

|GROUP|IB|

# **DarkPath scammers & Scam ads in social media**

# About Group-IB



Group-IB is one of the global leaders in providing high-fidelity Threat Intelligence and anti-fraud solutions

EUROPOL INTERPOL

Official EUROPOL and INTERPOL partner

OSCE

Recommended by the Organization for Security and Co-operation in Europe (OSCE)

WORLD ECONOMIC FORUM

Member of the World Economic Forum and International AntiCounterfeiting Coalition (IACC)

1000+

successful investigations worldwide, including 150+ high-profile cases

\$300 mln

was returned to our clients thanks to Group-IB's efforts

Forrester Gartner

According to Forrester and Gartner, Group-IB Threat Intelligence is among the best services of its kind in the world

BUSINESS INSIDER

One of the top 7 most influential cyber security companies according to Business Insider UK

IDC

Leader of the Threat Intelligence Market



FROST & SULLIVAN

Bloomberg

InformationWeek DARK Reading

Forbes

Esquire



Media coverage:

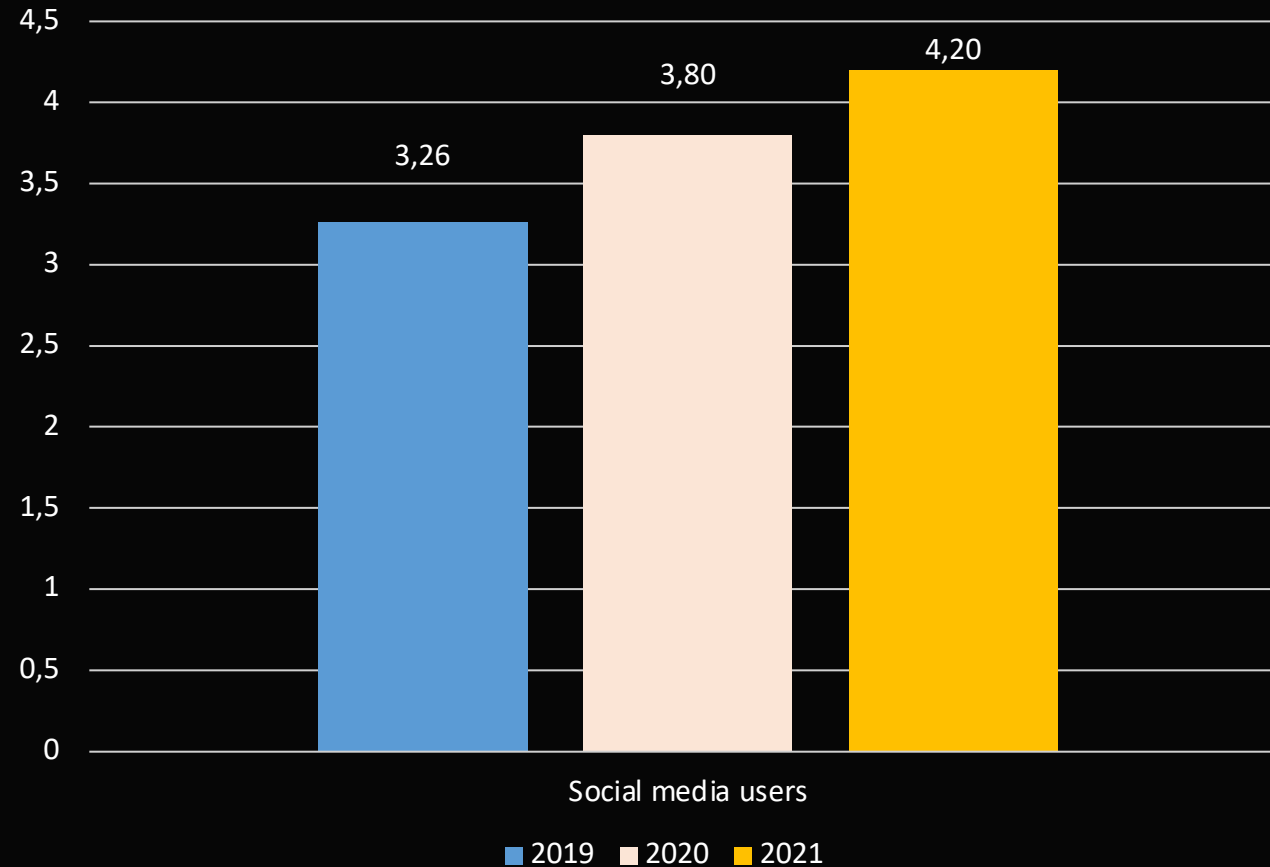
The Register

theguardian

REUTERS

CNN

**Over the last three years, the number of users of social networks has increased by almost a billion.**



Data from datareportal.com «DIGITAL 2019-2021: GLOBAL DIGITAL OVERVIEW»

