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

1000+

successful investigations worldwide, including 150+ high-profile cases

$300 mln

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

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)

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

CYBER SECURITY EXCELLENCE AWARDS WINNER 2021

FROST & SULLIVAN

Media coverage:

Bloomberg

InformationWeek DARKReading

Forbes

Esquire

SC MAGAZINE

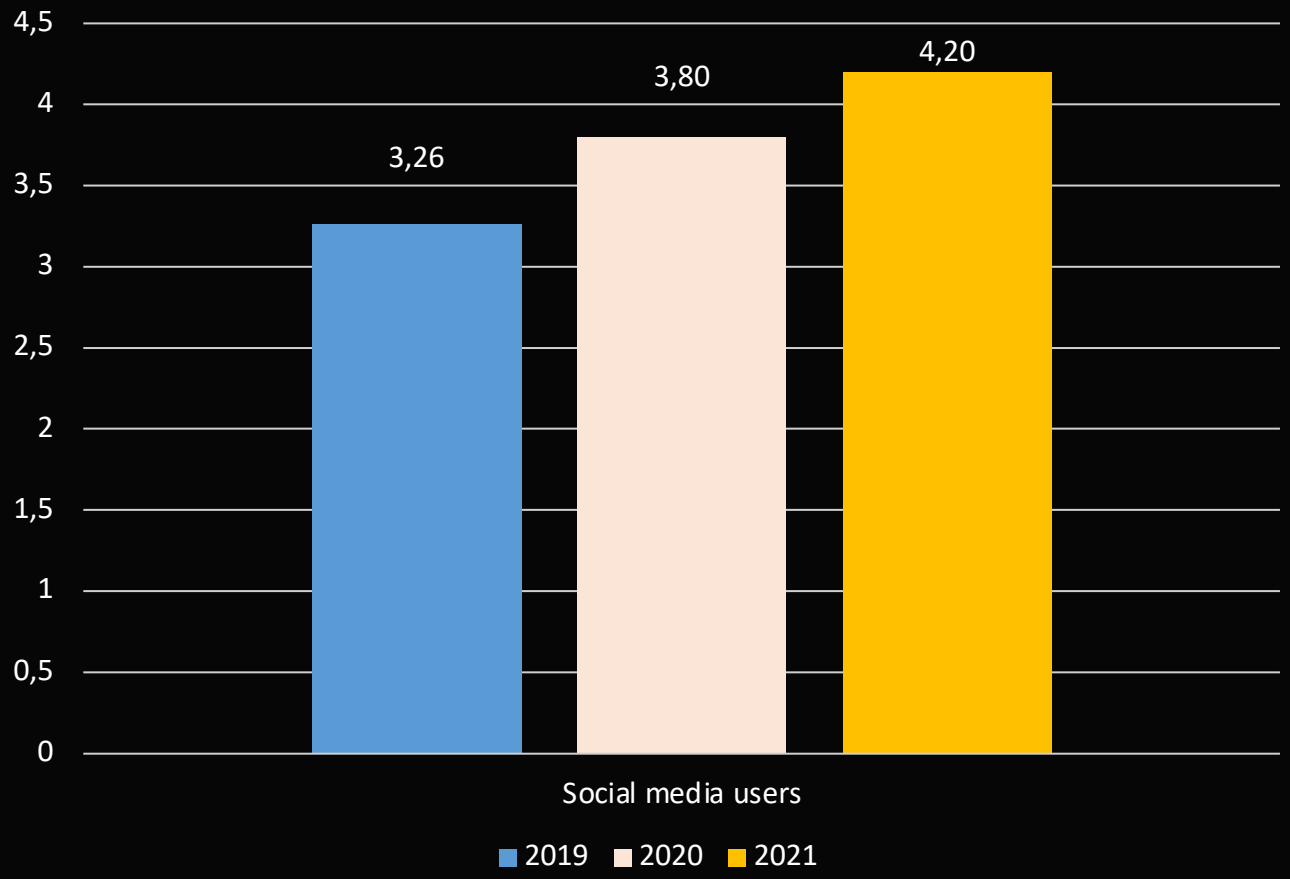
The Register

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»

