GROUP-IB

THREAT REPORT

DIGITAL RISK TRENDS 2023

GROUP-IB.COM

00 ↗

TABLE OF CONTENTS

01 ↗

KEY FINDINGS

1. Fraudulent resources mimicking legal brands increased by **304%** in 2022.
2. The number of phishing sites created by scammers in 2022 rose **62%** compared to the previous year.
3. Financial institutions were the most targeted organizations in 2022, accounting for **74%** of fraud and **24%** of phishing attacks.
4. Scammers show the highest interest in brands from the APAC and MEA regions, with a **211%** and **135%** surge in fraudulent resources, respectively.
5. Automation has significantly contributed to the growth of scams, reducing the time spent on preparation and scamming a victim to **10 minutes**.
6. Large-sale scam campaigns have become as cybercriminals turn to scale to make their schemes more viable. If a scam campaign has more resources, it's harder to take down.
7. Scammers are getting more involved in other cybercrimes, such as malware distribution.
8. Adversaries moved from fake account creation to hijacking verified accounts.

02 ↗ FORECASTS

1. The number of branded fraudulent attacks across the globe will continue to grow. Scam schemes will begin to extend to less popular brands. In addition, threat actors will look to new markets, where users are less informed about scam and phishing techniques.

2. New attack vectors that leverage Telegram will appear. Cybercriminal groups, which have built their ecosystems inside popular messengers (chats, channels, bots), have significantly shaped the current landscape. The number of people participating in scam activity is growing considerably, as are the number of attacks. Therefore, more people will look for new ways to make money using Telegram.

3. The growing popularity of affiliate programs is attracting a new generation of cybercriminals. The division of duties among fraudsters in the Phishing-as-a-Service and Scam-as-a-Service partner models has been effective and profitable for cybercriminal gangs, and the trend towards this format of organization will continue. The pool of participants will increase as a result of the lucrative potential rewards available in an industry where only limited or even no technical knowledge is now necessary.

4. Greater optimization of fraudulent campaigns with tools built on artificial intelligence technologies. For example, services like ChatGPT can be used to create authentic texts for social engineering or they can even write simple malware code.

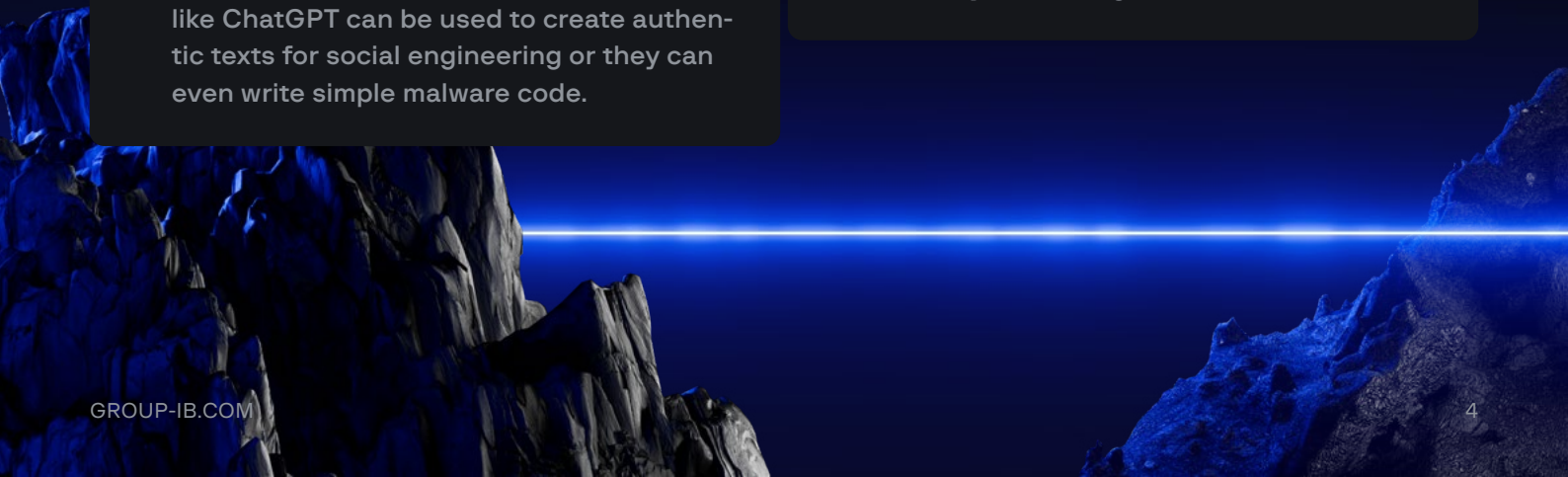
5. Increased use of automation within scamming attacks is expected. Attackers already use third-party or self-written scripts, bots, and software to scale their criminal schemes. Increased automation will lead to an increase in the number of fraudulent resources and victims.

6. Growing political and economic tensions will provide scammers with new opportunities in the digital space. Furthermore, old schemes can be adapted to the current information landscape.

7. Scammers actively exchange experience and knowledge, and Group-IB expects to see greater specialization within the industry. As a result, groups specializing in one type of violation will develop. Malware distributors, for example, follow the same principles to build their communities.

8. A large number of targeted and personalized attacks are expected. The number of data leaks is growing every year, giving fraudsters more targets to attack. Leaks of employees' personal information can lead to attacks on businesses.

9. Cryptocurrency will have an even more significant role in the cybercriminal world. This applies both to the increase in the number of attacks aimed at stealing cryptocurrency, and the greater use of this digital currency circulating between criminals.



INTRODUCTION

Figure 1. The Global State of Scams Report 2022

An epidemic of digital scams continues to grip the world. The most recent **Global State of Scams Report (Figure 1)** by Global Anti-Scam Alliance and ScamAdviser revealed that scams caused over **$55 billion** in damages in 2021, a **15.7%** increase compared to 2020.

The number of reported scams grew by **10.2%**, from **266 million** in 2020 to **293 million** in 2021. However, only between **3%** to **17%** of all such violations are brought to the authorities and law enforcement, depending on the country. According to the World Economic Forum only **0.05% of scams are prosecuted** which makes this type of crime a potentially low-risk option for cybercriminals.

According to Group-IB statistics, scams continue to be the most common form of cybercrime, outpacing phishing and other cyber threats, such as malware, ransomware, DDoS, etc.

