September 30, 2019

Daniel Lee
Assistant U.S. Trade Representative for Innovation and Intellectual Property (Acting)
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508

In re: Docket No. USTR-2019-0013

Dear Mr. Lee:

Attached please find RIAA's submission in response to your request for comments identifying Internet and physical markets based outside the United States that should be included in the forthcoming Notorious Markets List (List). The online and physical markets identified in our comments are harming American creators, businesses, and the American economy.

The U.S. music industry is highly dependent on the Internet and, in turn, fuels other parts of the Internet economy, job growth, and trade surplus. In the first half of 2019, 80 percent of U.S. record label revenue came from digital streaming sources, with over 60 million subscriptions for music streaming services.[1]

RIAA members license their music globally, with several hundred licensed platforms operating around the world. This contributes significantly to the U.S. digital trade services surplus, and to the U.S. economy generally. Intellectual property rights (IPR) licensing – of which music is a core part – globally generated an $80 billion digital trade surplus for the U.S. in 2016, according to a U.S. Department of Commerce report entitled *Digital Trade in North America*.[2] A 2018 report found that the music industry creates $143 billion annually in value when both direct and indirect effects are included and supports 1.9 million American jobs across a wide range of professions.[3]

While the growth in music streaming is promising, the music industry recovery continues to be threatened by online marketplaces that infringe our members' music, as well as by sales of counterfeit products over ecommerce platforms, outdated laws and their misapplication and abuse, and lack of proper enforcement mechanisms. In fact, the emergence of the digital piracy

[1] Source: RIAA.
[2] Nicholson, Jessica; U.S. Department of Commerce, Economics and Statistics Administration, Office of the Chief Economist; *Digital Trade in North America;* pp. 3-5; January 5, 2018, available at https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/digital-trade-in-north-america.pdf. See also Statement of the Recording Industry Association of America (RIAA) before the United States International Trade Commission Global Trade 1: *Market Opportunities and Key Foreign Trade Restrictions*, April 21, 2017, which describes the relationship between music and smartphone growth, and Internet growth generally.
[3] Siwek, Steven, *The U.S. Music Industry: Jobs and Benefits, April 2018,* prepared for the Recording Industry Association of America, available at http://www.riaa.com/wp-content/uploads/2018/04/US-Music-Industries-Jobs-Benefits-Siwek-Economists-Inc-April-2018-1-2.pdf. *See also* 50statesofmusic.com for more detailed information about the impact of music in various states in the United States.

coincided directly with a decade of declining revenues for the recording industry, where 2010 revenues were less than half of 1999 levels, and our 2018 annual revenues were roughly 33 percent less than what they were in 1999.

In this submission, we first address the issue focus of malware and other security risks posed by sites and services that facilitate online infringement. This highlights that the concerns and impact of infringing sites extends well beyond the infringing activity.

We then identify some of the major online infringing actors that threaten our industry's recovery and jeopardize the U.S. competitive advantage in digital trade, along with the challenges we face with identifying and enforcing our rights against those rogue actors. This infringing activity creates distortions in the marketplace that undermine the music industry prosperity, which in turn negatively impacts the U.S. trade surplus.

Finally, we identify physical markets that continue to flood ecommerce platforms with high quality counterfeit CDs that unwitting buyers are purchasing at full retail price. These counterfeits result in a one-for-one displacement of legitimate sales.

We hope you find this information useful, and we look forward to continuing to work with the U.S. government to find solutions to these problems.

Sincerely yours,

/ George York /

George York
Senior Vice President, International Policy
Recording Industry Association of America (RIAA)

2019 SPECIAL 301 OUT-OF-CYCLE REVIEW OF NOTORIOUS MARKETS

ISSUE FOCUS – MALWARE AND ONLINE PIRACY

Rogue actors often use the lure of free – and unauthorized – content to attract users to their online infringing services, and then those rogue actors target those users with malware and other malicious activity. This malicious activity has been studied and reported on regularly over the years. A 2015 report called "Digital Bait" identified how cybercriminals use content theft sites and malware to exploit the user and their computer, and estimated the cost of such malicious activities.[4] It conservatively estimated that malware-related revenue attributable to content theft sites was $70 million annually.[5] A 2016 news release, also from Digital Citizens Alliance, noted research that found that 1 in 3 content theft sites expose users to malware.[6] A 2018 analysis from Professor Telang of Carnegie Mellon University concluded that "doubling the time spent on infringing sites leads to 20 percent increase in total malware files and 20 percent increase in malware files after removing potential adware."[7] Another 2018 report stated that "[i]llegal pirating sites are the most common source of malware infection on the internet," and that nearly 1 in 10 children have been affected by malware.[8]

This correlation between infringing services and malware, identity theft and potentially unwanted programs, extends not only to infringing websites, but also to streaming devices, and mobile and device apps. For example, a 2019 report noted the prevalence of malware in connection with infringing streaming devices and related apps.[9] A 2017 article reported that hundreds of music player apps on the Google play store had some form of malware.[10] As the form of online piracy morphs, rogue actors also modify their approach to malware and malicious activity to further exploit visitors to, or users of, those infringing services.