|GROUP|IB|

# **Scam ads in social media**

# History of scam

|GROUP|IB|

Emails

Sites

Traffic attraction  
SEO, Advertisement

Mobile

Mobile applications

2010

2021

**5%** web traffic  
mobile users

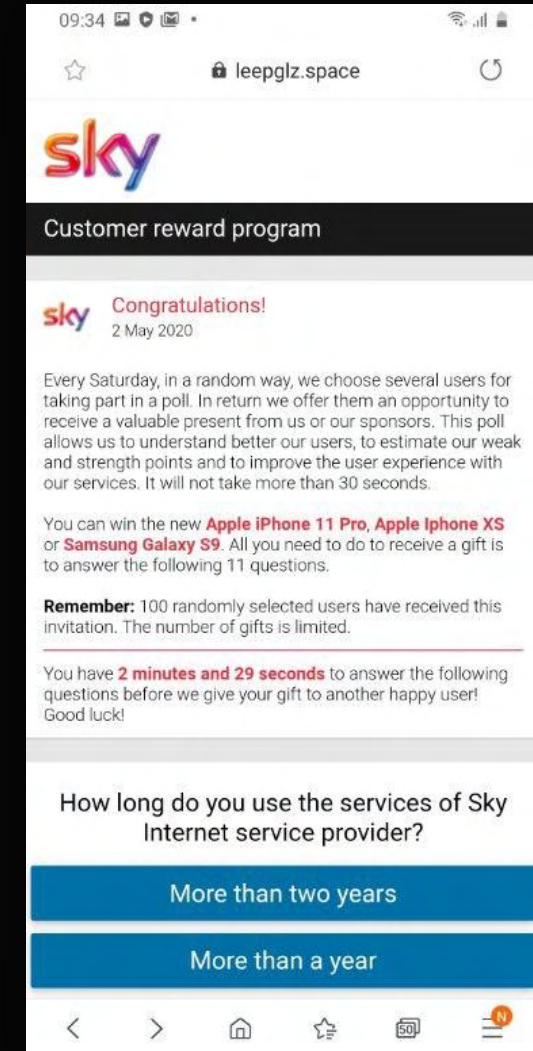
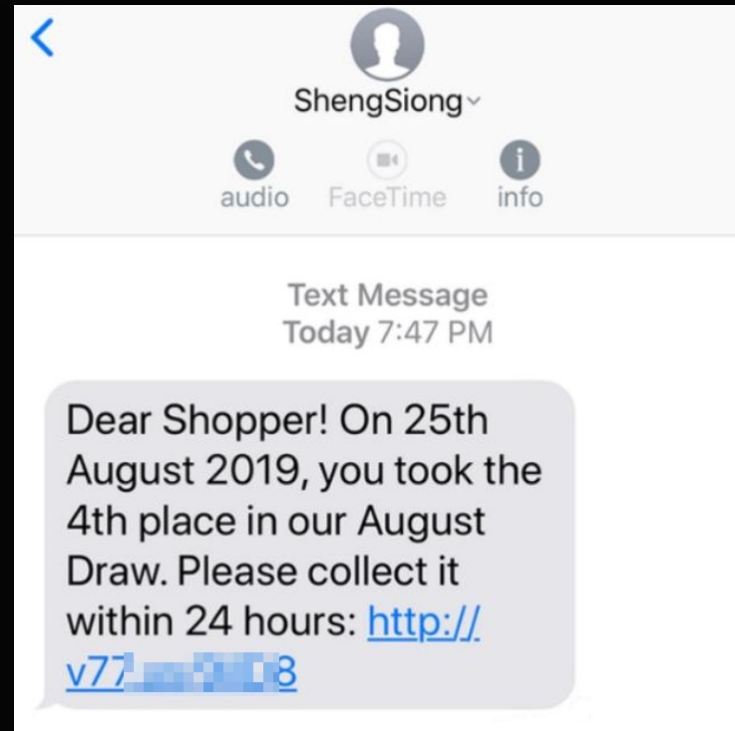


**56%** web traffic  
mobile users

Only 8% of  
users time

# Benefits of mobile targeting

- Personal
- More targeted
- Fast decision
- Hard to verify



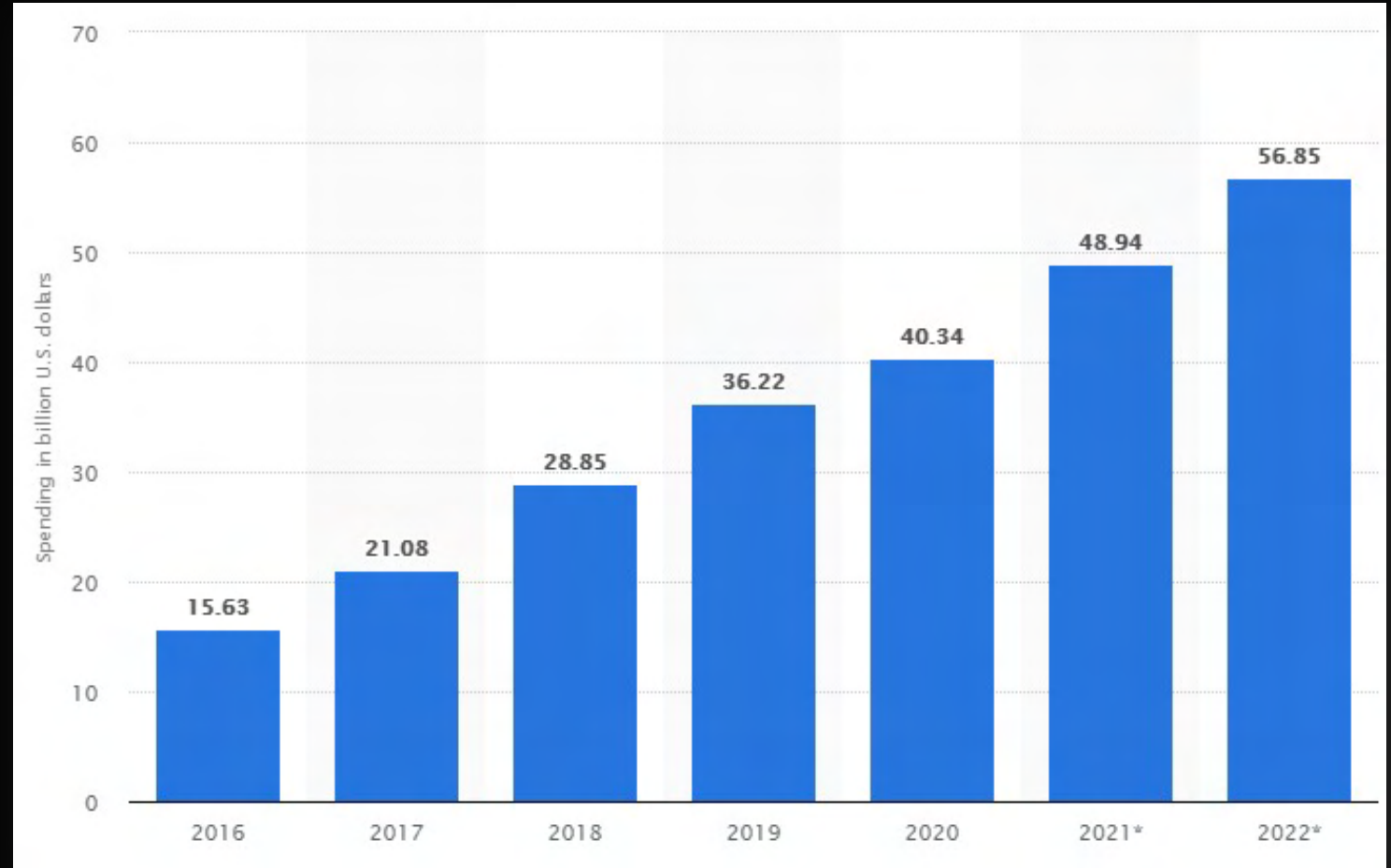
# Benefits of social networks

- Easy
- Scalable
- Distributed
- Fail-safe
- Almost undetectable
- Everybody uses it and uses a lot
- Trustworthy
- User has no chance to verify



# Damage

- Distrust to the brand
- Inflation of the ad price
- Wrong customer journey



Social network advertising spending in the United States from 2016 to 2022  
(in billion U.S. dollars)

Source: <https://www.statista.com/statistics/736971/social-media-ad-spend-usa>



# Targeting

|GROUP|IB|

Select the location, age, gender and interests of people you want to reach with your ad.

