Breaking (B) ads:

How Advertiser-Supported Piracy Helps Fuel A Booming Multi-Billion Dollar Illegal Market

digitalcitizens alliance | whitebullet

August 2021

Table of Contents

Executive Summary

For nearly as long as the modern entertainment industry has offered content to the public, it has relied upon advertising and on subscription services for its financial lifeblood. With the emergence of the Internet, the means to deliver movies, TV shows, and other forms of content have changed, but the advertising and subscription models have endured.

But while the legitimate means of distributing entertainment has evolved, so have the tactics of criminals who exploit stolen content for profit. These criminals now offer stolen movies, TV shows, games, and live events illegally through websites and, to an increasing degree, through illicit devices and apps. And it is big money, in large part funded by advertising, including by well-known and iconic brands.

This report is the result of a year of investigation of the content theft business model and how it generates advertising revenues. The report, prepared by the online consumer safety group Digital Citizens Alliance and piracy and advertising specialists White Bullet Solutions Limited, reveals that the bad actors who operate in the illegal, underground market for pirated movies, TV shows, and other forms of content theft are **reaping an estimated $1.34 billion in annual revenues** through advertising on websites and illicit streaming apps.

In doing so, they harm creators, damage the reputation of brands and the overall advertising ecosystem, expose consumers to fraud and malware, and pose new challenges for law enforcement, via both websites and apps. The year-long investigation of ad-supported piracy reveals that:

- **The top websites that offer stolen content generate $1.08 billion in global annual ad revenue. For the major players, it's big business: the investigation found that the top five of these websites made an average of $18.3 million in revenue from advertising.** Many of these websites are in a constant state of churn, meaning they are changing domains and redirecting to avoid enforcement and bypass advertising blocklists.
- **The top apps that offer stolen content generate $259 million in global annual ad revenue. Just as with websites, piracy apps and advertising can be quite lucrative: the top five of these apps made an average of $27.6 million in ad revenue.** These apps remain a smaller piece of the piracy pie than websites, but they are growing at a more rapid pace. As they appear to be more profitable than websites (commanding high advertising bid values and generating greater margins), they are likely to continue to proliferate.

- **The brands who place the most digital ads overall, which include many of the Fortune 500 companies ("Major Brands"), are among the key revenue sources for pirate operators**. Due in large part to the proliferation of advertising on piracy apps, these Major Brands paid pirate operators roughly $100 million in the last year to advertise on their platforms. One in four ads on piracy apps are from well-known companies. This shift to apps comes after a concerted effort over the last eight years by these brands to stop their ads from showing up on illicit websites. The emergence of piracy apps threatens to undermine this progress.
- **Amazon, Facebook, and Google dominated the list of Fortune 500 companies found on these piracy apps.** Ads for these three well-known companies accounted for **73 percent** of all Major Brands that appeared frequently on piracy apps during the year-long investigation. That means these three companies are supporting these piracy operators with potentially tens of millions of dollars in advertising on piracy apps alone.
- **There has been a recent significant decline in Amazon-branded ads showing up on piracy websites and apps.** This demonstrates that the issue can be addressed when a brand makes it a priority.
- **Piracy websites and apps are highly risky for consumers.** Roughly one in three piracy websites and apps have risky advertising that exposes consumers to fraud and malware.

While piracy causes direct harm to creators and others who lose income when their content is stolen, the impact goes well beyond the entertainment industry. **Consumers who use piracy websites and apps are three times more likely to be exposed to malware**, according to a recent survey. And Major Brands face reputational risks when their advertising appears on illicit websites.

As the piracy environment grows, so does the threat and challenge it poses. In August 2020, Digital Citizens issued a report with content protection specialist NAGRA that found that piracy service operators generate over $1 billion in the sale of illicit *subscription* services. In combination with this report focused on *advertising* revenues, we now have a better sense of the scope of the overall piracy ecosystem – and it is enormous. Through advertising and subscriptions, the operators of piracy platforms are estimated to generate a **combined $2.34 billion dollars** in annual revenue.

The sheer size of the piracy ecosystem should be troubling for policymakers, the advertising industry, and those dedicated to consumer protection. Indeed, the $2.34 billion figure *undercounts* the profitability of the industry: it reflects only a portion of piracy websites and apps; it doesn't include the income the operators make from partnering with hackers to spread malware through the websites and apps consumers use to watch pirated content; and it does not include the income generated from peddling extracted personal data or selling the illicit streaming devices themselves.

This new report lays out for the first time just how much ad-generated revenue goes to the broad ecosystem of "pirate publishers" (piracy websites and apps) and provides a deeper dive into the roles played by three key parts of the pirate advertising ecosystem: the Major Brands, the piracy platform operators, and the "Ad Tech" entities that serve as intermediaries between them. The report also spotlights the unique role Google plays in the piracy advertising world and suggests steps that should be taken to address the issue of ad-driven piracy.

The revelation that the piracy ecosystem is, conservatively, a $2.34 billion market also underscores the importance of efforts by law enforcement, which only recently was provided sufficient statutory tools in the United States to combat these illegal services. Anecdotal evidence suggests that some, and likely many, of these entities do not report their illicit income to tax authorities. And at a time when digital platforms are under fire for their role in other illicit online activities, revelations that they are helping facilitate the placement of ads on illicit piracy websites and apps is troubling.

Digital Citizens will use the research conducted over the last year to engage and educate key audiences on the scope of the ad-supported piracy market and its impact on online safety and trust. Given the richness of the data uncovered, Digital Citizens and White Bullet are preparing a follow-up report that will delve deeper into how piracy advertising is promoting fraud and malware that are increasingly worrisome to both consumers and businesses.

Combating an illicit rogue advertising market requires the collective efforts of government regulators, law enforcement, the advertising ecosystem, Major Brands, and consumer protection groups. That means ensuring that well-known companies are alert to how their advertising is misused, encouraging law enforcement to use the new anti-piracy streaming statute to crack down on criminals, and promoting a renewed vigilance and responsibility by ad networks and intermediaries to protect their clients and their own reputations. By putting a spotlight on this illicit ecosystem, Digital Citizens hopes to contribute to that process.

Part I. Ad-Supported Piracy: By the Numbers

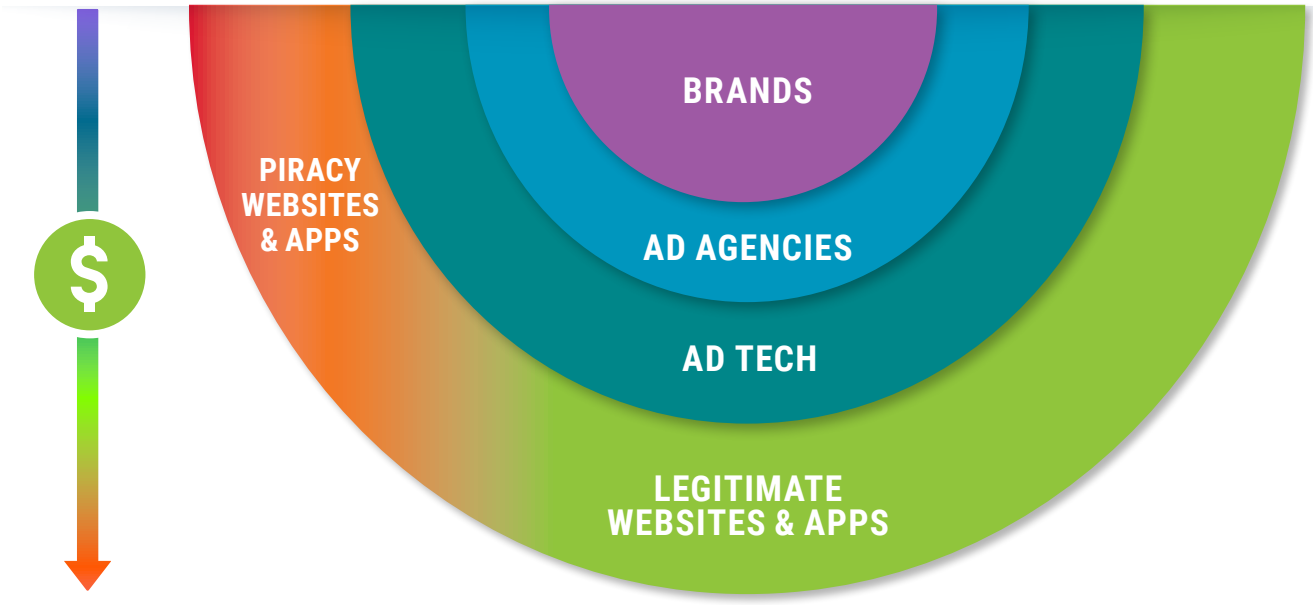
Introduction: An Overview of the Digital Advertising Ecosystem

To understand how $1.34 billion ad dollars land in the bank accounts of piracy websites and apps, it is helpful to sketch out how the digital marketplace for advertising operates.

The websites and apps that users visit typically have a "blank space" reserved for advertising. To get an ad that fills that blank space – and therefore is seen by a consumer - requires a multitude of entities playing different roles. But when simplified to its essence, there are three major types of actors: brands buying space, publishers selling space, and Ad Tech enabling the transactions.

Below is a depiction of the key players in the process that leads to advertising appearing on websites and apps.

Figure 1. Flow of money from brands to publishers (websites and apps), via ad agencies and Ad Tech companies facilitating digital ad placement.



The brands that want consumers to see their products and services create ads. The brands or the ad agencies they hire work with intermediaries – called Ad Tech companies – to place a given ad on a given publisher's space made available to the market. Ultimately, the ad appears on websites and apps.

Pirate operators realized years ago that they could dramatically increase their profits by selling advertising adjacent to popular stolen content that attracts consumers. They succeeded because the advertising ecosystem was either unaware that they were assisting an illicit industry, or it simply didn't care. This lack of diligence by brands, ad agencies, and Ad Tech companies has caused embarrassment when Major Brands' ads appeared on illegal services.

Pirate Revenue from Advertising

To assess the amount of revenue piracy websites and apps siphon from the system, DCA commissioned White Bullet, whose team of investigative and analytic experts sit at the intersection of content protection and digital advertising safety. White Bullet used its comprehensive database on ad-supported piracy to measure the volume and value of advertising going to piracy websites and apps over the last twelve months and calculated revenue estimates based on the findings.

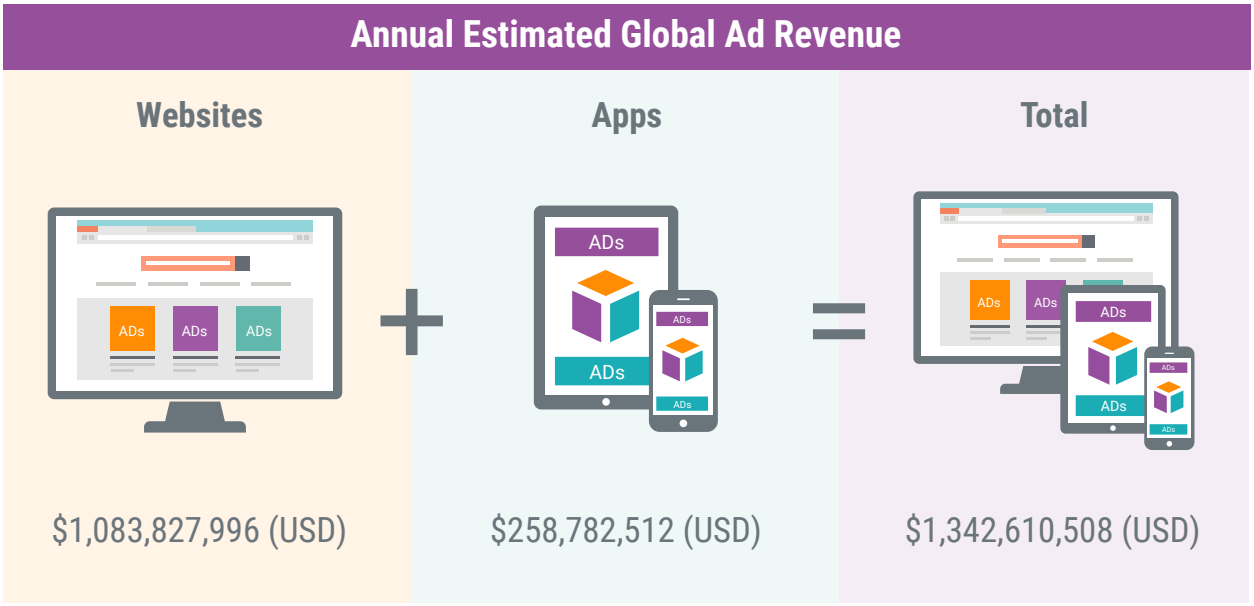
For this investigation, White Bullet identified over 84,000 websites and apps that offered access to infringing copyrighted content, referred to in this report as piracy websites and piracy apps (see Methodology section for more details). White Bullet tracked those piracy websites and piracy apps that were active and displayed digital advertising over a year-long period, from June 2020 through May 2021. For the purposes of this investigation, White Bullet analyzed over 664 billion ad impressions across the most popular 6,194 piracy websites and 884 piracy apps that had advertising and cross-referenced them against White Bullet's advertising revenue matrix to model the estimated revenue flows.

Based on that research, White Bullet found both a legacy network of piracy websites and an emerging piracy apps market that is growing at a fast pace.

Based on its analysis and modeling, White Bullet found that piracy websites generated over $1 billion in ad revenue and piracy apps generated over $250 million. Given that there are nearly seven times as many piracy websites as piracy apps identified in the study, it's not surprising that there is more revenue produced by advertising on these websites.

However, White Bullet found that piracy apps earned four times more per ad than piracy websites, due in part to improved targeting on mobile devices. This makes it likely that app advertising revenue will increase dramatically and further incentivize piracy website operators to diversify to apps.

Figure 2. Annual estimated global ad revenue generated by most popular 6,194 piracy websites and most popular 884 piracy apps during the study.

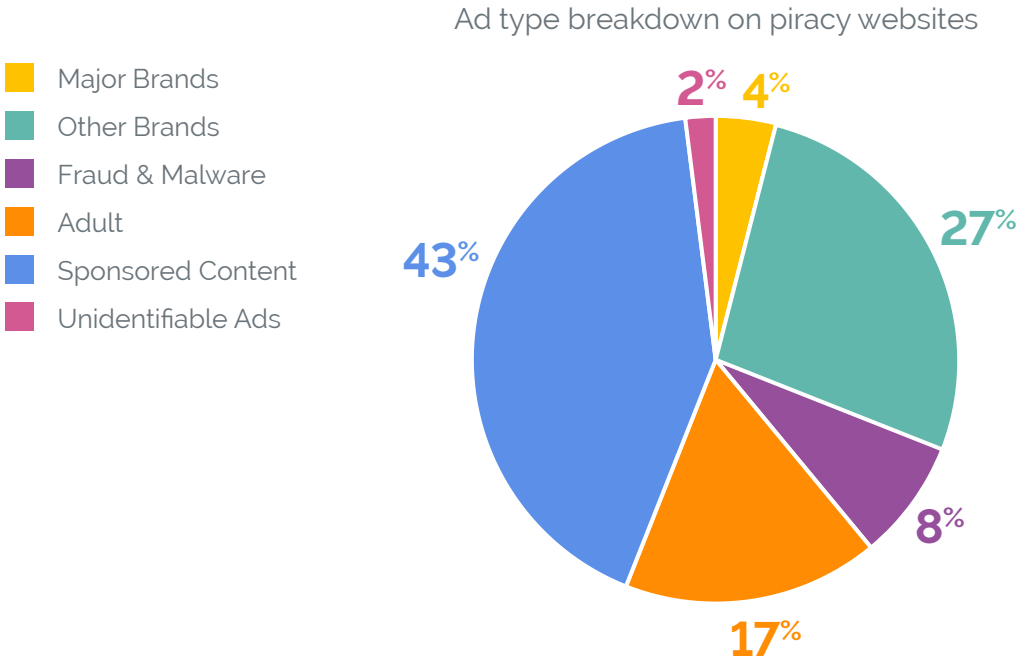


In terms of global annual advertising revenues, the piracy websites analyzed by White Bullet averaged around $175,000; by comparison, the piracy apps analyzed averaged around $293,000 - over one and half times more. Of course, these are averages, and as in any business some will be larger and more lucrative than others.