Scam ads in social media

History of scam

Emails

Sites

Traffic attraction
SEO, Advertisement

Mobile

Mobile applications

2010

2021

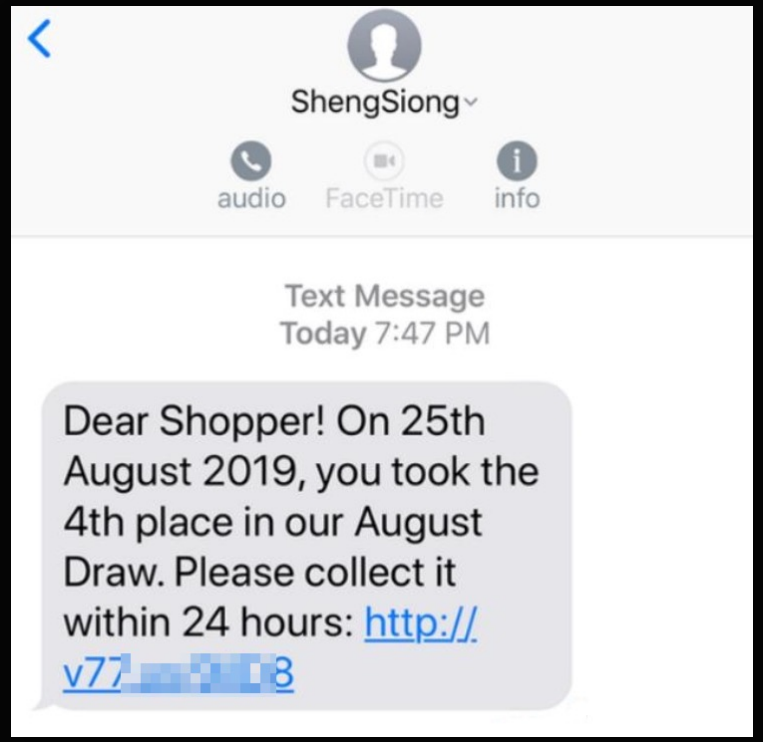
5% web traffic mobile users

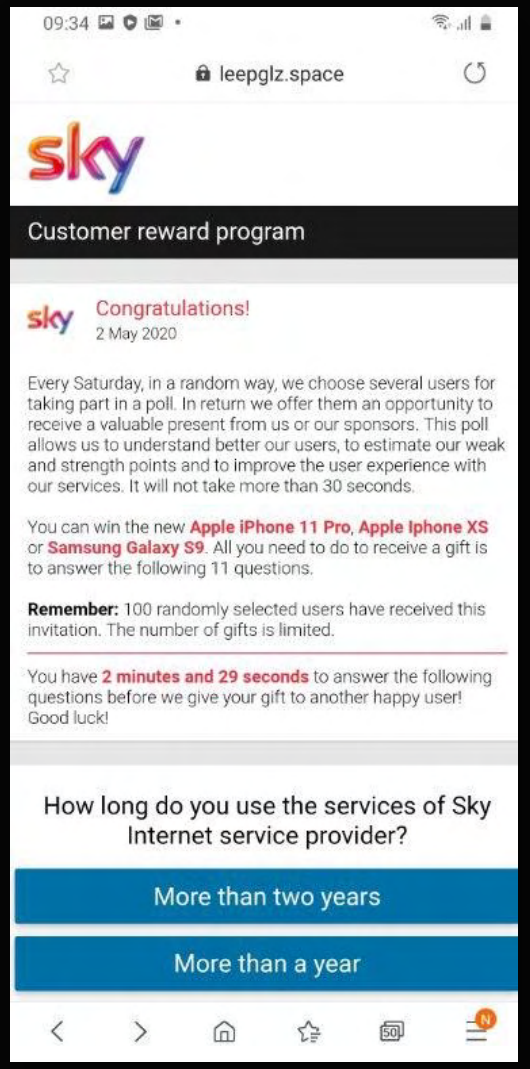
56% web traffic mobile users

Only 8% of users time

Benefits of mobile targeting

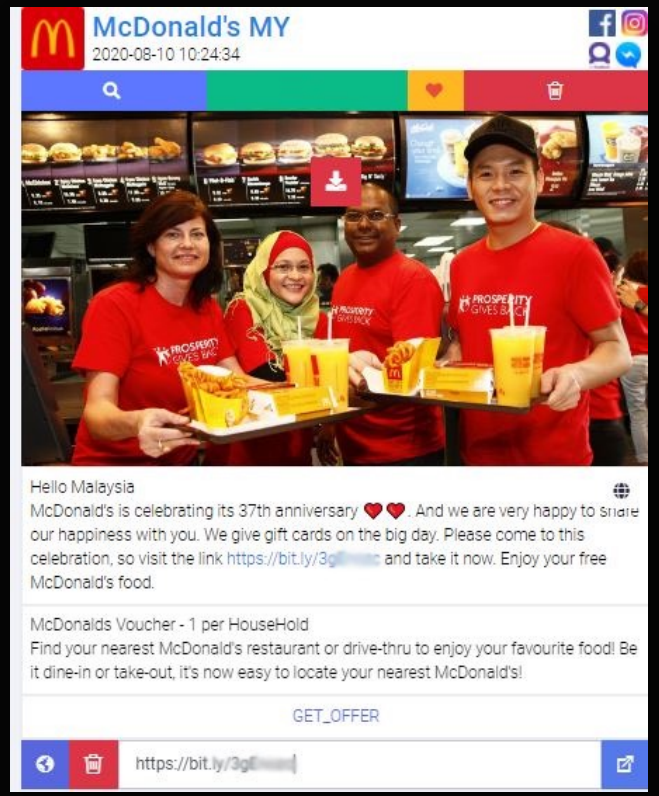
- Personal
- More targeted
- Fast decision
- Hard to verify





