THE PROBLEM

The use of advertising to fund websites and mobile apps offering pirated content has become an insidious practice in the online piracy landscape. While online pirates sometimes opt for subscription-based services as a means to finance their illegal activities, many rely on the placement of ads on their sites or apps, which allows them to generate large amounts of illicit income without having to charge users for the illegal content they offer.

As piracy sites and apps offer popular content for free (e.g. live streaming of football matches, the latest movies and TV shows, popular TV channels) they become attractive places for advertisers to target their preferred audiences and reach a wider customer base. At the same time, they also become hotbeds for the spread of other malicious activities.

Piracy sites and apps try to present themselves as legitimate services, making it harder for the users and the brands to detect and avoid them. Owing to the complexity of the advertising ecosystem and the diversity of actors involved, legitimate brands end up inadvertently financing piracy sites, which not only lines the pockets of criminals and helps create the perception that their services are legitimate – through association with reputable brands – but also causes serious reputational damage to the brands themselves.

A significant amount of advertising on piracy sites and apps comes from legitimate brands and is placed (mostly unknowingly) by legitimate advertising companies. This premium and legal advertising generates real income for criminals, which, paradoxically makes their IP-infringing activities a crime in several EU jurisdictions and is considered criminal income in all. In some jurisdictions, IP infringement only becomes a crime if it aims to obtain direct or indirect financial gain. For example, direct income in this context is the provision of subscription-based access to the copyrighted material, while indirect income includes the revenue generated by advertising on piracy websites or by selling subscribers' personal details to a third party.

Investigators, prosecutors and judges may not immediately think of advertising as a form of revenue when handling digital piracy cases. This is because advertising is not directly tied to the criminal activity – without it, online pirates would still be able to run their websites and apps and offer illegal content to users.

NATIONAL CASE-LAW ON ADVERTISING AS A FINANCING METHOD

Case 16-86.881, Court of Cassation (FR)

The accused founded and managed the eMule Paradise website – one of the most popular sites for the illegal downloading of copyright-protected content – which he operated between 2005 and 2007.

Users of the site could choose from more than 7 000 movies, series and software to download via the P2P network eMule. During the two-year period, the website facilitated more than six million downloads. The accused relied to a large extent on advertising, which allowed him to generate more than EUR 400 000 over the two-year period. The profits were transferred to three offshore companies in Belize, Luxembourg and the United States.

The lower court had sentenced the accused to a 14-month suspended prison sentence and the payment of substantial damages to the civil parties. The latter part of the sentence was annulled by the Court of Cassation and sent back to the Court of Appeals for reconsideration.

To access the full judgment, click here.

Case 117/2016, National High Court (ES)

Between June 2009 and May 2012, two Spanish nationals, aided by five individuals based in Ukraine, made a large volume of copyright-protected content available to the public without the rightholders' consent. They created a webpage where users could access 17 000 publications (books, magazines, newspapers) from various countries.

Access to the content was free of charge for the users. The accused made their profits from the advertisements placed on the webpage in the form of banners and pre-roll videos. To manage the revenue generated by the advertisements, the two main accused established a company with a third person. In total, they made a profit of almost EUR 200 000 from the advertising, which was paid into several bank accounts.

In assessing the element of profit required for the existence of digital piracy crime in Spain, the court took the view that the required intent to obtain a financial benefit was clear from the income generated indirectly by the advertising on the webpage.

The three accused were sentenced to three years in prison for an aggravated crime against IP and for the crime of promoting and establishing a criminal organisation.

This decision was appealed by the accused and later upheld by the Spanish Supreme Court.

To access the full judgment, click here.

THE SCALE OF AD-FUNDED DIGITAL PIRACY

According to research carried out by experts in the field, piracy in general generates an estimated USD 1.34 billion in annual revenue thanks to digital advertising. The same research found that the top five pirate websites generated an average of USD 18.3 million in advertising revenue within a one-year period.

While the market for mobile apps offering illegal access to copyrighted content is still growing, advertising has already proven to be a gold mine. The top five illegal apps generated up to USD 27.6 million in profit from ads in one year. A study by White Bullet commissioned by the EUIPO also found that between January and September 2021, 5 758 illegal and high-risk IPR-infringing websites and apps generated as much as EUR 969.8 million through advertising.

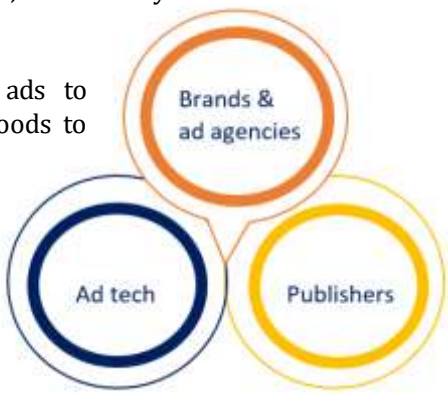
Apps are relatively easy to develop and deploy, and they can help advertisers target consumers more effectively. As they prove more profitable – in-app advertising is now several times more valuable than web-based advertising – criminals will gradually move into this space in search of opportunities to further maximise the profit from advertising.

