

02.10.2024

# Marketplace scams

Neanderthals hunting Mammoths with Telekopye

**Jakub Souček**

Senior Malware Researcher & Manager

**Radek Jizba**

Malware Researcher



Digital Security  
Progress. Protected.



## Jakub Souček

Senior Malware Researcher & Manager

[jakub.soucek@eset.com](mailto:jakub.soucek@eset.com)



## Radek Jizba

Malware Researcher

[radek.jizba@eset.com](mailto:radek.jizba@eset.com)

## Online marketplace scams in numbers

**40%**

**Targeted**

[\[Besedo survey, 2024\]](#)

**70%**

**Success rate**

Consistently since 2015

[\[Statista, 2024\]](#)

**\$101**

**Average loss**

[\[Forbes, 2024\]](#)

**33%**

**Fraud listings**

[\[TSB, 2024\]](#)



# Terminology

## ✔ Mammoth

- Someone you want to “screw over” (Russian slang)

## ✔ Neanderthal

- The scammer (reversing the logic 😊)

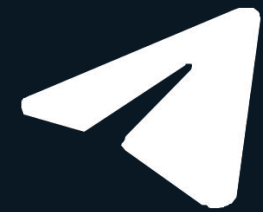
## ✔ Telekopye

- Telegram + копье (spear in Russian)



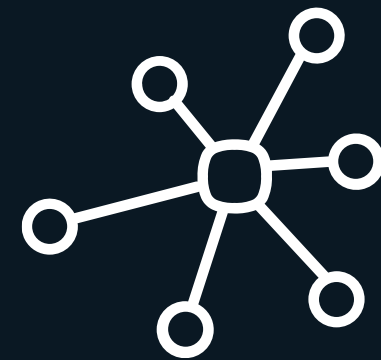
# Meet Telekopye

## Meet Telekopye



### Telegram bot

- Discovered by ESET in 2023
- Used since 2015 (at least)
- Automates the scam process
- Generates phishing emails, messages, webpages
- Coordinates scammers



### Many variants

- Samples on VirusTotal
- Willful code sharing
- Easy code manipulation (PHP)



### Many groups

- Dozens
- Each operating modified Telekopye
- Clear hierarchy



### Business-like

- Roles
- Taxes
- Teachers
- Newcomer applications
- Payouts



ОПЛАТА 10X

# STALIN *Team*

Of all the valuable capital in the world, the most valuable and most decisive capital is people

Join

Read more



## FEATURES *Bot*



- High quality Fakes
- Convenient Bot
- Responsive and kind TC
- Reliable laundering
- Free Avito Accounts
- Payments BTC/Qiwi
- CDEK/Boxberry sites
- Automatic Emails

TC - @NavZT

Бот - @stalinabot

## Meet Telekopye

**Fast payouts** ✈️

**Unique domains** 💎

**High quality bot** 👍

**24/7 support** 💬

Our bot

@MBINSCAMTEAM\_bot

Payments

Basic 80% | Refund 70%

Payments form 1 ruble

Our services

Avito YULA BOXBURY CDEK

BLABLACAR CIAN

1.0 2.0

Application form

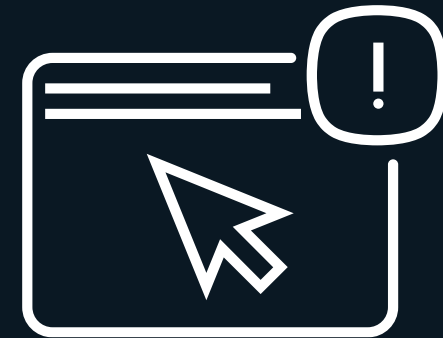
1. Link to UFOLABS profile
2. Your experience
3. How much time are you willing to devote

## Telekopye - targeting



### Financial theft

- Credit card data
- Online banking credentials
- Other sensitive information



### Fake paygates

- Well-made copies of known payment gate providers
- Often without graphical or language issues