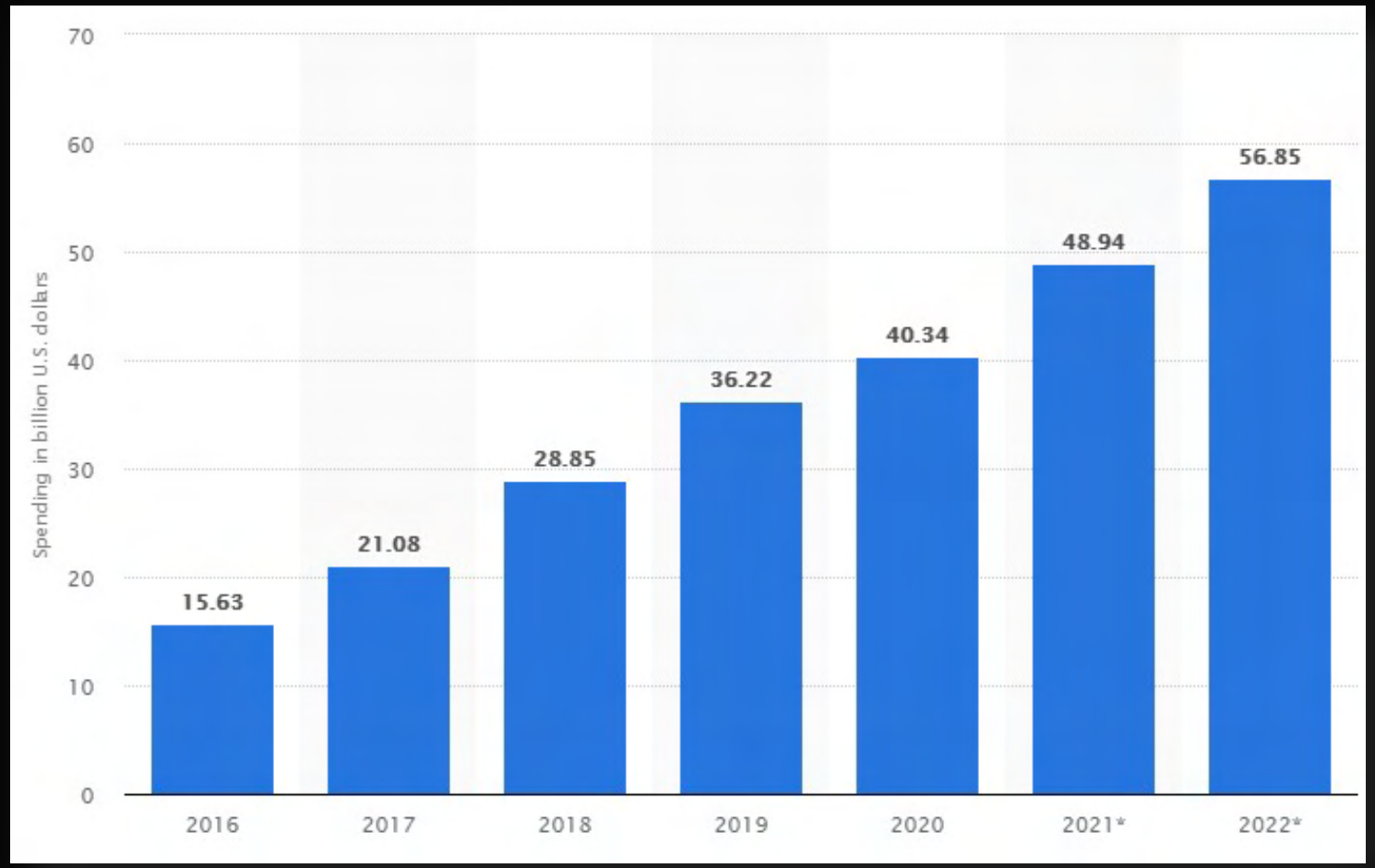
Benefits of social networks

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



Damage

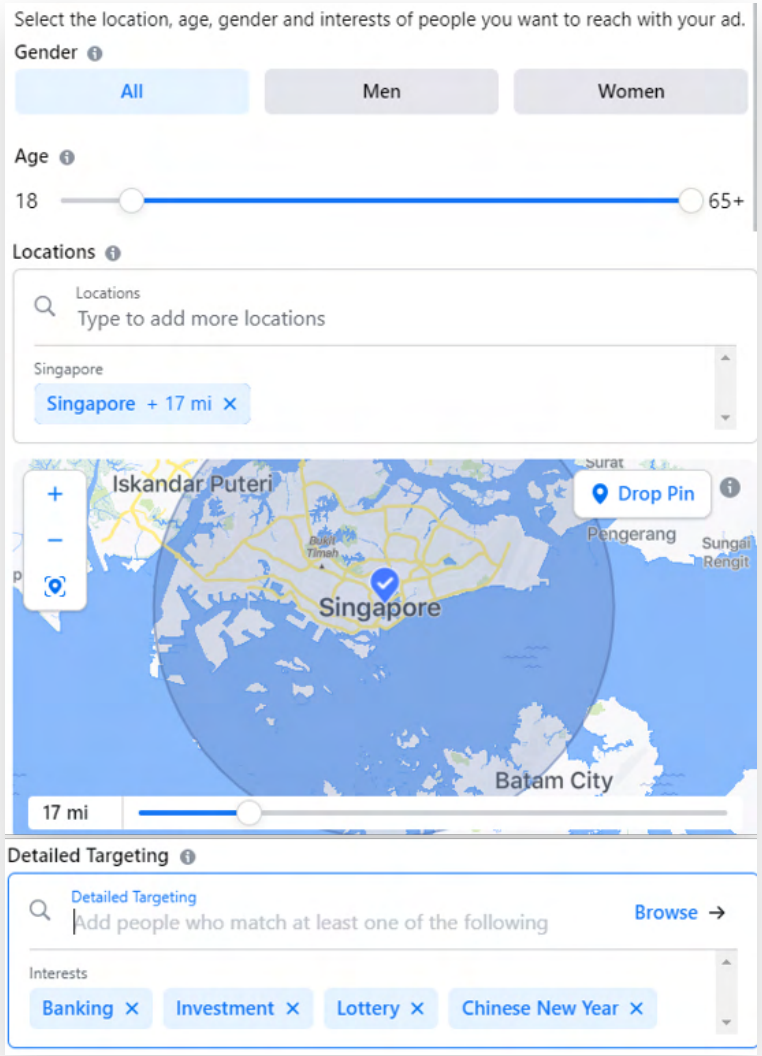
- Distrust to the brand
- Inflation of the ad price
- Wrong customer journey

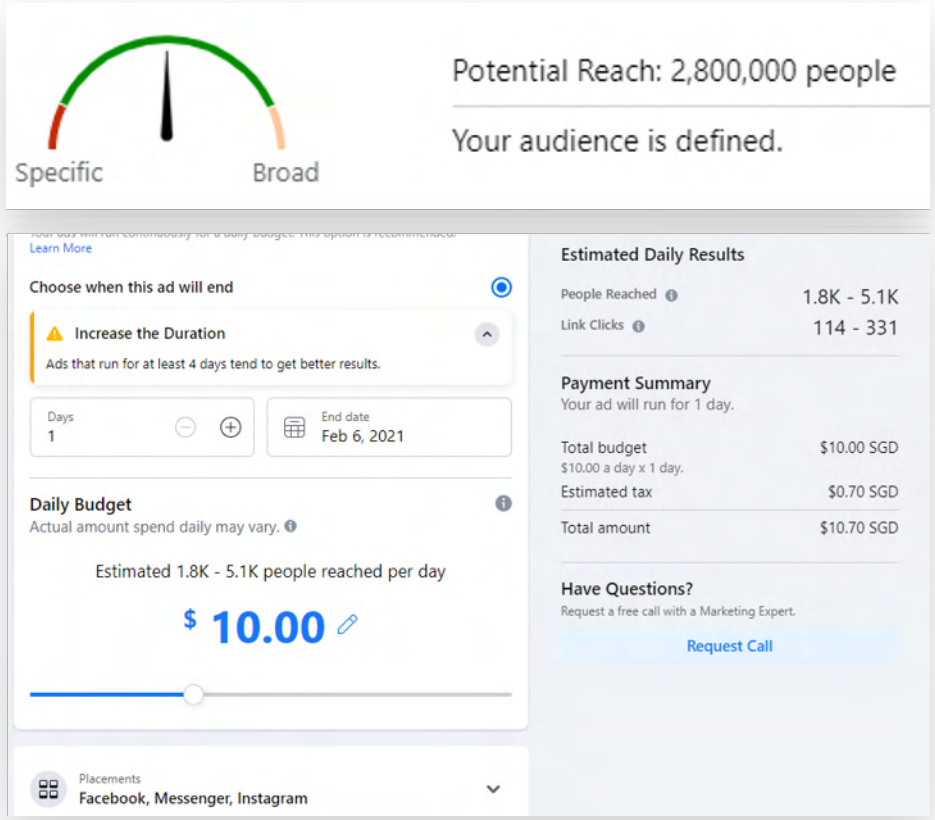


Social network advertising spending in the United States from 2016 to 2022 (in billion U.S. dollars)

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

Targeting





$1
for 500 views

5%
conversion

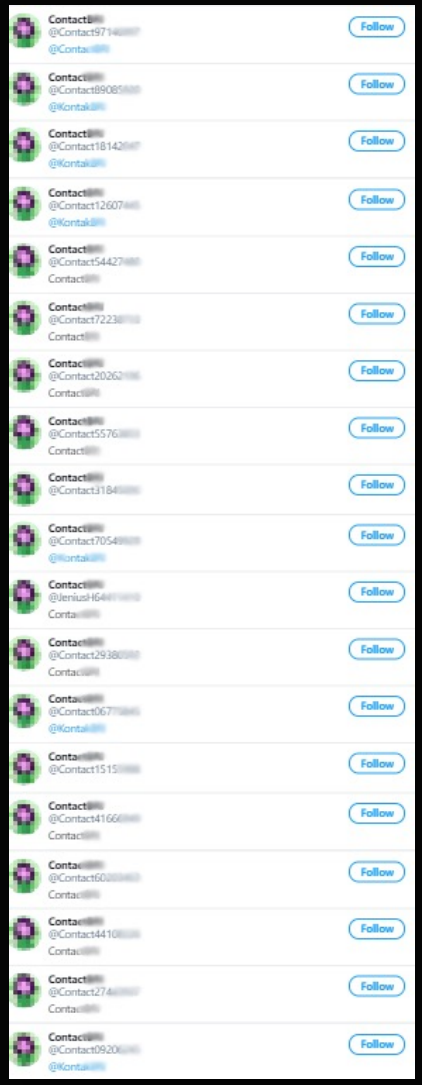
$0.04
per click

$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

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.

https://www.ftc.gov/news-events/blogs/data-spotlight/2020/10/scams-starting-social-media-proliferate-early-2020

GROUP-IB

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.

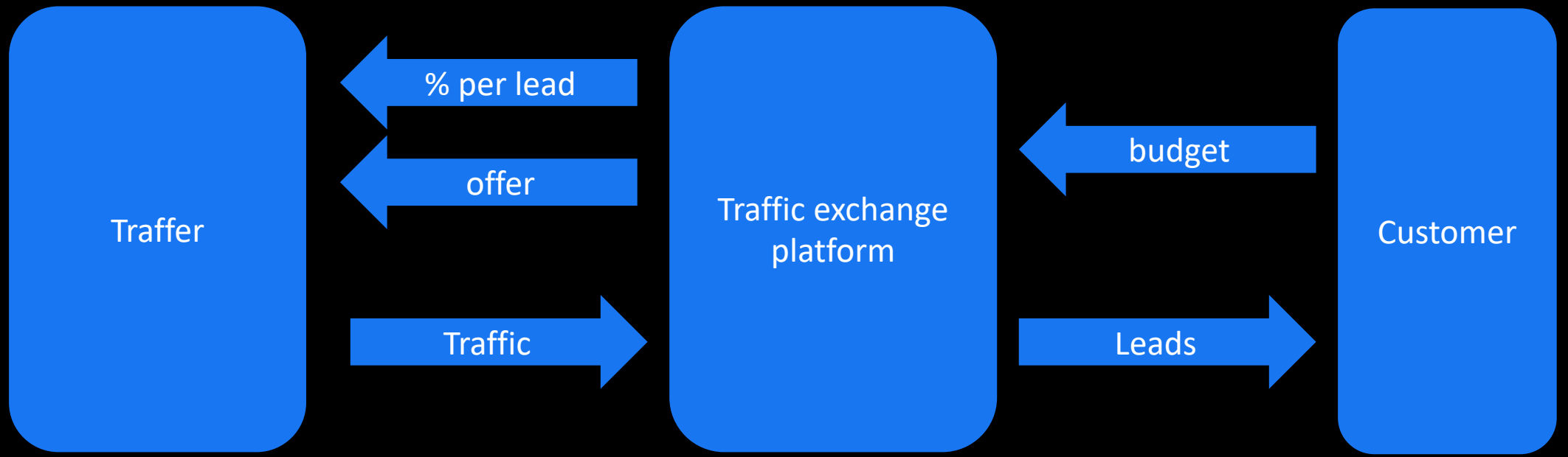
In the weeks leading up to voting day, Facebook moved some of its ad monitors off their usual tasks to **focus on helping political advertisers buy as much inventory as they wanted**