Several authorities and cybersecurity professionals have warned about this problem. For example, in

---

[4] Digital Citizens Alliance, *Digital Bait*, December 2015, available at https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/digitalbait.pdf.

[5] Id.

[6] See Digital Citizens Alliance news release at https://www.digitalcitizensalliance.org/news/press-releases-2016/dangerous-partners-digital-citizens-investigation-finds-that-malware-operators-and-content-theft-websites-assisted-by-u.s.based-tech-firms-are-targeting-millions-of-consumers/.

[7] Telang, Rahul, *Does Online Piracy Make Computers Insecure? Evidence from Panel Data*, March 12, 2018, available at SSRN: https://ssrn.com/abstract=3139240 or http://dx.doi.org/10.2139/ssrn.3139240.

[8] Internetmatters.org, *Internet Safety and the Dangers of Digital Piracy: Understanding the Risks for Children*, July 2018, available at https://www.internetmatters.org/wp-content/uploads/2019/04/Internet-Matters-Report-Dangers-of-digital-piracy.pdf.

[9] Digital Citizens Alliance, *Fishing in the Piracy Stream: How the Dark Web of Entertainment is Exposing Consumers to Harm*, April 2019, available at https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf.

[10] HackReed, *Android Malware Found in Hundreds of Music Player Apps on Play Store*, Nov. 20, 2017, available at https://www.hackread.com/android-malware-found-in-hundreds-of-music-player-apps-on-play-store/.

2017, 15 U.S. state attorney generals released a national public service campaign warning about the risk of malware from pirate websites.[11] The United States Federal Trade Commission has also warned about the dangers of malware from pirate websites.[12] Cybersecurity professionals have also issued warnings about malware and infringing apps in recent years.[13] The problem continues unabated.

In terms of solutions, some options include the following:

- Search engines should promote known, verified authorized sites over unverified sites for any searches for movies, music, books, software, or other well-known, copyrighted material that is vulnerable to infringement;
- App stores should develop up-to-date best practices to review apps associated with music and other popular content before they are placed on the storefronts to check for vulnerabilities or exploits that may be available in the app. They should perform similar diligence after the app has been available on their storefront for some time, and with respect to each update that the app developer releases for the app;
- App stores should also promote known, verified authorized apps that offer access to music or other popular content over unverified apps that offer access to similar content;
- The government should require that true name, address, and contact information be verified and posted in connection with any online domain, site, service, or app that purports to provide access to popular content – this includes ensuring that true and accurate registration or WHOIS data is verified and accessible; and/or
- The government should consider legislation that would increase the penalties for operators that facilitate the dissemination of malicious activity via infringing sites, services, and apps, and obligate U.S. intermediaries to take action to deter such activity.

ONLINE MARKETPLACES

The following is a list of online markets that we request to be included on the 2019 Notorious Markets List. These markets are based outside the United States and engage in the unlicensed sale, streaming, and/or distribution/downloading of sound recordings that significantly damage the rights of U.S. companies, and/or also engage in circumvention activities that violate 17 USC § 1201.

These services harm U.S. artists, record labels, and music publishing companies by (i) disseminating music without authorization and without providing any compensation to the creators and owners of the music, and (ii) artificially distorting the market value of the music, thereby reducing the compensation to the creators and owners from licensed services. Recognizing the enormous cost of such IP theft to the United States, this Administration identified intellectual property theft as a significant threat to American prosperity in the December 2017 National Security Strategy of the United States, and again in the 2019 Special 301 Report. Further, as stated in the 2019 Special 301 Report, "a key objective of the Administration's trade policy is ensuring that U.S. owners of IP have a full and fair opportunity to use and profit from their IP around the globe."

Many of the services disseminating infringing content that we have included in this year's submission unfortunately have been included in the past. While some of these sites have made

[11] See Digital Citizens Alliance news release at https://www.digitalcitizensalliance.org/news/press-releases-2017/state-ags-warn-consumers-about-malware-risks-from-pirate-websites-in-national-public-service-campaign/.

[12] See https://www.consumer.ftc.gov/blog/2017/04/free-movies-costly-malware. Cybersecurity professionals have also warned about the malware risks posed by pirate sites. See, e.g., US CyberSecurity, *The Consequences of Digital Piracy*, available at https://www.uscybersecurity.net/digital-piracy/.