### Online marketplaces

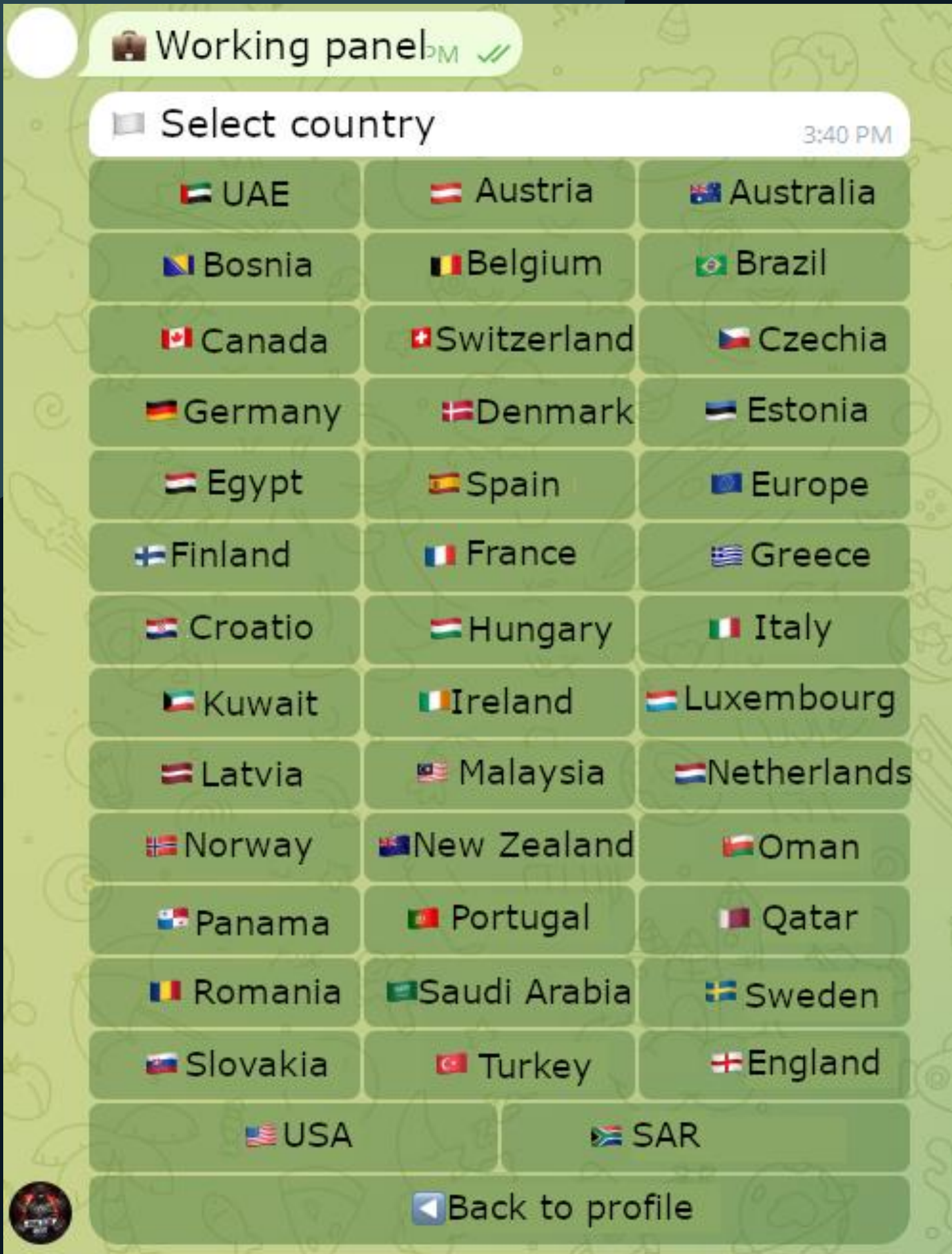
- Large number of targets
- Good knowledge of each platform (visuals, processes)



### Broad range

- Asia
- Europe
- US
- ...





### Telekopye - targeting



### gates

es of known  
providers  
raphical or

### Online marketplaces

- Large number of targets
- Good knowledge of each platform (visuals, processes)

### Broad range

- Asia
- Europe
- US
- ...