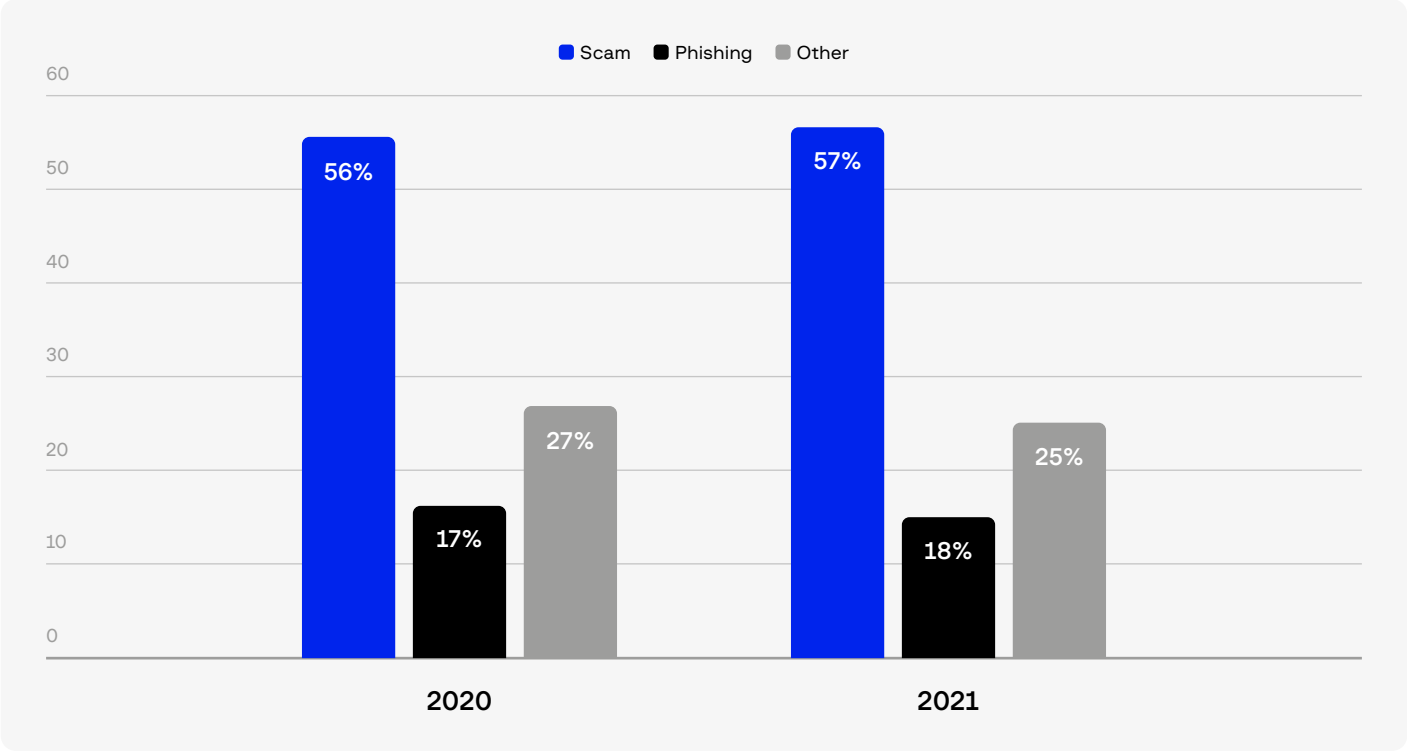


Figure 2. Share of scams and phishing in relation to other cyber threats[1]

In this report, we will reveal the main trends of 2022 in the fields of scams and phishing, and provide our forecasts for 2023. Our study focuses on Europe, the Middle East and Africa (MEA), and the Asia-Pacific region (APAC), as these are Group-IB's core markets.

Our findings are based on:

- statistics gleaned from providing **Digital Risk Protection** services to our clients
- data gathered as a result of anti-phishing activities
- information obtained from closed sources, including cybercriminal communities
- open-source intelligence

[1] Such as DDoS, malware, hacking, etc.

KEY TRENDS

The key trends observed in 2022 have set a precedent for cybercrime in 2023 and beyond. What we see uniting all of these trends is a shift in threat actors' tactics towards scale attacks and their supported operations to cause greater disruption and damage.

Figure 3. Demystifying Classiscam Report by Group-IB

1. Automation of crime

An increasingly broader ecosystem is being built around mass cybercrime, aimed at improving the safety of scammers through role distribution, as well as increasing the involvement of more people in criminal activities by simplifying processes.

A typical group of scammers includes software developers who build and maintain fraudulent websites and organizers who assemble and manage teams. Roles in each team are also distributed based on the tasks performed.

In the **Classiscam** scheme, scammers had to do almost everything manually at first, including finding a suitable ad, communicating with the victim, getting a phone number, etc. The only automated task was the creation of phishing pages with the assistance of Telegram bots. Now scammers gather information from various resources via parsers – the software that automatically collects suitable ads, finds the seller's phone number, and then, using the auto-link, sends them a WhatsApp message. The threat actor only needs to lure the victim onto the phishing site, arrange payment to an e-wallet through the bot, and receive money.

Ultimately, the automation of processes increased from 20% to 80% in the space of a few years. In the past, preparation and scamming a victim could take days. **Now scammers can manage the whole process in 10 minutes**.

Automation is also used to create phishing sites that impersonate banking companies. Group-IB discovered the **IBANKING V1.0** PHP script, which is used for the rapid deployment of a fake banking site. The script allows scammers to install fake banking systems in 5 minutes without any technical knowledge.

2. Expansion of the geography and coverage of schemes

As a rule, a scam scheme that achieved success in the region of its origin can often be exported successfully to other countries. In 2022, the conflict between Ukraine and Russia intensified such processes. Some cybercriminal community organizers and members relocated as a result of the conflict and brought their old tricks to new markets.

For example, the Classiscam scheme that originated from Eastern Europe has now spread across the globe. Group-IB has identified **1,366** scam groups in total and obtained detailed statistics on **393** of them. The observed groups have carried out a total of **486,081** attacks, emulating **251** brands from **79** countries. The total damage caused by this scam is estimated to amount to **$64,549,215**. The number of individuals believed to be involved in scam activity reached **38,000**.

3. Developing countries are under attack

Although cybercrime is rising in all regions, scammers' interest in brands from developing countries has grown rapidly. The average number of scam resources per brand in APAC in 2022 increased by an astronomical **211%** compared to 2021.[2] MEA takes second place with a surge of **135%**[3] followed by Europe **(+74%)**.[4]

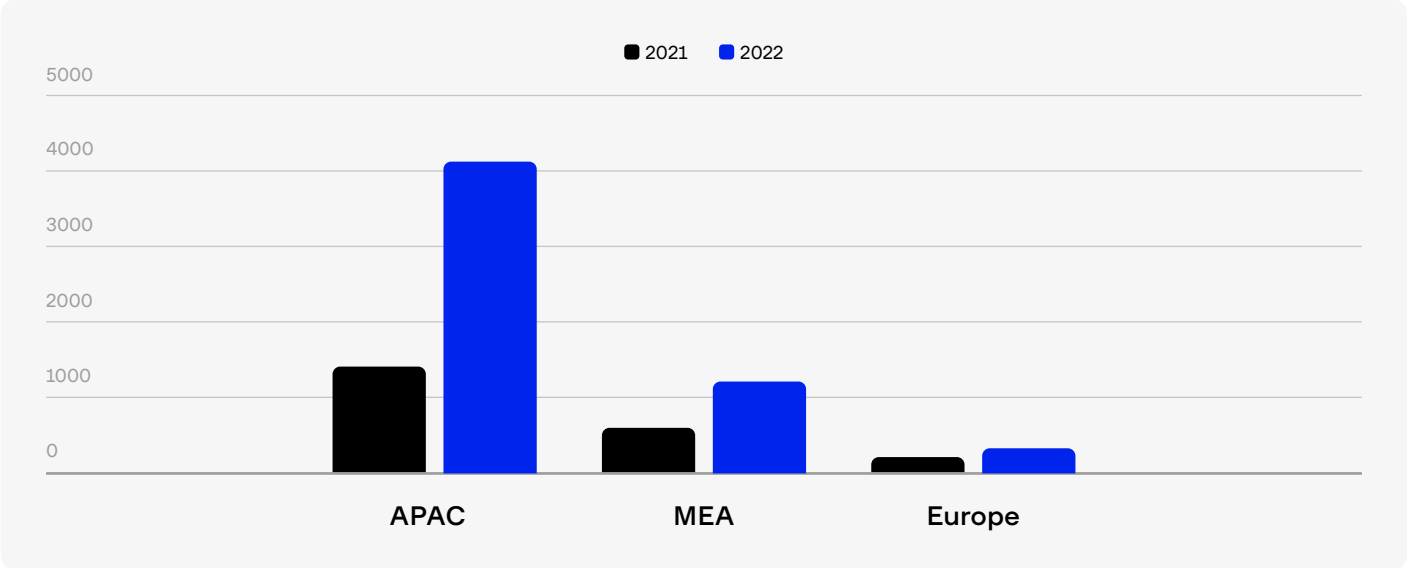


Figure 4. Number of scam resources by region

[2] Accounting for following economic sectors: Financial Institutions, banks, telecommunications and media, oil and gas, aviation, insurance, manufacturing.