Ad-driven piracy can be big business for shady operators. Reflecting their power in this illicit marketplace, the top five piracy websites and top five piracy apps generated an average of $18.3 million and $27.6 million, respectively. That represents $229 million, or 17 percent, of the total ad revenues estimated by White Bullet.

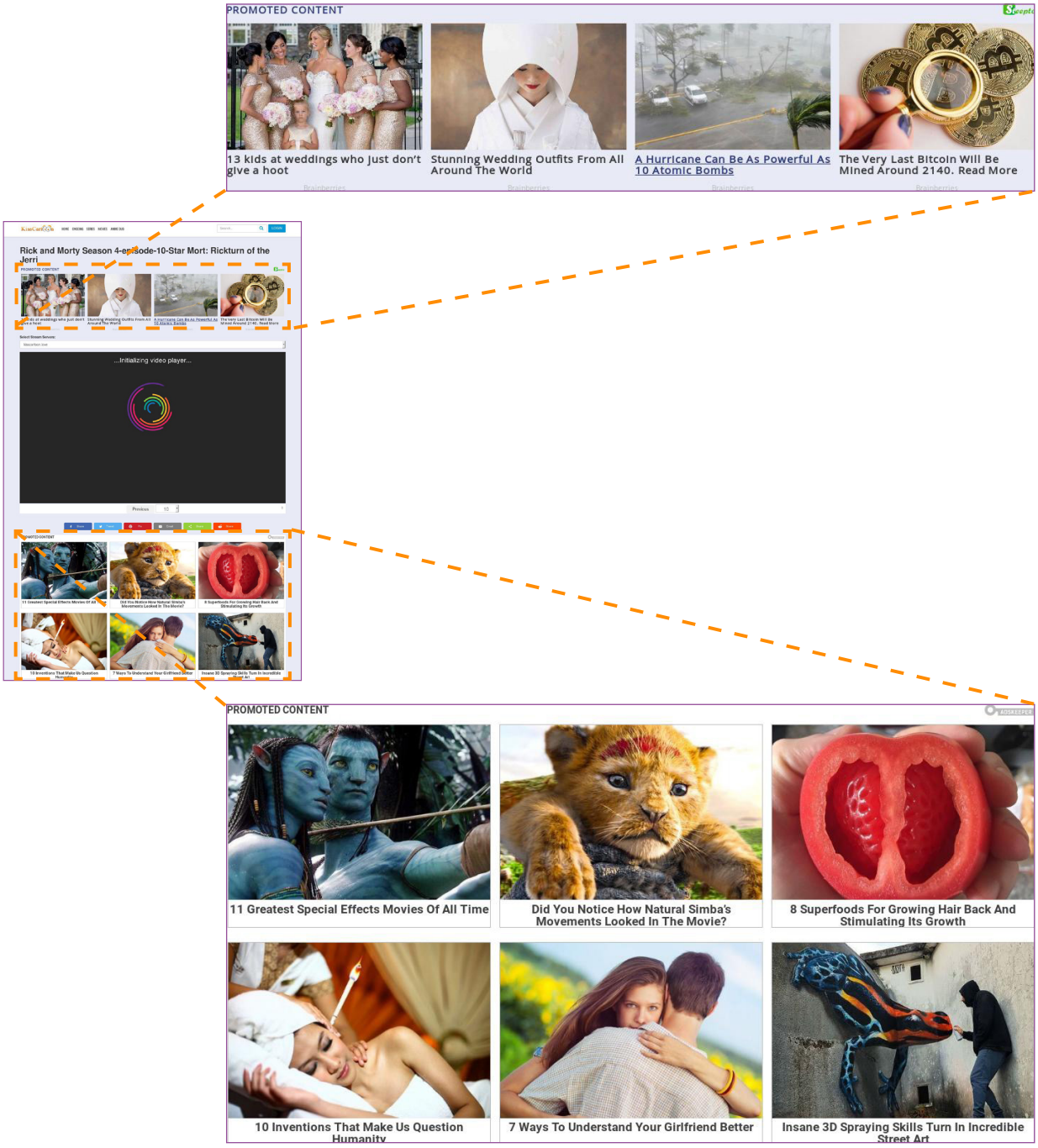
Types of Advertising on Piracy Websites

Figure 3. Breakdown by ad type on piracy websites.



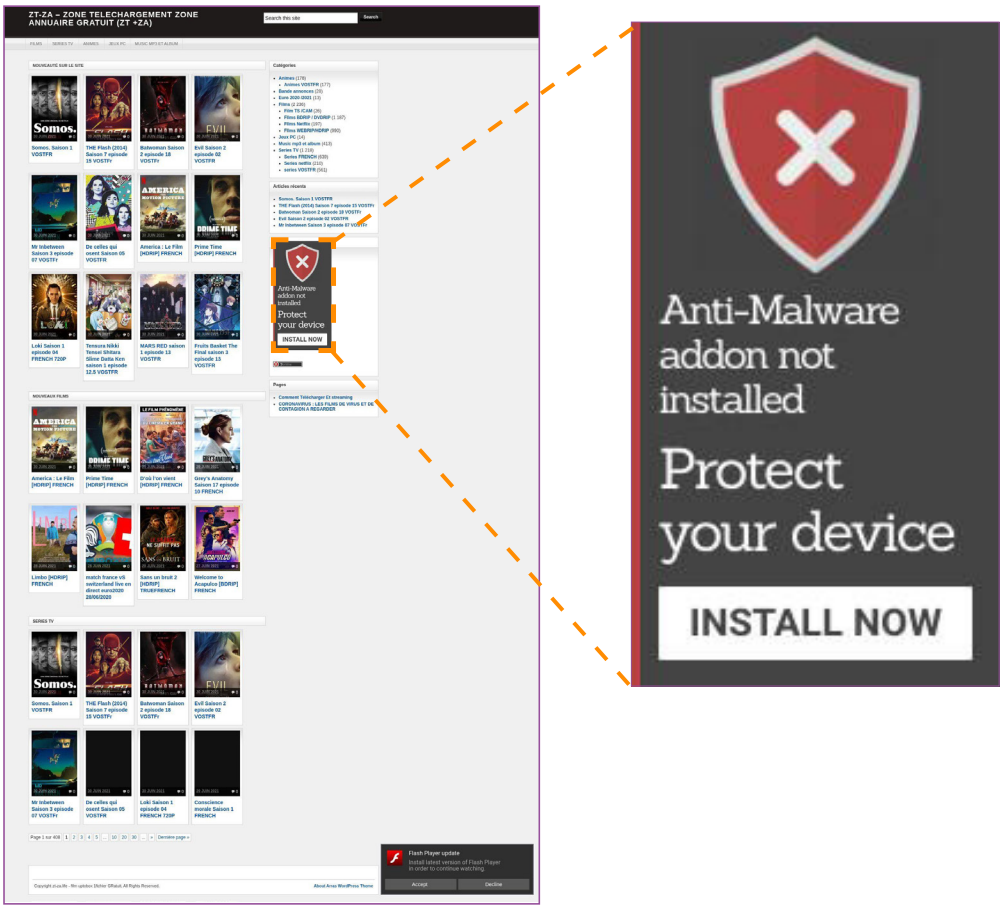
The largest segment of advertising on piracy websites, constituting 43 percent, was poor quality advertising known as "Sponsored Content." This can take the form of "clickbait," comprised of sponsored links embedded within images that are shown in advertising boxes alongside page content. These links tempt users to click on the image by blending promotions with what may appear to be gossip, a news story, or interesting video.

Figure 4. Two separate Sponsored Content ad boxes on piracy website kisscartoon.love. This website provides illegal streaming of the latest animated TV episodes including titles from Hollywood studios (e.g. Rick and Morty and Family Guy). The website, like many of the other piracy websites discussed in this report, has been determined by government authorities in one or more countries to be a copyright infringing website, and Internet Service Providers have been directed to block access to the website ("Blocking Order"). The first ad box has four separate sponsored links delivered by the Ad Tech company Steepto. The second ad box has six separate sponsored links delivered by the Ad Tech company AdsKeeper. Each of the images takes users to different web locations and generates revenue for the website owner.



One in 12 ads seen on piracy websites were not only low quality, but actually risky to consumers. These included misleading or fake ads that misrepresent content in order to elicit a click that generates revenue for both the publisher and the ad serving entity, or were ads simply loaded with malware. One such ad appears below; other examples are cited later in the report.

Figure 5. Malicious ad on piracy website zt-za.live, which is subject to a Blocking Order in France. This website provides downloads of the latest movies, games, ebooks and TV series. The ad purports to assist the visitor by suggesting a security installation be added. Code behind the ad reveals this is not a legitimate security add-on, but belongs to WebSecurerr, a browser hijacker and redirect virus. It generates revenue from triggering unwanted pop-up ads and by theft of personal and confidential data, including for sale to hackers. Installing the software tool not only redirects searches but also slows downs computer performance and modifies the computer registry causing system crashes.



Major Brand advertising on piracy websites (discussed in detail in the next section) represented a modest segment of their advertising revenue, but the massive volume of over $1 billion in overall advertising revenue means that a small percentage is still quite lucrative. "Adult" advertising, including sex games and "XXX" offerings, represented 17 percent of advertising on piracy websites.

The remainder of the advertising on piracy websites came from "Other Brands" (27 percent). These are lesser-known brands that do not fall into the other categories and likely have less reputational concern than the Major Brands do about their ads appearing on piracy websites. Many of these ads are low quality and include promotions for free online games, obscure online casinos, and relatively unknown virtual private networks (VPNs). It is not surprising that VPN advertising represented nine percent of ads in the Other Brands category: visitors to piracy websites often wish to hide their identifying IP address, so shady VPNs likely intentionally target this audience.

Types of Advertising on Piracy Apps

The makeup of advertising on piracy apps was quite different. In this app world, Major Brands had a significant presence, representing a quarter of all ads. Only advertising by lesser-known brands, such as obscure gaming and blog ads, made up a larger portion (54 percent).

Figure 6. Breakdown by ad type on piracy apps.

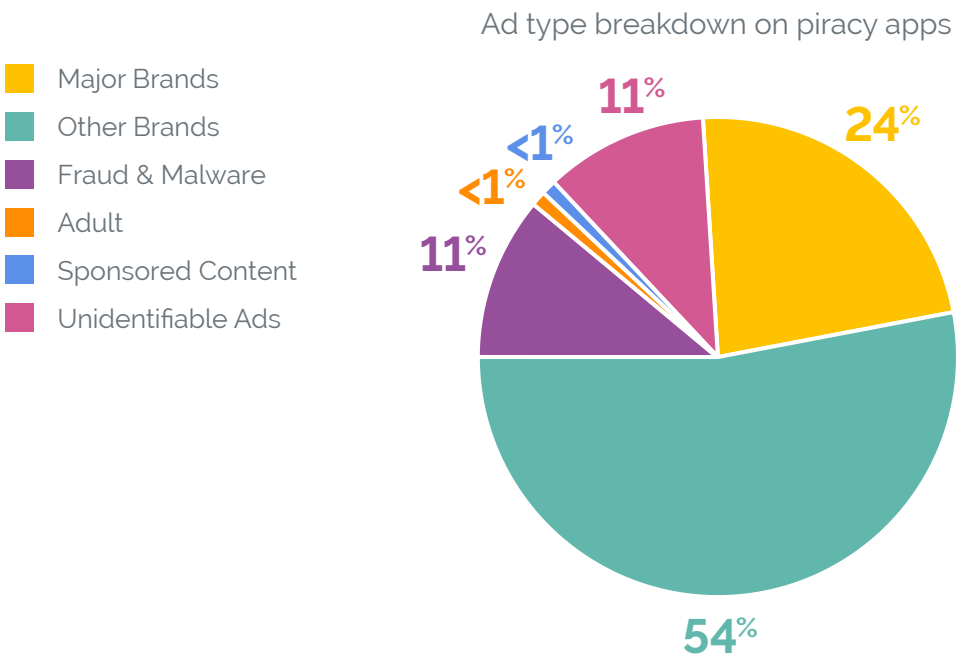
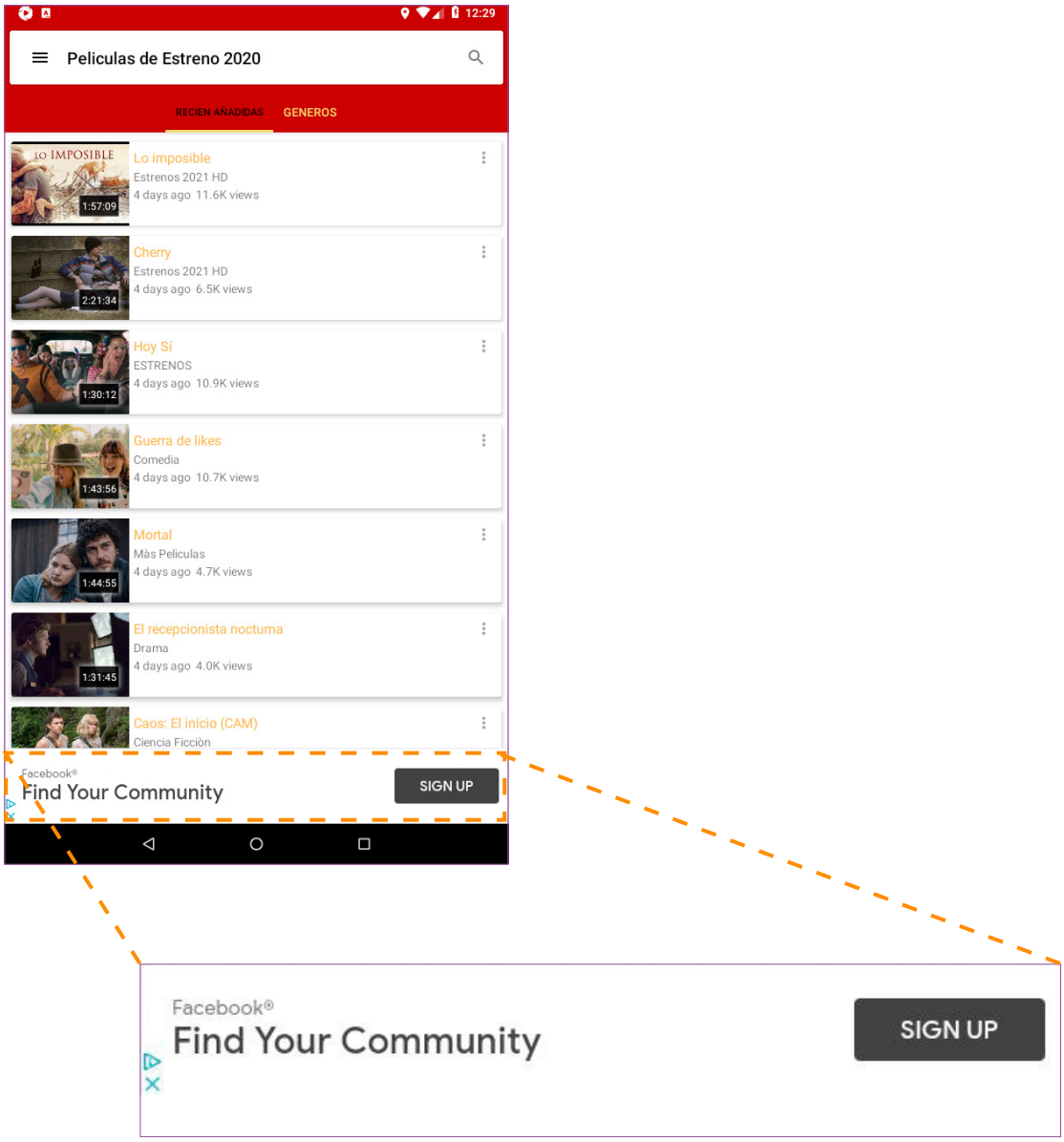


Figure 7. Facebook ad on piracy app Peliculas de Estreno 2021. This app allows users to stream pirated movies, and is on industry-wide infringing app lists, including TAG's "Piracy Mobile App List" ("PMAL").