[13] See, e.g., Naked Security by Sophos, *Super Free Music Player in Google Play is Malware: A Technical Analysis*, May 2, 2017, available at https://nakedsecurity.sophos.com/2017/05/02/super-free-music-player-in-google-play-is-malware-a-technical-analysis/; and Kaspersky Daily, *All Apps on Google Play are Safe: Fact of Fiction?*, Sep. 11, 2019, available at https://www.kaspersky.co.uk/blog/google-play-malware/16674/.

incremental changes to the way they operate to limit some of their exposure, unfortunately the traffic to these sites remains high and the damage inflicted on the U.S. recording industry is immense.

We continue to engage in various forms of "self-help" to try to address this infringing activity, including sending traditional infringement notices, warning letters, and cease and desist letters, and engaging in civil litigation and criminal enforcement referrals where sites refuse to respond. These actions, along with efforts to highlight the problems and engage other governments in solutions, such as through the Notorious Market Report, have been helpful in modifying the behavior of some illegal services.

However, we continue to face significant challenges in our investigation and enforcement efforts. One challenge we face is that the sites that have shut down can reappear as quickly as they disappeared. In some cases, they reemerge with the same second-level domain name but on a different top-level domain, from the same hosting Internet service provider (ISP), and with the same functionality (what we call domain-hopping). In other instances, they return with slightly altered domain names with new hosting ISPs, new registrars, and/or new registrant information. We also often see "copycat" infringing services pop up as well. In fact, infringing operations these days are often multi-jurisdictional and based on complex, dynamic structures involving various types of third-party intermediaries. Such complex and dynamic structures are often deliberate as they increase the time, cost, and difficulty of enforcement action, and thus reduce the right of any action being taken against the operators. The dynamic and low-cost nature of the Internet presents unique challenges in comprehensively identifying and addressing notorious markets.

In addition, in today's environment, it has become exceedingly difficult to track, enforce against, and accurately associate various notorious websites because of, among other things:

- **Severely Restricted Access to Domain Name Registration Data** – Since May 2018, access to Domain Name Registration Data has been severely and overly restricted by ICANN and the registrars and registries in their quest to reduce their liability risk under the European Union's General Data Protection Regulation. Despite promises to establish a policy to provide uniform and consistent rules on how users can access such registration data, including for intellectual property protection and enforcement purposes, ICANN has yet to develop such rules. Furthermore, it appears that no significant progress will be made before the November 2019 target date set by the National Information and Telecommunications Administration (NTIA) for policies to provide such uniform and consistent access to such data. As previously noted, this continues to frustrate our ability to contact the registrant directly to address infringement issues, investigate relationships between infringing sites, and analyze our other enforcement options.[14]

- **Privacy/Proxy Protected Domain Name Registration and False Domain Name Registration Data** – In addition, operators of pirate sites typically hide their identity behind privacy/proxy services or appear to submit false or incomplete registrant information, further creating obstacles to enforcement against these sites. Despite ICANN having a fully approved, bottoms up, multi-stakeholder policy to require privacy/proxy service providers to disclose true registrant data in cases of clear, infringing activity, ICANN continues to delay implementation of that policy.[15] With estimates of over one third of all domain name registrations behind a privacy/proxy service, this failure of ICANN to implement disclosure policies for privacy/proxy services only serves to embolden online infringers and others that

[14] It also leads to increased problems with cybersecurity threats and brand protection concerns. See, e.g., Vayra, Fabricio, *The End of the Road: ICANN, WHOIS, and Regulation*, Circle ID, September 25, 2019, available at http://www.circleid.com/posts/20190925_the_end_of_the_road_icann_whois_and_regulation/.

[15] See September 5, 2019 letter from ICANN to Keith Drazek continuing the delay of implementation of the privacy/proxy services approved policy, available at https://www.icann.org/en/system/files/correspondence/namazi-to-drazek-et-al-05sep19-en.pdf.

engage in malicious activity online with only minimal risks of identification and reprisal. In addition, ICANN has failed to adopt meaningful solutions to improve the accuracy of registrant information, despite discussions on this topic for the last several years.

- **Prevalent Use of Reverse Proxy Services to Obfuscate Hosting ISP** – These services are utilized by pirate websites to hide the identity and location of actual hosting ISPs. More and more pirate sites employ reverse proxy services, most commonly Cloudflare, to obfuscate their IP address, creating obstacles to enforcement against such sites. While Cloudflare will provide the underlying IP address upon request when presented with an infringing URL, the Cloudflare also notifies its customer of the request, whereby the customer can quickly migrate its site to a new hosting ISP while continuing to utilize Cloudflare. Since there is no real-time access to the site's location, any IP address provided by Cloudflare one day may be inaccurate the next.

