When crisis strikes, cybercriminals thrive

While the financial turbulence caused by the global pandemic has put aside any goals other than survival, criminals have increased their profits, withdrawing huge amounts of money. One of the main veins of the underground economy is online piracy.

PIRATES OF THE DIGITAL SEA

ROOT LEVEL RESOURCES

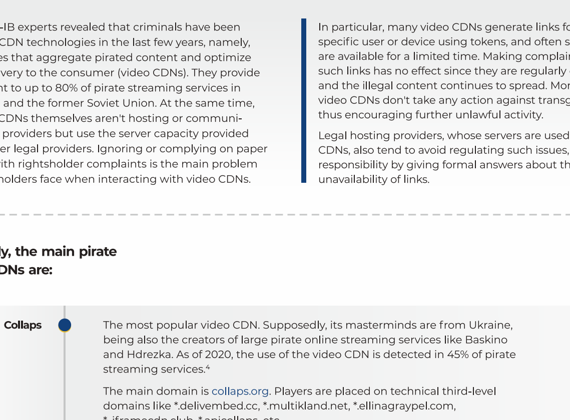
In recent years, the scale of media piracy has expanded tremendously. Russian-speaking cybercrime conglomeates have moved into international markets, thus making it possible to increase the capitalization of their underground business.

The United States, as the largest media industry in the world, incurs heavy losses. According to the U.S. Chamber of Commerce's Global Innovation Policy Center, the U.S. economy loses up to $29.2 billion due to online piracy.[1]

We should face up to the fact that pirate sources[2] have well adapted to the counteractive operational environment. Their infrastructure is resilient to the emergence of new technologies and specific legal initiatives.

The current structure of the video piracy market consists of:

1. **Dedicated advertising networks** (bookmakers, casinos, alcohol, etc.), sponsoring CamRip groups,[3] translators, video CDNs, and websites featuring pirated content
2. **Video CDNs**, providing hosting and distribution capacity for streaming video. In turn, pirate websites purchase the above capacities from legal hosting providers
3. **Pirate websites** that integrate the player of one or more video CDNs, thus being able to monetize content by showing ads to users
4. **Users** who access pirate websites mainly through search engines or social networks.



Group-IB experts revealed that criminals have been using CDN technologies in the last few years, namely, services that aggregate pirated content and optimize its delivery to the consumer (video CDNs). They provide content to up to 80% of pirate streaming services in Russia and the former Soviet Union. At the same time, video CDNs themselves aren't hosting or communication providers but use the server capacity provided by other legal providers. Ignoring or complying on paper only with rightsholder complaints is the main problem rightsholders face when interacting with video CDNs.

In particular, many video CDNs generate links for a specific user or device using tokens, and often such links are available for a limited time. Making complaints about such links has no effect since they are regularly changed, and the illegal content continues to spread. Moreover, video CDNs don't take any action against transgressors, thus encouraging further unlawful activity.

Legal hosting providers, whose servers are used by video CDNs, also tend to avoid regulating such issues, declining responsibility by giving formal answers about the unavailability of links.

Currently, the main pirate video CDNs are:

Collaps

The most popular video CDN. Supposedly, its masterminds are from Ukraine, being also the creators of large pirate online streaming services like Baskino and Hdrezka. As of 2020, the use of the video CDN is detected in 45% of pirate streaming services.[4]

The main domain is collaps.org. Players are placed on technical third-level domains like *.delivembed.cc, *.multikland.net, *.ellinagraypel.com, *. iframecdn.club, *.apicollaps, etc.

HDVB

The second most video CDN. As of the end of 2020, the use of the video CDN is detected in 39% of pirate streaming services.

Video traffic originates from domains that are regularly updated, such as *tesswalton.pw, *bernardjordan.pw, *elmerwatson.pw, *alfredcurry.pw, *quinnnash.pw, *frankfoley.pw, *rexhammond.pw, *janenoble.pw, *nadiapattel.pw, etc.

VideoCDN

The third most popular video CDN. As of the end of 2020, its use is detected in 33% of pirate streaming services.

The main domain is videocdn.tv.