[3] Accounting for following economic sectors: Oil and gas, financial institutions, banks.

[4] Accounting for following economic sectors: Financial institutions, banks,video games, real estate, manufacturing, healthcare, transport and logistics, aviation.

The major growth in scam activity is driven by a significant increase in the number of fake accounts created by scammers on social networks. In the MEA and APAC regions over the past year, social networks accounted for **92%** and **76%** of all types of scam sources. In Europe, messengers were used in scam schemes more often (**48%** of all scams).

The simplicity of social media scams led to the growing popularity of this method in the MEA and APAC regions. Such scams negate the need for technical skills, investments in infrastructure, or the purchase of phishing and scam kits.

Despite having less scam resources per brand than APAC and MEA, Europe continues to be affected by scam attacks. Group-IB analysts assert that the low base effect can explain the slower growth of scams in this region. Europe already has a well-established cybercrime community heavily influenced by professional criminal organizations.

4. Involvement of scam communities in other cybercrimes

The scam community has built a solid and effective pattern of interaction that has now extended to other types of cybercrime, in particular, malware distribution. For example, Group-IB researchers discovered that as many as **34 Russian-speaking** cybercriminal groups were distributing information stealers (find out more **here**) – malicious software that collects account credentials and payment information from the browsers of infected computers and sends it to the operator.

5. Massive scam campaigns

Scam campaigns are not only having a greater quantitative impact when it comes to the number of brands they are targeting. Schemes are now more complex, and more convincing to prospective victims. In order to evade counteraction, ensure the viability of the scheme, and introduce scale, scammers are now using a huge number of domains and social media accounts.

Over the past year, Group-IB researchers uncovered multiple major scam campaigns, including:

- **FIFA World Cup 2022 campaign**, which involved more than **16,000** fake sites that included fake surveys, tickets, merchandise, and jobs both ahead of and during the world's largest football tournament.
- **Multi-brand surveys campaign**. This technique using fraudulent survey sites has been around for more than five years but has recently surged in popularity. In 2022, Group-IB experts identified over **120,000** domains hosting survey templates for over **1,973** brands from **176** countries.
- **Delivery scam**. Group-IB experts detected a phishing campaign that involved over **270** domains impersonating postal brands from the MEA region since September 2020. Globally, scammers have mimicked over **30** brands of national postage services and relevant organizations from over **20** countries worldwide to target their victims.
- **Airlines campaign**. Scammers use fake websites, phone numbers, and call centers to impersonate the customer service departments of various airlines. Group-IB believes that the campaign may have started in 2014, as the oldest active websites date from that year. The campaign includes **30** fraudulent sites that were visited approximately **120,000** times per month. In total, the campaign affected customers of 73 airlines from all over the world. According to our calculations, the estimated damage from this attack is **€1.8 billion ($2.0 billion)**.

- **HR scam campaign**. Group-IB detected at least two large-scale campaigns targeting users looking for work. The first scheme was discovered in the MEA region. It involved more than **2,400** newly created Facebook pages that appropriated the brand identities of well-known companies in **13** countries to promote fake vacancies on their behalf. The second scheme targets unemployed applicants, especially from Vietnam, Thailand, Italy, Spain, and the USA who are pursuing a career with cruise liners. The fraudsters spread job descriptions on Facebook, Instagram, Twitter, and free user-generated content (UGC) platforms, such as Blogspot.
- **Vietnamese phishing campaign**, which affected **27** highly reputed banks and financial institutions. Fraudsters use an OTP hijacking scheme, as well as customized and targeted communication tactics. The campaign was launched back in 2019 but is still active. This scheme has affected, according to Group-IB's estimates, at least **7,800** people.
- **Manpower agency scam campaign**. This campaign mimics pages of a leading workforce agency in Saudi Arabia, targeting individuals looking to procure services of a domestic worker, to steal users' credentials for banks and online governmental service portals. The scheme includes emulations of 11 leading regional banks. In total, Group-IB analysts discovered more than 1,000 fraudulent resources related to this campaign.
- **Investment scam campaign**. The most common technique used by scammers to promote so-called zero-risk investments through fake articles with positive comments. Scammers often compromise accounts to publish fraudulent posts on social media networks, such as Facebook or Youtube. In the MEA region, domain names similar to well-known local news agencies or newspapers are commonly used. In Europe, scammers employ IP telephony and call centers to carry out social engineering attacks by voice. During their research, Group-IB analysts uncovered over 10,000 rogue resources aimed at users in Europe, Asia, and North America.

6. Growing popularity of account hijacking

Fraudsters have long impersonated well-known brands or reputable personalities to increase the credibility of their scams. The main tactic used is fake account creation. However, scammers are increasingly hacking into verified accounts and acting on their behalf.

Scammers not only hunt for pages belonging to specific people or brands, but they also pay attention to other verified accounts. After taking over the account, the hackers change its name to one that suits their aims. Meanwhile, users still see the verification mark.

For example, Group-IB discovered a novel scam campaign aimed at gaining access to users' bank accounts in **Indonesia**. Over **600 hijacked Instagram accounts** were used to spread phishing links to fake websites disguised as login pages for one of Indonesia's leading financial institutions' mobile banking apps. To distribute phishing content, scammers used over **1,000** affiliated fraudulent domains.

7. New phishing and scam techniques

As old schemes and techniques lose their effectiveness over time, attackers are constantly coming up with new ways to deceive victims. In 2022, scammers developed the following new techniques:

- **The browser-in-the-browser (BitB)** phishing technique was described by the researcher mr.d0x in spring 2022. This method sees the scammers create a fake browser window indistinguishable from the genuine one. Unlike classic phishing, this technique allows an attacker to display data in a pop-up window. The URL in the address bar belongs to a third-party site the victim is trying to access and fully replicates the real one. Moreover, the fake window always displays the lock icon of the valid SSL certificate.
- **Bitrix Hijacking**. This phishing technique exploits the vulnerabilities in outdated versions of the Bitrix24 CRM platform. Scammers insert a JS script into the secure website code and redirect users to phishing resources. When a user attempts to access a page from a search engine, the JS script launches a chain of redirects. The latter leads to a malicious resource selected according to a user's geolocation and the number of clicks on the link.
- Scammers in the MEA region are using **legitimate CRM services for email spoofing**. They mimic victims' accounts on those services. Emails sent via such tools appear much more convincing to victims. Additionally, CRM services can facilitate communication with victims by arranging and storing large amounts of data, including details about the already contacted victims, and the results of the previous attacks.
- In the APAC region, scammers started to **utilize popular map services** more frequently. Fraudsters post deceptive texts, videos, and photos containing fake customer service numbers on Google Maps listings. Victims then use these contacts when they attempt to reach out to the customer service departments of the legitimate businesses via WhatsApp chat. After clicking on these links, the scammers ask the victims to provide personally identifiable information (PII) and account credentials.