Fraud and malware also had a foothold, comprising one in nine ads on these apps. Interestingly, adult-themed advertising and Sponsored Content ads had yet to develop any significant presence (less than one percent each of ads).

Part II. A Deeper Dive into the Key Players in the Piracy Ecosystem

Major Brands

Major brand advertising on piracy websites and apps is a $100 million problem. That's the projection of how much operators made in the last year from Major Brands alone, based on White Bullet's analysis of the piracy advertising ecosystem. But it's not just an issue of dollars and cents.

The appearance of ads for Major Brands on piracy websites and apps is beneficial to pirate operators for two reasons. First, it provides them revenue. Because the pirates pay nothing for the products they offer, even a small amount of ad revenue to a website can keep it profitable and provide an incentive for pirate operators to persist with their criminal activity. Second, advertising by Major Brands lends a veneer of legitimacy to the pirate website or app. Ads for Major Brands appearing on a website or app with a professional-appearing user interface may lead a consumer to believe that the publisher is an authorized distributor of such content, and not part of a criminal organization.

While Major Brands represented only four percent of ads on piracy websites, given the size of the market, it still amounts to significant money. Although not a precise projection, four percent of $1.08 billion amounts to roughly **$40 million.**

The situation on piracy apps is even more troubling. Major Brands made up one in four advertisements on these apps. That would extrapolate to roughly **$60 million or more in ad revenues** for the operators of these piracy apps.

The fact that these criminals are making **as much as $100 million annually from Major Brands** should be of concern to all involved in the advertising industry.

How that Major Brand advertising flows to pirate operators has changed over the years, and now depends on whether the operator is running a website or an app.

Major Brands and Piracy Websites

In 2014, Digital Citizens investigated how advertising drove piracy profits on websites with its report, "Good Money Gone Bad." In that study, Digital Citizens showed how the largest piracy websites generated average advertising revenues of $4.4 million annually, with profit margins of 80 percent or more. In addition, the report highlighted how nearly 30 percent of piracy websites at that time carried ads for blue-chip brands.

Since that report, the digital ad industry has mounted a campaign to reduce Major Brand advertising on piracy websites. Advertising industry efforts included the creation of an industry association focused on piracy and other chronic problems in digital advertising (the Trustworthy Accountability Group or "TAG"), widespread adoption of "Do Not Advertise" lists that included piracy websites, and ongoing alerts to brands found advertising on piracy websites, such as TAG's Project Brand Integrity.

Now, only four percent of ads on piracy websites come from Major Brands. Nevertheless, the industry's success to date with keeping Major Brands off piracy websites does not mean that the legitimate advertising ecosystem can relax its vigilance (see figures 8a and 8b for examples of Major Brands on piracy websites).

Amazon is a good example of both the problems that can occur when a brand lets down its guard and the results that can be reached when it devotes resources and attention to the problem. Amazon ads had been appearing with disturbing regularity on piracy websites. Since Amazon was alerted to this issue by TAG in early **2021 there has been a 78 percent decline in advertising placed by Amazon on piracy websites**, highlighting the effectiveness of outreach and engagement.

Figure 8a. Ali Express ecommerce ad on piracy website freefilm.to. This website allows visitors to stream pirated movies for free including latest Hollywood studio releases.

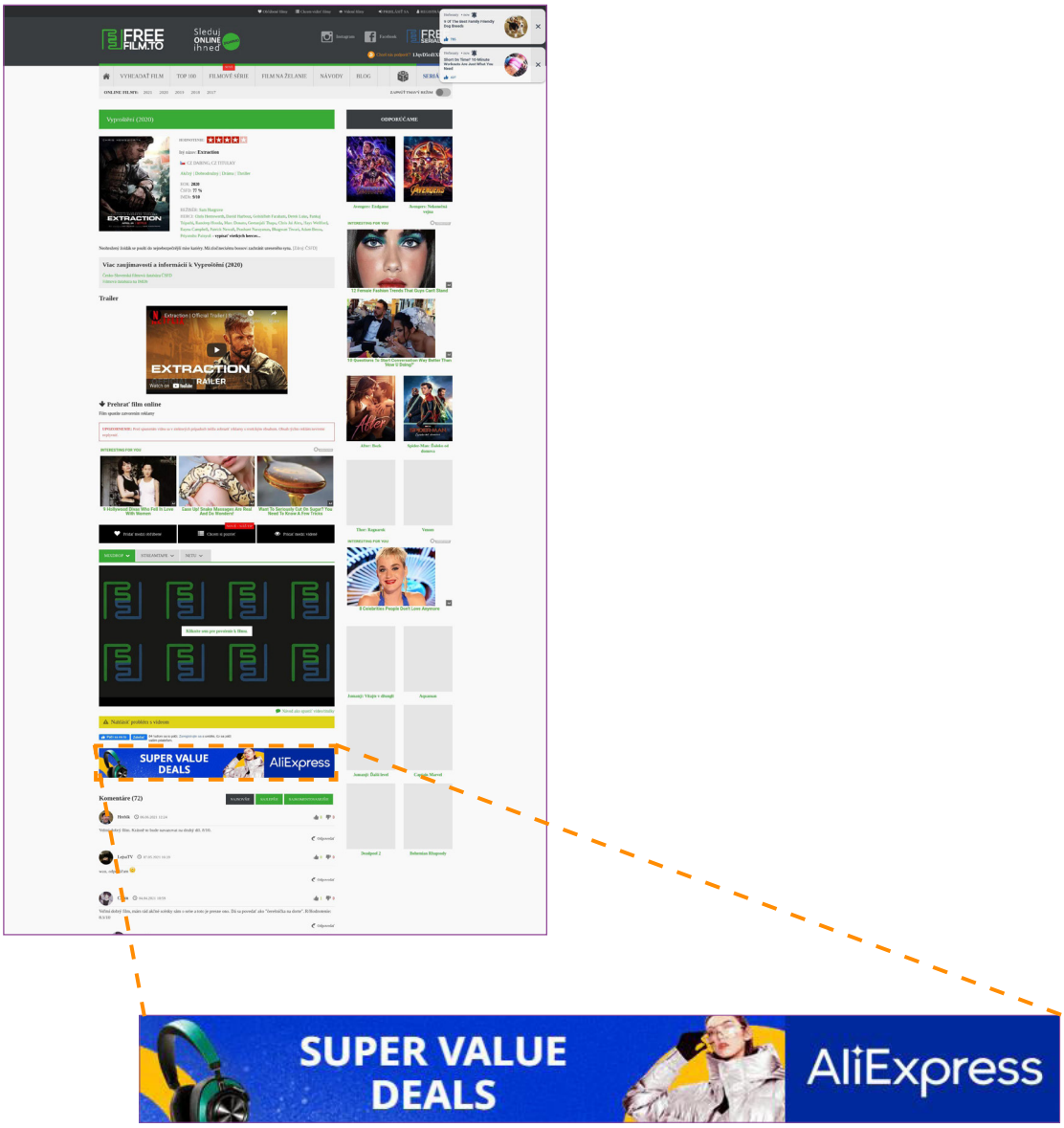
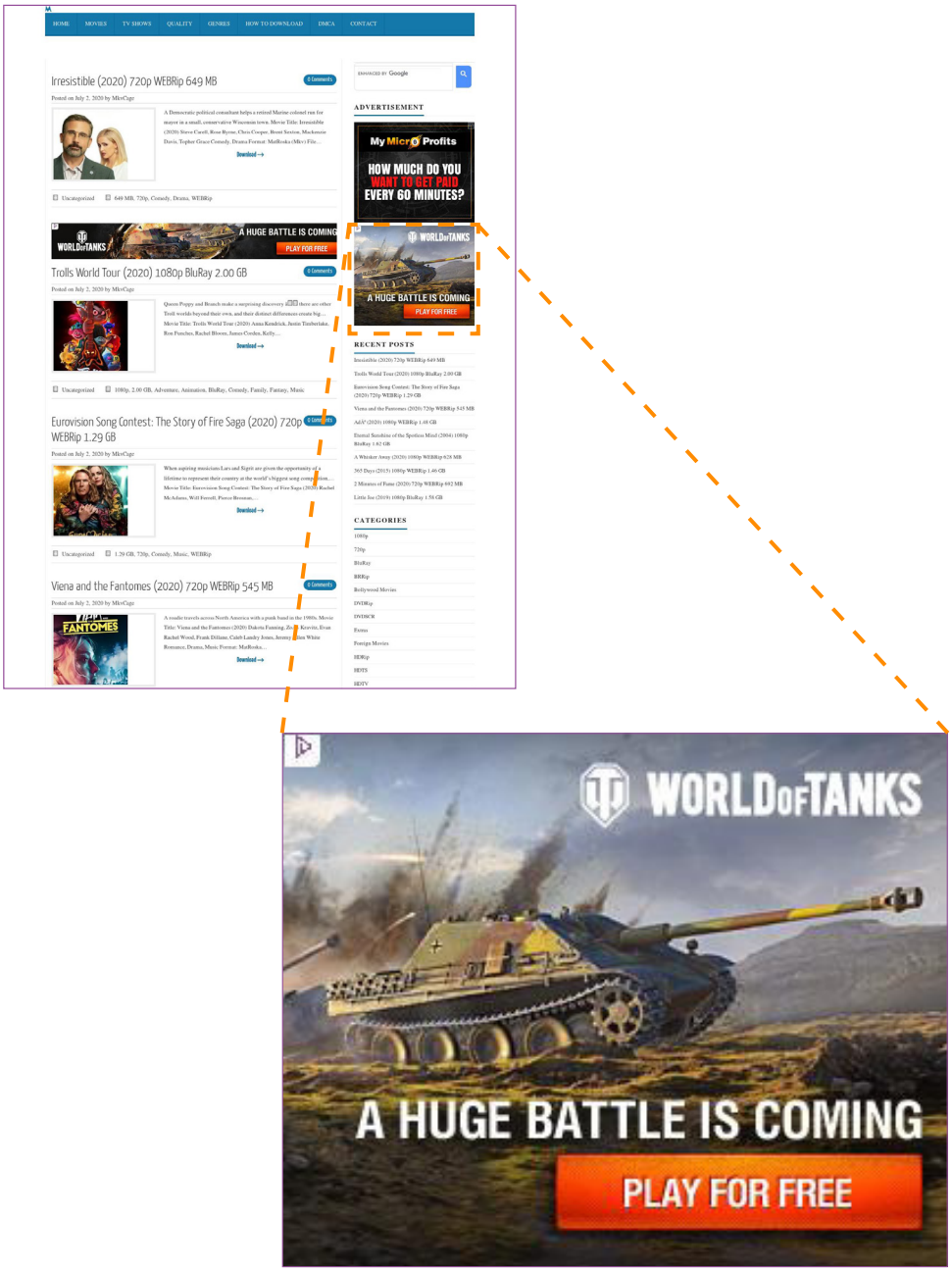


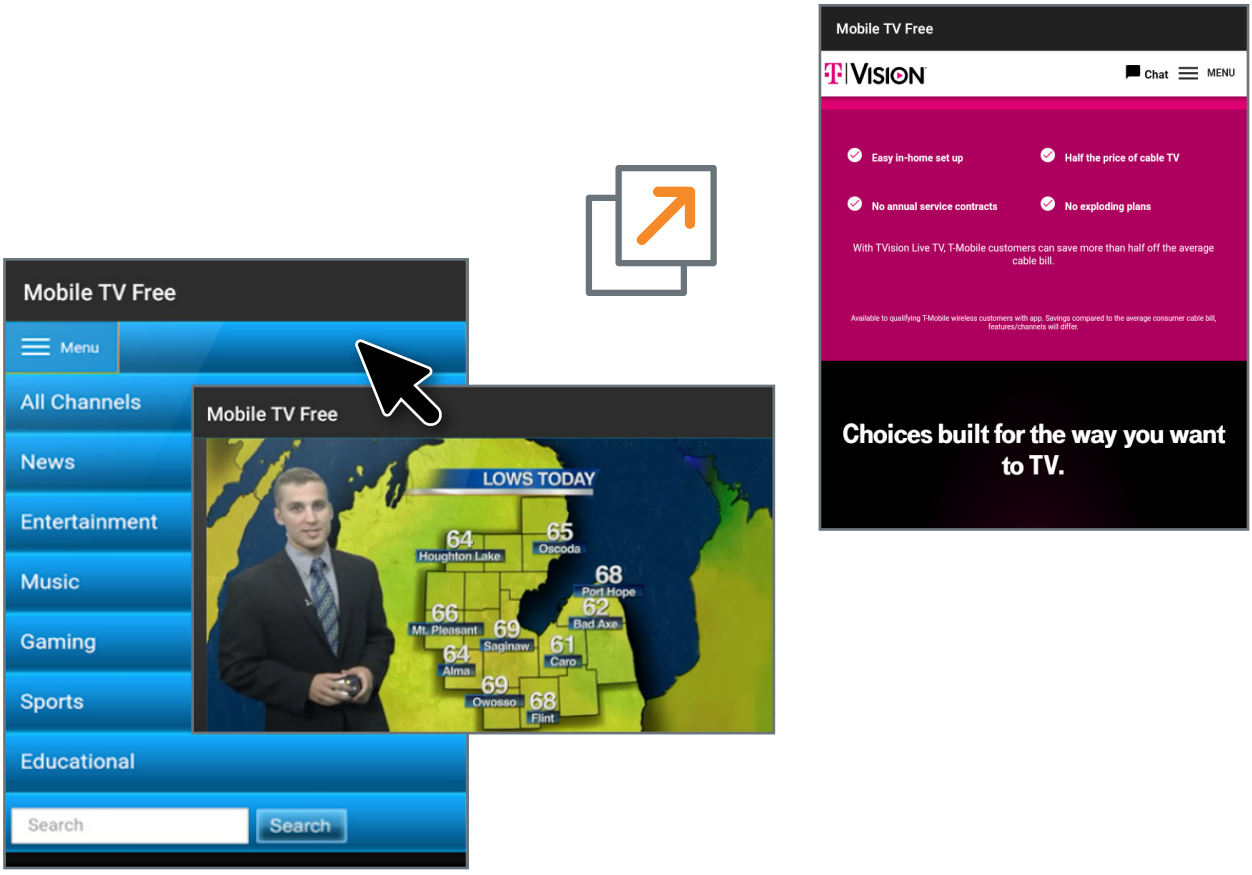
Figure 8b. Wargaming online gaming ad on piracy website mkvcage.site.