Gender ⓘ

All

Men

Women

Age ⓘ

18

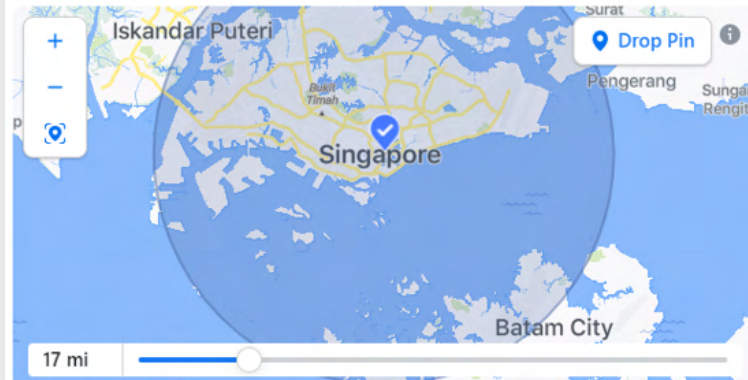
65+

Locations ⓘ

Locations  
Type to add more locations

Singapore

Singapore + 17 mi X



Detailed Targeting ⓘ

Detailed Targeting  
Add people who match at least one of the following

Browse →

Interests

Banking X

Investment X

Lottery X

Chinese New Year X



Potential Reach: 2,800,000 people

Your audience is defined.

Learn More

Choose when this ad will end

⚠ Increase the Duration

Ads that run for at least 4 days tend to get better results.

Days  
1

End date  
Feb 6, 2021

Daily Budget

Actual amount spend daily may vary. ⓘ

Estimated 1.8K - 5.1K people reached per day

\$ 10.00

Estimated Daily Results

People Reached ⓘ 1.8K - 5.1K

Link Clicks ⓘ 114 - 331

Payment Summary

Your ad will run for 1 day.

Total budget \$10.00 a day x 1 day. \$10.00 SGD

Estimated tax \$0.70 SGD

Total amount \$10.70 SGD

Have Questions?

Request a free call with a Marketing Expert.

Request Call

Placements  
Facebook, Messenger, Instagram

**\$1**  
for 500 views

**5%**  
conversion

**\$0.04**  
per click

**\$450**  
daily budget for  
new accounts

# How it can be used

- Data collection
  - Fake promo
  - Phishing
  - Information attacks
  - 3rd party promotion
  - Scam
- 
- Online Shopping
  - Romance scams
  - Economic relief scams
  - Income opportunity scams
  - Grant money
  - Giveaways
  - Multi-level marketing MLM
  - Pyramid schemes
  - Blessing circles/gifting schemes
  - Recruiting scam



# Numbers

**200**

fake accounts

**190**

fake pages (sites)

**1-2 days**

each campaign duration

**6 months**

total attack duration

**1 mln visitors**

for 1 website



# Numbers

Report of scams that started in social media



Figures based on fraud reports directly to the FTC indicating a monetary loss where the method of contact was specifically identified as social network, and reports where the method of contact was not specified, specified as internet, or consumer initiated contact, if the comments field also included mention of Facebook, Instagram, LinkedIn, Pinterest, Reddit, Snapchat, TikTok, Tumblr, Twitter, or YouTube. The analysis excludes reports categorized as complaints about social networking services, internet information services, mobile text messages, and unsolicited email.

**50%**  
Instagram scam  
rise in 2020  
in the UK



# Internal reasons?



Facebook's continued reliance on a small army of **low-paid, unempowered contractors** to manage a daily onslaught of ad moderation and policy enforcement decisions

Facebook created a **financial symbiosis with scammers, hackers, and disinformation peddlers** who use its platforms to rip off and manipulate people around the world.

In the weeks leading up to voting day, Facebook moved some of its ad monitors off their usual tasks to **focus on helping political advertisers buy as much inventory as they wanted**

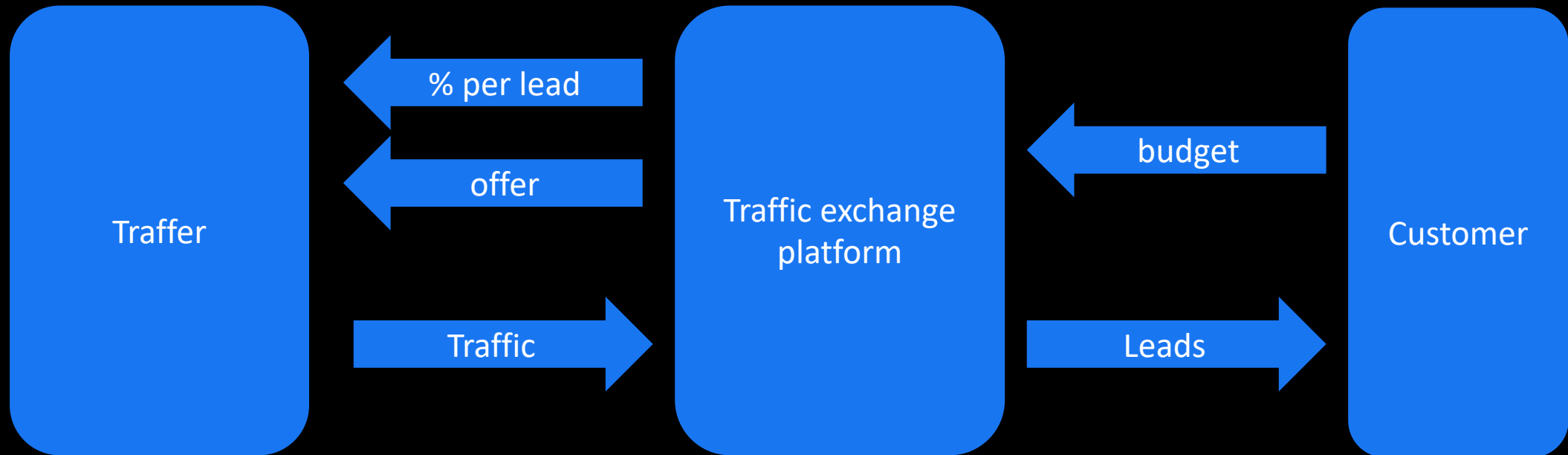
It earned more than **\$50 million in revenue** over two years from a single shady San Diego marketing agency that ripped off Facebook users by tricking them into hard-to-cancel subscriptions and investment scams