## Scam anatomy

### Seller (1.0)

- ✔ Neanderthal creates a listing for non-existent item
- ✔ Neanderthal persuades Mammoth to pay online
- ✔ Mammoth enters card / online banking details into fake paygate

### Buyer (2.0)

- ✔ Neanderthal looks up “suitable” Mammoth
- ✔ Neanderthal shows interest and persuades *Mammoth* to “pay”
  - Platform brand abuse
  - Courier brand abuse

# Buyer scenario + platform brand abuse

The screenshot shows the Etsy website interface. At the top, there is a search bar with the text "Search for anything" and the Etsy logo. Below the search bar, there are navigation links for various categories: Jewelry & Accessories, Clothing & Shoes, Home & Living, Wedding & Party, Toys & Entertainment, Art & Collectibles, Craft Supplies & Tools, and Vintage. The main content area features a product listing for a "Bag and Purse Set" priced at 40.00 EUR. The product image shows a blue and white patterned bag and purse. To the right of the product, there is a section titled "How you'll receive" with radio buttons for different payment methods: VISA, Mastercard, American Express, Diners Club International, PayPal, and G Pay. Below this, a summary table shows "Item(s) total" as 40.00 EUR, "Payment status" as "Receiving funds", and "Total (1 items)" as 40.00 EUR. A large black button labeled "Proceed to receiving" is positioned below the summary. At the bottom of the product card, it says "Payment status: Receiving funds" and "Estimated delivery: NOV 24". At the very bottom of the page, there is a small icon and text: "Etsy offsets the carbon footprint of each delivery".

Etsy

Search for anything

Jewelry & Accessories Clothing & Shoes Home & Living Wedding & Party Toys & Entertainment Art & Collectibles Craft Supplies & Tools Vintage

Contact shop

Bag and Purse Set 40.00 EUR

How you'll receive

VISA Mastercard American Express Diners Club International PayPal G Pay

Item(s) total 40.00 EUR

Payment status Receiving funds

Total (1 items) 40.00 EUR

Proceed to receiving

Payment status: Receiving funds

Estimated delivery: NOV 24

Etsy offsets the carbon footprint of each delivery

The screenshot shows a white background with a large orange exclamation mark icon at the top. Below the icon, the word "Attention" is written in a bold, black font. Underneath, there is a line of text: "The bank requested additional bank card information to verify card ownership." Below this text, there is a rectangular button with a blue border and the text "Card balance". At the bottom, there is a green button with the text "Submit".

Attention


The bank requested additional bank card information to verify card ownership.

Card balance

Submit



# Buyer scenario + courier brand abuse

 [Sledovat balík](#) [Poslat balík](#) [Vyhledat Balíkovnu](#) [Pro podnikatele](#) [MOJE BALÍKOVNA](#) CZ

### INFORMACE O DORUČENÍ

### TELEFONNÍ ČÍSLO PRODEJCE PRO KONTAKTOVÁNÍ OPERÁTORA

### ZPŮSOB PŘÍJMU FINANČNÍCH PROSTŘEDKŮ

VÁŠ BANKOVNÍ ÚČET

### TYP DORUČENÍ

DORUČENÍ KURÝREM  NÁKLADNÍ DODÁVKA

### ČÁSTKA K PŘIPSÁNÍ

Kč

[POKRAČOVAT](#)



### Sledovat balík

Máte-li jakékoli dotazy, můžete **kontaktovat online** technickou podporu

Ještě **rychlejší odesílání** díky předvyplněným údajům.

Balíky **přehledně na jednom místě** pro lepší kontrolu.

Můžete si vybrat platební systém, který vám vyhovuje.

Garantujeme vám bezpečnost vašich transakcí a rychlý příjem prostředků na váš bankovní účet.