Major Brands And Piracy Apps

In-app advertising is a particularly attractive market for brands because mobile devices generally belong to a single person, making it easier to identify an individual and their ad preferences. In addition, fewer ad blocking technologies exist in the app ecosystem so ads in an app are more likely to be delivered and seen. The trend towards app usage continues to accelerate. For example, in the United States the average user spends 90 percent of their mobile time in apps versus the mobile web, so landing Major Brand advertising will be an increasingly attractive revenue source for pirate app operators.

Figure 9. T-Vision (T-Mobile) full-screen pop-over ad on piracy app Mobile TV Free, which features pirated local TV streams. This app provides unauthorized streaming to over 200 US TV channels and is on industry-wide infringing app lists, including PMAL.



The chart below sets out the top five Major Brand advertisers on piracy apps:

Figure 10. Top five Major Brands by percentage of ad volume of all Major Brands identified on piracy apps.

Rank	Brand	% of Major Brand Ad Volume
1	Amazon	41%
2	Facebook	27%
3	Google	5%
4	Vimeo	3%
5	Start.io	2%

Top Ad Spenders on Piracy Apps: Amazon, Facebook, and Google

All brands are susceptible to occasional instances that land their ads on a pirate app, especially since the process and entities that place ads on apps are different from those on websites. Many major digital advertisers, however, almost never appear on piracy apps, suggesting that their processes for protecting their brands are comprehensive and effective.

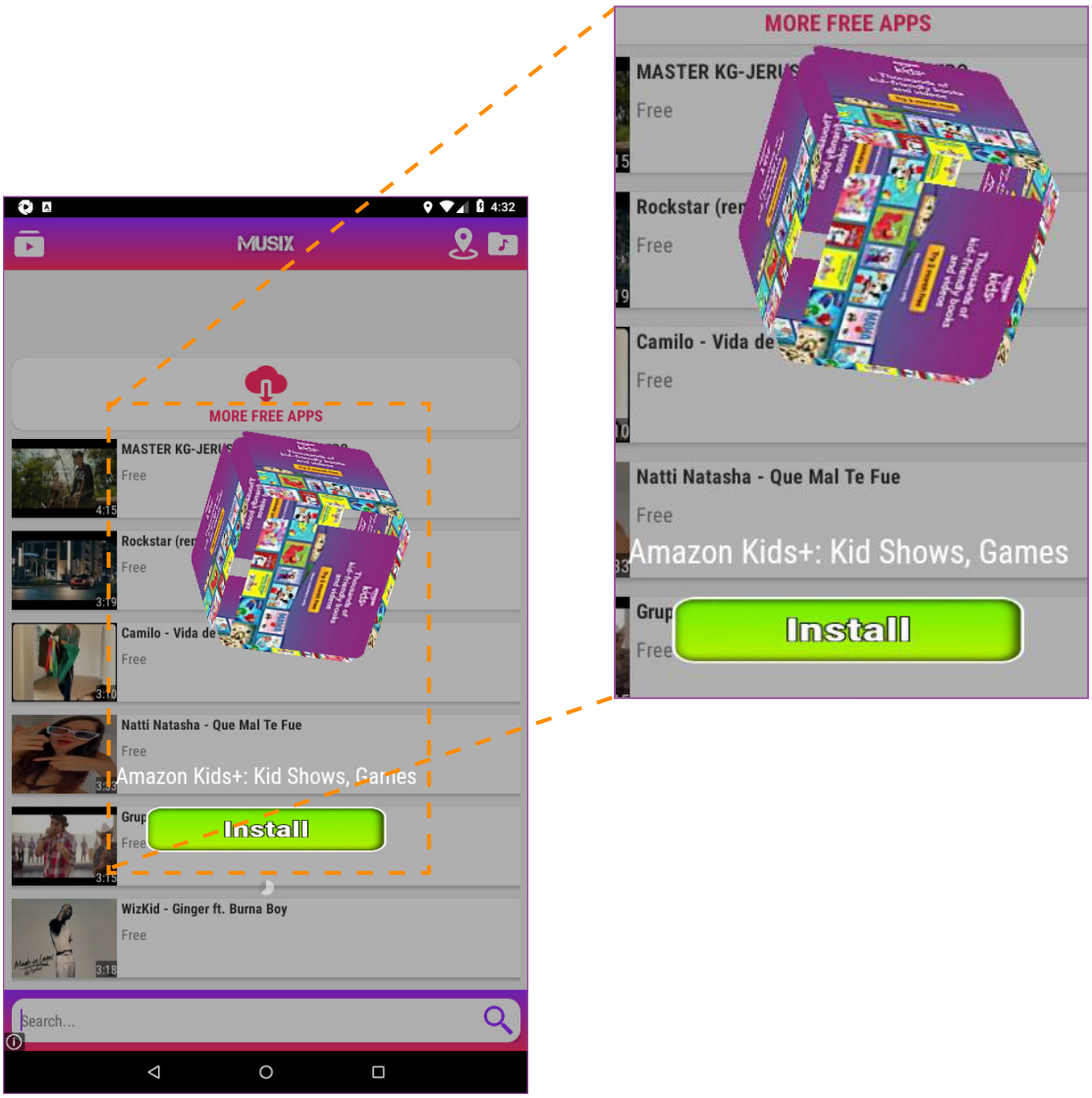
By contrast, three of the most profitable and sophisticated companies in the world with unparalleled knowledge about how the online advertising ecosystem works were the top three dominant advertisers on piracy apps during the study. These companies were: Amazon, Facebook, and Google.

These three companies together accounted for 73 percent of all Major Brand advertising appearing on piracy apps during the study. Given that ads on piracy apps generated $259 million annually, it is safe to conclude that **piracy app operators may potentially have made tens of millions of dollars from ads from just these three companies during the period analyzed.**

Digital Citizens shared high-level findings from the report with Amazon, Facebook, and Google.

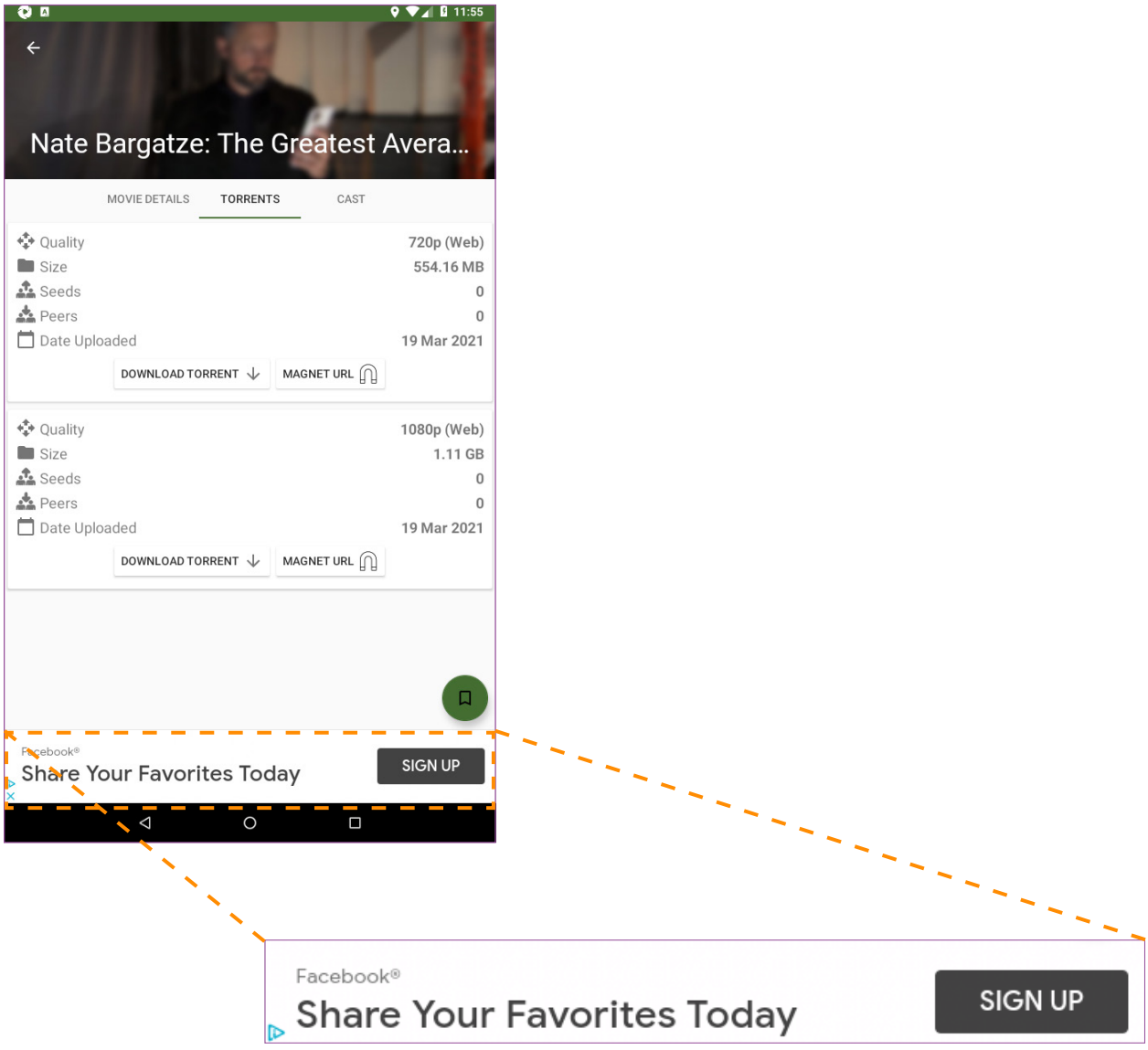
Amazon, the most valuable company in the world with revenues of over $385 billion, was the number-one Major Brand appearing on piracy apps. Two out of every five Major Brand ads that appeared on piracy apps during this investigation were for Amazon. At one point, Amazon accounted for 12 percent of all ads (major or otherwise) that appeared on piracy apps. **However, Amazon has clearly taken steps to address the issue – witnessed by a 57 percent decrease since January 2021 in its advertising showing up on these apps.** Given its efforts to remove its ads from both piracy websites and apps, Amazon deserves credit for taking the issue of ad-supported piracy seriously after it was brought to its attention.

Figure 11. Amazon Kids+ ad on piracy app My Muzik. This app allows users to illegally stream music titles and is on industry wide infringing app lists, including PMAL.



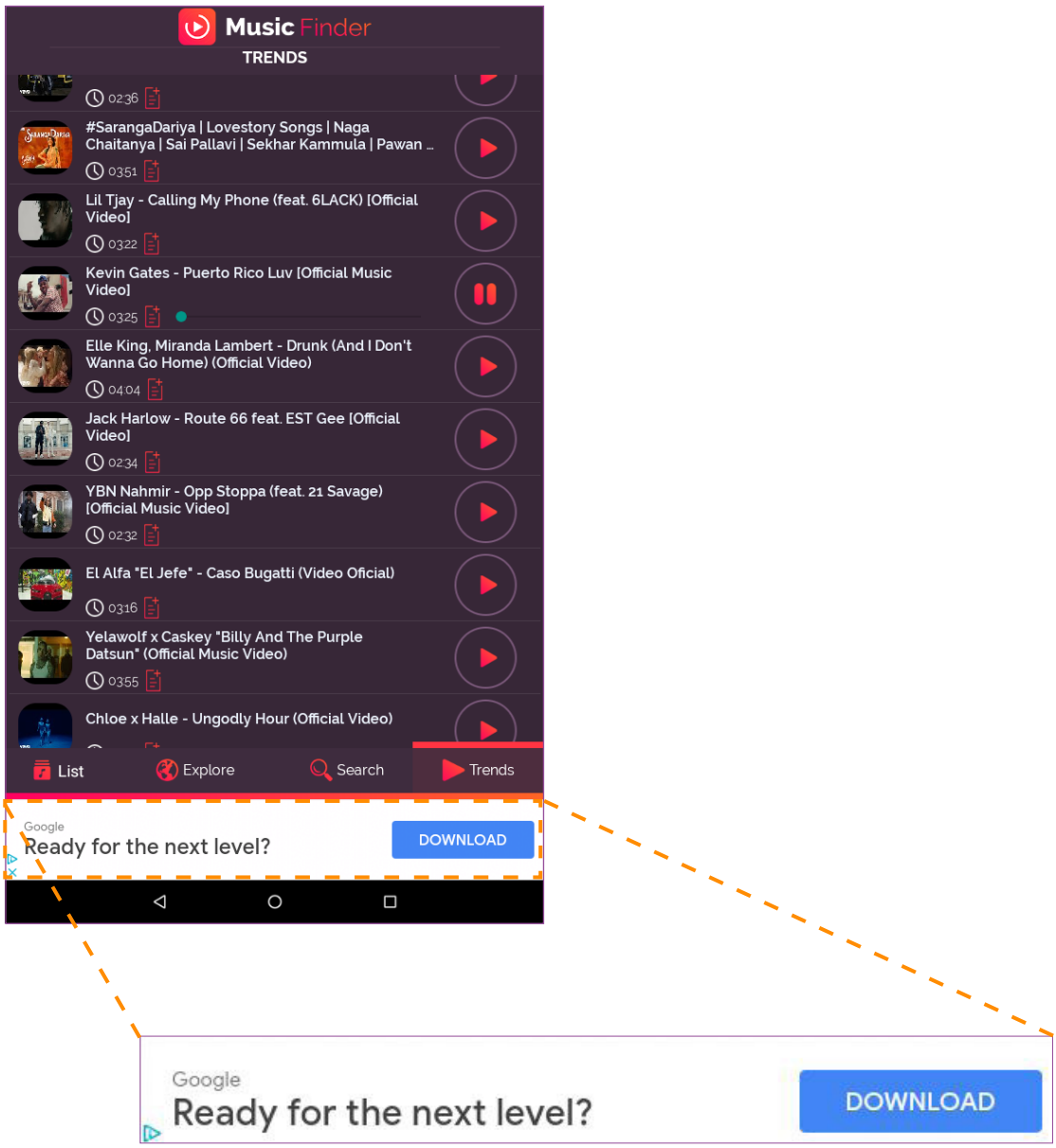
Similarly, Facebook, which should be expected to be savvy about digital advertising, made up about one in four (26 percent) of Major Brand ads on piracy apps.

Figure 12. Facebook ad on piracy app YTS Movies. This app allows users to download pirated movies and TV series.



Rounding out the piracy advertising triumvirate is Google, which accounted for five percent of Major Brand advertising on piracy apps.

Figure 13. Google ad served by Google's own ad system on piracy app Music Finder. This app allows user to illegally stream music and is on industry-wide infringing app lists, including PMAL.



Google, in fact, is in a class all by itself because it's both a major advertiser and plays a dominant role in the buying and selling of ads themselves. Google's unique role in advertising, including how it appears to fund and facilitate piracy apps, is spotlighted later in the report.