|GROUP|IB|

**DarkPath scammers**

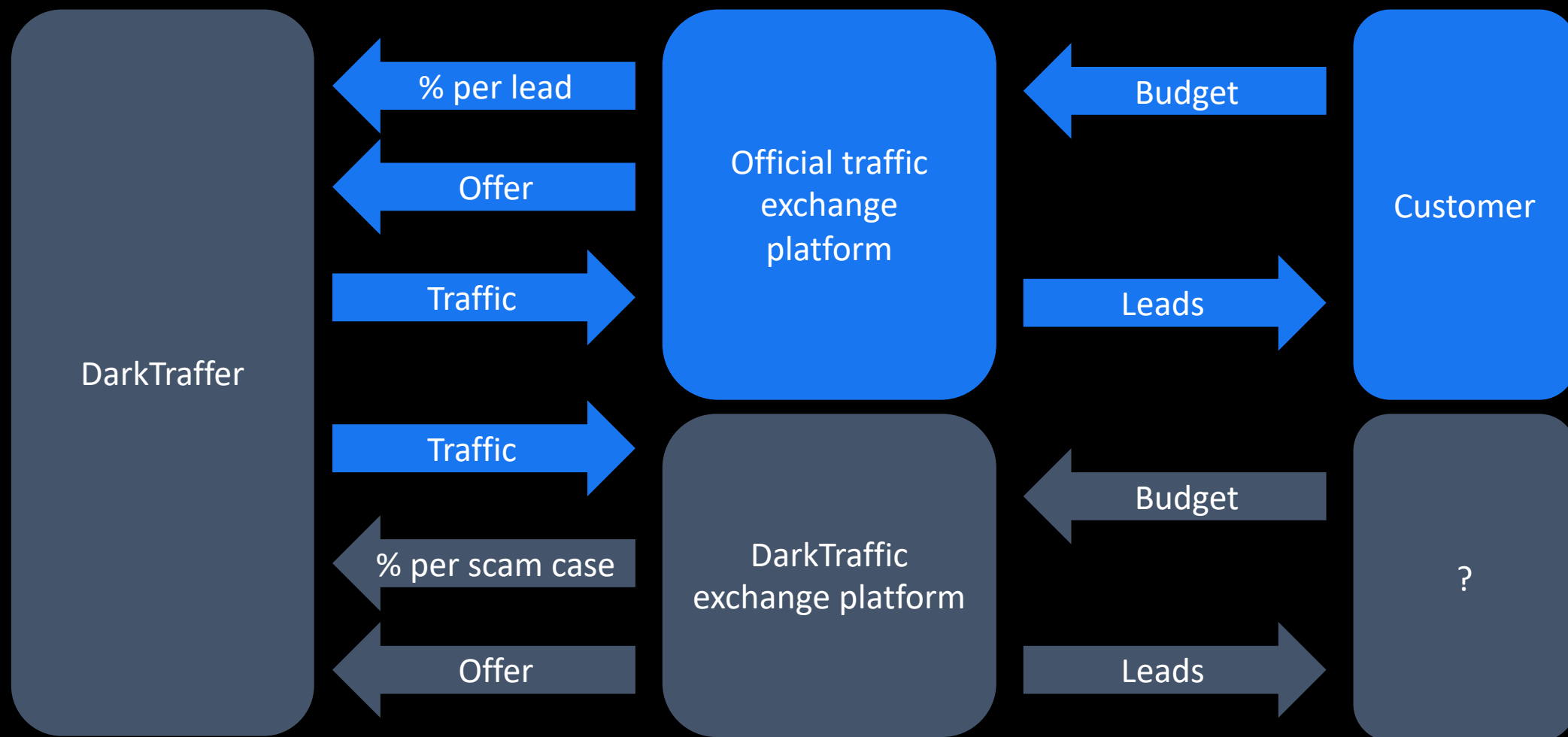
# Expectation

|GROUP|IB|



# Reality

|GROUP|IB|





# Traffers' business example

\$'' 1.9#8\*' 1()\*  
:83.(); '\*.<

=' (>)\*?.9#7)4'''\*  
:(\*1@@ '\*.<

A)%' (-B-%5#(+, '

! "#\$%&' %()\*+ #), (-)%./

! ((\*18(-)%#), (-)%./

!"#\$%&' %()

! Black Friday offer  
! ! "#\$%&' (#)'\*+, -. %  
! /-0".12"1%#\$3-2, "1\*#%A-1\*  
! 45&-1""6"7-. ""."\$"#\*"

Ideas

8' #+\$7#5&+#9: .#+%;; "<)

! C(+>"6\*4%""\*  
! D1\$1""9, 4.#3)'>"6\*4%""A""%3E

Ideas

\*+, %#"-. /, 0%(1+&2&)

! 89: #1; '-77434#\$3#2, #4<1  
! =">'?9, .- (+3%  
! ?92#\*\*2"(4#, .-2-%A-1

Ideas

3%4, .5, 67"#, .', #5&+47

! @#; ""2"(4341"  
! @#; "1">\*A'3\$43; '6#4%\*  
! B"\$6.4%) , .- (+3%\*

>%+4.#+%;; "<)

! : -%1""\*  
! I --.>#)\*  
! F, #2  
! F>#2, 41<A""%3E

Leads

?((, 0%0)

! 5&4\*&41<  
! F3#2'#1('7.#+(  
! G#\$>#. ""417"3%A-1  
! J", +%#%A-1#\$#%#3; \*

(, 0%0)

! K5C'-. 'K5G  
! G#1#<"2"1%7""

@+, :)

! J""\$\$41<%. #7743'L6.->\*"".'  
1-%4743#%A-1\*A', +\*&'#\$"".%\*A'  
."(4."3%\*M  
! : #(' , .- (+3%""\$\$41<  
! 5#4('"+6\*3.4, %A-1\*

0\*1%"#! 23.' #)\*#4' 514#3.15'

67'1(-%5#3.'\* #1%"#4' 514#1\*%-5.