The content is hosted on technical domains like *.cloud.hotlan.by.

Kodik

The video CDN is used mainly for cartoons and Asian films and TV series.

The content is hosted on technical domains like *.get.kodik-storage.com.

Videoframe

The main domain is iframe.video.

Video content is distributed using technical domains like *.cdn.videoframe.space.

The video CDN also owns his own online movie theaterrknfilms.com (smotrihd.com previously).

Ustore

The main domain is ustore.bz.

Streaming video is distributed using technical domains like *.u-cdn.org и *. u-stream.in.

Alloha

The main domain is alloha.tv.

Streaming video is distributed using technical domains like *.streamalloha.live.

Protonvideo

The main domain is protonvideo.to.

Streaming video is distributed using technical domains like *.cdn.protonvideo.to.

The typical features of risk leveling by the CDNs were:

- Frequent changes of technical domains and IP pools
- Use of geo-distributed infrastructure
- Availability of duplicate and backup channels for content distribution, which are usually rented from different providers

These measures have turned ineffective the current practices laid down by the anti-piracy legislation.

Existing threats of pirate websites

ROOT LEVEL RESOURCES

Given the popularity of pirate websites (online streaming services, torrent trackers, etc.), they are a perfect platform of spreading harmful software for stealing money and users' personal data. Such sites can act both as a direct threat source[5] and as a target for other cybercriminals.

Group-IB experts identified three categories of threat during the inspection of resources that distribute pirated copies of audiovisual products:

Safe websites

Visiting such sites poses no threat to users.

Relatively safe websites

Currently, there are no threats detected on such websites, but there are various vulnerabilities that can potentially be used for illegal activities. Usually, such vulnerabilities are caused using outdated or hacked software[5] (e.g., CMS).[6]

Dangerous websites

These websites contain various threats, including malicious software, or these sites are "blacklisted" by anti-malware companies and search engines.

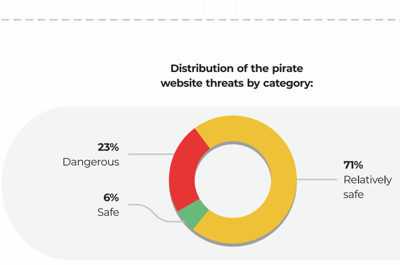
Distribution of the pirate website threats by category:

.ru	24%
.net	11,1%
.online	7,2%
.com	6,7%
.org	5,7%
.site	4,2%
.xyz	4,0%
.top	3,1%
.club	3,1%
.info	3,1%
.me	2,6%
.cc	2,6%
.fun	1,8%
.su	1,6%
.pw	1,5%
.biz	1,5%
.pro	1,3%
.tv	1,1%
.co	0,9%
.ml	0,8%
Others	12,1%

The majority of pirate resources use outdated or cracked software and self-written code fragments that may have vulnerabilities. The lack of money on creating and maintaining the site and the poor technical background of website administrators explains the existence of so many relatively safe websites.

It is worth noting that the largest number of dangerous resources is located in the .RU domain zone. Generally, skilled webmasters use foreign, including offshore, domain zones to locate their resources. Registering a pirated resource in the . RU domain zone is simpler and more intuitive for beginners, although it involves several legal risks. In turn, such webmasters often do not possess sufficient technical competence and means to ensure the security of their resource.

Distribution of dangerous resources by type:



The economics of illegal resources:

ROOT LEVEL RESOURCES

The main drivers of brand and copyright protection activities on the Internet under the "follow the money" principle and the beneficiaries of the "treasure island"[8] are illegal casinos and bookmakers.

Affiliate programs make up the central part of the structure of pirated income. Pirate websites are used as an advertising platform aimed at attracting new users. Based on the terms of most gambling affiliate programs, the remuneration is paid as a percentage of the amount of money lost by the attracted players.

Other terms under the CPA (cost per action) model can be set for large partners. In this case, payments are made for the agreed list of players' actions, regardless of the amount of their losses.

There are three types of advertising material:

- **Affiliate link**
- **Promo code**
- **Banner**

Affiliate links and banners are mainly used on websites, while promo codes or domain advertising are usually found directly in broadcasts and videos.