05 ↗

COUNTERMEASURES

To prevent and remediate the negative consequences of digital crime, it is crucial to pay attention to the following steps:

1. Reconnaissance to collect data on current and potential attacks
2. Education to train your staff to recognize and neutralize such attacks
3. Audit to discover vulnerabilities before attackers find them
4. Response to stop attacks and mitigate the damage

Reconnaissance

- Be present in cybercriminal groups, especially those on the Telegram messaging platform, to conduct reconnaissance and learn about impending attacks. Companies can also retrieve highly useful data from cybersecurity solutions such as **Threat Intelligence** and the Scam Intelligence unit found in **Digital Risk Protection**.
- Monitor the illegitimate use of your intellectual property online for all potential sources of fraudulent activity (websites, social networks, messengers, advertising, and mentions on the darknet).
- Track mentions of your brand and assets on the Internet. This includes the media and for its mention in the context of ongoing cyber attacks.
- Watch all threat vectors, not only traditional cyber attacks using phishing or malware.
- Check user messages and opinions outside the company's perimeter. Track your brand perception online and pay attention to any unexpected changes.
- Keep an eye on new opportunities that could be exploited in an attack. Monitor emerging technologies, such as deep fakes and other AI-enabled services.

Education

- Educate your staff about safety on the Internet. Conduct regular training sessions with employees and simulate attacks that contain highly relevant scenarios, including those that use artificial intelligence.
- Promptly and proactively inform your customers about possible dangers and current attacks. Handle user reports carefully and set up a system where any security incident involving the company and its customers is processed.

Audit

- Know your digital assets and track their status. Forgotten assets are often the most vulnerable to attacks.
- Be mindful of the data you share with partners and other third parties. Take into account that the usage of AI-based public services may result in data leakage. Furthermore, if individuals interact with neural networks, these interactions help shape the neural networks, which are also accessible by other users. Attackers can potentially take advantage of the vulnerabilities of neural networks in order to obtain information of a limited nature using targeted queries (prompts) or, on the contrary, try to train neural networks with fake data in order to mislead other users.
- Conduct periodic audits to assess how much of your employees' data has been leaked onto the Internet.
- Ensure the safety of your crypto wallets. In the case of using cryptocurrencies in business, ensure that users have clear, easily available information about official crypto wallets to ensure that users have clear understanding as to whether they are transferring money to a scammer or not.

Response

- Learn how to remove illegal information from the Internet. Keep in mind that services and websites may be located in other jurisdictions, which makes collaboration and building trust extremely important.
- Analyze the websites that are most likely to contain illicit information related to your brand and have checklists for eliminating the violations.
- Create rules for reporting incidents that are easily understandable for your employees. Provide support in solving these problems. For example, you can help your workers respond to personal data leakages and minimize possible damage.
- Remember that negative mentions of your brand are not a violation of intellectual property rights. Aggressive attempts to remove any information you don't like can result in the Streisand effect and reduce your credibility in the eyes of regulators.

06 ↗

STATISTICS

Group-IB separates the concepts of phishing and scamming, given the fact that these cyber threats have different outcomes and, most importantly, fall under different legal rules when it comes to incident response.

Phishing is a generally recognized violation that results in the theft of personal information, such as account credentials or bank card data. Cybercriminals consider an attack to be successful when they receive such data. To combat phishing, a system of computer emergency response teams was created, of which **CERT-GIB** is a member.

Scams refer to any attempt by a cybercriminal to deceive a victim into voluntarily handing over money or sensitive information. To achieve the end goal, scammers create a whole infrastructure of sites, social media and messenger accounts, advertisements, and mobile applications around their campaigns.

Scams are difficult to prove legally because fraudulent resources appear legitimate at first glance, and the final interaction with a victim is often carried out through a private conversation.

Scamming is a criminal offense, and Group-IB, as a private company, is not authorized to charge anyone with it. However, given the fact that scammers appropriate the name and legally protected likeness of well-known brands to deceive victims, Group-IB is able to detect and block scams on the basis that they constitute a violation of intellectual property regulations.

1. Total number of violations

A. Phishing

The number of phishing websites detected by Group-IB in 2022 was **62%** larger than the corresponding value registered in the previous year.

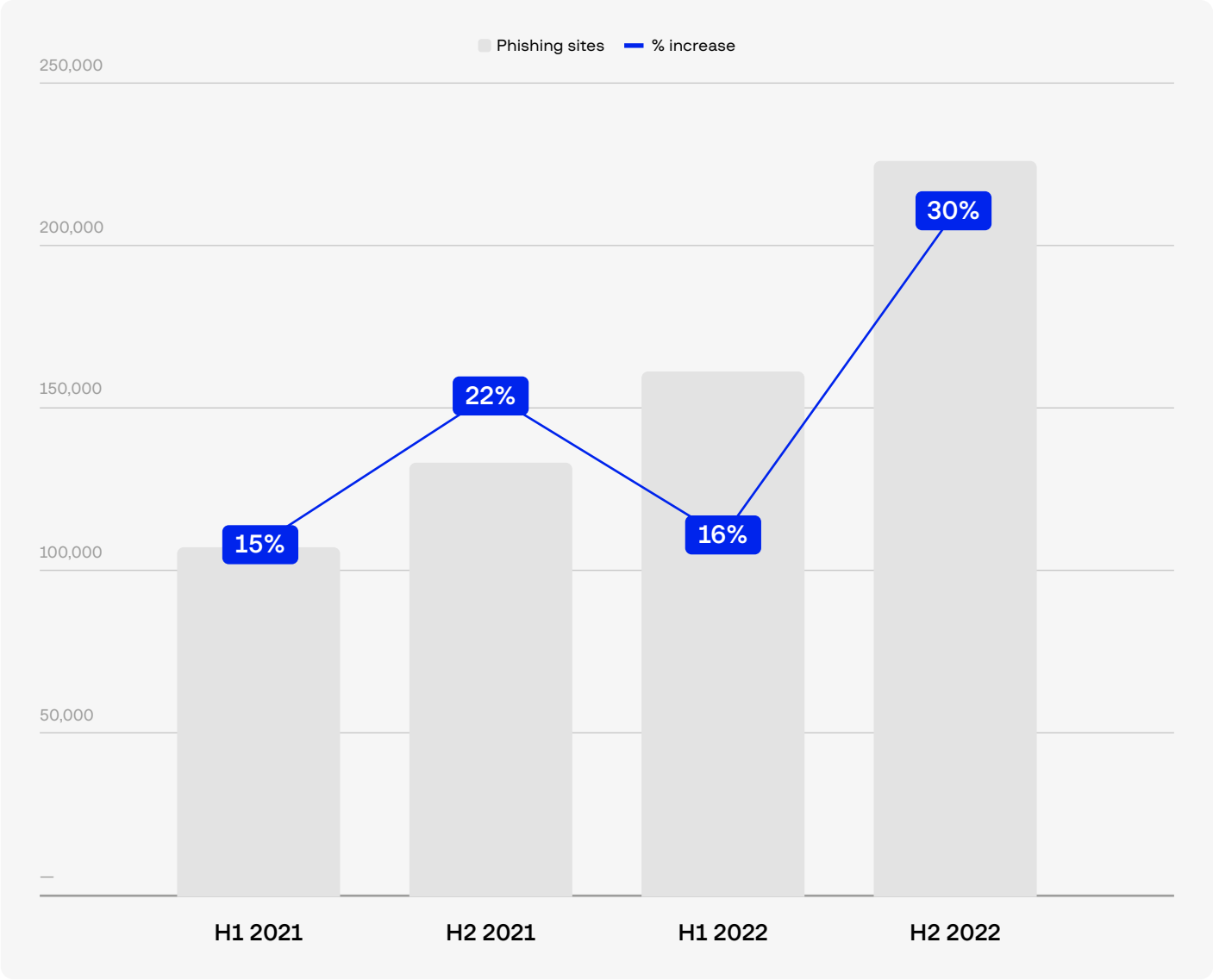


Figure 5. Total number of phishing websites detected by Group-IB in 2021 – 2022

The graph above represents the number of unique phishing sites discovered by Group-IB and includes the following:

- Phishing on various domains
- Phishing on subdomains if such domains target different brands
- Phishing on URL shorteners and similar services

B. Scams

The number of fraudulent resources increased significantly year-on-year. The sharp surge observed in the first half of 2022 can be explained by the rapid spread of a surveys scam scheme in this period. After Group-IB started blocking fraudulent domains, scammers began deleting pages that impersonated the targeted brands. This resulted in a **34%** decrease in the number of scam resources detected in the second half of 2022. Despite this, the overall number of fraudulent resources that utilized the name and likeness of legitimate brands increased by **304%** compared to the year before.

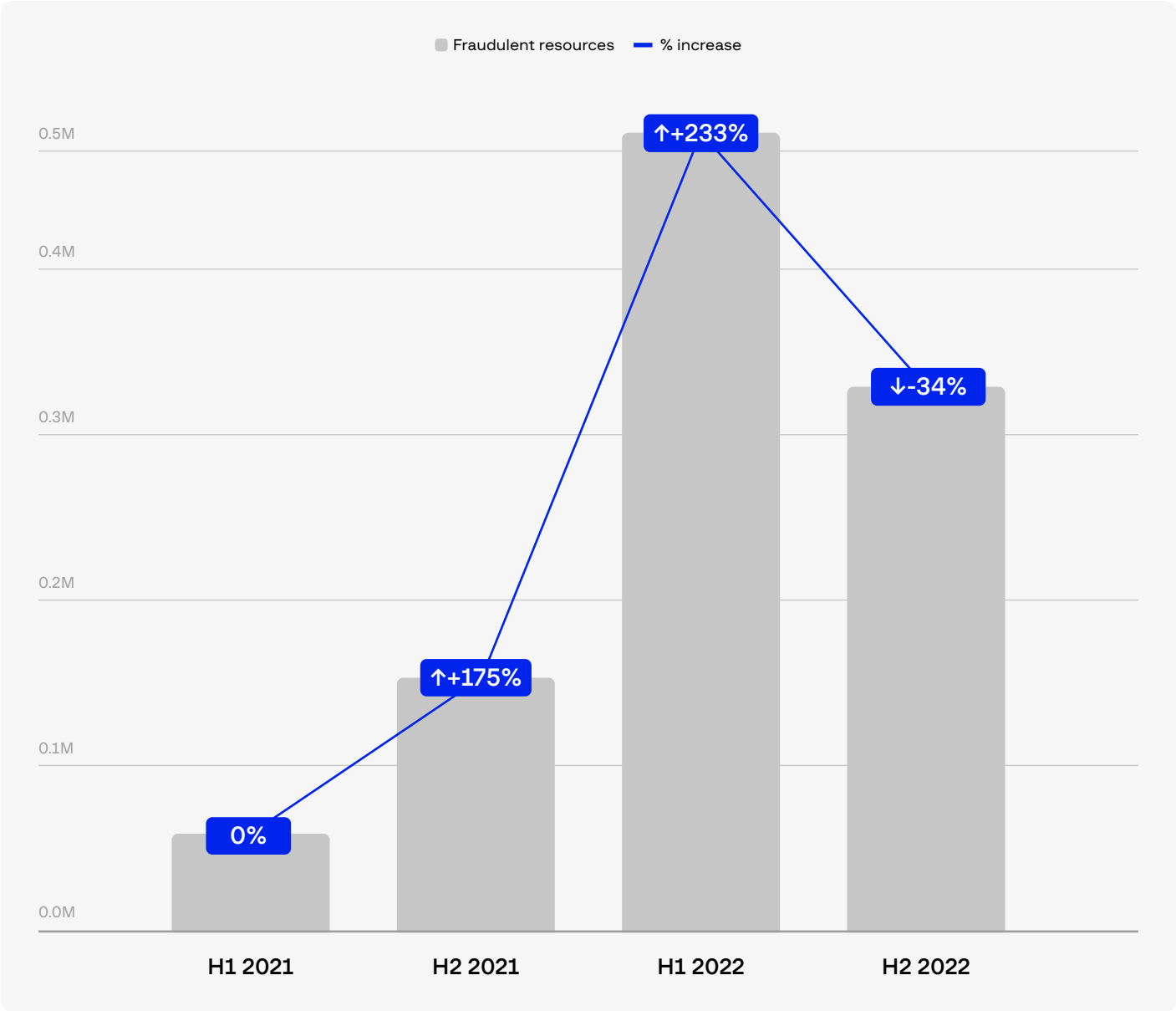
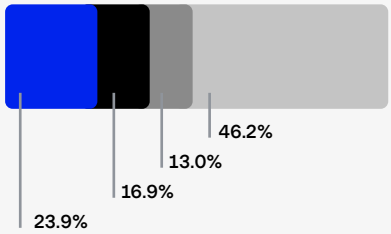


Figure 6. Total number of fraudulent resources detected by Group-IB in 2021 – 2022

2. Violations by industry

A. Phishing

The statistics below represent the industries most affected by phishing attacks. Financial institutions and social media remain the two most targeted sectors. Meanwhile, the amount of phishing resources spoofing companies in the delivery sector nearly doubled compared to the previous period.



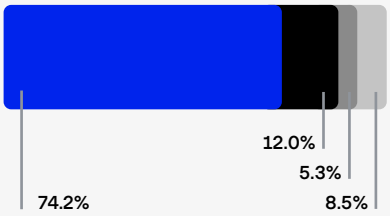
Phishing by industry	%
Financial institutions	23.9
Social media	16.9
Email	13.0
Delivery	5.0
Payment Services	4.4
Crypto	3.5
Cloud Storages	1.8
ISPs	1.8
Bookmakers	1.5
Other services	28.2

Figure 7. Phishing by industry breakdown in 2022

8.48%

B. Scams

The diagram below provides a proportional breakdown by industry of intellectual property violations, such as illegal usage of trademarks, misrepresentation of brand partnerships, scam advertising, fake social media and messenger accounts, and illegal distribution of branded mobile apps.



Violation by industry	%
Financial institutions / Banks	74.2
Lotteries	12.0
Oil and gas	5.3
Retail and e-com	3.2
Investments	2.3
Other	3.0

Figure 8. Number of violations by industry in 2022

The distribution of violations by industry is broadly in line with previous years. However, several industries suffered a dramatic increase in infringements.

First of all, scammers' interest in the **financial sector** skyrocketed. This industry has always been the most popular target for cybercriminals of this type, but, in 2022, the average number of scam resources created per brand increased year-on-year by **186%**.