- **Use of "Bulletproof" ISPs** – Several infringing sites use off-shore hosting ISPs that support the sites' infringing activities. These "Bulletproof" ISPs support various types of criminality through considerable leniency in the kinds of materials they permit to be uploaded and distributed via their networks. These ISPs do not respond to notices of infringement or warning letters that the ISP is hosting and supporting known infringing sites. We describe two of these types of ISPs, namely Ecatel/Quasi Networks and FlokiNet, below as a class of notorious markets that harm the U.S. music sector.

- **IP Address Space Subleases** – IP address space is often subleased to another ISP hosting service, which adds a further level of complication to our investigative efforts.

In fact, there are thousands of websites on the Internet that are dedicated to piracy, with new ones appearing all the time and existing ones frequently changing their online location (whether domain or hosting environment, or both) to avoid enforcement. This list of notorious markets is therefore by no means comprehensive. We focus instead on those sites and services that inflict the most damage on the U.S. recording industry either globally or in specific country markets.

We monitor traffic to the sites using Alexa.com for overall global rankings and SimilarWeb, a web traffic analytics company, to track website visits. The ranking and traffic data used in this submission is based on the data available in September 2019 from these two sources.

1. Streamripping Sites

As noted in the 2019 Special 301 Report, "[s]tream-ripping, the unauthorized converting of a file from a licensed streaming site into an unauthorized copy, is now a dominant method of music piracy, causing substantial economic harm to music creators and undermining legitimate online services."[16]

The distribution of permanent downloads of files from streaming services deprives the record companies and artists of streaming revenue by eliminating the need for users to return to YouTube and other licensed services every time they listen to the music. They harm premium streaming services that offer tethered downloads for off-line listening. Streamripping services also undercut pay-for-download sites like iTunes, Google Play, and Amazon by providing permanent downloads for free. The overall popularity of these sites and the staggering volume of traffic they attract evidence the enormous damage being inflicted on the U.S. record industry.

Several countries around the world have found these streamripping services to be unlawful, including Australia, Denmark, Russia, Spain, and Italy. Several streamripping services have also shut down

[16] 2019 Special 301 Report.

after a demand or lawsuit from the record companies. Unfortunately, however, new or variant streamripping services rise up to take their place.

We are currently tracking more than 200 active streamripping sites. The most popular and, hence, the most damaging of these streamripping sites are:

Mp3juices

Domain: mp3juices.cc
Registrant: Uses the privacy/proxy service Global Domain Privacy Services, Panama
Registrar: Pananames - URL Solutions, Panama
Hosting Provider: Servers.com and United Network, LLC, both in Moscow, Russian Federation; backend content servers – OVH (France)
Traffic: Global Alexa ranking of 2759, with nearly 1.3 billion visits in the past year
Revenue Source: Advertising

Mp3juices permits a user to select YouTube music videos and to make a permanent download of an audio-only mp3 file that can be added to the user's music library. The site itself provides search functionality to locate desired YouTube videos and then utilizes a separate service as the back-end for its distribution of mp3 downloads to the user. When users request an mp3 download, the files are served up from a separate domain that is not otherwise publicly accessible. This back-end function is currently operating from the domain *eaoe.cc*, has the same Whois registrar and privacy proxy service as *mp3juices.cc*, and is hosted on the same ISPs in Moscow.

Please note mp3juices.cc modified its infrastructure this past year changing the domain name of the back-end site and moving it from OVH in France and changing the back-end domain from *yxww.xyz to eaoe.cc*. The last publicly available Whois information identified the site registrant as an individual in Turkey.

Ytmp3 (formerly youtube2mp3.cc)

Domain: ytmp3.cc (formerly youtube2mp3.cc)
Registrant: Uses privacy/proxy service Global Domain Privacy Services, Panama
Registrar: Pananames - URL Solutions, Panama
Hosting Provider: Servers.com and United Network, LLC, both in Moscow, Russian Federation; backend content servers – OVH (France)
Traffic: Global Alexa ranking of 667, with over 1.2 billion visits in the past year combined to both domains
Revenue Source: Advertising

Ytmp3 is likely connected in some way to *mp3juices. Mp3juices* and *ytmp3.cc* are hosted on the same ISPs, and both use a separate back-end domain to copy, convert, and deliver the download file to the users. Content accessed through *ytmp3* site is also delivered through a domain that is not publicly accessible – in this case *oeaa.cc* – which operates with the same registrant information, registrar, and hosting provider as *ytmp3. Mp3juices* and its back-end delivery domain also operate from the same registrant information, registrar, and hosting provider. *Ytmp3* differs from *mp3juices* only in that it does not offer the YouTube search capability. Rather, it requires the user to otherwise locate the desired file on YouTube and then cut and paste a YouTube URL into its conversion bar, and the site then delivers an audio-only mp3 file ripped from the original video file.