# Credentials / card / MFA

# Revolut

## Log in using your phone

To keep your account secure, we'll send you a code to log in. New to Cash App?  
[Create account](#)

Mobile number

+1 (123) 456-7890

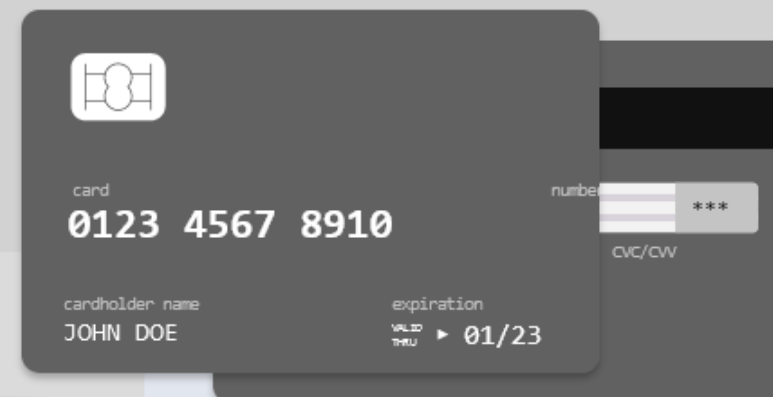
Password

Your password

Log in

By entering and clicking Next, you agree to the Terms, E-Sign Consent,  
& Privacy Policy

## Inserting a bank card



Name and surname of the cardholder

John Doe

Card number

0123 4567 8910 1112

Expiration date

MM/YY

CVC/CVV

\*\*\*

Continues

Order number	21492174
Produkt	ff
Cena	0 \$
Charge	0,0 \$
Total	0 \$

## Подтверждение операции ?

Магазин OZON

Сумма 3708 ₺

Номер карты \*\*\*\* \* 9184

Комментарий -

Для подтверждения операции на Ваш номер телефона было отправлено смс сообщение с кодом подтверждения. Введите его в поле ниже.

Код из смс:

Введите код из смс...

Запросить повторно через 0149

Отправить код

# Internal culture

GIPSY | Money 🍷  
Forwarded from GIPSY | Money 🍷



🎁 **НОВОГОДНИЙ КОНКУРС** 🎁 на 3.5% от общего банка на период с 1.12 до 30.12

- 🏆 Победители получают:
- 1. - место — 2% от 🏠
  - 2. - место — 1% от 🏠
  - 3. - место — 0.5% от 🏠
  - 4-6. - место — 1.000₽
  - 🎁 Случайно среди остальных — 1.000₽ (x3)
- P.S. узнать статистику /promo в чат



👤 **КОДЕРЫ** кто занимается созданием фишей ?  
🔥 Есть свежие интересные офера, есть работа 🔥  
📝 **Подробности:** @specagentmoney 5:13 PM



✅ FULL WORK! ✅  
🇵🇱 Польша 🇫🇮 Финляндия 🇳🇱 Нидерланды 🇵🇹 Португалия  
🇪🇸 Испания 🇬🇷 Греция 🇨🇪 Чехия 🇸🇰 Словакия 🇫🇷 Франция,  
🇱🇺 Люксембург 🇨🇭 Швейцария  
🇩🇪 Германия  
✅ Перед началом ворка просьба убедиться что ваш ТПшер онлайн! По возможности прыгайте на других! 9:20 AM