ACTORS OPERATING IN THE ADVERTISING ECOSYSTEM

Online advertising is complex and involves many actors, all of whom play an essential role in ensuring that an ad can be displayed on a (pirate) website and/or app and viewed by end users. In simple terms, the ad ecosystem relies on four main types of actors:

The **brands** that create ads to promote and sell their goods to consumers.

The **advertising agencies** that are entrusted by brands to buy ad space and handle the advertising process on their behalf.



Website and app operators (publishers) that sell ad space to advertisers.

Advertising technology (ad tech) refers to the ecosystem of technologies and tools that mediate between brands, agencies and publishers and help to optimise advertising campaigns by delivering relevant ads to specific customers. Ad tech includes tools such as **ad exchanges** – digital marketplaces where ad space can be bought and sold across a range of websites and mobile apps. These connect to **demand-side platforms (DSPs)** – software used by advertisers and agencies to automatically buy ad space – and **supply-side platforms (SSPs)** – used by publishers to automatically sell ad space.

To learn more about each actor in the ad tech industry, click here.

LINKS TO MALVERTISING AND OTHER CRIMES

Piracy websites not only engage in the illegal distribution of copyrighted material, but they also help to spread harmful content and facilitate other crimes.

According to a 2022 study, as legitimate brands take concrete steps to move away from advertising on piracy sites and apps, online pirates have increasingly turned to other malicious actors as a way to finance their illegal operations. This has resulted in an increased use of malvertising – malware-laden digital ads.

Malvertising works by tricking website and app users into clicking on the ads and performing a variety of actions, such as downloading security tools, anti-virus software and services, installing browser extensions, enabling browser pop-ups or updating media players, all of which are loaded with malware.

Once installed, the malware can take many forms – adware, browser hijackers, Trojans, keyword loggers – all designed to infect a user's computer and make it more vulnerable to further attacks. The malware also enables criminals to take over a device and use it to launch cyberattacks against other internet users. In particular, the use of malvertising on piracy sites and apps has been linked to the spread of ransomware, as well as cases of fraud, data theft and scams.

RANSOMWARE

Ransomware is a specific form of malvertising that consists of multi-stage cyberattacks, designed to infect a computer system. Once launched, ransomware allows data to be exfiltrated and files on a computer to be encrypted, denying its user access to them. Ransomware is a form of blackmail that involves demands for the payment of a ransom to decrypt the files. However, paying the ransom does not guarantee that the user will regain access or fully recover all encrypted files. Failure to pay the ransom can result in the data stolen being leaked to the public.

FRAUD, DATA THEFT AND SCAMS

Malicious ads are delivered in the form of fake promotions or prizes designed to entice the user to click on them and undertake certain actions, such as completing surveys that require providing personal data – including credit card details – to claim a popular product. This technique not only enables cybercriminals to infect users' computers with malware, but it allows them to steal users' data, which can then be sold to third parties or used to commit fraud and a variety of other scams.

TYPES OF ADVERTISING

Online pirates rely heavily on different types of advertising to fund their illegal activities. The most important include:

Branded advertising

Ads that belong to a particular brand, including premium brands (those with a well-established reputation in the market) and lesser-known ones. Although most legitimate brands do not want to be associated with illegal content providers, their ads sometimes end up on piracy sites and apps, either because of a lack of due diligence or because it is difficult to distinguish between legitimate and illegal sites. The large amounts invested by these companies in marketing their products means that when their ads are placed on piracy sites, they help rogue operators make very high profits.

Sponsored content

Ads that sponsors pay to produce and publish on behalf of a brand or service provider. This type of ad comes in various forms (infographic, video, article) and blends in with the surrounding content of the webpage, making it less intrusive for the user. Sponsored content consists of sponsored links embedded in images that blend promotions with other types of content, such as stories, videos or gossip, tempting users to click on them. The images are usually placed in a box located alongside the content of the piracy site.

Fraudulent and malicious advertising

Ads that carry fraudulent or malicious activity and entice users to click on them. These may be disguised as ads that simulate fake brands, deceptive images or fraudulent promotions. Clicking on them unleashes malware, including browser hijackers, Trojans and adware that can cause further harm to users' computers.

▶ Example of a sponsored content ad on a piracy website.

Source: White Bullet & Digital Citizens Alliance, 'Breaking (B)ads: How advertiser-supported piracy helps fuel a booming multi-billion dollar illegal market', August 2021

EXISTING EU INITIATIVES TO COMBAT ADVERTISING ON PIRACY SITES

In 2018, the European Commission helped to negotiate a Memorandum of Understanding (MoU) to help minimise the presence of advertising and payment services on internet websites and mobile apps that provide access to IPR-infringing content on a commercial scale.