Flvto & 2Conv

Domain: flvto.biz and 2conv.com
Registrant: Uses the privacy/proxy service DomainsbyProxy (DBP)
DBP disclosed the operator of both sites as Tofig Kurbanov, Russian Federation
Registrar: GoDaddy
Hosting Provider: Flvto.biz – IP Volume, Inc., The Netherlands; 2conv.com – Serverius Holdings, BV, The Netherlands
Traffic: Flvto.biz has a global Alexa Ranking of 597 and 2conv.com has global Alexa ranking of 1396; collectively the two sites have had over 1.7 billion visits in the past year.
Revenue Source: Advertising and questionable software downloads

Flvto.biz and *2Conv* are operated by the same individual in Russia and serve downloads of converted YouTube videos to users as digital audio files. All the user needs to do is to copy and paste a YouTube link into a conversion bar and click on a "convert to" button. As noted in our 2017 submission, these sites are essentially dedicated to the mass-scale piracy of our members' copyrighted sound recordings that are available on YouTube. Following some of our enforcement activity, they sites changed their operations slightly, but nonetheless continue to engage in unauthorized distribution of our members' music. We also have reason to believe that the operator may be involved in other streamripping sites as well.

U.S. record companies filed a lawsuit against these sites in 2018 in the United States District Court for the Eastern District of Virginia, alleging copyright infringement on a massive scale. The court granted the Russian defendant's motion to dismiss for lack of personal jurisdiction, despite substantial facts that support jurisdiction over the defendant in the United States. For example, in 2018 alone, the sites had almost 32 million United States users who, collectively, conducted over 96 million streamripping sessions and downloaded hundreds of millions of songs from defendant's servers to their own personal devices in the United States. The decision is now on appeal to the United States Court of Appeals for the Fourth Circuit.

MP3-YouTube

Domain: mp3-youtube.download
Registrant: Last publicly available information – Hedi Chaibi, Roubaix, France
Registrar: OVH SAS
Hosting Provider: OVH SAS, France
Traffic: Global Alexa ranking of 1301, with over 700 million visits in the past year
Revenue Source: Advertising

As its name implies, *mp3-youtube,* offers users the ability to convert a YouTube video to a free downloadable mp3 audio file. The site touts that "there is no simpler and faster youtube converter: you just paste the video URL link you want to download…and a few seconds later you get an mp3 in original quality." Its homepage goes on to boast that their "youtube mp3 converter is not only able to download videos from Youtube to mp3, it is compatible with the most popular websites: Facebook, Vimeo, Soundcloud, Instagram, etc."

Y2mate

Domain: y2mate.com
Registrant: Uses privacy/proxy service Whois Privacy, Panama; registrant believed to be Ken Nguyen, Hanoi, Vietnam
Registrar: NameCheap, Inc.
Hosting Provider: Hetzner Online GmbH, Germany
Traffic: Global Alexa ranking of 238, with nearly 775 million visits in the past year
Revenue Source: Advertising

Y2mate offers a search capability to locate YouTube videos or allows the user to cut and paste a YouTube URL into the search bar. Users are enabled to download either an audio-only mp3 or the entire audio-visual work as an mp4 file. The site also appears connected with the streamripping site youtubeconverter.io and provides users with a link to this service if they are unable to download the mp3 file via y2mate.

Converto

Domain: converto.io
Registrant: WhoisGuard Protected Inc., Panama
Registrar: NameCheap, Inc. USA
Hosting Provider: INSPIRIA Networks Ltd, Belize
Traffic: Global Alexa ranking of 6938. There have been over 90 million visits globally in the past year
Revenue Source: Advertising

Converto allows users to cut and paste a YouTube URL into the conversion bar on the homepage following which all the user needs to do is click on the "Convert" button. Users have the option to download either an audio-only mp3 file or the entire audio-visual work as an mp4 file. The site also allows users to cut a video, edit ID3 tags, and amend the filename.

2. ***Mp3 Search-and-Download Sites***

This class of sites directly or indirectly offers unauthorized on-demand streaming and/or downloading of our members' music, including their most popular and valuable content. Commonly, these sites also provide unauthorized downloading of pre-release music, i.e., tracks and albums that have not yet been commercially released to the public. As noted above, such infringing activity clearly harms U.S. artists, songwriters, record labels, and music publishers by disseminating their works without authorization and severely diminishing the commercial value of those works.

Newalbumreleases

Domain: newalbumreleases.net
Registrant: Uses privacy/proxy service Super Privacy Services, last identified registrant believed to be Sergey Kobilin, Svetogorsk, Russia
Registrar: Dynadot, LLC
Hosting Provider: WIBO (Czech Republic)
Traffic: Global Alexa ranking of 9,440, with nearly 64 million visits in the past year
Revenue Sources: Advertising

Newalbumreleases makes available a substantial library of newly released popular music content, as well as albums not yet commercially released. The site features the most recently uploaded albums on the homepage using album artwork. In addition, it organizes earlier posts by genre under menu tabs for Rock, Pop, Metal, etc. The homepage also offers a search capability for content by artist or title. The site hosts its content on cyberlockers and provides users with links to services like Rapidgator.net and Hitfile.net from which the files are available for download. All the files appear to have been uploaded to the cyberlocker sites by *Newalbumreleases*, as the download files usually include "newalbumreleases" in the file name. As the uploaders of the files, *Newalbumreleases* are direct infringers. Takedown notices sent by rights holders to this site are ineffective. The domain was suspended briefly in 2018 but the service resumed.