These revelations spur a question that only the companies themselves can answer: does it matter to them that their brands are associated with illegal activities?

If so, they can work more diligently with advertising agencies and Ad Tech entities to ensure that their ads don't appear on piracy websites and apps. Many solutions now exist and are being effectively used, as discussed in the conclusion to this report.

If brands do not make reasonable efforts to stay off piracy websites and apps, then time will tell if they pay the price for their apparent willingness to associate their brand with criminals and illicit online operators.

Pirate Operators – The Criminals And Their Tactics

While most brands take steps to keep their ads off piracy websites and apps, pirate operators work to obtain ad revenue by contravening these efforts and gaming the system.

While piracy is a crowded field, with a large number of operators peddling piracy, White Bullet's investigation found the players and market dynamics have changed in recent years.

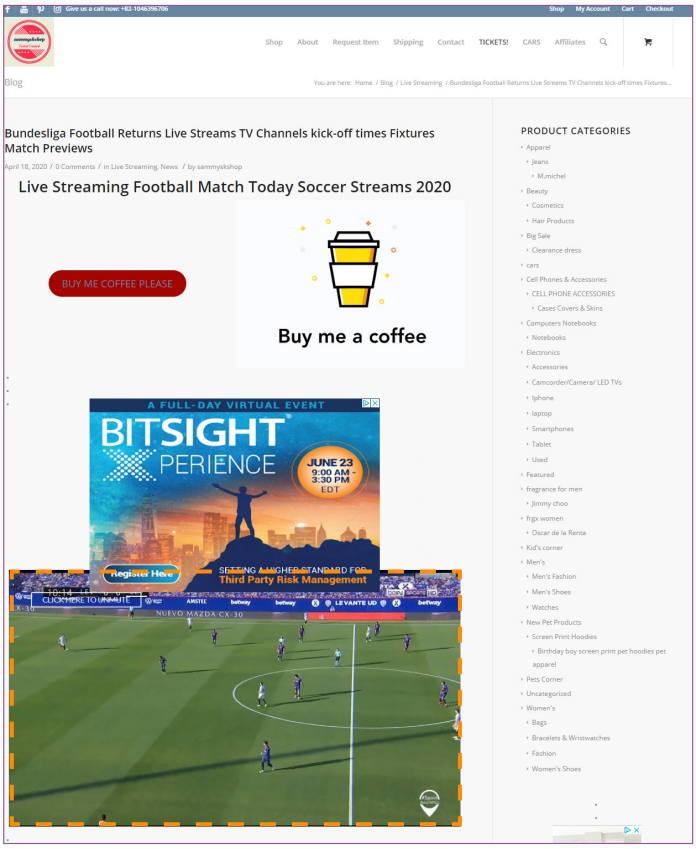
The dominant players of the past, such as MegaUpload and The Pirate Bay, are either shut down or greatly diminished. While the key players today may be less well-known, just like their predecessors they enjoy robust profits from advertising. As noted above, **the top 10 highest-earning pirate operators (combined top five piracy websites and top five piracy apps) collectively generated over $229 million in global annual revenues from advertising during the period analyzed**.

Regardless of their size or notoriety, the modus operandi of pirate operators is the same: they strive to maximize profits from all aspects of digital advertising by warping the tools of the legitimate advertising market to obtain ads never meant to be placed on their websites.

The digital advertising ecosystem is complex, and pirates take advantage of that complexity. It is challenging for brands to audit all their daily bid transactions to check which may have been served to piracy websites and apps. Pirates count on a lack of audit transparency to hide among billions of legitimate placements.

Additionally, many pirate operators use a host of techniques to disguise their illicit activities to elicit ads. For example, they often name their websites and apps in a neutral manner to avoid raising suspicion by generic brand safety verification tools, or change their name frequently to avoid suspicion and evade being added to "Do Not Advertise" blocklists. When visitors go to a pirate domain, it may automatically redirect them from known piracy websites and apps (where ads are blocked) to innocent-sounding publishers where the ads will be placed and the pirate will still profit. And a few even create fake innocent-looking content and then inject pirate content for limited periods at certain times, driving traffic to these specific webpages through timed social media promotions.

Figure 14. Webpage temporarily streaming a pirated soccer game injected into sammyskshop.com – an online clothing and electronic store.



But pirate operators go beyond naming trickery; they engage in outright ad fraud to make money. This may include use of "pixel stacking," where ads are compressed to 1x1 pixel size, invisible to the naked eye, and stacked in layers of hundreds of repeated ads. White Bullet has identified evidence of such fraud on piracy websites in the past, which permits pirate operators to get paid for ads that no human ever views.

Beyond manipulating the infrastructure, pirates also rely on "malvertising" to boost their coffers. This term includes fake branded ads, fraudulent promotions, and deceptive images that misrepresent the content behind them and may actually trigger the download of malware on the user's computer.

Fraud, malware, and piracy have been linked for years, and White Bullet found a robust and lucrative market where pirates peddle fraudulent and malicious ads for profit. Roughly one in three piracy websites and apps analyzed during the study carried such malvertising and exposed consumers to risk.

During the study, many ads were identified that triggered a range of malware. This included annoying "adware" - software that automatically displays or downloads advertising when a user goes online. But they also included dangerous "browser hijackers," which change a user's homepage and default search settings as a means to control viewing paths, typically receiving commission for being attributed to new traffic. The malware may also redirect users' browsers to specific ads, typically for unwanted browser extensions, surveys, adult websites, online web games, fake software updates, and other unwanted programs. These in turn can introduce additional malware to the user's environment.

In addition to browser hijackers, White Bullet found ads hiding "keyword loggers," which trace usernames and passwords for later sale or use for hacking. They also found "Trojans," which can deliver a range of payloads, including opening backdoors to steal data from computers.

Malicious advertising can be highly lucrative for a publisher. The purveyor of the malware not only pays the publisher for placing the ad, but may also provide additional commission for every resulting malware infection or fraudulent installation. In this way a complex symbiosis develops between piracy and malware that ultimately harms both consumers and rights owners. Below are several examples of malicious ads designed to dupe consumers and maximize pirate profits.

Figure 15a. Malicious ad served by REKMOB on piracy website layarmovie21.xyz, which is subject to a Blocking Order in Asia. Code behind the ad reveals this is not a legitimate prize offering. The "Win iPhone X" pop-ups are a social engineering scam that tries to trick users into completing different surveys with an offer of winning an iPhone, and then asks them to subscribe to different paid services. These "Win iPhone X" fake messages are not from Apple, but rather from a scam group which tricks users into subscription services from which they cannot unsubscribe, as well as stealing personal information.

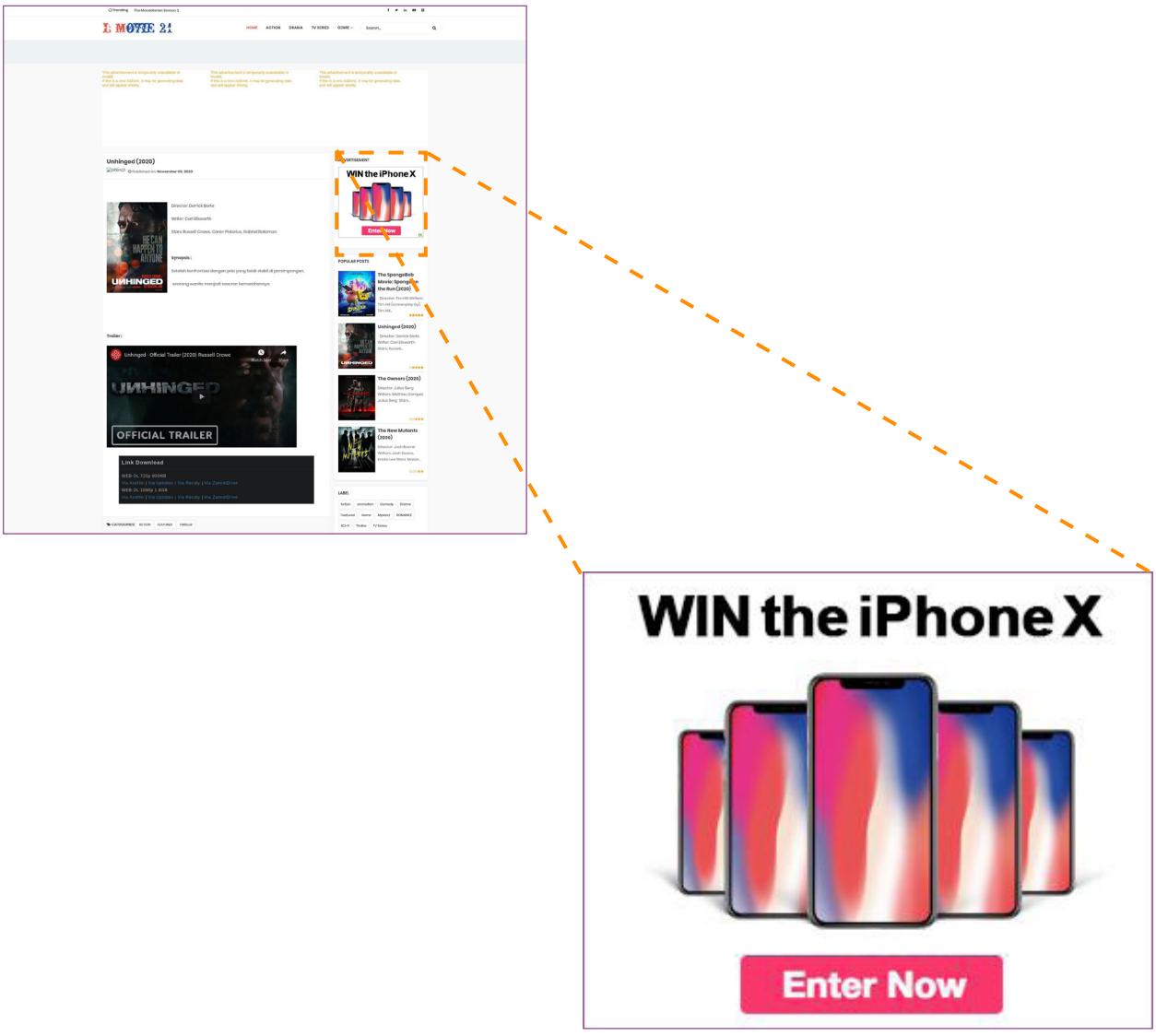
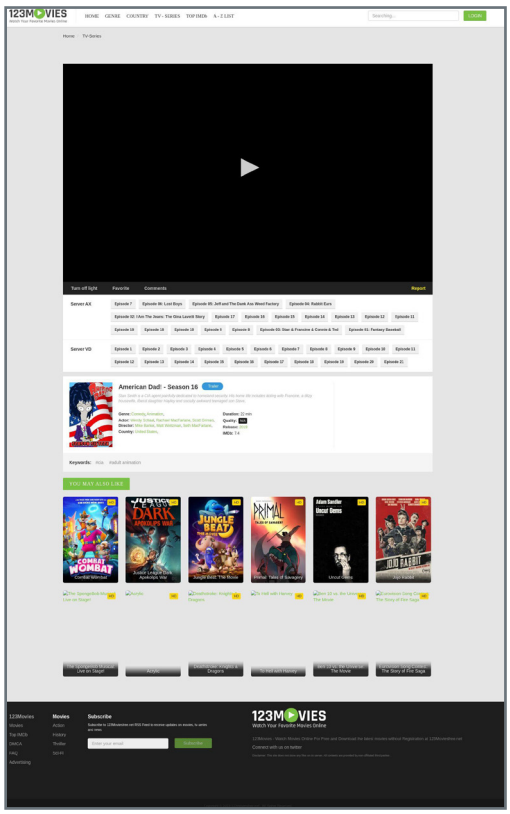


Figure 15b. Malicious pop-under ad served by a string of anonymized Ad Tech entities on piracy website 123moviesfree.net, which is subject to Blocking Orders in Europe and Australia. Code behind the ad reveals this is not a legitimate prize offering. The "You've made the X-billionth search" page is a browser-based phishing scam intended to collect personally identifiable information by fraudulently appearing to be Google offering a tech prize (e.g. Samsung Galaxy, MacBook Pro, iPhone) in return for completing a survey. If users complete this survey, they are asked to enter personal information such as credit card details, email, and home address, or to subscribe to unneeded paid services. No prize is ever delivered, but the personal data is likely sold to brokers.



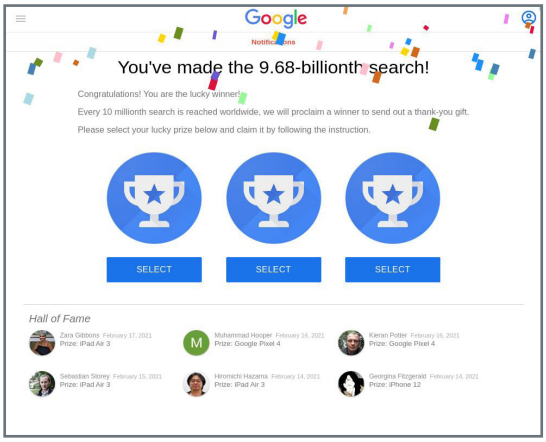
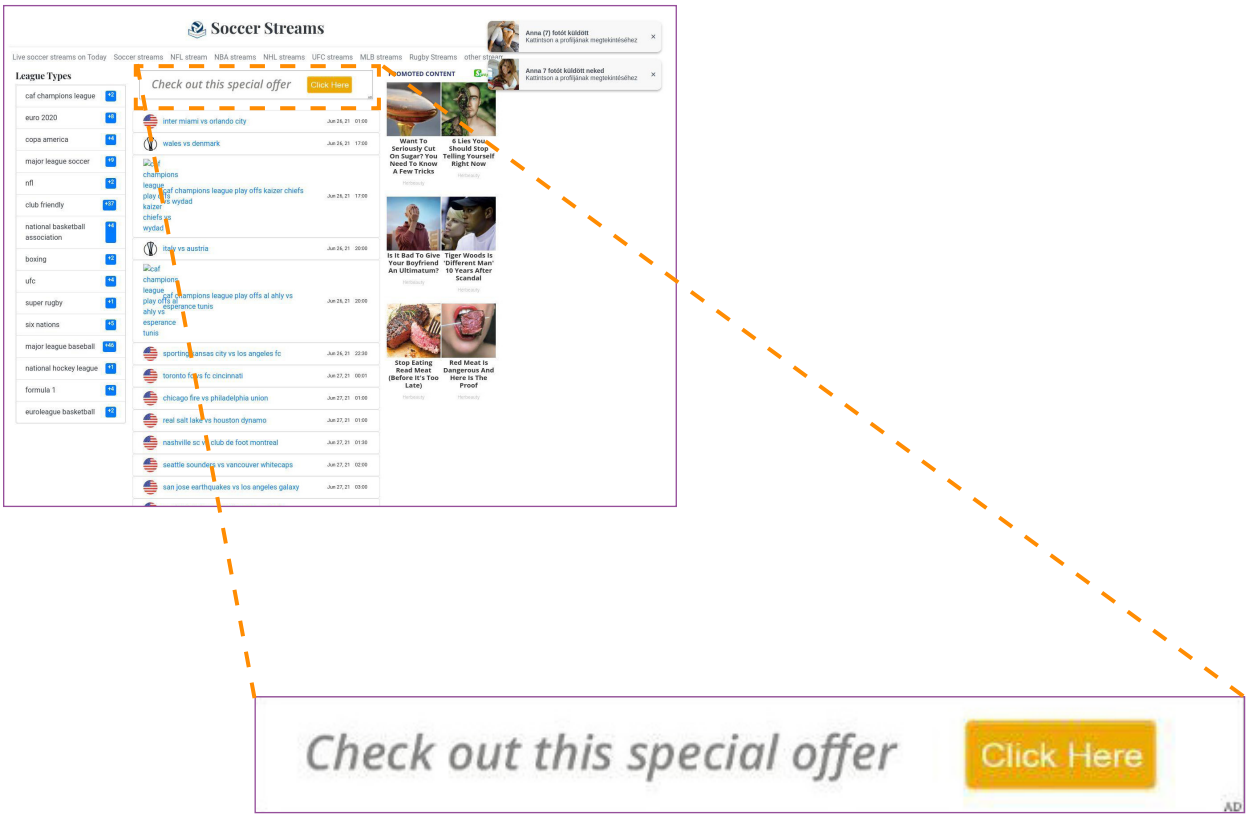


Figure 15c. Researchers found on the piracy website fomny.com (left), which is on the UK City of London Police IP Crime Unit's Infringing Website List and is subject to Blocking Orders in Asia, a malicious ad served by bestaryua.com (right). Analysis of the ad reveals this is not a legitimate sign-up page to a service. Instead, the visitor who clicks on the ad is redirected to a bestaryua.com landing page, which then further redirects users to websites that offer PUPs (potentially unwanted programs), scams, and general riskware such as backdoor Trojans, which open the user's environment to other risk and infection.