The **oil and gas sector** also became a target for many scammers. Threat actors took advantage of the unstable political situation by using infomercials depicting changes in gasoline prices, fraudulent resources selling fuel cards, and fake surveys that claimed to be created on behalf of oil and gas companies. As a result, the average number of scam resources discovered per brand increased by **112%**.

The **manufacturing** industry was not spared as well. The average number of threats per brand in this sector increased by **55%**.

3. Violations by domain zones

A. Phishing

The diagram depicts the most popular top level domains (TLDs) used for phishing in each half of 2022. Apart from the usual fluctuations, a drastic rise in the usage of free domains (.tk, .gq, .ml) can be seen, which we attribute to the massive Bitrix hijacking campaign observed last year.

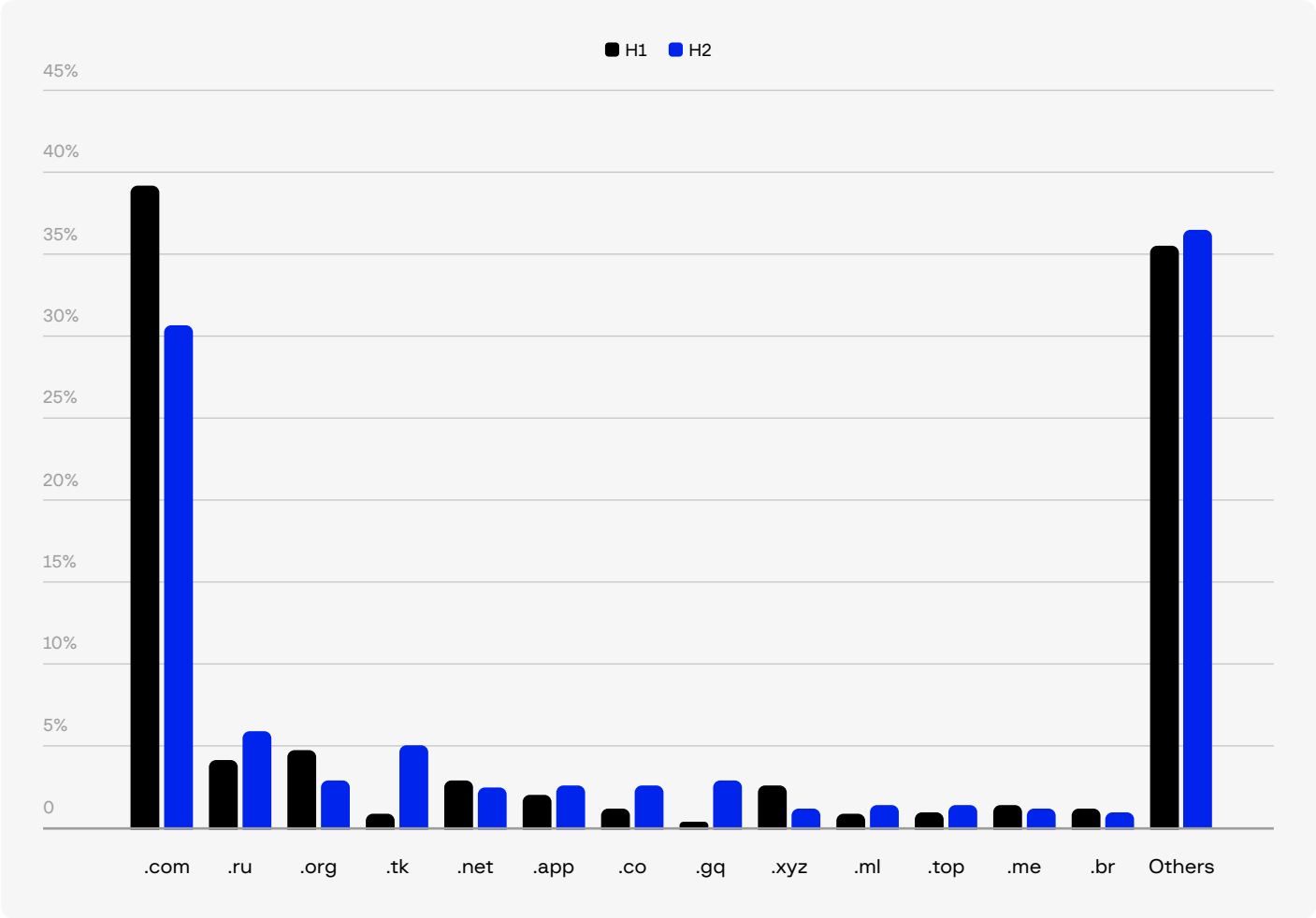


Figure 9. Most used domain zones for phishing websites in 2022

B. Scams

In the second half of 2022, scammers started publishing websites on the **.tk domain** that included the illegal use of branded assets. This activity may be explained by the growth of affiliate programs that pay commissions to participants for attracting traffic to thematic offers. Affiliate platforms automatically generate links in the .tk domain zone.