# Scheme: the Health Day case

\$'' 1.9#8\*' 1()\*  
:83.(); '\*.<

= ' (>)\*?.9#7)4''' \*.  
:(\*1@@ '\*.<

A)%' (-B-%5#(+, '

! "#\$%&' %() \*+ #), (-) %./

! ((\*18(-)%#), (-) %./

! "#\$%&' %()

! Black Friday offer  
! ! "#\$%&' (#)'\*+, .-%  
! /-0".12"1%#\$3-2, "1\*#%A-1\*  
! 45&-1""6"7-. ""."\$"#\*"

\*+, %#"-. ,./, 0%(1+&2&)

! 89: #1; '-77434#\$3#2, #4<1  
! =">'?9, .- (+3%  
! ?92#\*\*2" (4#, .-2-%A-1

3%4, .5, 67"#, .', #5&+47

! @#; ""2" (4341"  
! @#; "1">\* 3\$43; '6#4%\*  
! B"\$6.4%) , .- (+3%\*

8' #+\$7#5&+9: .#+%;;"<)

! C(+&'>"6\*4%""  
! D1\$41""9, 4.#3)'>"6\*4%""A""%3E

=, (, -%#.#.(, 0%(#+%;;"<)

! /.-+, \*-1'F-34#\$G" (4#  
! C(0".%41<'1"%>-.; \*  
! H2#4\$\*""1 (9-+%A""%3E

>%+4.#+%;;"<)

! : -%1""\*  
! | --. >#)\*  
! F, #2  
! F>#2, 41<A""%3E

?((, 0%0)

! 5&4\*&41<  
! F3#2'#1 ('7.#+(  
! G#\$>#. ""417"3%A-1  
! J", +%#%A-1#\$#%#3; \*

(, 0%0)

! K5C'-. 'K5G  
! G#1#<"2"1%"7""

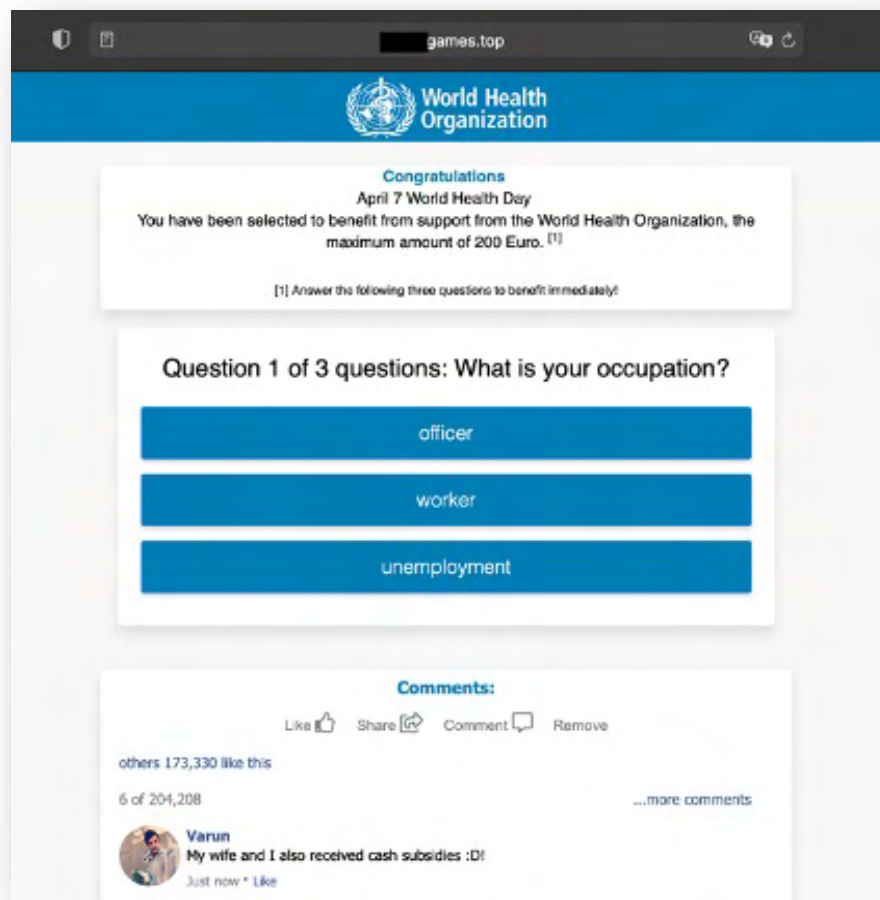
@+, :)

! J""\$41<%.#7743'L6.->\*".'  
1-%4743#%A-1\*A', +\*&'#\$".%\*A'  
." (4."3%M  
! : #(' , .- (+3%""\$41<  
! 5#4('\*+6\*3.4, %A-1\*

0\*1%"#! 23.' #) \*4' 514#3.15'

67'1(-%5#3.' \* #1%"#4' 514# 1\*%-5.

# The Health day



- Distributed network of **134** fraudulent websites
- Is aimed at **millions** of users worldwide
- Directing traffic to fraudulent sites

# Viral distribution of multistage scheme

World Health Organization

Western Union MoneyGram Mastercard VISA

World Health Organization:

After considering your answers, set the subsidy amount to 300 dollar and complete the steps to obtain the withdrawal code from the electronic counter

-You may get the subsidy with only one step, please click the "Invite Friends/Group" button to share the subsidy information with 5 groups or 15 friends on WhatsApp

Invite friends/groups

-After sending the invitation, click the "Get withdrawal code" button:

Get withdrawal code

Note: If you do not complete this step correctly, you will not get help.

Personalised content based on:

- Geolocation
- User agent
- Language settings

The language and currency of the reward varies depending on the location of the user

Всемирная организация здравоохранения

Western Union MoneyGram Mastercard VISA

Всемирная организация здравоохранения:

Обдумав свои ответы, установите размер субсидии на 3000 рублей и выполните действия, чтобы получить код вывода с электронного счетчика.

-Вы можете получить субсидию всего за один шаг, нажмите кнопку «Пригласить друзей / группу», чтобы поделиться информацией о субсидии с 5 группами или 10 друзьями в WhatsApp.

Пригласите друзей / группы

-После отправки приглашения нажмите кнопку «Получить код вывода»:

Получить код вывода

Примечание. Если вы не выполните этот шаг правильно, вам не помогут.