Figure 15d. Malicious ad served by Ad Tech company Revenuehits on piracy website soccerstreams100.net, which is subject to a Blocking Order in Russia. This website provides pirate streaming of live US sporting events. Code behind the ad reveals this is not a genuine special offer. Clicking on the ad/offer installs a risky adware program redirecting to clcksite.com with undesirable and intrusive pop-up ads that slow down the user's system. In addition, unwanted malicious programs and redirects may be offered through these ads that install malware or execute scripts that download and install malware behind the scenes. Malicious programs can record consumer keystrokes, logging data such as usernames and passwords including bank logins, with developers sharing such confidential data with hackers.



Ad Tech – The Enablers

Pirate operators would not be able to reap $1.34 billion in advertising revenues without the help of key players who sit at the center of the ad ecosystem. These Ad Tech companies are the ones who broker the ad space, coordinate the ad bidding, and serve the ads themselves – taking a cut on every sale of ad space.

While the identity of the Ad Tech entity that placed a specific ad online is not readily apparent to a user, White Bullet's technology is able to extract the code behind each ad on piracy websites and apps that it finds. By this process, it is able to identify from that code which Ad Tech entities have been involved in filling the ad space. Depending on the complexity of the brokering, more than a single party may be involved; however, the data always reveals who is behind the placement.

Most Ad Tech companies are responsible operators that have nothing to do with placing ads on pirate publishers, or only do so on rare occasions through deception by the publisher. However, several Ad Tech companies appear to live comfortably in both the legitimate world of advertising and at the fringes of the criminal world of piracy. Aside from a couple of household names, they are not well-known to anyone but the players in the ad ecosystem.

White Bullet has identified the Ad Tech entities that appear to have oversized roles in funding pirate publishers. They may do this by placing substantial volumes of legitimate branded ads on pirate publishers, or by placing risky advertising (fraud or malware ads) on piracy websites and apps.

The chief culprit in enriching piracy websites by risky ads during the study was an advertising network called Revenuehits. White Bullet found that a stunning 74 percent of risky ads on piracy websites were facilitated by Revenuehits. Revenuehits offers its services on a "self-service" basis to websites, allowing them to use its technology to facilitate automated filling of their ad space. Revenuehits is a subsidiary of intango - an Israeli media company offering a range of media and marketing services with offices in New York City and Tel Aviv. (For an example of a malvertising ad served by Revenuehits on a piracy website, see figure 15d.)

Pirates Scurry to the Ad Tech Boom

The rise of what is known as "programmatic" advertising, in which algorithms and data are leveraged to ensure targeted ads are rendered to visitors at lightning speed, has transformed the digital advertising space and been a driving force in the $129 billion global programmatic spend in 2020. The attraction of programmatic advertising is the ability to efficiently coordinate bidding and sale of ad space appearing simultaneously to millions of website and app visitors. When available data is aggregated, the top ten global brokers – or ad exchanges – facilitate over a trillion ad bid requests daily across all types of publishers. And as digital advertising matures, that number keeps rising.

Many companies, both new and well-established, have been attracted to the financial opportunities programmatic advertising brings. Some focus on the "buy" side (brands) and some on the "sell" side (publishers), while companies such as Google and Facebook have rapidly developed in-house capabilities to offer an apparently seamless advertising process for both buyers and sellers.

With fast-changing technology and many new entrants over the last years, the industry has struggled at times to coordinate regulation. Some companies have taken advantage of this lack of transparency to line their pockets from ad-funded piracy. With the largest pirate publishers having in excess of 800 million unique page views monthly, the revenue to be made from funding piracy quickly stacks up.

White Bullet identified several key Ad Tech companies enabling piracy on websites and apps.

Figure 16. Top five Ad Tech entities by percentage of ads served on piracy websites and apps during the study.

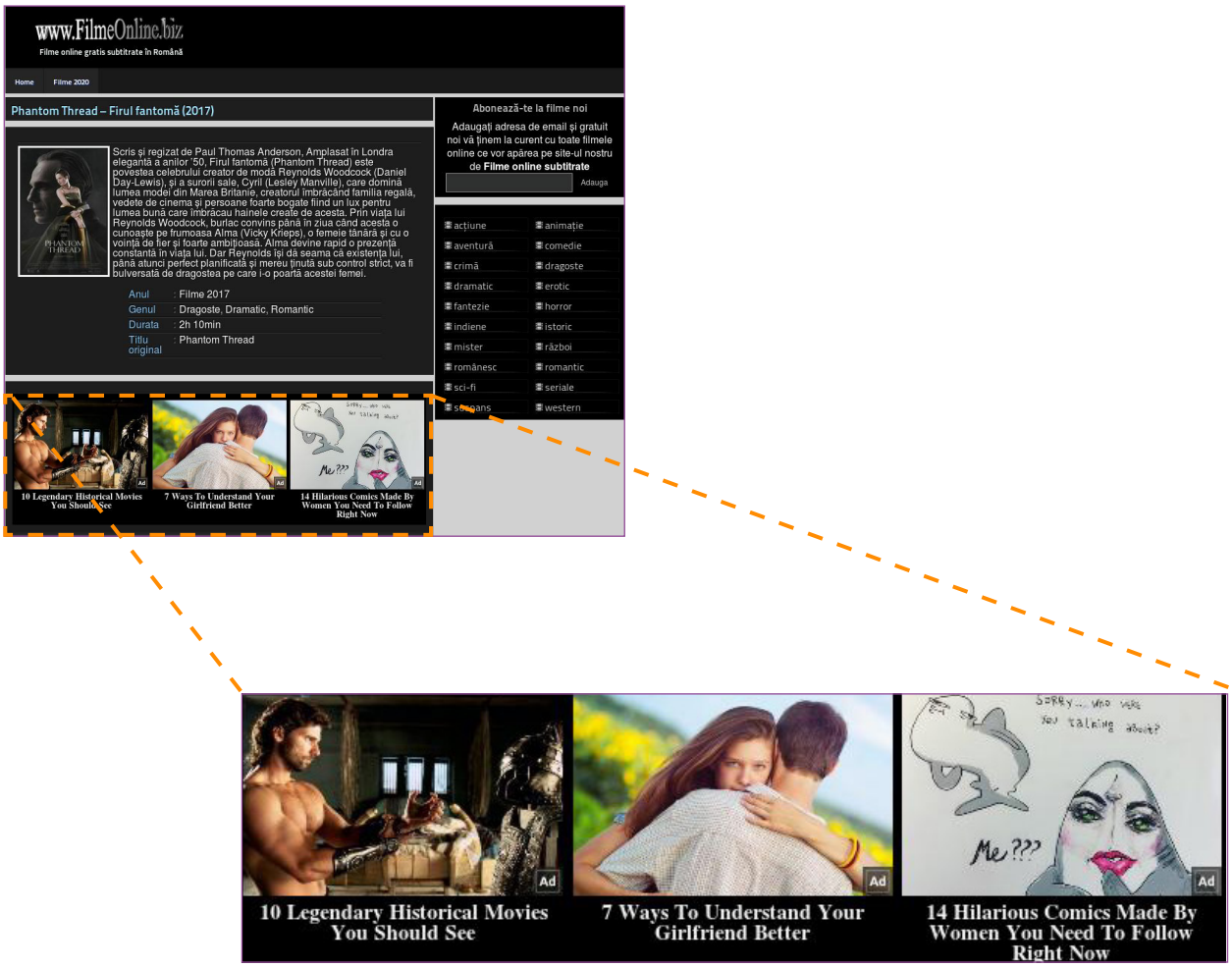
Piracy Websites		
Rank	**Ad Tech**	**% Of All Ads**
1	AdsKeeper	27%
2	RUNative	16%
3	Traffic Stars	9%
4	Bebi	8%
5	MGID	6%

Piracy Apps		
Rank	**Ad Tech**	**% Of All Ads**
1	Google CDN	38%
2	Start.io	34%
3	Google Ad Tech	13%
4	Rev Content	2%
5	3globalport.ru	1%

Piracy websites and Ad Tech

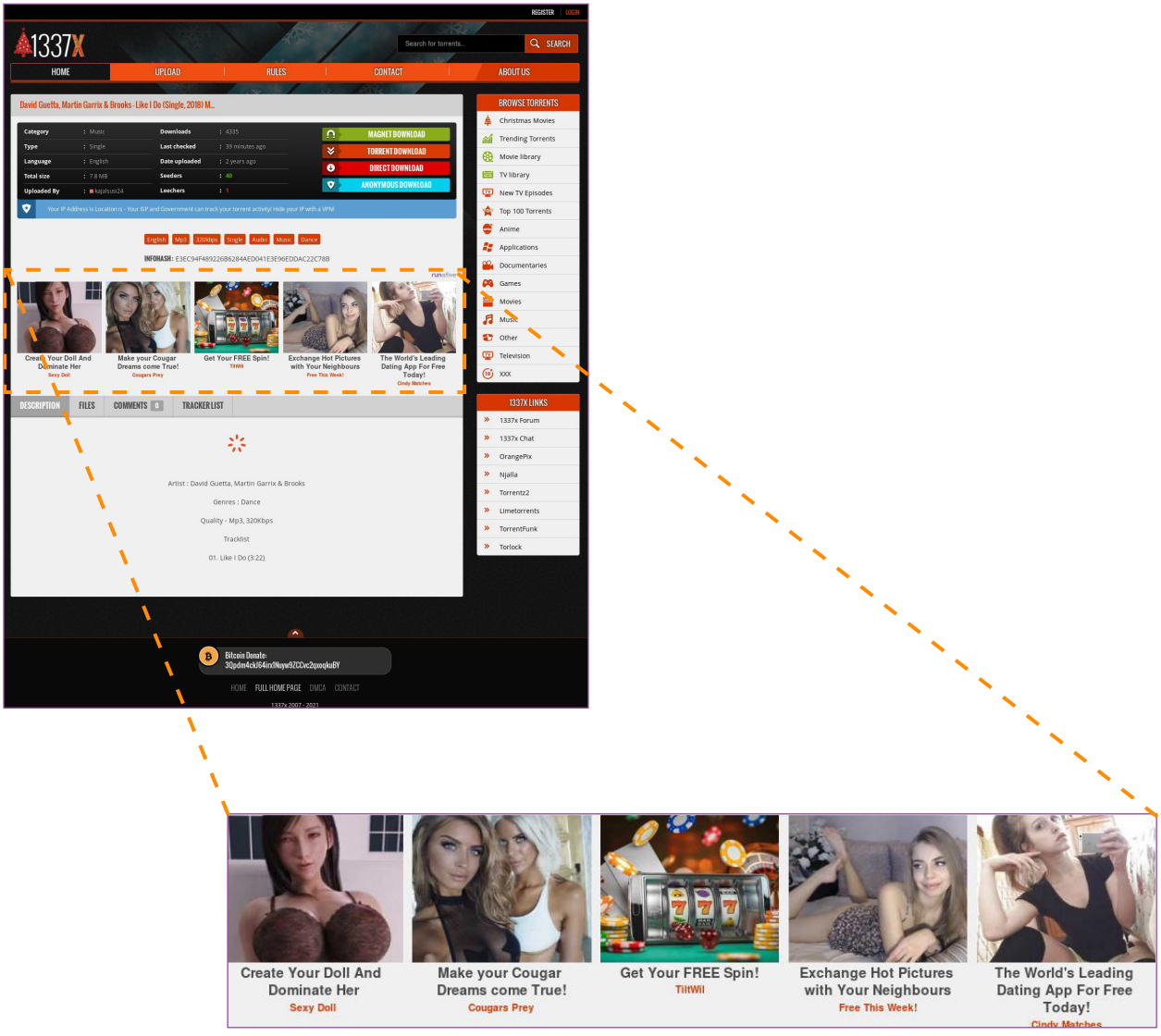
One company, AdsKeeper, accounted for 27 percent of all advertising on piracy websites during the one-year investigation conducted by White Bullet. AdsKeeper is a UK based firm established in 2013 that facilitates 'native' advertising that seeks to match the look and feel of the content of the webpage. This includes Sponsored Content ads. It was one of the ad intermediaries named in a landmark 2018 lawsuit that granted a media firm the right to seize advertising revenues from piracy websites. "The sites in question used advertising services from a variety of well-known networks, including Google AdSense, MGID, Popads, AdsKeeper, and Bidvertiser. None of these companies responded in court after the initial seizure order, suggesting that they did not object," according to World Justice News.

Figure 17. Sponsored Content ad served by AdsKeeper on piracy website filmeonline.biz, which is on the UK City of London Police IP Crime Unit's Infringing Website List and is subject to Blocking Orders in Europe.



RUNative, a Cyprus-based Ad Tech company, is another key player in ad-driven piracy, accounting for one in six ad dollars that flowed to websites peddling stolen content. Based in Barcelona and Cyprus, the company bills itself as a self-service advertising network and ad-exchange. According to its website, it accepts PayPal for its payments.