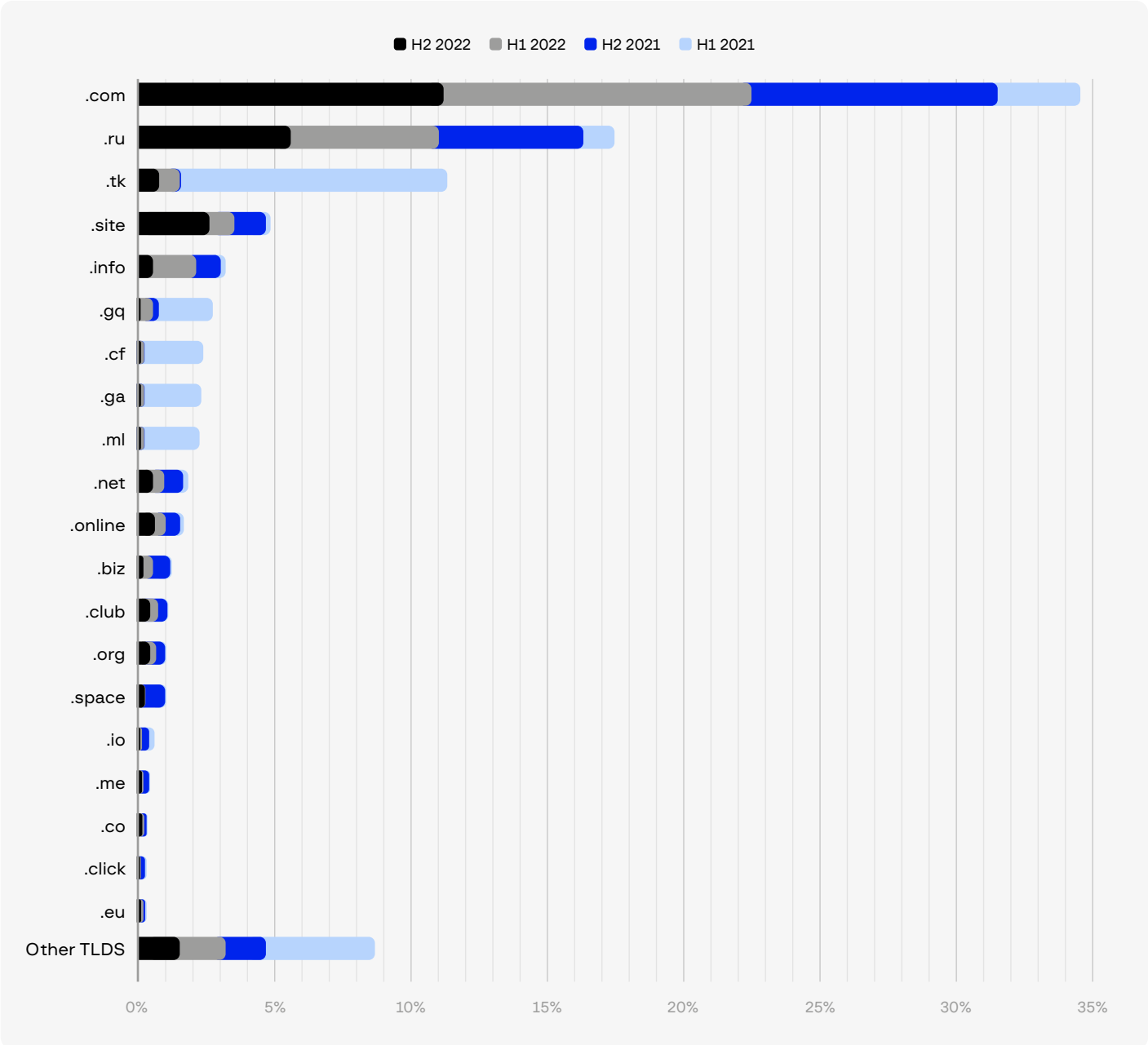


Figure 10. Top domain zones for scam sites (2021 – 2022)

4. Violations by hosting provider

A. Phishing

The graph shows which countries hosted the most phishing websites servers in 2022. Although the USA is still the leading country with the largest hosting providers, such as Amazon, GoDaddy, and Google, Russian servers accounted for slightly less than 10% of the world's phishing activity. Group-IB researchers believe that this is due to the significantly low cost of services and the growing prevalence of bulletproof hosting providers in Russia, which are able to create difficulties in the takedown of sites that contain violations.

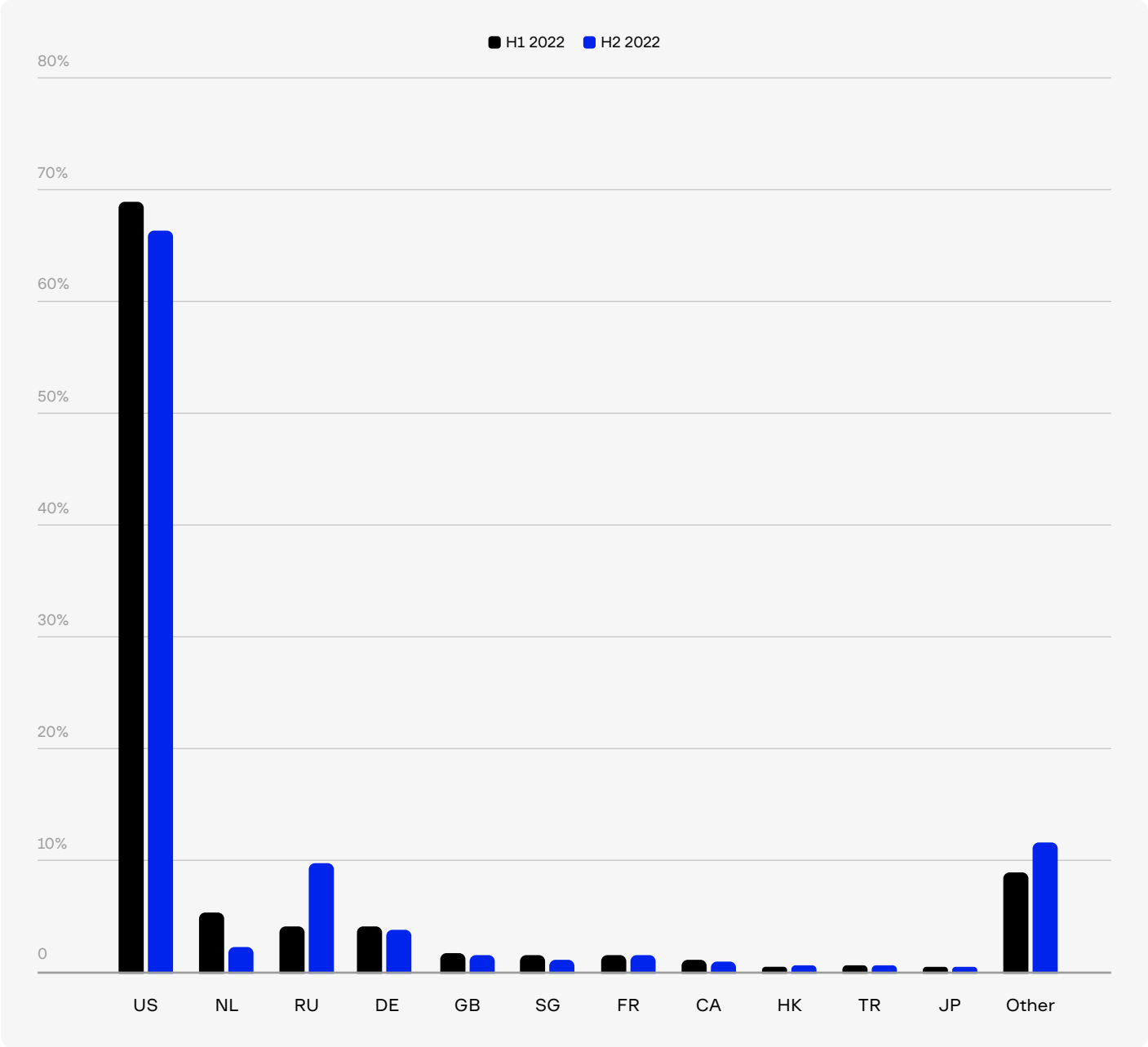


Figure 11. Top phishing hosting countries in 2022

B. Scams

As with phishing sites, the majority of scam sites made use of hosting, content delivery networks, or cloud services with US-based companies. Notably, US-based services were used on **more than 90%** of scam sites seen by Group-IB in 2022. This trend largely reflects the growing use of Cloudflare services for scam sites. In 2021, just under 19% of scam sites seen by Group-IB used Cloudflare services. This figure rose to **more than 70%** one year later.