The signatories – currently 30 – include actors involved in buying, selling, facilitating and placing advertising, such as advertising agencies, platforms, networks and exchanges, publishers and IPR owners. Representatives or associations of these groups are also signatories to the MoU.

Efforts under this initiative focus primarily on websites and mobile apps that have no substantial legitimate use and those that have been declared by judicial, administrative or other enforcement agencies to be infringing copyright or distributing counterfeit goods on a commercial scale. Under the MoU, the parties have agreed to monitor the volume, type and value of ads on piracy sites and apps, and to establish a discussion forum to share their actions, expertise and best practices.

According to the latest evaluation report on the impact of the MoU, the estimated ad revenue generated by the sites and apps monitored in 18 EU Member States increased by 40% (from EUR 73 million in 2020 to EUR 102.5 million in 2021). Nevertheless, this increase was significantly lower than the advertising revenue generated in non-monitored countries. In these countries, ad revenue increased by a staggering 241% (from EUR 75.87 million in 2020 to EUR 258.599 million in 2021). These figures highlight the scale of the problem worldwide.

To learn more about the MoU and the current state of ad-funded piracy in the EU, please consult the materials on the dedicated page here or scan the QR code.

FORMATS OF ADVERTISING ON PIRACY SITES

The ads placed on pirate sites mostly appear in the form of banners – a type of display advertising that has been around for some time and remains a popular and widely used form of advertising.

Banners are rectangular ads placed along the top, side or bottom of a website that combine visual content with a call to action. They are designed to capture the interest of website visitors and divert them to the advertiser's online page, with the aim of converting them into new customers for a particular brand or service provider.

MAIN TYPES OF BANNERS USED IN ADVERTIISNG

Banner ads come in a variety of styles and formats. The most common types of banner ads used in online advertising include:

Static banner ads: consist of a still image accompanied by text.

Animated banner ads: incorporate motion and visual elements, such as a video or a GIF, to grab the user's attention and create a more interactive and dynamic viewing experience.

Expandable banner ads: dynamic ads that are activated (expanded into a larger size) as a result of an action by the user, such as hovering over the ad.

Regardless of their type, banners usually fall into two main categories:

Run of site banner ads

These are a type of banner ad that can appear in different locations on a webpage and in different formats (static or moving). With this type of ad, advertisers have less control over where the ad is placed on the webpage (i.e. bottom, side or top).

Pop-up banner ads

This type of ad is more interactive and appears in the centre of the webpage the user is visiting.

TIP

All these advertisements record user activity in some form, as the payment website owners receive for the advertising is based on it. It is important to keep in mind that by contacting the ad tech company, investigators can potentially gather valuable information on the visitors of the website hosting the illegal content.

To learn more about the Eurojust IPC Project and access its publications, please click here

REVENUE MODELS

Online pirates (and other ad hosts) are paid for the ads that are placed on their (illegal) websites, usually by legitimate advertisers. The most widely used revenue models are:

Cost-per-click (CPC)/Pay-per-click (PPC)

The host website owner is paid by the advertiser for every click that the ad receives. This means that if a website user only views the ad (ad impression) but does not click on it, there is no cost to the advertiser.

The price an advertiser pays for a click varies according to the market in which the advertiser operates. In some sectors, such as real estate, a click may cost more as the profit that each click can generate for a business is also higher. This model is very effective because it gives an advertiser information about the level of interest and engagement of the target audience.

Cost-per-acquisition (CPA)/Pay-per-acquisition (PPA)

This payment model requires the website visitor to click on the ad and to carry out a specific action (i.e. make a purchase, download a file or install a program). This type of revenue model is more cost-effective as it ensures that the ad viewer becomes a customer. Accordingly, the owner of the host website only gets paid by the advertiser for every successful customer acquisition generated by the ad.

Cost-per-impression (CPI)/Pay-per-impression (PPI)

In this model, the host website does not need the user to click on the ad. Instead, payment for an ad is based on the amount of exposure the ad receives. Every time an ad appears on a website, it counts as a single impression.

Advertisers using this method generally agree on a set amount for every thousand impressions the ad receives.

!

When considering the risk posed by advertising to users of piracy sites and applications, cost-per-click and cost-per-acquisition ads are of particular concern.

As these two types of advertisement require the user to take a specific action – click, download, provide personal information – they are also more effective at infecting user computers and spreading malware. As the action of clicking on the ad is considered a deliberate and intentional action by the user, it may not be detected by anti-virus software.

In these situations, the anti-virus software will not scan the newly installed program until the installation is complete, which may be too late to prevent the computer from being infected.

EN PDF • Catalogue number: QP-09-23-464-EN-N • ISBN: 978-92-9404-018-3 • DOI: 10.2812/324312