комментарий пользователя:

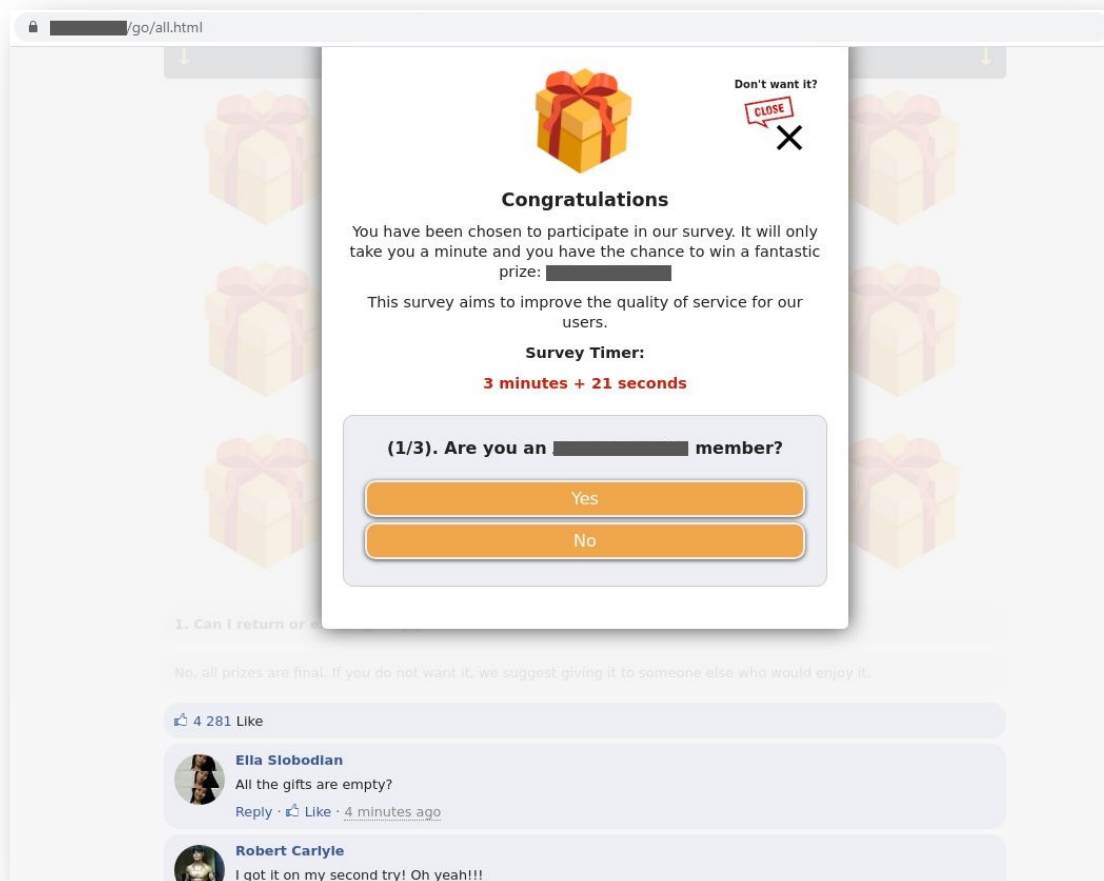
Like Share Comment Remove

others 204,208 like this

63 of 173,330 ...more comments

Варуи  
Мы с женой тоже получили денежную субсидию: Д!

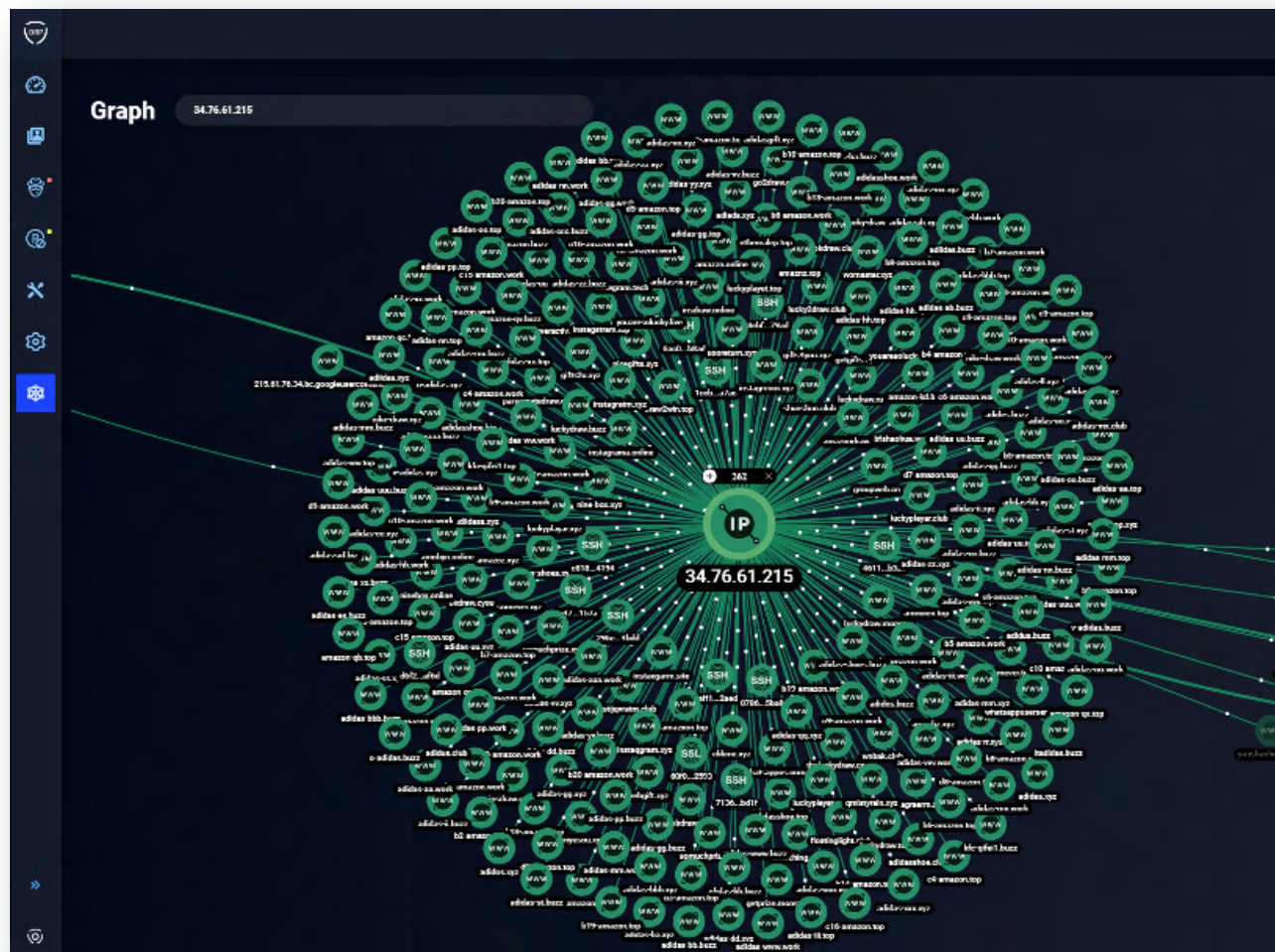
# Viral distribution of the multistage scheme