Rnbxclusive

Domain: rnbxclusive1.com
Registrant: Uses privacy/proxy service WhoisGuard
Registrar: Namecheap, Inc
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be Contabo GmbH
Traffic: Global Alexa ranking of 8,733, with over 8.4 million combined visits to the two domains in the past year
Revenue Sources: Advertising

Rnbxclusive is a popular Ukrainian-based service providing downloads for popular R&B and Hip-hop recordings, both full albums and popular tracks for free download. The site uses various problematic cyberlockers to host and distribute the files. Most recently, it began using two new cyberlocker sites, *suprafiles.me* and *cloudyfiles.me*. The site has also been a prolific domain-hopper, having hopped domains approximately 16 times since 2016, with 6 hops in 2018 alone.

Leakthis

Domain: Leakth.is
Registrant: Not disclosed
Registrar: Unavailable
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be Incrediserve LTD (Netherlands)
Traffic: Global Alexa ranking of 84,183, with over 7.5 million visits to the site in the past year
Revenue Sources: Advertising

Leakthis is, as its name implies, a site that specializes in the most damaging forms of piracy, which is the leaking of tracks and albums before their commercial release. The site itself is not a massively popular site, but it is the source of content that, once leaked, rapidly spreads across the entire music piracy landscape. Thus, its damage is measured not in how many users visit the site itself but by the massive distribution that takes place once the file is made available on the site.

Xclusivejams

Domain(s): Xclusivejams.in, Xclusivejams.net
Registrant: Newly registered domain, details protected
Hosting Provider: IP Volume Inc. Seychelles
Traffic: Global Alexa ranking of 162,114, with over 5 million visits to the two domains in the past year
Revenue Sources: Advertising

Xclusivejams makes available a substantial library of newly released popular music content, including albums and tracks that are not yet commercially released. The site homepage features the latest albums and songs made available by operators of the site for users to download. The site features a prominent search function that allows the easy access to sought after content. The site links to content via third-party websites including cyberlockers such as nippyspace.com.

3. BitTorrent Indexing Sites

BitTorrent indexing sites provide a searchable index of links to content which can be downloaded by users running the appropriate client software. Indexing services can generate revenue from advertising and/or user donations. The financial model, structure, and approach varies from site to site.

The following popular sites are the most egregious, based on: (i) the extent of the infringement, i.e., the number of users visiting the site to infringe copyright; (ii) the amount of unlicensed content on the site; and (iii) the site's failure to take steps to address the massive piracy problem across its network. Moreover, these BitTorrent index sites demonstrate they are dedicated to infringement by the way they organize and display the files they index. Files are typically organized into categories of movie, music, software, and games with file names clearly and unmistakably describing content in a way that the operators know they are distributing torrents for copyright-protected content.

Increasingly BitTorrent sites are registering multiple domains to mitigate the problem of their sites going offline if one of their domains is seized or blocked, and to work around search engine demotion algorithms. A simple change in the county code or other top-level domain allows the site to reappear in top search results.

ThePirateBay

Domain: thepiratebay.org (formerly thepiratebay.se, thepiratebay.vg)
Registrant: Fredrik Neij, Stockholm, Sweden
Registrar: easyDNS Technologies Inc.
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be Lir.bg EOOD, Bulgaria
Traffic: Global Alexa ranking of 169, with nearly 686 million visits in the past year. This figure does not capture the myriad of mirror sites that are constantly being generated to get around blocking orders against the site from numerous countries around the world.
Revenue Sources: Advertising, pay-per-install of potential malware

Thepiratebay remains the single most popular BitTorrent index site in the world. This continues to be the case even though courts in a multitude of countries around the world (including Austria, Belgium, Denmark, Finland, Iceland, Ireland, Italy, Portugal, Spain, and the UK) have issued orders blocking access to the site in their jurisdictions. Earlier this year, *thepiratebay* began blocking U.S. IP addresses. However, the site remains easily accessible using a free proxy service that makes it appear the user is accessing the site from another jurisdiction. The world's most popular and newly released films and vast catalogues of music can be downloaded via the site. The site makes no pretense of legitimacy, fails to respond to any takedown notices, and has previously ridiculed those who have sent them such notices.