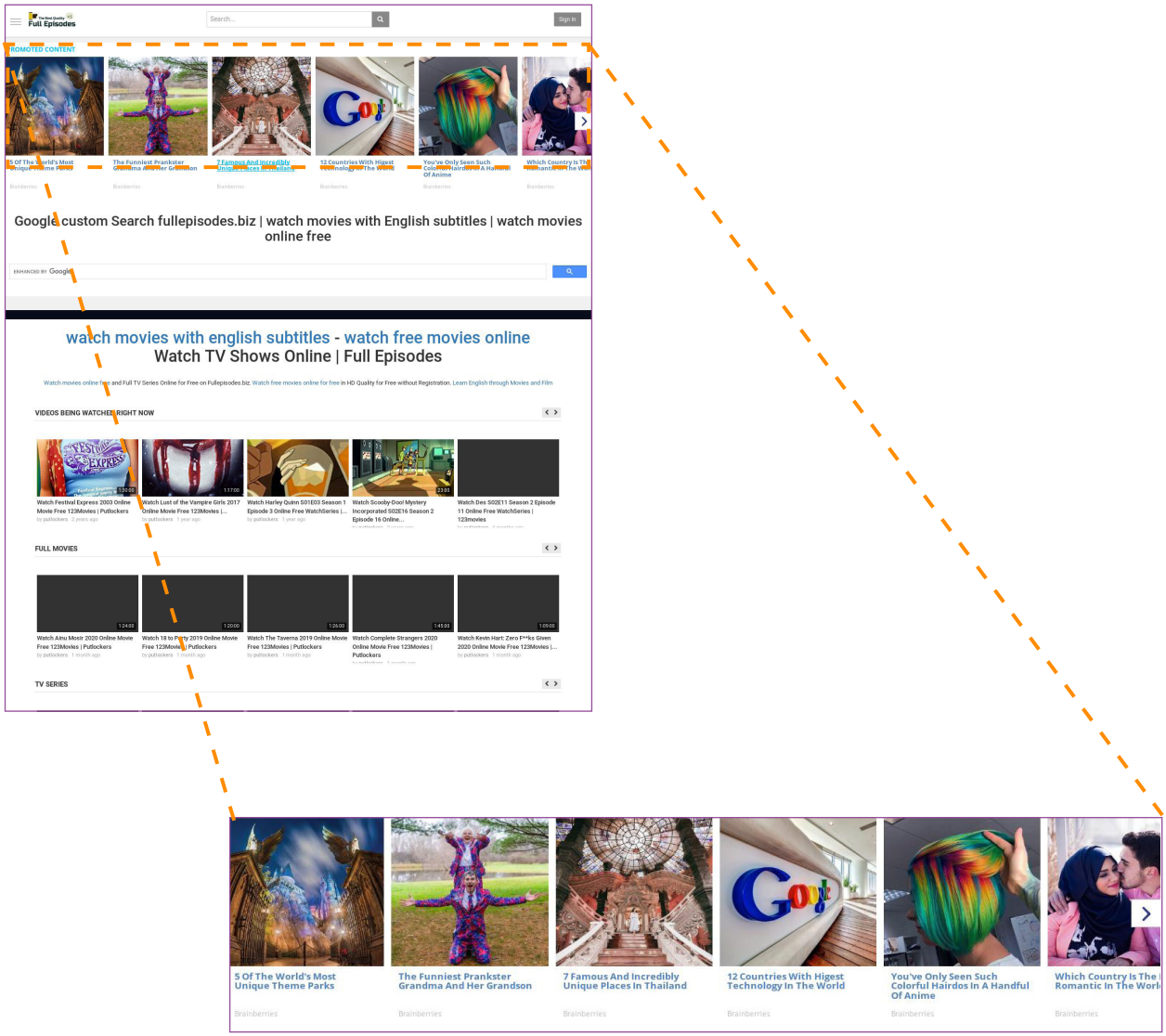
Figure 18. Sponsored Content ad served by RUNative on piracy website 1337x.unblocked.sh, which is subject to Blocking Orders in Europe. This website provides p2p Torrent downloads and direct downloads of the latest mainstream movies, games, series, ebooks, music, software.



There are also larger well-known players within the ad ecosystem that contribute to ad-supported piracy. One of them is MGID, a Santa Monica-based company that posts on its website an extensive list of content that it calls non-compliant with company policy. That list includes: "Violating third-party rights: copyright infringement, trademark, privacy, publicity or other personal or proprietary rights." Yet, White Bullet found it was responsible for six percent of ads on piracy websites.

Digital Citizens reached out to AdsKeeper, RUNative, and MGID to share high-level findings of the report.

Figure 19. Sponsored Content ad served by MGID on piracy website fullepisodes.biz. This website provides streaming of movies and TV series including mainstream Hollywood studio titles.



Piracy Apps and Ad Tech

On the piracy apps side, across all advertising, the snapshot showed a heavy concentration of ad enabling rested with just two companies: Google and Start.io.

Google's advertising technologies, which include its content delivery network (CDN) and advertising delivering systems (referred to here as Google CDN and Google Ad Tech) combined appear to have provided a majority (51 percent) of ads to piracy apps. Google's role is discussed in a separate section below.

Start.io (formerly StartApp) is the other key intermediary that appeared to heavily facilitate placing ads on piracy apps. Based in New York City, Start.io is an IAB (Interactive Advertising Bureau) member and helps apps fill their ad space. Start.io bills itself as a mobile data platform integrated with one million mobile apps but is also a leading intermediary that connects advertising to piracy, with one in three ads on piracy apps facilitated by the company during the study period.

Digital Citizens reached out to Start.io to share high-level findings of the report.

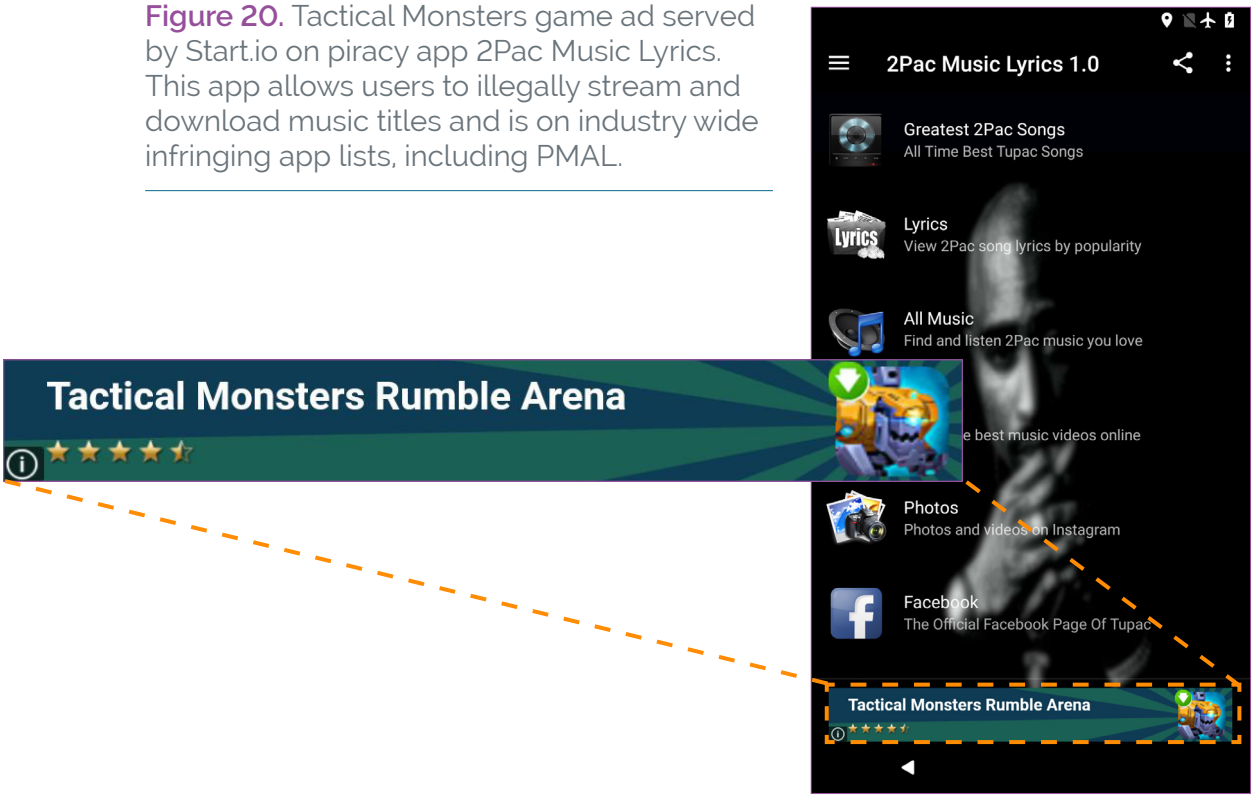
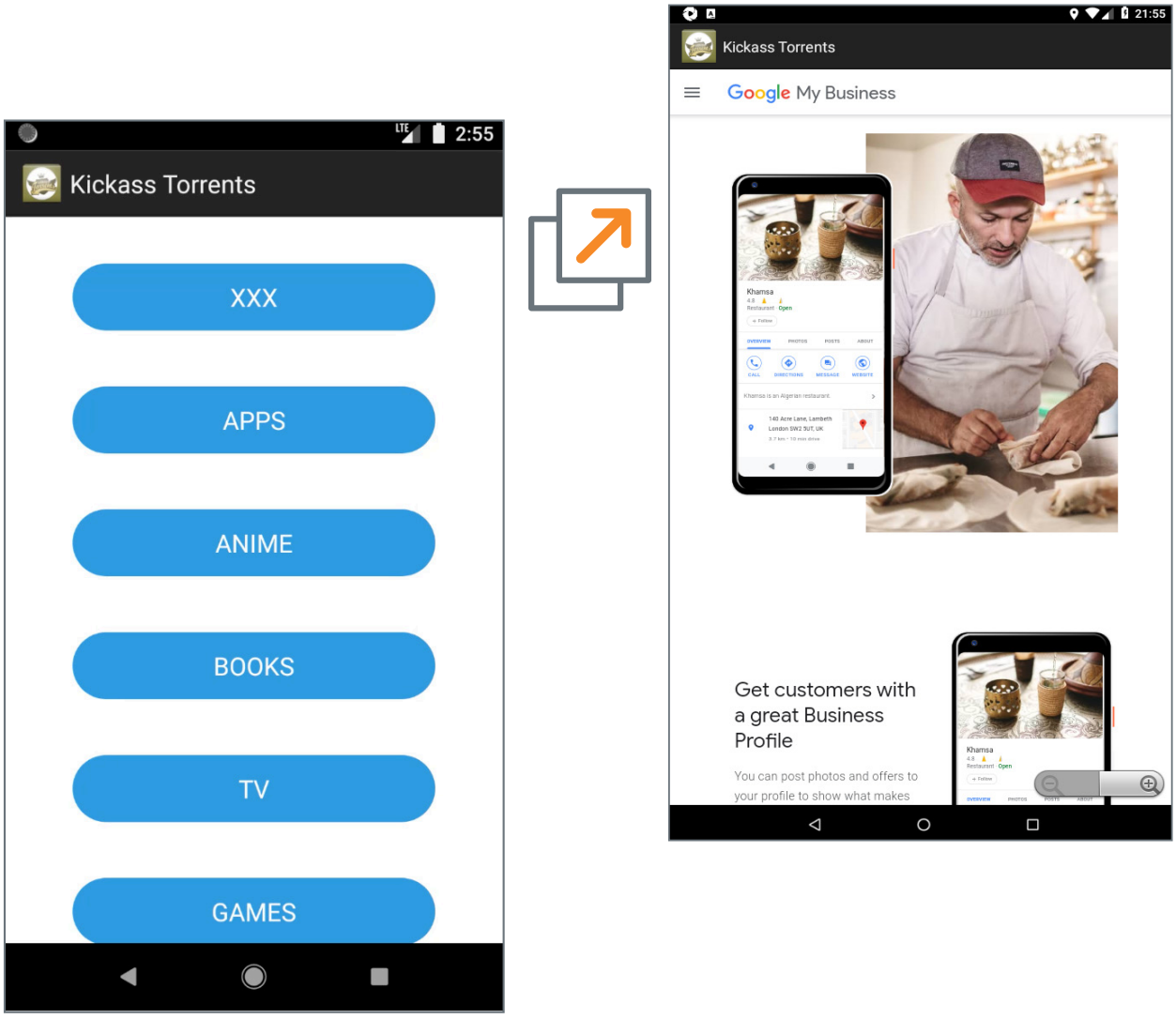


Figure 20. Tactical Monsters game ad served by Start.io on piracy app 2Pac Music Lyrics. This app allows users to illegally stream and download music titles and is on industry wide infringing app lists, including PMAL.

Google and Start.io were found to not only have facilitated the funding of piracy apps, but they also appear to have contributed to endangering consumers through the placement of risky ads on apps. Nearly half (48 percent) of all fraudulent and malware ads that appeared on piracy apps were facilitated by Start.io. Google CDN was involved in the placement of 44 percent of all fraudulent and malware ads on piracy apps, while Google Ad Tech facilitated less than one percent of these risky ads.

Figure 21. Google full-screen pop-over ad served by Google's own ad system on piracy app Kickass Torrents. This app provides unauthorized p2p torrent downloads for various types of infringing content and is on industry-wide infringing app lists, including PMAL.



While serving ads to piracy websites and apps may be lucrative, the risks of engaging in these practices appear to be escalating. Some of these companies are coming under increasing legal and public scrutiny. In the United Kingdom, the City of London Police IP Crime Unit (PIPCU) regularly tracks Ad Tech funding piracy in the UK and conducts outreach and warnings. These efforts have resulted in significant changes in the UK ad-funded piracy landscape.

And in the Ukraine, law enforcement authorities conducted a raid on an advertising agency suspected of brokering advertising for piracy websites through its Ad Tech functions. According to a news report, "The government reports that officers from its cyber police unit in conjunction with the National Police have carried out raids on an advertising agency in Ukraine. The currently unnamed company reportedly helped finance piracy sites by placing advertising on them, police say."

Ultimately, it's up to the advertising ecosystem to determine whether it wants to allow Ad Tech companies to serve both the reputable brands and publishers and the pirate operators, or instead to demand the entities choose whether to be exclusively on the legitimate or illegitimate side of the fence. But after this report, turning a blind eye to the entities that facilitate funneling $1.34 billion to pirates can no longer be an option.

Part III. Google & Piracy: Too Close for Comfort

Time after time during White Bullet's investigation of the ad-driven piracy, Google came up, in one guise or another. That Google is the 800-pound gorilla in digital advertising is nothing new. In fact, it is not possible to discuss digital advertising without dedicating time to Google. It's both a major advertiser of its services and, with its dominant role in facilitating online advertising, the most important go-between for brands and other intermediaries looking to place ads.

According to eMarketer, Google's share of the US digital ad market in 2020 was 29 percent, making it the largest Ad Tech company in terms of market size and facilitating the most digital ads across the overall ad ecosystem. Its role in the digital ecosystem provides it an outsized ability on piracy advertising to either be part of the problem or solution.

That is why it's disheartening that Google's role in ad-driven piracy appears to be so prominent.

Despite having a sophisticated and dedicated program to protect advertisers and block ads to illegal publishers, Google is a significant contributor to the piracy ecosystem, both as an advertiser paying piracy websites and apps for ad space, and as an Ad Tech enabler facilitating ad placement for third party brands on piracy apps. Google's role in ad-supported piracy is central and multifaceted, as evidenced by the following:

- Google's content delivery network appears to have been used to place 38 percent of all ads on piracy apps during the year-long investigation.
- Google's various ad brokering services appear to have been used in facilitating 13 percent of pirate ad placements, putting Google's Ad Tech services among those most relied upon by piracy apps to generate income.
- As a marketer of its own products and services, Google was among the leading advertisers on piracy apps, accounting for five percent of all Major Brand advertising. That means it's likely that during the year of investigation, **Google paid pirate operators millions of dollars** to place its own ads on their illicit piracy apps. Given the company's boasts about its analytical prowess and data expertise, it seems far-fetched that Google doesn't know how it's spending millions

of dollars. On the piracy websites, Google has done a better job of steering clear of pirate operators, accounting for fewer than one percent of Major Brand advertising.

Part of the challenge is that Google has a hand in almost all aspects of the advertising supply chain. It collects user data for targeting advertising, helps advertisers place ads, and sells ad space on websites and apps. Google collects a vast array of data on almost everyone whenever they interact with browsers, cookies, search, in chat, on email and more.