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

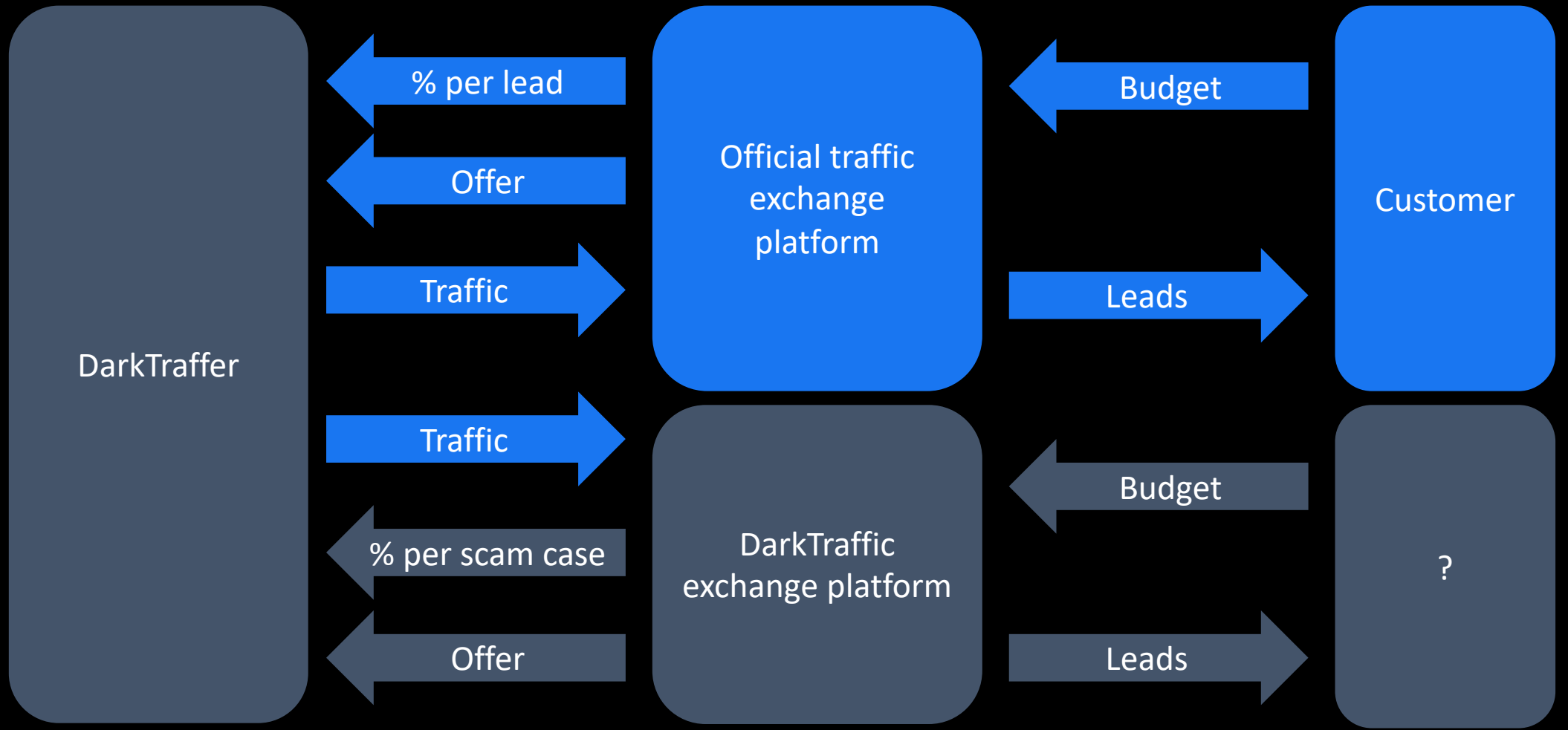
https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scams-revenue-china-tiktok-vietnam