February 6

🟢 FULL WORK 🤖 11:07 AM

🔴 STOP WORK ! 10:08 PM

February 7

🟢 FULL WORK 🤖 11:04 AM

🔴 STOP WORK ! 10:22 PM

February 8

🟢 FULL WORK 🤖 11:08 AM

🔴 STOP WORK ! 9:55 PM

February 9

🟢 FULL WORK 🤖 11:15 AM

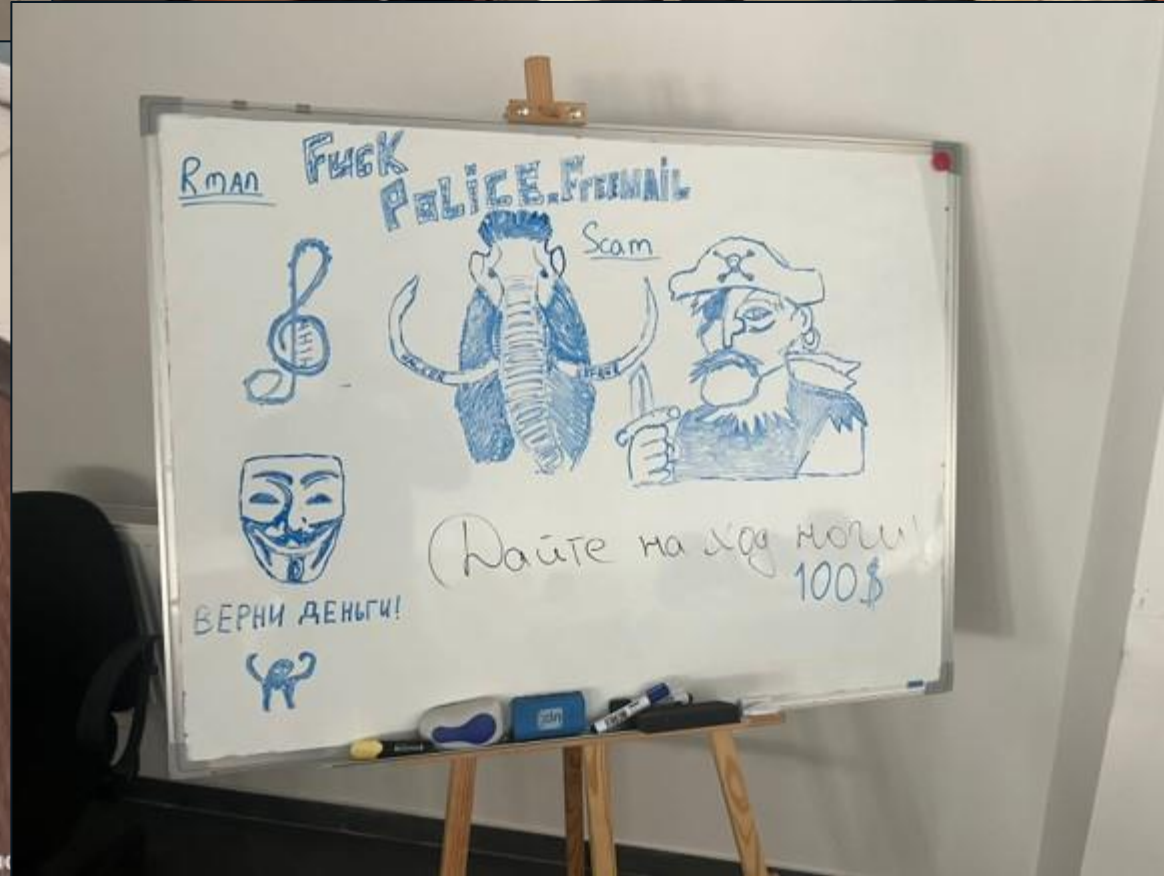
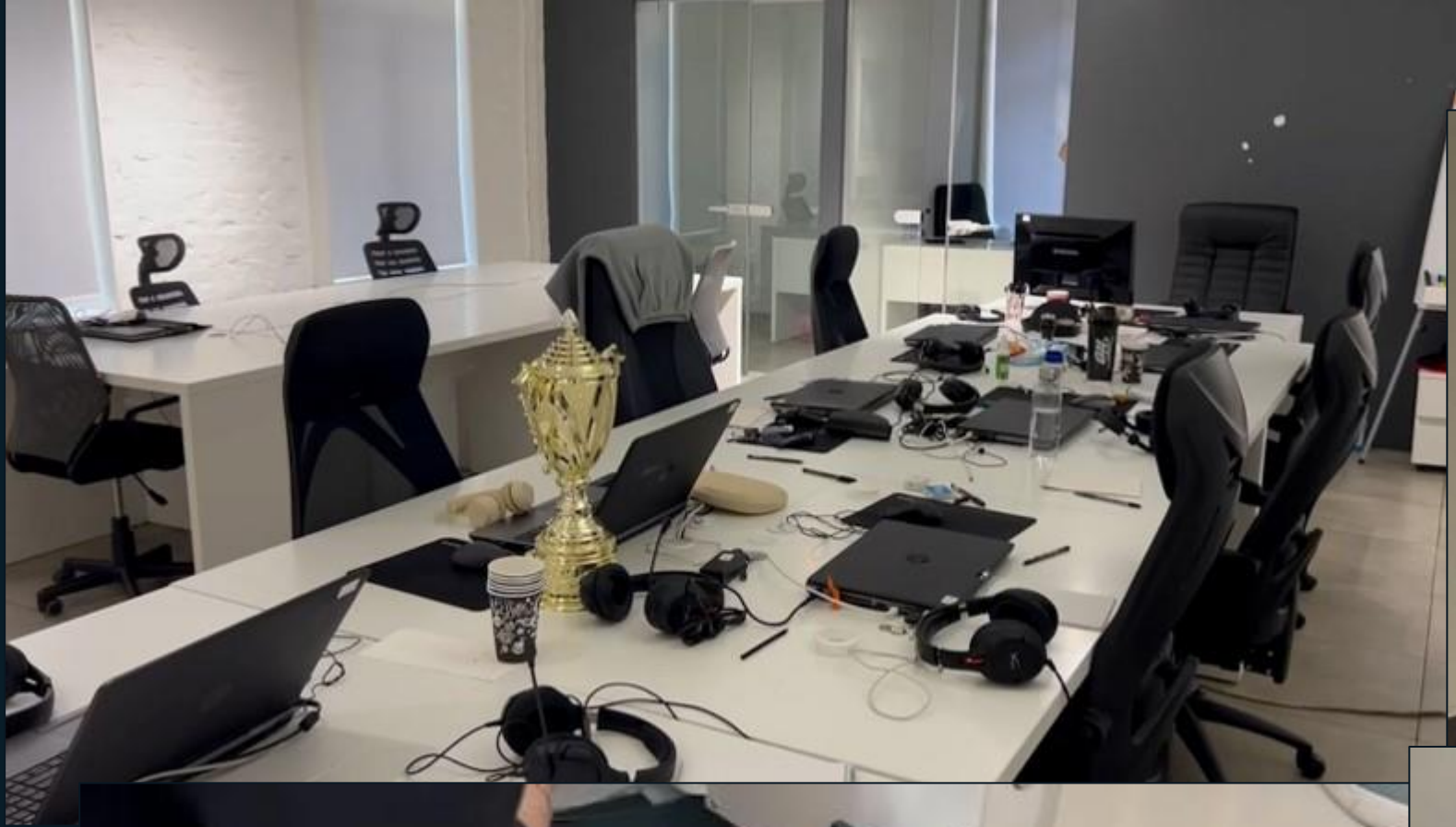
🔴 STOP WORK ! 10:10 PM