For conversion tracking and statistics recording, links and banners contain a unique identifier (referral), determining which website the user came from. Promo codes are used for the same purpose for ads embedded in the broadcast. To ensure that the promo code will be used at registration, players are given a small bonus, often at the expense of the pirate broadcast host (the bonus amount is calculated based on the total remuneration for the attracted player).

On the whole, due to the bonuses provided, players find it more profitable to register via a referral link or by a promo code. In this case, active players, especially those suffering from ludomania[9], can hold more than one account to diversify the risks associated with the withdrawal of money and account blocking.

The main advertisers for sports broadcasts are 1xBet,[10] Melbet, Parimatch, Linebet, Orca88, Bwin and others. On average, the streamer's income is from 20% to 40% of the loss of the player involved (depending on the affiliate program).

Given the correlation between payouts and the luck of the attracted players, there is no way to predict the income for each project. Moreover, over time, the passive income derived from previously attracted players grows.

Thus, in the **Melbet** affiliate program, beginners can earn an average of 10,000 rubles in the first month (for a resource with more than 7,000 subscribers and more than 14,000 views per day).

Clients involved in Melbet's affiliate program over a long time can earn up to 1.5 million rubles per month (for a resource with an average daily attraction of 70-80 players).

It should be noted that online casinos and bookmakers often use scams to reduce commission payments, despite the high-income rate of affiliate program participants.

For example, there can be delays or cancellations of regular payments based on various excuses. There can also appear underestimation of traffic and the number of players attracted, and the loss amounts of the attracted players. In addition, almost all bookmaker's offices make obstacles to the accounts of players who have been generating high incomes for a long time. As a result of such actions, the personal account of an affiliate program participant can even go into the red.

1XBET

A striking example illustrating the active promotion of a gambling brand on the Internet is the 1xBet company, whose primary audience is people from developing countries (India, Brazil, Thailand, CIS countries).

It is worth noting that official advertising providers rarely interact with pirate portals. The largest aggregators, such as Yandex and Google, include clauses in their licensing agreement to prevent the use of the content without the copyright holder's consent, due to which a symbiosis of gambling companies and pirate traffic has emerged.

According to Group-IB experts, over the past five years, 1xBet has sponsored the content for more than 17 illegal voice-over studios (which is 80% of the number of major studios), making it one of the main sponsors of the illicit distribution of TV series in the CIS countries:

Voiceover studio	Cooperation start date	Released content
Baibako	26.09.2015	*TV series Movies*
Gears Media	29.11.2016	*TV series*
Coldfilm	17.01.2017	*TV series*
Green Ray	01.04.2017	*TV series Movies*
NewStudio	07.03.2017	*TV series*
Idea film	24.05.2017	*TV series*
Omsk Bird	18.05.2017	*TV series Movies*
Hamster studio	09.10.2018	*TV series*
Alexfilm	05.03.2018	*TV series Movies*

Voiceover studio	Cooperation start date	Released content
Jaskier	17.06.2017	*TV series Movies*
Sunshine Studio	07.11.2017	*TV series*
Good People	12.08.2017	*TV series Dramas*
Kansai Studio	03.08.2017	*Anime*
Gostfilm	26.03.2018	*TV series*
Alternative Production	28.11.2018	*TV series*
Cinema US	01.02.2019	*TV series*
Muzoboz/ Kolobok	01.02.2019	*Movies*

Interaction with the voice studios proceeded as follows: the studio informed the 1xBet advertising manager about the possibility of producing content, and then 1xBet paid for it.

Thus, 1xBet itself did not order certain content, but sponsored it (interaction with CamRip groups was built in a similar way).

The voice studios and their representatives themselves searched for digital copies of content released abroad. The more relevant the content was, the more 1xBet representatives paid for it.

The average cost of dubbing one episode was $55,[11] for an already released film it was $65–70. On average, 1xBet invested about $5,000 - $8,300 per month for voice-over and CamRip filming in the CIS countries.

As for the CamRip, the average cost to produce one screen recording was about $400-1,000 (depending on the quality of the screen copy and the popularity of the content).