Further redirect:

- Fake giveaways
- Luring to a plug-in site
- Installations of a browser extension
- Ending up on a malware or phishing site.

# Sophisticated & distributed scam infrastructure



**134** domains were a part of a larger fraudulent network.

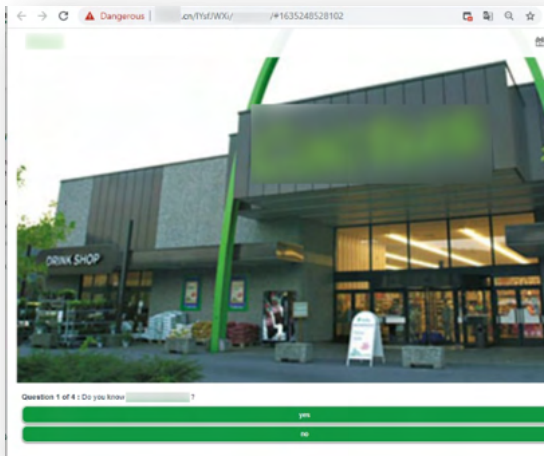
Around **200 000** people per day were attracted. Within a week, they were visited by **1.4 million** potential victims.

Often complicate the detection by using CDN services.

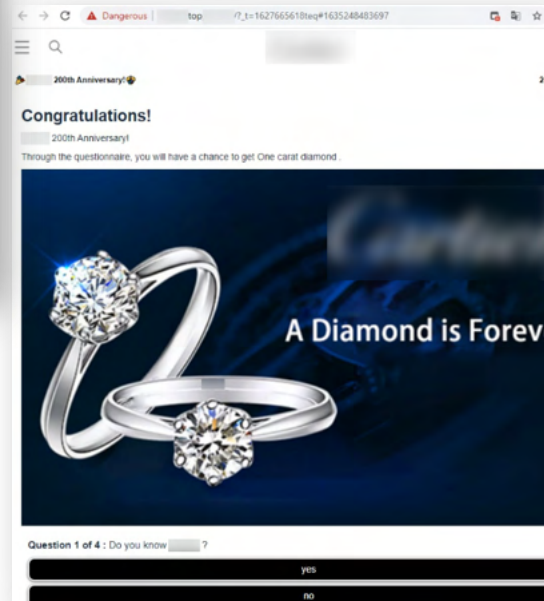
**134** rogue websites impersonating popular brands and organisations