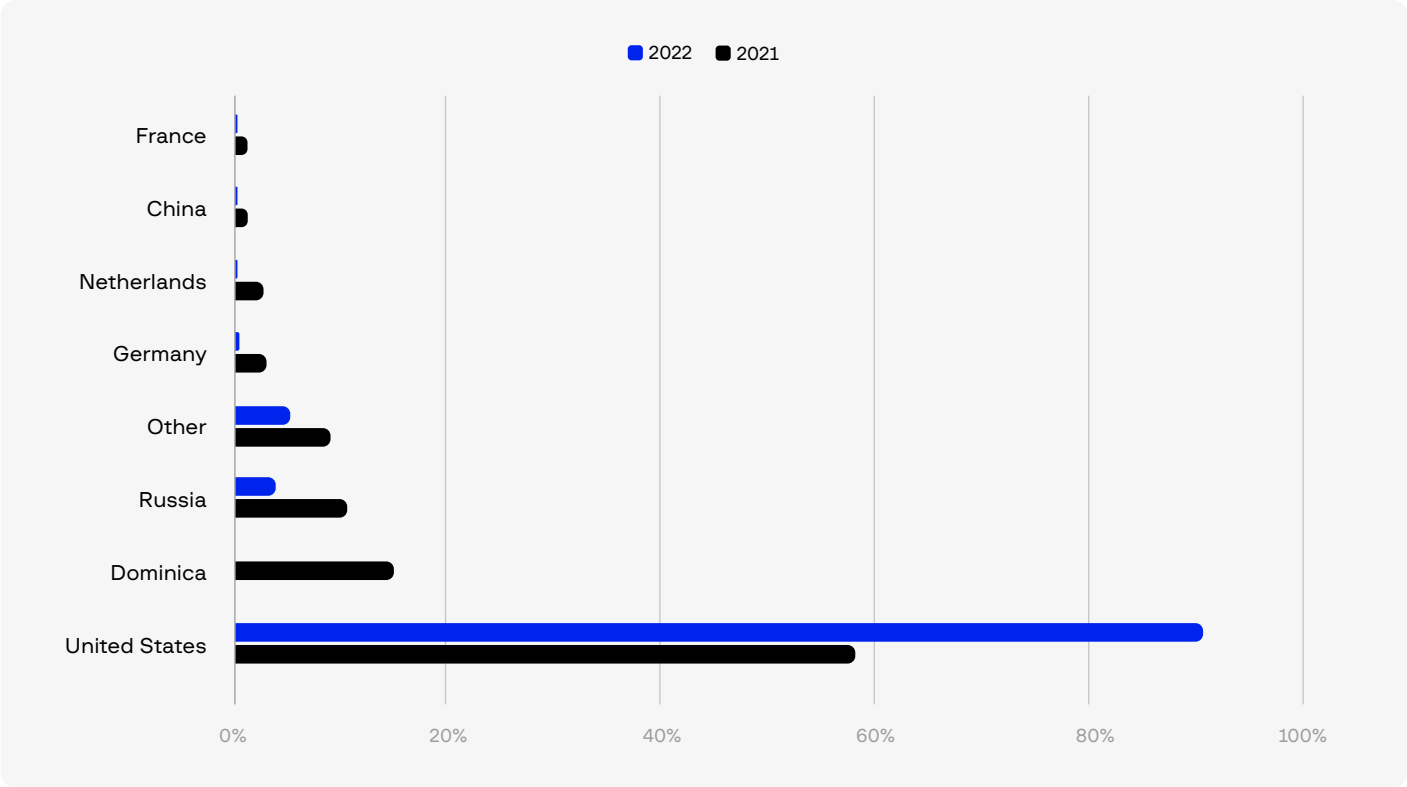


Figure 12. Number of violations in 2021 and 2022 by country of IP address

Scammers are taking advantage of the fact that Cloudflare's DNS system, designed to cache a website's content to improve the user experience, can protect a website's IP address from direct exposure. This can slow down the process of communicating with the hosting provider of a scam website over the takedown of violations, potentially extending the lifespan of scam resources. Cloudflare may reveal the hosting provider by request, but some hosting providers refuse to acknowledge violations, as they see Cloudflare's IP addresses instead of their own.

About Group-IB

Group-IB is a leading provider of innovations and solutions for detecting and preventing cyberattacks, eliminating fraud, and protecting brands from digital risks worldwide.

1,300+ successful investigations	**600+** employees	**550+** enterprise customers	**60** countries
$1 bln saved for companies	**#1*** Incident Response Retainer vendor	**120+** patents and applications	**3** unique Digital Crime Resistance Centers

* According to Cybersecurity Excellence Awards

Global partnerships

INTERPOL

Europol

Recognized by top industry experts

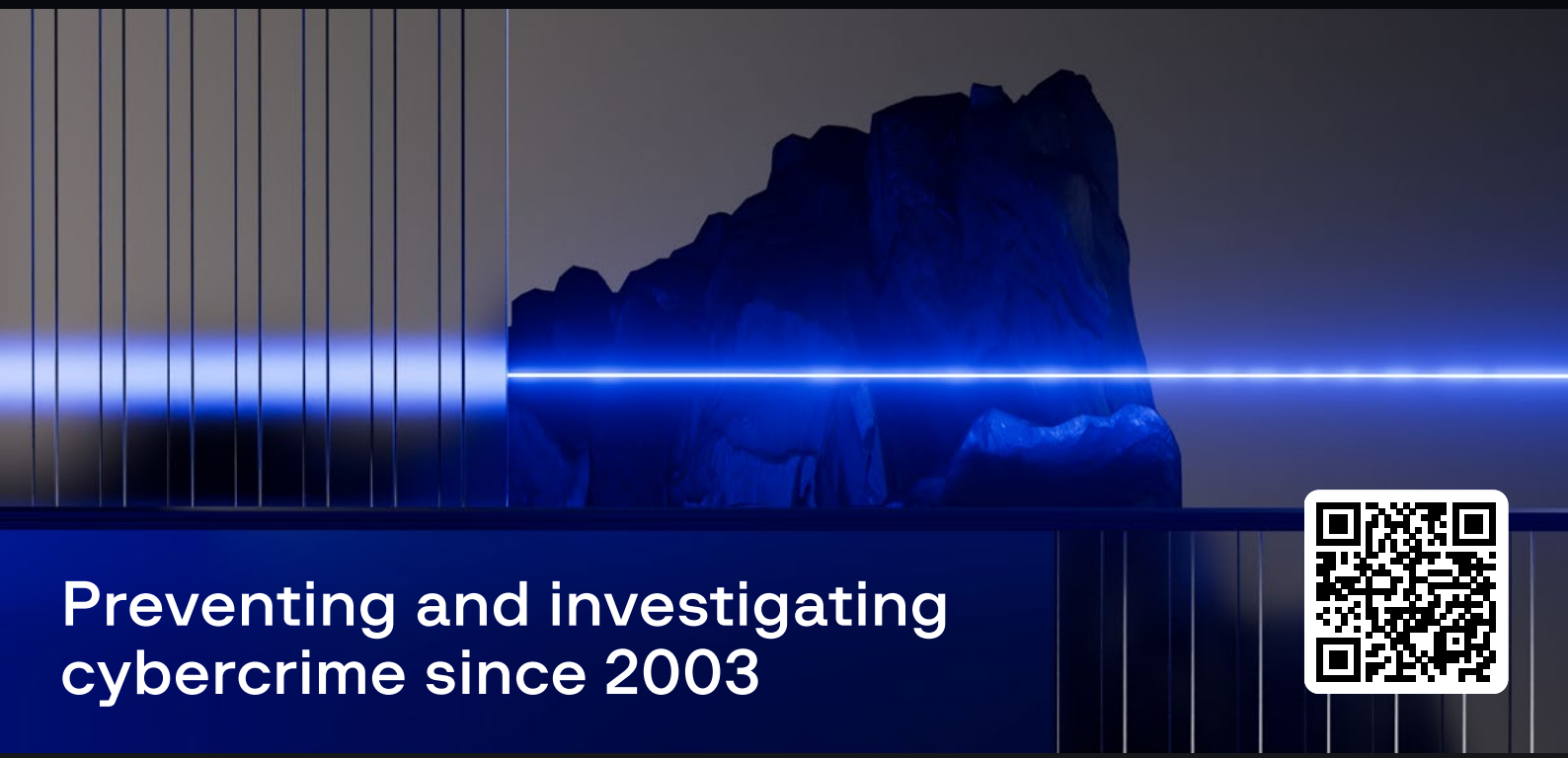
FORRESTER®

kuppingercole ANALYSTS

Gartner

IDC

FROST & SULLIVAN



Preventing and investigating cybercrime since 2003

FIGHT AGAINST CYBERCRIME

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 3798

EU & NA
+31 20 226 90 90

MEA
+971 4 508 1605