Collaboration on embedding ads in pirate CDN prerolls[12] has been ongoing since 2016.

Thus, 1xBet advertising was placed on more than 80% of all pirate resources (among the CIS countries).

Overall number of content pieces dubbed with the 1xBet support is more than 900 (movies and TV series) within the CIS.

In 2019, the well-known pirate group Koshara became an intermediary in the interaction between 1xBet and voiceover studios, starting to produce CamRip with integrated 1xBet ads.

More than 100 CamRip versions of movies have been produced since the beginning of the partnership with Koshara, averaging about three CamRips per week. 1xBet started producing content for foreign countries in 2018. 1xBet released an average of four CamRip versions of movies per week.

Underground online casino sharks are two affiliate programs **Lucky Partners** (founders) & **Welcome Partners** (investors), the conflict between which has been going on for more than 6 years.

Both affiliate programs exploit two types of illegal online casinos:

Unlicensed

Unlicensed casinos run on similar hacked software, which allows you to configure a random win rate. Another possible setting is that it makes it impossible to win.

Licensed

In some countries of the world, legal regimes allow the existence of online casinos. For this reason, a number of developers provide software for online casinos that meets the rules of gambling, i.e. there is a real possibility to win, and the earnings are based on a mathematical algorithm, so that the casino always remains in a small profit.

It should be noted that Lucky Partners are trying to dissociate themselves from the most famous casinos, in particular Azino777, but media investigations confirm that this casino is their project.

Along with online casinos affiliate programs are engaged in other projects based on gambling, such as small forex brokers and binary options (business associated with betting on exchange rates and cryptocurrencies, which is generally prohibited by international payment systems legislation in Russia and European countries), all kinds of lotteries and other similar products.

It is worth noting that the sharks are a step away from the leaders of the betting industry, Fonbet and 1xBet. At the same time, both provide support to the gambling industry.

Advertising traffic to these projects is attracted in two main ways:

- advertising in a community of webmasters evolved from the gofuckbiz.net, maultalk.com, and armadaboard.com forums. Members of the community often meet at various offline events, mostly abroad, to avoid the attention of law enforcement authorities. The forums are reportedly owned by capitalist.net.
- advertising through pirate websites by means of specialized advertising agencies. One of these agencies is Adwise Agency. The media confirmed the agency's connection to Lucky Labs.

Adwise Agency has been repeatedly suspected of illegal activities related to illegal online gambling and pirate websites (e.g. Kinogo, HDRezka, Filmix, Kinoprofi), including suspicions by law enforcement authorities. For example, in February 2020, the Ukrainian cyber police conducted searches in the office of Adwise Agency in relation to the financing of pirate sites kinosha.se, kinanema.net, kinoprofi.vip, rezka.ag, filmix.co.[13]

Russian infrastructure of illegal resources:

ZeroCDN (Mnogobyte, LLC)

One of the most popular services for hosting and distributing video content is ZeroCDN of the Russian company Mnogobyte LLC. As of the end of 2020, between 38% and 60% of pirate sites were using the ZeroCDN project infrastructure.

Thus, ZeroCDN servers have been used by :

- VideoCDN
- Videoframe
- Kodik
- Protonvideo

In addition, such projects as Hdrezka (attendance of more than 52 million people per month) and Kinogo (attendance of more than 35 million people per month) use ZeroCDN servers.

As stated on the company's website, the Mnogobyte network has direct links to Russia's largest backbone operators, including Beeline, MTS, TransTeleCom, as well as to Moscow and regional operators. Large Ukrainian telecom operators (Eurotel, Dataline, Datagroup, Topnet) and Beltelecom, the largest operator of the Republic of Belarus, are also linked to the Mnogobyte network. It is a participant of several traffic exchange points (MSK-IX, DATAIX, W-IX, Global-IX).

- In 2015, the company launched the ZeroCDN project aimed at storing and transmitting large volumes of audiovisual content.
- Since 2017, the company has been officially cooperating with the Swiss provider DigitalOne AG.[14]

DDOS-GUARD LLC

The Russian company DDOS-GUARD LLC provides services to protect against DDoS-attacks and content delivery, being also a hosting provider.[15]

By order of the Ministry of Communications of Russia No. 326 dated 26.06.2017 DDoS-Guard Protection software is registered as a means of information security in the Unified Register of Russian programs for electronic computing machines and databases.