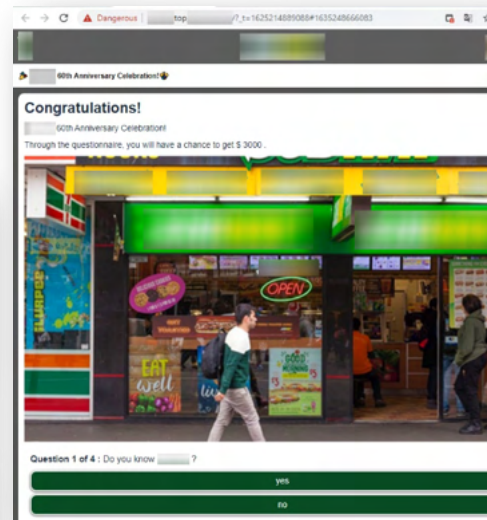
# Worldwide distribution



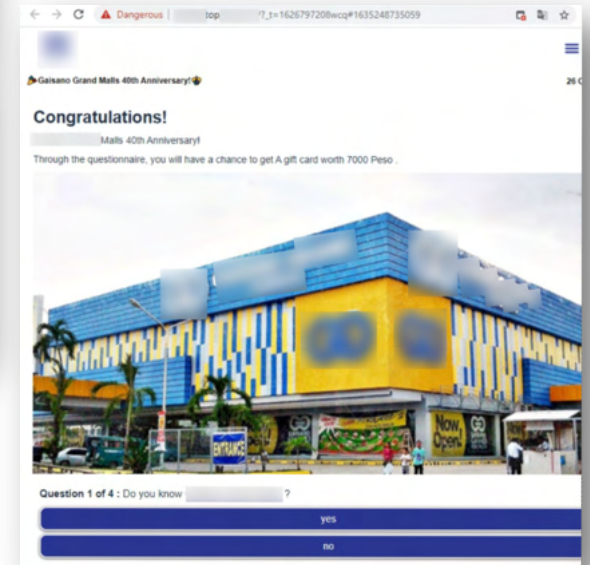
Luxemburg



France



USA

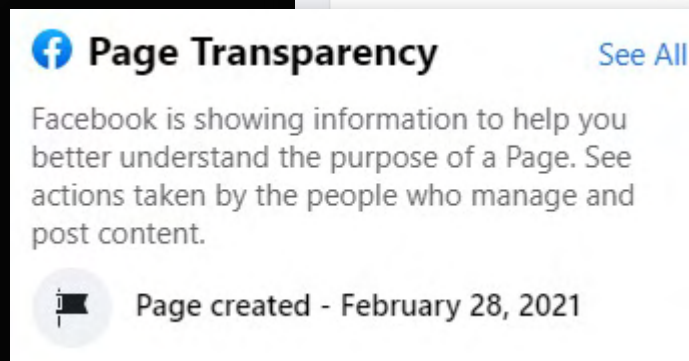
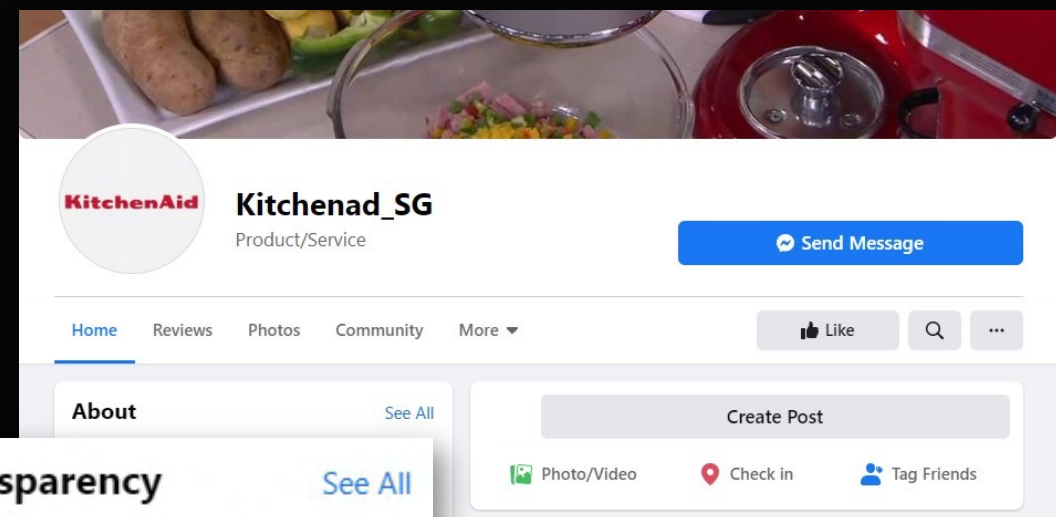


Philippines

# Signs of the attack

- Newly created accounts with branded userpics and a few posts
- Accounts with mistypes in the name
- Consonant domain names
- Reports on similar activity in the industry
- Social media tweets and posts

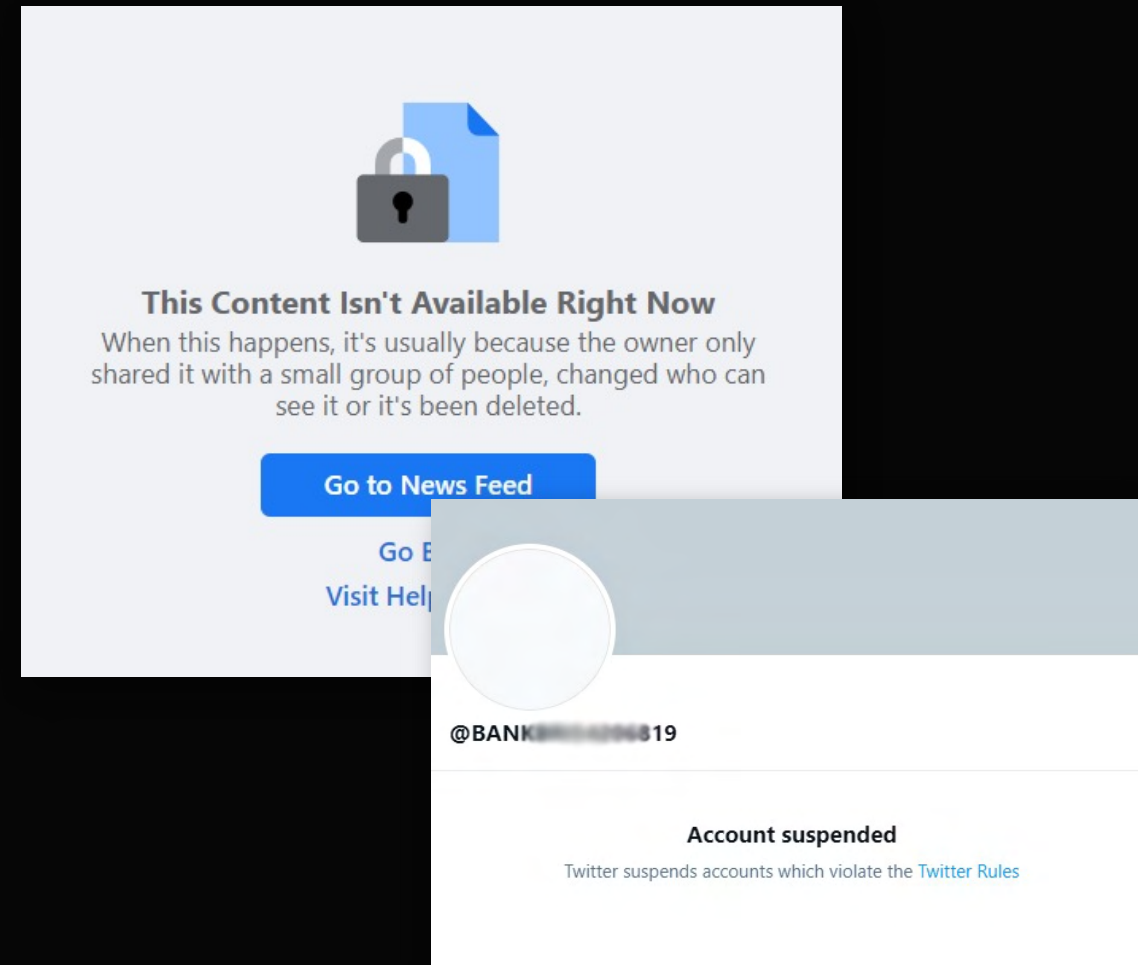
Recommendation:  
try to understand the attack fully





# Response

- Only social media administration can block it
- Violation can be not active anymore
- Better to have registered trademark
- Visibility of the full scheme helps a lot in response
- The proper approach is constant monitoring and response to prevent



# Key thoughts

- Monitoring landscape should be constantly being expanded
- Build the customer working reporting process
- Scammers are evolving and growing
- Industry is growing very fast
- If the brand is global – attack will be global too
- Sophisticated attacks stay below the radar
- Partial visibility can solve only the part of the problem





# Preventing and investigating cybercrime since 2003



**Dmitriy Tiunkin**

Head of Digital Risk Protection, Europe

tunkin@group-ib.com

[www.group-ib.com](http://www.group-ib.com)

[group-ib.com/blog](http://group-ib.com/blog)

[info@group-ib.com](mailto:info@group-ib.com)

+65 3159 3798

[twitter.com/groupib](https://twitter.com/groupib)

[facebook.com/groupib](https://facebook.com/groupib)

[t.me/group\\_ib](https://t.me/group_ib)

[instagram.com/group\\_ib](https://instagram.com/group_ib)