**Fighting back**

## Operations RIP & VICTORY

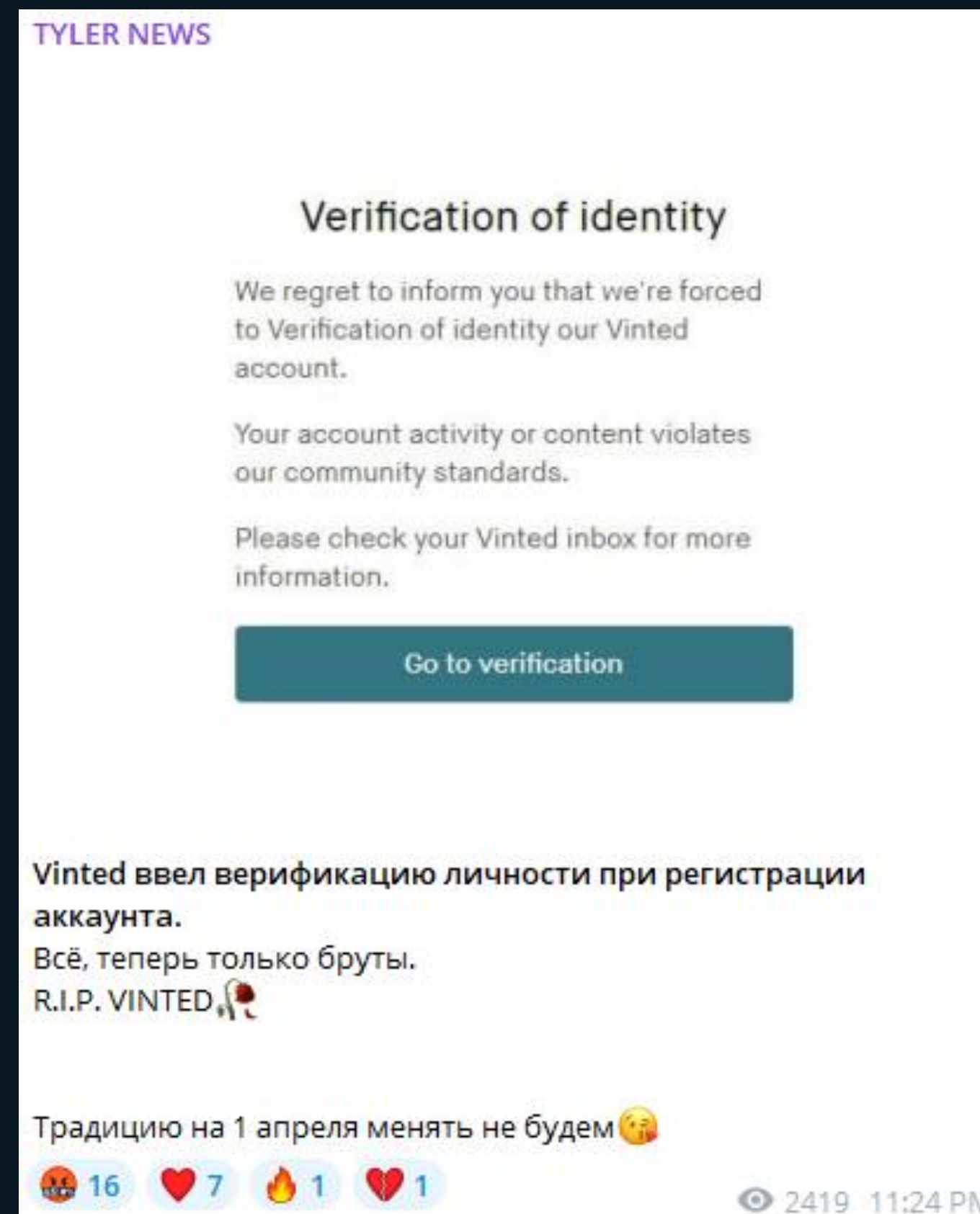
- ✔ CZ and UA police arrested tens of Neanderthals
- ✔ Estimated at least €5 mil since 2021
- ✔ Organized by middle-aged men from Eastern Europe and West and Central Asia
- ✔ Recruited people in difficult life situations
- ✔ Recruited on job portals and even universities
- ✔ Related “call center” operation – confiscating passports, threatening family members





# Platforms' defense

- ✓ ESET was in contact with several such platforms – they are definitely not defenseless / unaware
- ✓ Techniques
  - User verification
  - Display of user information
  - On-platform chat
- ✓ Main issue: quantity and speed
- ✓ Example:
  - Platform with few million users
  - Up to 1000 customers targeted each day, focus on new ones
  - On occasions, more than half of such users hit per day
  - (At least) 14 groups target this platform
  - More than 100 new domains daily



**Expansion - accomodation**

# Accommodation scenario

- ✓ Acquire credentials of advertisers on accommodation websites
- ✓ Target users that
  - Recently booked their stay and paid
  - Recently booked their stay and didn't pay yet
- ✓ Create very targeted phishing website
  - Pre-filled dates, guest information, price, ...
- ✓ Pressure to pay
  - Issue with payment
  - Running out of free rooms

< Request to book

**This is a rare find.**  
This place is usually booked.

**Your trip**

**Dates** Edit  
June 5 - 12

**Guests** Edit  
2

**Choose how to pay**

**Confirmation of booking**   
Please note this is not a payment, but a booking confirmation.  
To confirm the reservation, the amount will be debited from your card and returned back

**Pay part now, part later**   
Pay now, and the rest will be automatically charged to the same payment method. No extra fees.  
This feature is not available