There are a number of other very popular BitTorrent index sites that operate in essentially the same fashion as *thepiratebay*, making a broad range of copyrighted content downloadable using the BitTorrent P2P protocol. The worst of these sites include:

1337x

Domain: 1337x.to (site lists mirror infringing domains as including 1337x.se, 1337x.st, x1337x.ws, x1337x.eu, and x1337x.se)
Registrant: None provided for .to TLD
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be the bulletproof ISP FlokiNet, Ltd.

Traffic: Global Alexa ranking of 344, with nearly 710 million visits in the past year
Revenue Sources: Advertising, pay-per-install of potential malware

Rarbg

Domain: Rarbg.to
Registrant: None provided for .to TLD
Hosting Provider: Nets App/S A and A Stroi Proekt EOOD, Bosnia and Herzegovina
Traffic: Global Alexa ranking of 262, with 1.5 billion visits in the past year
Revenue Sources: Advertising, pay-per-install of potential malware

Torrentz2

Domain: torrentz2.eu (mirror or copycat sites may include torrentz2eu.xyz, torrentz2.is)
Registrant: None provided for .to TLD
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be Private Layer, Inc.
Traffic: Global Alexa ranking of 573, with 547 million visits in the past year
Revenue Sources: Advertising, pay-per-install of potential malware

Limetorrents

Domain: Limetorrents.info
Registrant: iWebsPro, Panama
Hosting Provider: Fishnet Communications, LLC, Russia
Traffic: Global Alexa ranking of 2,127, with 201.9 million visits in the past year
Revenue Sources: Advertising, pay-per-install of potential malware

Seedpeer

Domain: Seedpeer.me
Registrant: Contact Privacy Inc.
Hosting Provider: BlueAngelHost Pvt. Ltd, Bulgaria
Traffic: Global Alexa ranking of 23,547, with 16.83 million visits in the past year
Revenue Sources: Advertising, pay-per-install of potential malware

4. Cyberlockers

A "cyberlocker" is a type of website/service which enables users to upload, store, and distribute digital files on a dedicated storage infrastructure on the Internet that is controlled, managed, and maintained by the website's operator. Although there appears to be some similarity between cyberlockers and legitimate cloud storage services (as they both allow users to upload files to servers for storage and sharing), their business models are strikingly different. The business model for legitimate storage services is principally based around personal file storage and limited ability to share access to the files. Cyberlockers are all about maximizing and monetizing traffic to their service. Nothing draws traffic like popular copyrighted content that can be downloaded for free. Thus, their business model is, at its heart, the distribution of unlicensed content.

Cyberlockers typically earn revenue from one or more of the following means: advertising such as banner and "pop-up" ads, which typically appear on the pages where the files to be downloaded are accessed; and sale of "premium accounts," which offer users benefits such as greatly increased download speeds, no-wait downloads, and simultaneous downloads – all features of particular

interest to users who want to download large files such as films and albums. Some cyberlockers provide financial rewards to uploaders whose content draws large volumes of traffic to the site (which translates to advertising dollars) or when a downloader purchases a premium account after accessing an uploader's content. Conversely, cyberlocker sites often have a policy of deleting content uploaded by non-paying users that is not regularly downloaded by others – in other words, content which is not drawing traffic to the site. Finally, these services provide little if any accountability for infringing uploaders. Files can often be uploaded without even opening an account, or free accounts can be opened with nothing more than an email address. Thus, there is no ability to police uploaders nor effectively remove repeat infringers from their system. The fact of the matter is that, for many of these services, there would be no economic viability in the absence of traffic generated through piracy.

To a limited extent, rights holders can attempt to tackle these infringements by sending takedown notices to the site operators. However, this often entails monitoring thousands of third-party link resources – e.g., blogs, forum sites, and search engines – to locate the information that is needed to notify the locker of infringements occurring on their own services. These services are in a much better position to identify infringing content being uploaded to or distributed from their own servers if they really had an interest in conducting their business legally. There are efficient and reasonable technological solutions available that would assist in this. Some cloud services, for example *Mediafire* and *Depositfiles*, have successfully employed such technology.

The following are some of the most problematic cyberlocker sites plaguing the U.S. music industry:

Zippyshare

Domain: zippyshare.com
Registrant: Uses privacy/protection service Contact Privacy Inc. (Canada)
Registrar: Tucows Domains Inc. (Canada)
Hosting Provider: OVH SAS (France)
Traffic: Global Alexa ranking of 335, with 1.2 billion visits in the past year
Revenue: Advertising, pay-per-install of third-party applications

Zippyshare is operated by an individual in Poland, has particularly high traffic, and is notably used for downloads of infringing music over other forms of content. Like other cyberlockers, it generates shareable URLs to content uploaded to its servers by users and, when those URLs are accessed, it makes those files available to download or stream via an embedded music player. Its revenue is derived primarily from advertising (notably it does not offer reward schemes or premium accounts). While the site responds to takedown notices, it permits the anonymous upload of content to the site so there is no way to screen out those who abuse the service or simply repeatedly re-upload content that was previously removed. The Google Transparency Report reveals (as of September 2019) that Google has received notices to delist over 13.5 million *Zippyshare* URLs from its search results. Proceedings alleging that the site is directly liable for copyright infringement are currently underway before the High Court of England and Wales.