This data can be used to help advertisers target ads to individuals wherever they go online. In addition, Google Ads is a tool offered to businesses and brands to place their ads in front of consumers (acting for the "buy" side to target individuals). A brand chooses the type of audience it wants to reach and Google places the ad on the websites most likely to reach the target demographic.

Google's advertising subsidiaries - including AdSense and AdMob – also help websites and apps sell their ad space (acting for the "sell" side). AdSense is an advertising network that provides fast and easy access to brands that are looking to advertise. AdMob provides a similar service for apps. Both are used by pirate publishers.

The AdSense and AdMob ad networks only operate in the Google ecosystem, which prevents competitive bids on ad space from non-Google ad networks. This departure from open competition has put Google in the spotlight. The European Commission opened an anti-trust investigation in June 2021 to assess whether Google favored its own Ad Tech over competitors and whether that violates EU competition rules. The EU is also examining whether Google distorts competition by restricting access to third parties to user data for advertising purposes while keeping this data for its own ad supply chain.

In June of this year, France's competition authority fined Google over $260 million for abusing its dominant position in the online advertising market, with Google settling and agreeing to operational changes in France. Other countries are also considering action. It is yet to be seen what these changes will be and how they affect competition.

What is clear is that the dominant position of Google in the legitimate ad supply chain clearly carries across to the pirate ecosystem. Google surely has the knowledge and expertise to both stop its advertising dollars from flowing to pirate operators and assist other brands from ending up on piracy websites and apps. The question is whether they have the will to do so.

Conclusion: How to Address a $1.34 billion Piracy Advertising Problem

Ad placement next to content has always been important. For example, an airline wouldn't want its advertising featured next to a news article about a plane crash. But in the digital era, the issues of brand suitability and brand safety have become more complex.

Let's start with the obvious: you can't have $1.34 billion in advertising revenue on piracy websites and apps, and no one know it - whether it's the Major Brands or the advertising and technology companies that facilitate the relationships within the ad ecosystem.

So, it comes down to this: do these brands know their advertising is appearing on illicit piracy websites and apps, and do they care?

If Major Brands don't know, this report should serve as a wake-up call for them to follow an emerging set of best practices to protect their brand safety and thwart the efforts of pirate platforms. These best practices include implementing programs to audit ad placements, working with safe and certified safe Ad Tech firms, and utilizing technology to assess publishers for risk. Brands, publishers and Ad Tech firms should consider becoming part of TAG, and seeking its Brand Safety Certification, which requires taking appropriate steps to keep reputable brands off piracy websites and apps.

If the brands do know that their ads are appearing on piracy websites and apps but decline to follow these best practices, then they should explain why. Given that many consumers now expect their favorite brands to be socially responsible, having to explain why these companies allow their advertising dollars to enrich criminal ventures that spread malware and fraud may be a difficult conversation.

The first stage of addressing a $1.34 billion piracy advertising problem is raising awareness. What the Major Brands do with that information will be telling. Amazon took an important step towards responsibility on ads on piracy websites and their ads are declining also on pirate apps; now we'll see if that trend continues. Google is also a huge factor; due to its

unique place as both a buyer, seller, and operator of an exchange, it plays a major role in the advertising ecosystem.

In its 2014 "Good Money Gone Bad," Digital Citizens wrote, "Efforts to deter or degrade these activities through legal, technical, or industry initiatives continue to face a challenge." Nonetheless, the urgency to do so has never been greater in light of advertising trends, technology advances, and a growing intent among individual and organized global bad actors to capitalize on these profitable opportunities.

Spurred perhaps by the spotlight, responsible leaders in the advertising ecosystem took sustained efforts to counter the rise of advertising on piracy websites. As noted, that effort achieved results: the percentage of Major Brand advertising on piracy websites in the United States fell from 30 percent in 2014 to four percent in 2021.

For the sake of a healthier and safer Internet, that same level of diligence should be applied to all pirate operators, whether they are operating websites or apps. That will, once again, require responsible leaders in the Ad Tech space to work with Major Brands to develop a strategy to prevent these ads from appearing on piracy apps.

Finally, it will require law enforcement to crack down on piracy streaming services, including multi-national investigations of major ad-supported operations and, in the United States, use of new statutory tools that reflect the seriousness of the pirate operators' criminal conduct.

While it's certain that both Major Brands and content creators would welcome additional law enforcement focus on ad-supported piracy, the benefit would extend beyond them. As discussed in this report – and to be elaborated on in an upcoming report – the pervasiveness of malware and fraudulent advertising on piracy websites and apps poses a significant risk to Internet users who are targeted by an unholy union of pirate operators and hackers to infect and infiltrate their devices for profit.

The complexity of the challenges faced when piracy and advertising intersect is vast. But that complexity cannot be the cause for Major Brands, intermediaries, and law enforcement to fail to take meaningful steps to address the problem. A multi-billion illicit industry made up of criminals and bad actors poses too great a danger to ignore.

Annex: Methodology

White Bullet is a technology solutions company that specializes in detecting and demonetizing online intellectual property infringement. Its AI-led system identifies, continually monitors, and dynamically scores websites and apps engaged in IP infringing activity, whilst tracking the digital advertising funding them and its value. This system and the data gathered is available for use through White Bullet's IP Infringement Platform IPIP™. White Bullet provides intelligence on piracy, advertising and advertising revenues to policymakers, rights owners, brands and advertising companies.

White Bullet's IP Infringement Platform (IPIP™)

IPIP™ is a unique database of real-time piracy intelligence. It detects instances of piracy across multiple digital ecosystems. It does this at massive scale using specialized live data feeds covering more than 50 app stores and 430 million websites.

As piracy is highly dynamic, with websites and apps changing daily, White Bullet discovers new and evolving threats drawn from over 400,000 daily domain registrations and app submissions provided by specialized databases. White Bullet also undertakes independent smart web crawling searching for infringing titles to maximize its data collection techniques. It also crawls app stores to identify new app submissions within media categories. White Bullet combines this vast dataset with data from its integrations with live ad bidding processes at digital ad exchange level to provide information on the most popular publishers with advertising.

From this vast dataset, White Bullet identifies piracy publishers. It does this by scoring the websites and apps for piracy risk using custom machine learning techniques. These are informed by hundreds of features extracted from each website and app and combined with contextualization techniques. White Bullet also draws data from judicial and administrative databases of known adjudicated pirate publishers to assist in training the AI. In this way machine learning can both analyze the vast dataset at speed for potential IP infringement, and examine the context of the infringement for continually re-scored accuracy. Targeted use of human review is used to ensure quality assurance of the AI processes.

White Bullet scores websites and apps at a granular level from 0 to 1000 with scores falling into three categories: low piracy risk (0-250), medium piracy risk (251-750) and high piracy risk (>750). Medium piracy risk may include websites and apps that offer pirated content together with legitimate content.

White Bullet's Ad Monitoring System

White Bullet has developed its proprietary digital advertising monitoring system ("Ad Monitoring System"), which captures high volume data about advertising placed on IP infringing websites and apps (defined as infringing copyright online). Using White Bullet's Ad Monitoring System, parties may monitor advertising profile changes in the online piracy ecosystem.

White Bullet's Ad Monitoring System:

- visits IP infringing websites and navigates IP infringing apps from localized internet protocol addresses ("IP Addresses") to track locally served ads,
- captures images of ads found during visits in the context of the infringing web or app page,
- uses White Bullet's AI classification technology that leverages text and image recognition techniques to identify and classify the brands found in the advertising collected, and
- identifies Ad Tech entities engaged in the placement of the advertising by capturing and analyzing data from the web or app ad code on all the intermediaries involved in the process of targeting, placement and delivery of ads.

Methodology for this Study

White Bullet was commissioned to identify the most popular piracy websites and apps consistently active during the time of the study and to further identify those with digital advertising. Those with advertising were tracked to capture the ads placed on them during the period June 2020 – May 2021. The advertising was analyzed to identify the brands and Ad Tech companies involved in placing the ads and the estimated value of that advertising calculated using a proprietary methodology relating to that same time period.

White Bullet drew on data in IPIP™ to identify a pool of IP infringing websites and apps and then used popularity data from sources such as Alexa and SimilarWeb and app stores, combined with automated status and advertising data checks, to assess and determine the most popular active high and medium piracy risk websites and apps to be tracked

for advertising. Any high or medium piracy risk publisher that was either consistently inaccessible or had no advertising present was excluded from consideration for ad tracking.

From the 65,240 websites and 19,147 apps identified at the start of the study as popular publishers which provided access to pirated content, 6,194 websites and 884 apps were deemed suitable for ad monitoring under the study. These included websites and apps (i) on industry-wide piracy watchlists such as TAG's Pirate Mobile App List, USTR and EU notorious market lists, (ii) specifically cited as infringing copyright by law enforcement agencies, judicial and administrative bodies such as the UK City of London Police Infringing Website List and blocking orders from various countries, (iii) self-identifying as pirate distributors of content, (iv) identified by White Bullet's AI and verified by experts as providing access to unauthorized copyrighted content. As a result, not all websites and apps selected for analysis under this study were dedicated exclusively to piracy, and may have been unknowingly or negligently providing access to pirated content.

The data collected from web and app ad tracking was analyzed to identify each brand and ad tech company into standard categories, allowing us to assess the ratio of advertising that fell into each category. Categorization included identifying branded advertising where brands were identifiable by logo, image or text, as well as risky ads such as adult advertising and ads that led to fraudulent or malicious content. Categories include:

- "Major Brands", where the brand, or parent company of the brand, was present on one of the following lists or with a strong presence in multiple search engine results globally indicating potential significant marketing reach and consumer recognition:
  - AdAge Global Marketers Index,
  - Millward Brown Global and National brand ranking lists,
  - Ranking the Brands Top 100 List,
  - WFA membership,
  - ANA membership, or
  - Forbes Global 2000.
- "Other Brands", defined as brands that are not major but are also not fraudulent, adult, or malicious.
- "Adult" ads, defined as ads that display sexually explicit imagery or wording.
- "Sponsored Content" ads, defined as native ads placed within content boxes and including multiple advertorials in a single inventory slot.

A small proportion of advertising could not be identified as belonging to any of the above categories and was classed as "Unidentifiable Ads."

Digital advertising is highly dynamic and ads that appear to some parties may not appear to others. Repeat visits to websites and apps may not yield the same ads nor recreate the same environment and as such different advertising may be displayed when later visited by human interaction or through different third-party vendors. Data from this study are therefore a snapshot in time of advertising displayed to White Bullet's Ad Monitoring System from the websites and apps visited.

Ad revenue estimation methodology

Estimated annual ad revenue is the potential estimated revenue that websites and apps could generate from digital advertising worldwide annually. The results were derived from actual advertising data collected by White Bullet's Ad Monitoring System, incorporating available daily pageview data (for websites) and daily session (usage) data (for apps) and extrapolating to include full annual coverage for all countries.

White Bullet calculated estimates of the potential ad revenue of piracy websites and apps by combining multiple independent and proprietary data sources within a revenue calculation algorithm. This included:

(i) data about actual ads captured by White Bullet during ad harvesting visits,

(ii) for websites, daily pageview data for those websites drawn from independent third-party sources indicating traffic volume, and for apps, daily session data calculated using reported app store install numbers and industry estimates for usage (see below specific detail on daily sessions), and

(iii) advertising valuation data based on a proprietary matrix created from industry advertising payment and bidding values identified in major advertising exchanges where White Bullet is integrated, industry published average ad bidding values by ad sector and format, and ad bidding values identified by White Bullet directly from the code behind captured ads where available.

To estimate daily sessions for app usage, White Bullet created a calculation as no third party data is available for app usage that is the equivalent of daily pageviews for websites. Daily session data was created by taking the number of installs for each app from app store sources, estimating how many of those installs may be retained on user's devices based on third party data averaging retention rates for media sector apps, applying a factor for how many retained users use the apps each month based on third party usage data, and finally applying a factor to determine how many of those retained monthly users might use each app daily based on a conservative once weekly usage.

To create the advertising valuation matrix for websites and for apps, White Bullet applied multipliers to core base values for the three dominant payment models in digital advertising: Cost Per Mille (CPM), Cost Per Click (CPC), and Cost Per Action (CPA). White Bullet's methodology used a different core base value for CPM, CPC or CPA advertising drawn from industry estimates from third-party sources, which depend on various data components, including digital ecosystem (e.g. desktop web, mobile web, app, search, social), market sector (e.g. health, finance, travel), ad format (e.g. display, pop up/under) and media type (e.g. image, video, rich media). Multipliers applied were dependent on the advertiser type (e.g. Major Brand, clickbait), ad dominance (e.g. density of ads on the publisher page where relevant) and country where the ad was displayed (a multiplier was applied to each ad for that country based on average advertising spend by internet user for that country as a percentage of average advertising spend by internet user benchmarked against the US). For CPC and CPA advertising, core base values and related click-through rates depended on market sector, and multipliers were applied to both core base values and click-through rates depending on the ad format, media type, as well as advertiser type, ad dominance and country, again drawn from industry estimates from third-party sources. Data points collected from ad harvesting visits by the Ad Monitoring System were cross referenced with the advertising valuation matrix, after which extrapolation calculations were created using estimated third-party pageviews to those websites or daily session in those apps, and ratio of ads to visits by brand by country. Third-party data included in the above calculations was drawn from numerous sources, including publicly available data from Statista, eMarketer and Google AdSense, as well as data from industry experts and ad exchange bid data available to White Bullet.

Estimated advertising revenue data in this report are estimates of potential revenues based on extrapolated data and as such may vary from sums actually generated by publishers. Advertising values are heavily dependent on a range of factors and are therefore estimates based on extrapolating data using statistical correlations. White Bullet used conservative core base values and multipliers within the ad revenue matrix and conservative daily pageview and daily session extrapolations, understanding that websites and apps might command varying advertising rates with different buyers. The values in the ad revenue calculation algorithm were periodically reviewed and updated as needed to reflect the digital marketplace.

About Digital Citizens Alliance

The Digital Citizens Alliance is a nonprofit, 501(c)(6) organization that is a consumer-oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet. Digital Citizens wants to create a dialogue on the importance for Internet stakeholders—individuals, government, and industry—to make the Web a safer place.

Based in Washington, DC, the Digital Citizens Alliance counts among its supporters: private citizens, the health, pharmaceutical and creative industries as well as online safety experts and other communities focused on Internet safety. Visit us at digitalcitizensalliance.org.

About White Bullet Solutions

Founded in 2013 by a leadership team of experienced Intellectual Property lawyers from the media and advertising industries, White Bullet offers companies piracy risk data and protection, brand safety solutions and full transparency on their advertising placement and digital supply chains.

White Bullet works collaboratively with brands, policy makers and the advertising industry to safeguard advertising spend and prevent ad placements from appearing on IP Infringing domains and apps. White Bullet is a certified anti-piracy solutions provider under the advertising industry regulator TAG and is a stakeholder to the EU Commission Memorandum of Understanding on Advertising and IPR.

White Bullet comprises IP experts and dedicated technical engineers who specialize in AI, big data models and predictive machine learning. The team includes highly skilled investigators and data analysts experienced in tackling the funding and distribution of pirated content. With offices in London, New York and Los Angeles, White Bullet advises policy makers and government bodies on regulatory and compliance programs globally."

digitalcitizens alliance | whitebullet