DarkPath scammers

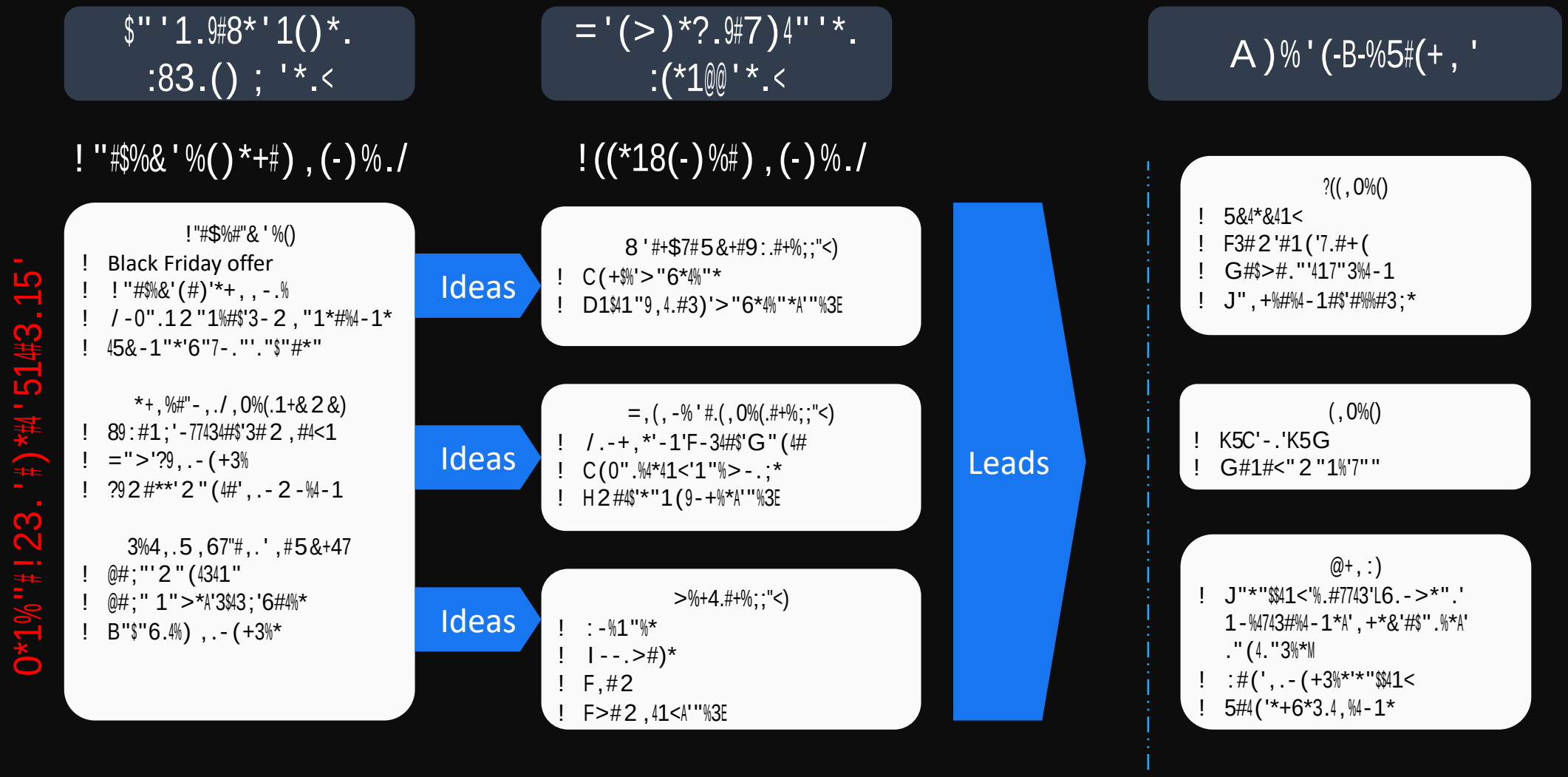
Expectation



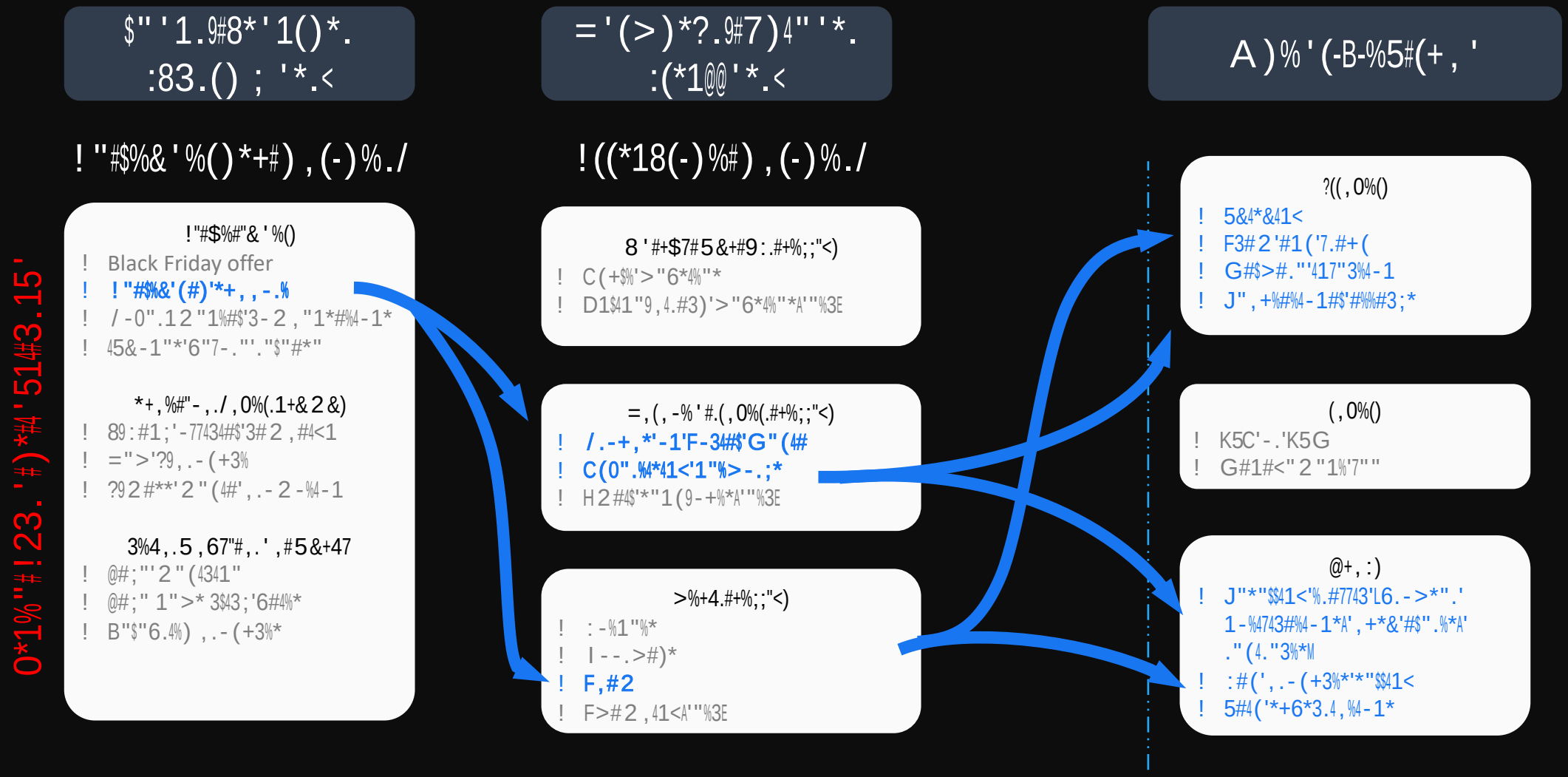
Reality


DarkTraffer
% per lead
Offer
Traffic
Traffic
% per scam case
Offer
Official traffic exchange platform
DarkTraffic exchange platform
Budget
Leads
Budget
Leads
Customer
?