**Log in or sign up to book**

Country/Region  
United States (+1) ▼

Phone number  
(XXX) XXX-XXXX

We'll call or text you to confirm your number. Standard message and data rates apply. [Privacy Policy](#)

**Continue**

 Hotel Paradise  
★ 5.0 • Superhost

---

**Price details**

Price	€100.00
Service fee	€15.00
<b>Total (EUR)</b>	<b>€115.00</b>



# Customized features



# Creation speedup

- ✓ Traditional approach = fill in questionnaire
  - Mammoth name
  - Item name
  - Item image
  - Item price
- ✓ Neanderthals developed parsers for popular marketplaces
- ✓ URL is sufficient
- ✓ Significant speedup





# Chatbot with automatic translation



**New message**

Vinted: 235321553  
Name : Light blue denim FatFace summer dress, XL / 42 / 14  
Cost : 4.5 GBP

Text: Where do I find CVC on my credit card?  
Translation: Где мне найти CVC на моей кредитной карте?  
3:18 PM

Answer

Она находится на обратной стороне вашей кредитной карты  
3:22 PM ✓

✗ Message not sent!  
Reason: The text contains Cyrillic  
3:22 PM

It is on the back of your credit card 3:22 PM ✓

It is on the back of your credit card  
✓ Message sent 3:22 PM

Write again

It is on the back of your credit card  
👁 Message seen 3:23 PM

Card number  
1234 1234 1234 1234

Name on card  
Name on card

Expiration date  
MM YY

CVV/CVC  
CVV/CVC

Support Chat

Where do I find CVC on my credit card?

It is on the back of your credit card

Your message...



# Generation on web

GREEDY RENT Auth key: bae\*\*\*\*fe116

**Manual mode** Parser

Service name  
DPD

Country  
Хорватия

Version  
2.0

Product name  
Nintendo Switch Lite

Creation date  
04.08.2024

Transaction date  
06.08.2024

Delivery address  
Hickory Street 3, Philadelphia

Price  
20 €


**Create Ad**

Request status **Completed**

UNI-link <https://dod.onlyoffer-check.com/22290733>

link <https://dpd.onlyoffer-check.com/order/22290733>

Generate QR cod



Copy link Download





# How to stay protected



# On the platform

- ✓ Be extra careful if you are new
- ✓ Look for grammar issues
- ✓ Careful with overly eager buyers / sellers
- ✓ Verify the person you are dealing with
  - History on platform
  - Age of their account
  - Rating
  - Location
- ✓ Be aware that Neanderthals also use stole accounts
- ✓ Insist on in-person exchange whenever possible
- ✓ Otherwise
  - Seller → manage delivery options yourself
  - Buyer → pay on delivery
- ✓ Don't leave the platform





# Outside of the platform

- ✓ Some platforms, mostly for legacy reasons, defer to email communication post-agreement
- ✓ Popular messaging apps like WhatsApp should be considered red flags
  - “I am on a business trip”
  - “I have to leave my computer now”
- ✓ Double-check every link





# On the phishing website

- ✔ Pay extra attention to
  - URL
  - Content
  - Certificate
- ✔ You can try to enter invalid data and observe
- ✔ Anti-malware solution
- ✔ If you are unsure, verify with your bank / payment provider





# When you got scammed

- ✓ Report your case to your bank
- ✓ Do it ASAP, if there is still chance to save the money
- ✓ Banks value such reports, as they can inform their other customers
- ✓ Do not remove any evidence from your machine and contact the police, especially if
  - Sensitive information was shared
  - Monetary loss happened
  - You have valuable information for possible prosecution



# Conclusion



## Conclusion

- ✔ Telekopye is responsible for a significant portion of online marketplace scams
- ✔ Scam setup is fast and easy
- ✔ Scamming groups are well organized
- ✔ Neanderthals are adapting and expanding
- ✔ The best defense is awareness



## Q & A



[Telekopye: Hunting Mammoths using Telegram bot](#)

[2023-08-24]



[Telekopye: Chamber of Neanderthals' secrets](#)

[2023-11-23]