The company's services are used by a large number of illegal resources, including pirated and fraudulent ones. Usually, the company does not react in any way to complaints about such resources.

DDOS-GUARD LLC company:

- Provides fraudulent websites with its computing power, which is used to ensure the functioning of these websites
- Hides the real hosting provider and makes it difficult to identify website owners

It should be noted that the policy of using the services provided by DDOS-GVARD LLC stipulates that the client agrees to use these services only for lawful purposes. Thus, it is prohibited to arrange gambling and cheating schemes.[16]

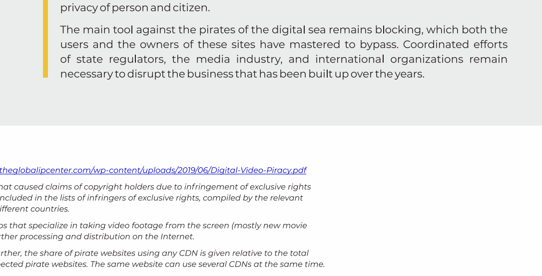
Despite this, DDOS-GVARD LLC does not comply with its own policies. In accordance with the procedure established by Articles 15.1-15.6-1 of Federal Law No. 149-FZ of 27 July 2006 "About information, information technologies and on information protection", Roskomnadzor (The Federal Service For Supervision Of Communications) restricts access to a significant number of sites on which illegal information is distributed and which are hosted or were hosted on the network addresses of DDOS-GVARD LLC.

As of June 24, 2020, **453 similar resources** (domains or URLs) were blocked, including:

- **442 resources** with network addresses included in the subnet 185.178.208.0/24
- **6 resources** with network addresses included in the subnet 185.129.100.0/24
- **5 resources** with network addresses included in the subnet 185.129.102.0/24

Besides pirate resources, such socially dangerous resources as Shadowmarket, an online marketplace where illegal goods and services are bought and sold, as well as numerous drug stores, were blocked.

Violations for these resources are distributed as follows:



ROOT LEVEL RESOURCES

The amount of illegal content, as well as illegal online downloads, is steadily growing worldwide. Weak legal regulation mechanisms and lack of personal responsibility of users are the main reasons behind this growth. Pirate content distribution syndicates hinder the development of legal video services. Meanwhile, a wave of protests and actions of "pirate" legal groups supporting the free download of films, music and software periodically sweeps the globe. Their main slogan is freedom and privacy of person and citizen.

The main tool against the pirates of the digital sea remains blocking, which both the users and the owners of these sites have mastered to bypass. Coordinated efforts of state regulators, the media industry, and international organizations remain necessary to disrupt the business that has been built up over the years.

1 – https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf

2 – Resources that caused claims of copyright holders due to infringement of exclusive rights and resources included in the lists of infringers of exclusive rights, compiled by the relevant authorities in different countries.

3 – Piracy groups that specialize in taking video footage from the screen (mostly new movie releases), its further processing and distribution on the Internet.

4 – Here and further, the share of pirate websites using any CDN is given relative to the total number of inspected pirate websites. The same website can use several CDNs at the same time.

5 – When the intruder is the administrator of such a website

6 – Hereinafter referred to as software

7 – CMS - Content Management System.

8 – Pirate streaming services and sports streaming

9 – Gambling addiction (also gambling)

10 – A betting company that emerged in 2007

11 – Prices are for the CIS region, for India the production price is unknown.

12 – An advertising video that is uploaded before the start of the online video requested by the user, lasting, as a rule, up to 30 seconds.

13 – https://ain.ua/2020/02/28/obyski-u-adwise/

14 – https://hosting.kitchen/mnogobyte/mnogobayt-i-digitalone-ag-podpisali-dogovor.html

15 – https://ddos-guard.net/ru/store/hosting

16 – https://ddos-guard.net/file/aup_ru.pdf