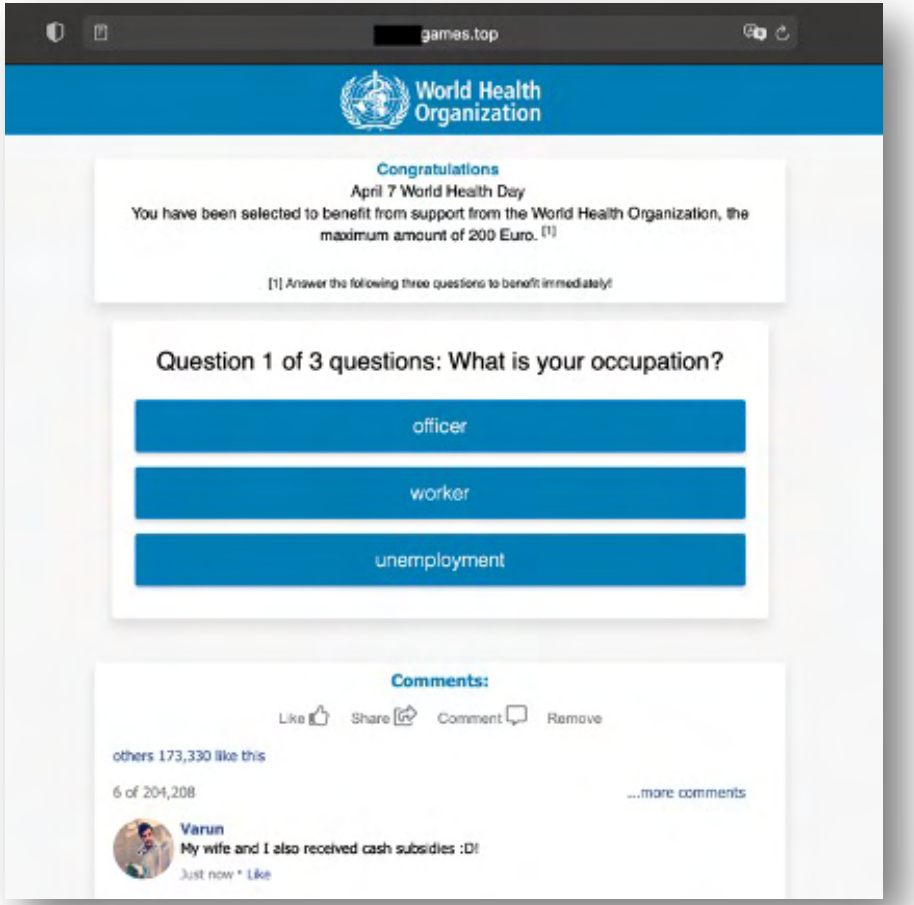
Traffers' business example



Scheme: the Health Day case

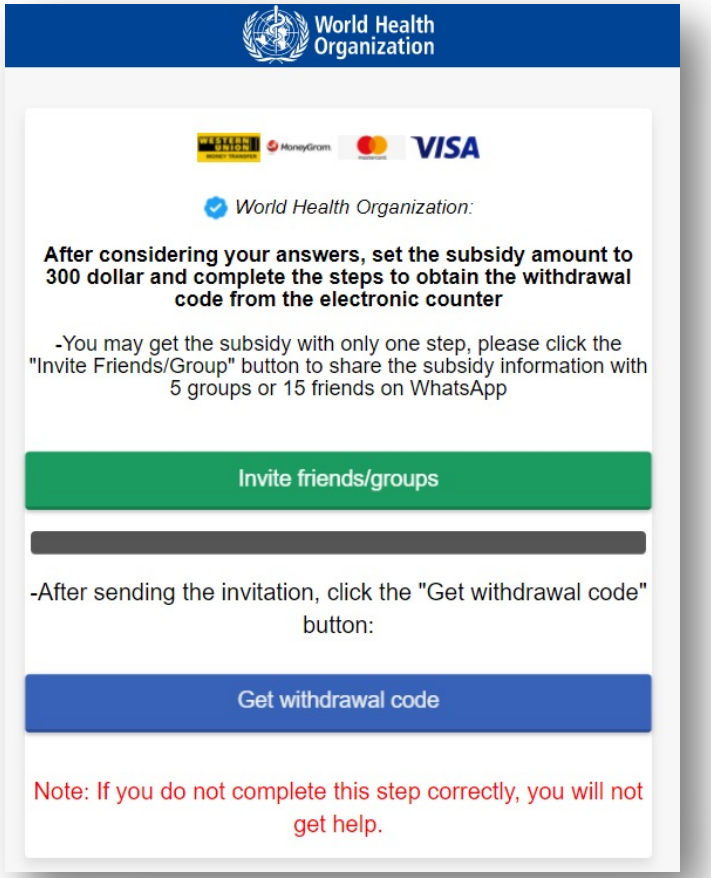


The Health day



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

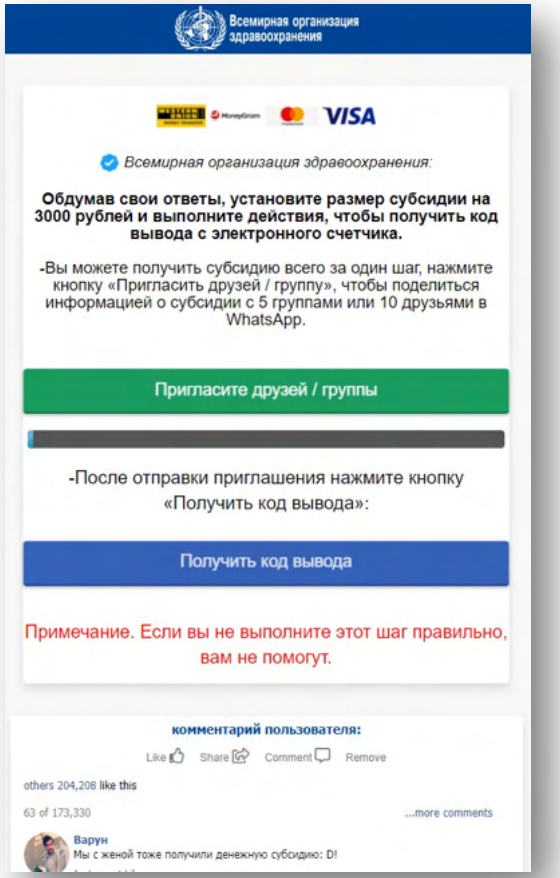
Viral distribution of multistage scheme



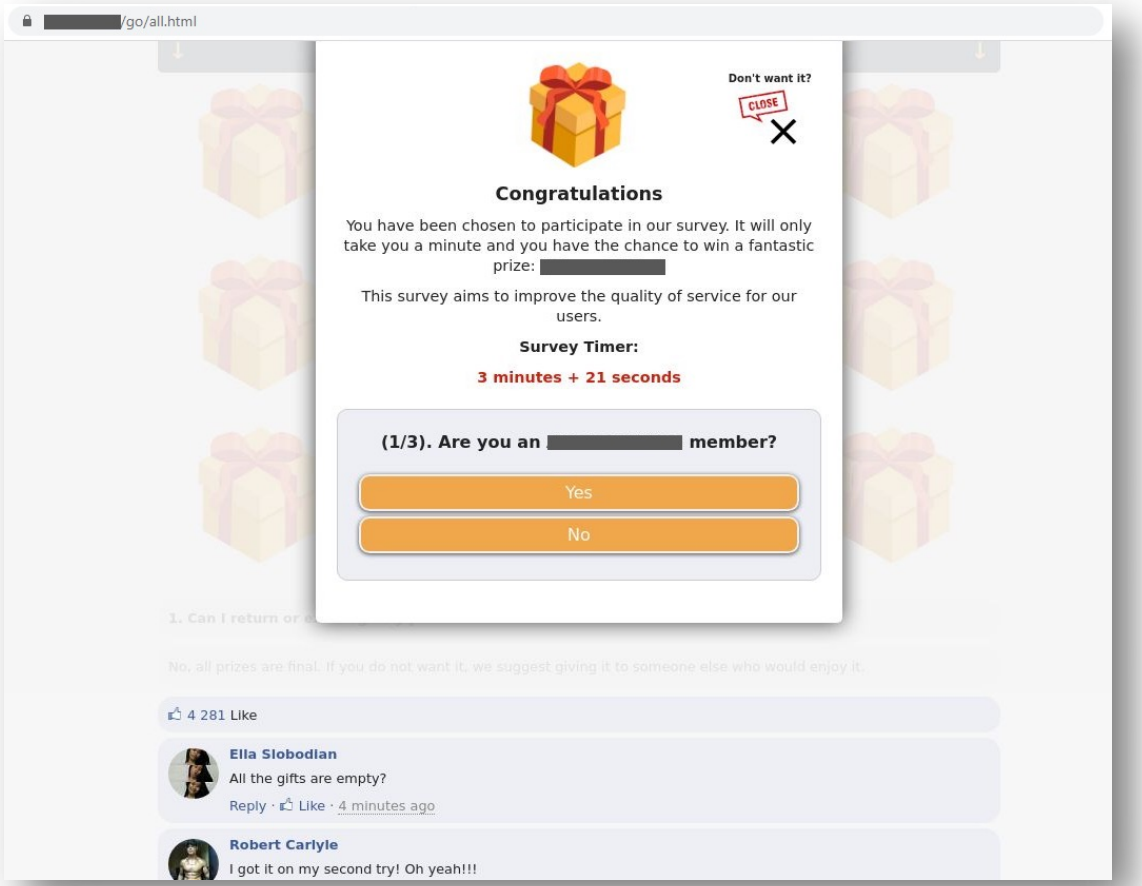
Personalised content based on:

- Geolocation
- User agent
- Language settings

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



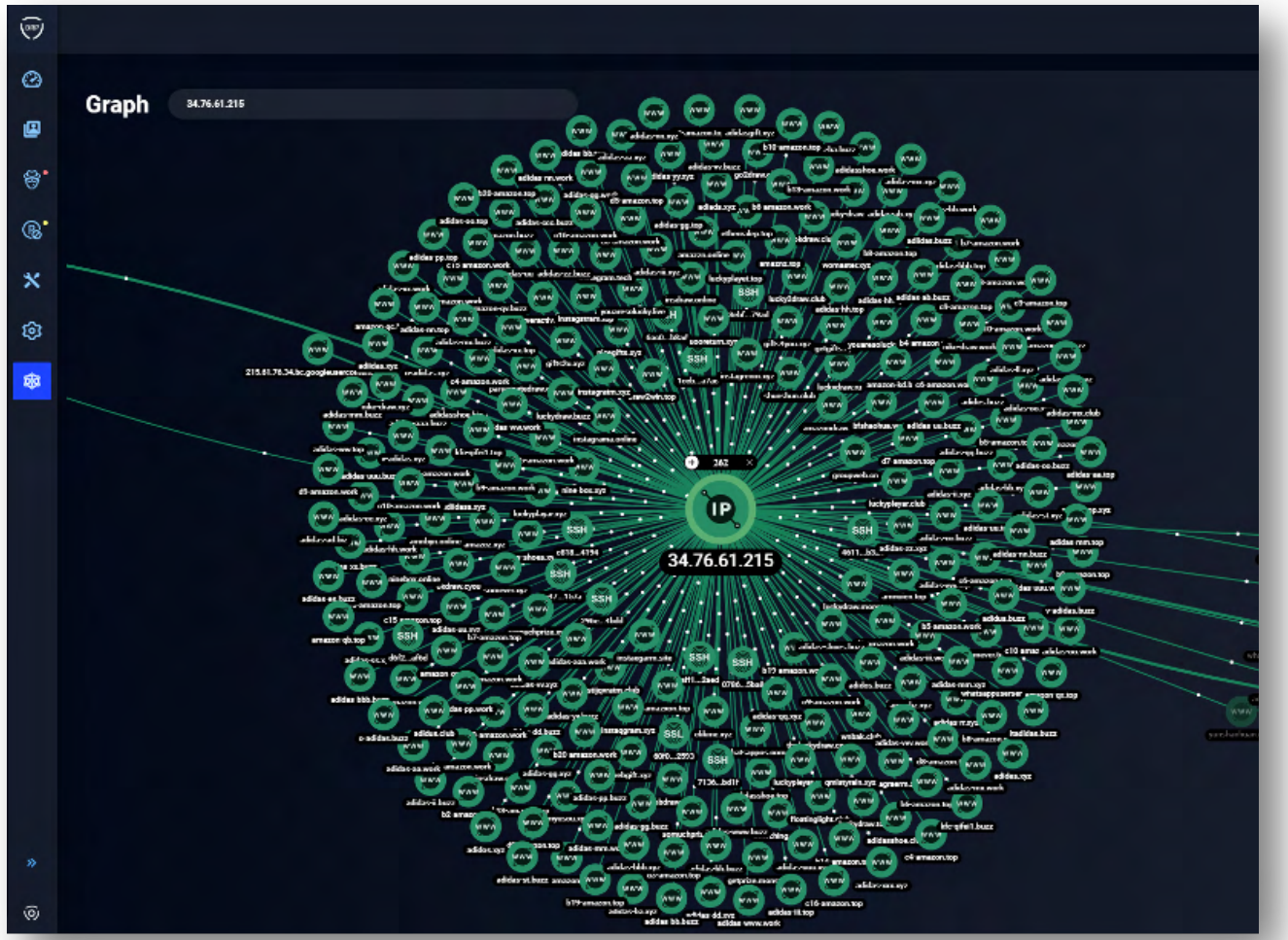
Viral distribution of the multistage scheme



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



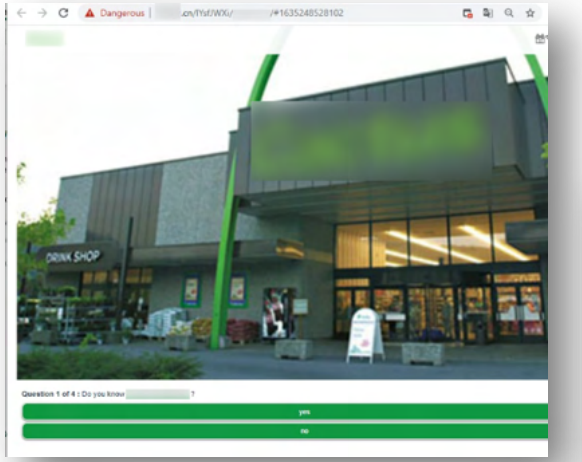
134 rogue websites impersonating popular brands and organisations

134 domains were a part of a larger fraudulent network.

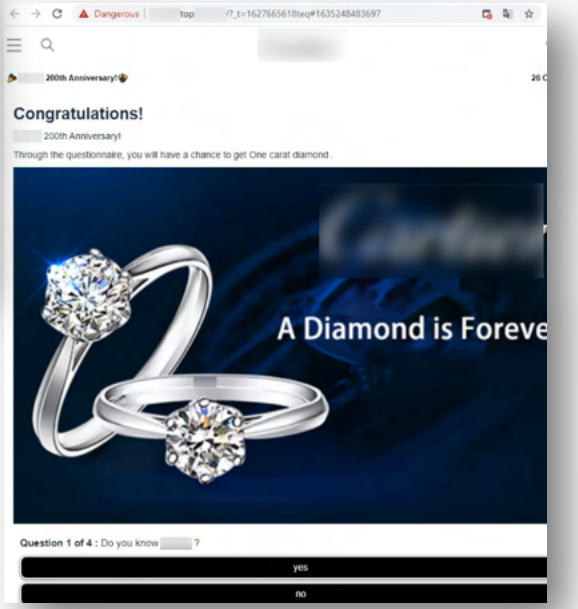
Around **200 000** people per day were attracted. Within a week, they were visited by **1.4 million** potential victims.

Often complicate the detection by using CDN services.

