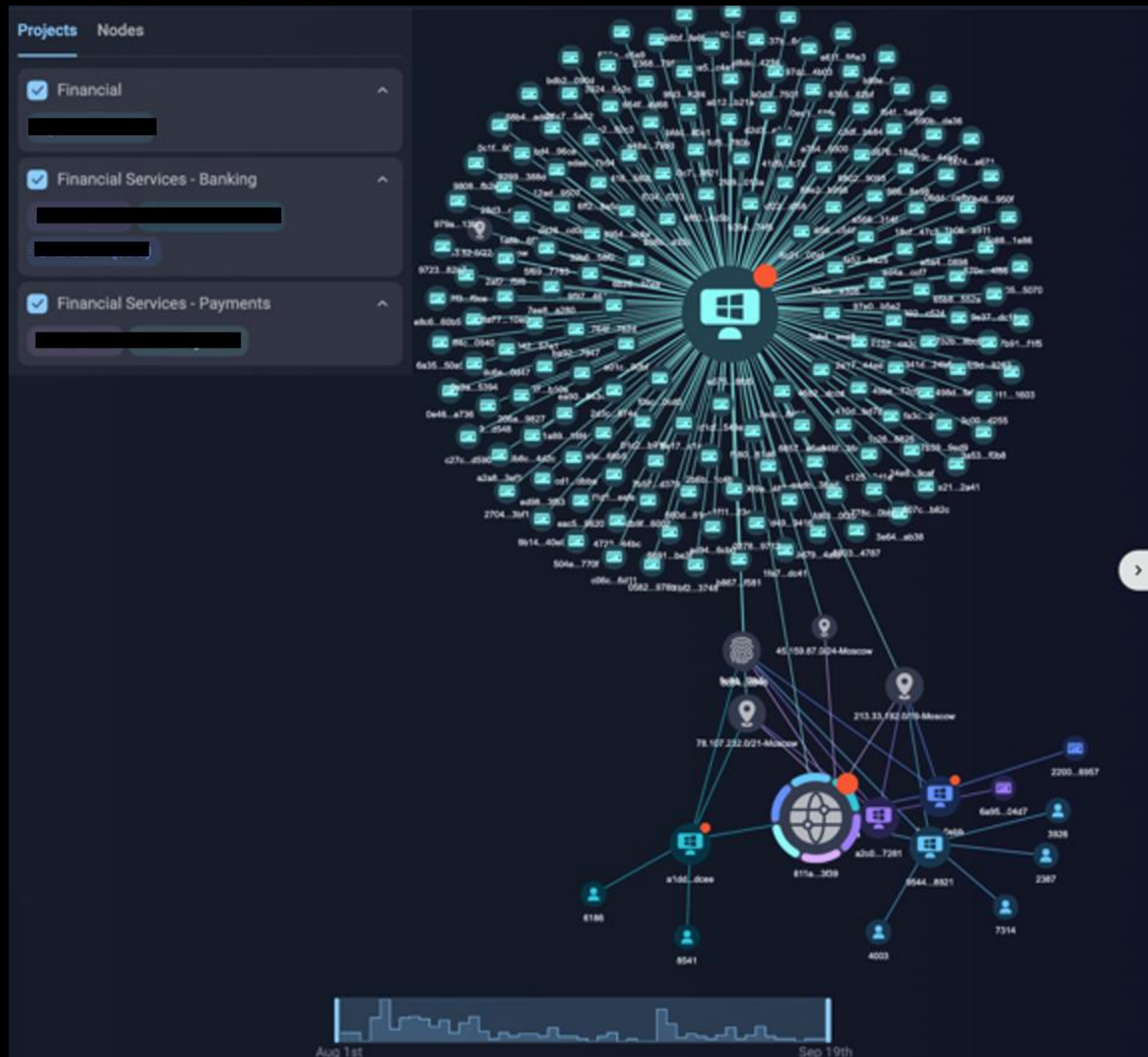
TÜRKİYE İŞ BANKASI

# ABUSE P2P (C2C) & BYPASS 3-D SECURE





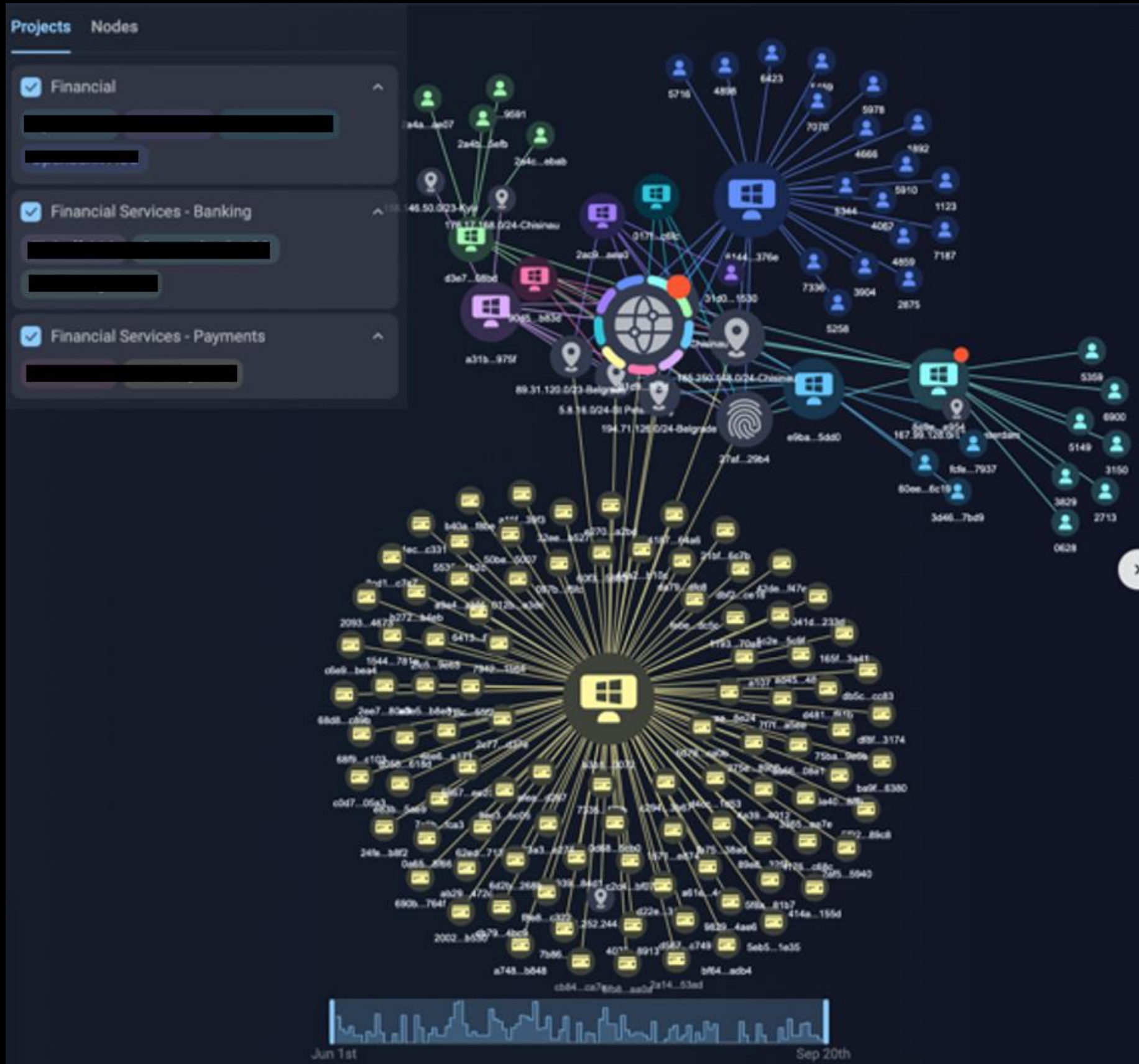
# A FRAUDULENT DEVICE SHOWN ON A GRAPH



For a long time, fraudsters use a single subnet and a single device to communicate with various banks (one digital fingerprint).



# A FRAUDULENT DEVICE SHOWN ON A GRAPH



For a long time, fraudsters use a single subnet and a single device to communicate with various banks (one digital fingerprint).

OUR MISSION



# FIGHT AGAINST CYBERCRIME

## FOR COMMON WELLBEING:

Our innovative technologies and in-depth investigations fight against cybercriminals to help this world become a safer place.

## FOR GROUP-IB'S CLIENTS:

We research, prevent potential attacks and react to real ones, investigate cases and solve issues to create the enabling environment for our customers and help their business boost.

## FOR GROUP-IB'S EMPLOYEES:

For us every team member is a hero. At any level or department, our employees are encouraged to innovate and solve real life problems, expected to be vigilant and provide all possible assistance to succeed in fighting against cybercrime.