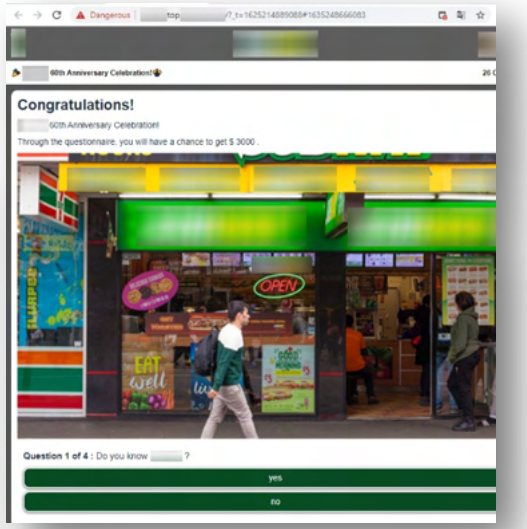
Worldwide distribution



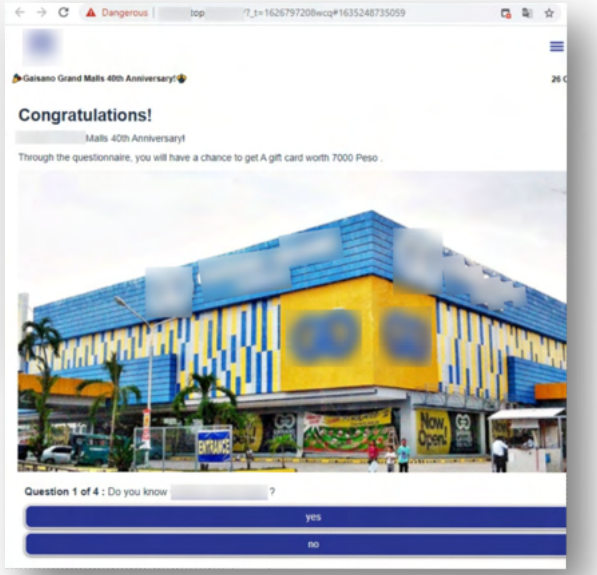
Luxemburg



France



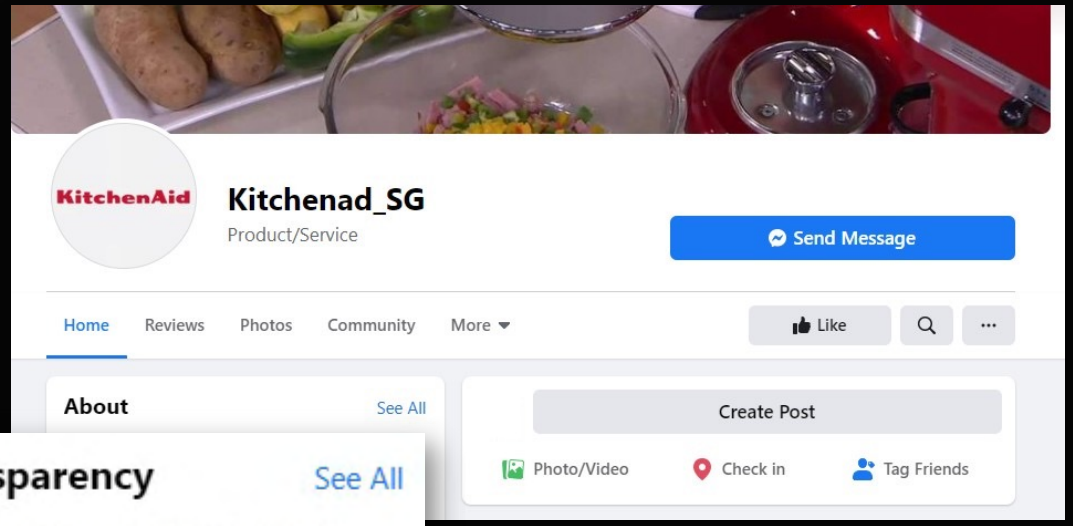
USA

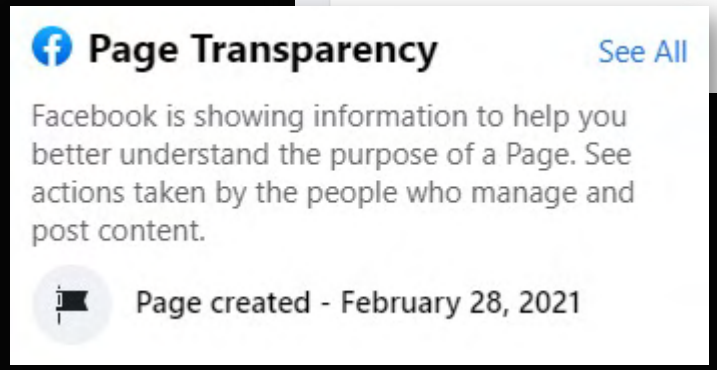


Philippines

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

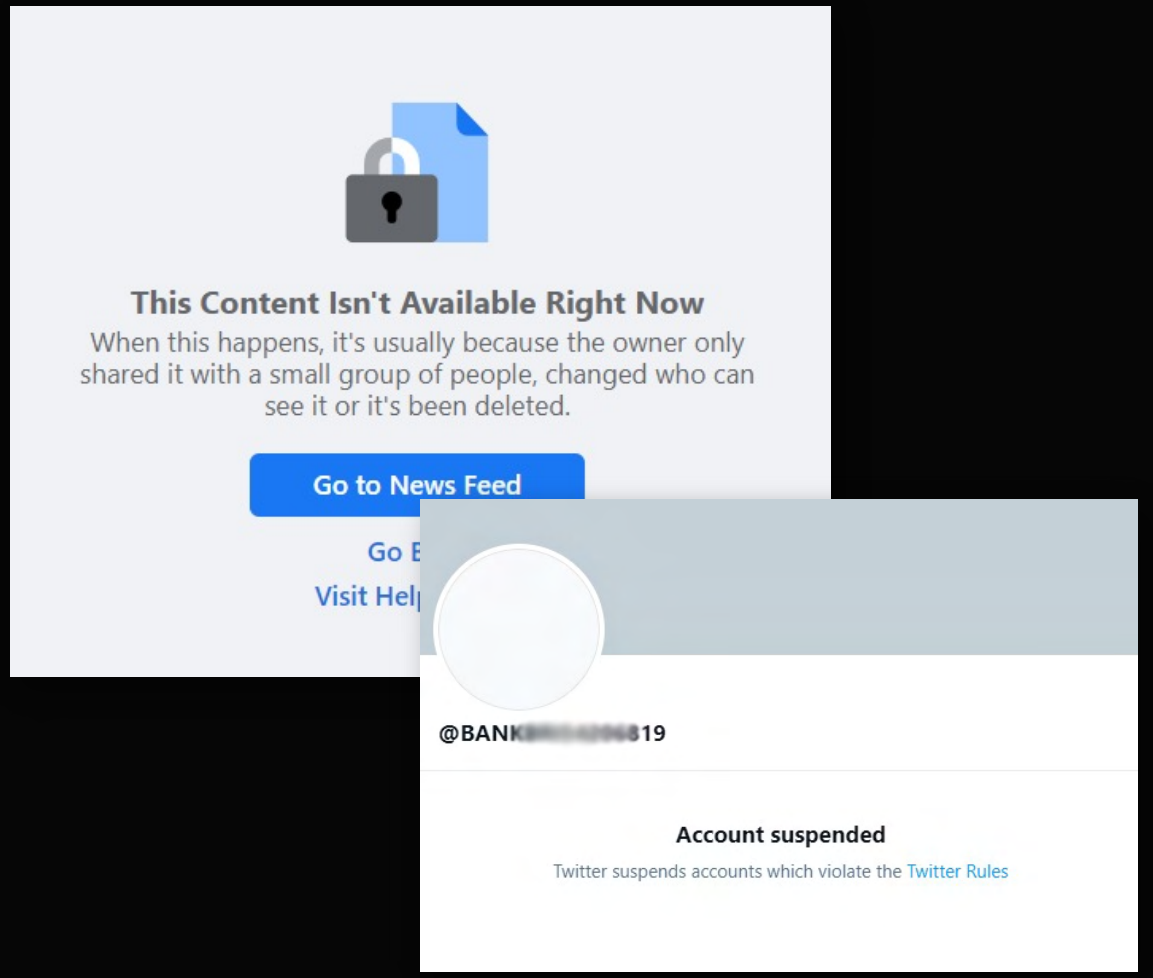




Recommendation:
try to understand the attack fully

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