Rapidgator

Domain: rapidgator.net (and rg.to, which redirects to rapidgator.net)
Registrant: Uses privacy/proxy service Whois Privacy Corp., Nassau, Bahamas *Registrar*: Internet.BS Corp.
Hosting Provider: NetVillage Ltd, (Russia)
Traffic: Global Alexa ranking of 906, with 313 million visits in the past year
Revenue Sources: Advertising, pay-per-install of potential malware, pop-unders and redirects to third-party sites, and premium accounts

This cyberlocker launched in October 2011 and has from the outset been a major source of the distribution of infringing music content. *Rapidgator* is also a major source of pre-release content, i.e., content leaked on the Internet without authorization prior to its public release date. The site offers a rewards program that shares revenue with uploaders whose material draws large volumes of traffic, thus encouraging the upload of popular copyrighted content (particularly pre-release) and undercutting any pretense that it is operating a simple cloud-based personal storage service. The Google Transparency Report reveals (as of September 2019) that Google has received delisting requests relating to over 33.7 million *Rapidgator* URLs. Despite the volume of infringements detected and removed from *Rapidgator*, the same content re-appears and there is no effective action being taken to prevent infringement by the service. Although it provides rights holders with a takedown account, this does nothing to prevent: i) content from being disseminated (via links generated by the site) in the window *before* rights holders can intervene to take it down; ii) content which is re-uploaded after removal; and iii) content which appears in multiple locations within the site, rendering such a takedown account not a sufficiently effective solution. Users complain on social media of being ignored when trying to cancel premium accounts and failure to deliver on premium services. In 2018 and 2019, on applications brought by the game and music industries, the German courts issued preliminary decisions finding the site liable for copyright infringement, and in 2019 the Russian court ordered ISPs to block access to *Rapidgator*. The corporate structure of *Rapidgator* uses a sophisticated network of offshore companies and specialized corporate vehicles to obscure the underlying beneficiaries. It is believed to be operated from Russia.

Turbobit

Domain: turbobit.net
Registrant: Uses privacy/proxy services Whois Privacy Corp., Nassau, Bahamas
Registrar: Internet.BS Corp.
Hosting Provider: Serverius Holdings, BV, The Netherlands
Traffic: Global Alexa ranking of 1282, with 327 million visits in the past year
Revenue Sources: Advertising, pay-per-install programs, paid premium accounts

Turbobit is one of the top cyberlocker sites for music piracy with nearly 360,000 infringing links identified in the past year. *Turbobit* along with *rapidgator* are two popular sites used by download sites like *newalbumreleases* to store infringing files for download. *Turbobit* derives revenue from premium accounts, advertising placed on the site, and through likely revenue-sharing arrangements with the uploaders of popular content that will attract the most traffic to the site. We believe the rewards/revenue-share arrangement is run via a separate website, costaction.com. *Turbobit* has been operated from the same IP address as (and is believed to be in common operation with) another cyberlocker called *hitfile* (described below). Its operators are unknown.

Hitfile

Domain: hitfile.net
Registrant: Uses privacy/proxy service Whois Privacy Corporation, Bahamas
Registrar: Internet Domain Service BS Corp.
Hosting Provider: ISPIRIA Networks Ltd, Netherlands
Traffic: Global Alexa ranking of 11448, with over 32.4 million visits in the past year
Revenue Sources: Premium accounts and advertising

Hitfile is another classic cyberlocker that has been in operation for over a decade. It makes available copyright protected content without authorization and offers a rewards scheme. It has been operated from the same IP address as (and is believed to be operated in common with) *turbobit*. Its operators are unknown. The Google Transparency Report reveals (as of September 2019) that Google has

received notices to delist over 900,000 *Hitfile* URLs from Google's search results.

Chomikuj

Domain: chomikuj.pl
Registrant: Unavailable (technical contacts for the site link it to Belize and Cyprus)
Registrar: Instra Corporation Pty Ltd (Australia)
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be LeaseWeb Netherlands, B.V. (Netherlands)
Traffic: Global Alexa ranking of 4,054, with almost 300 million visits in the past year
Revenue Sources: Advertising, paid subscriptions

This site is the most popular cyberlocker in Poland. Over 80% of the visitors to *chomikuj* are in Poland, but the site hosts a broad range of U.S. repertoire. The site enables users to upload files (e.g., music, films, images, software, books) to the site and then share links to the content. Users can choose a free account or pay for an account via subscription or paid text messages. The site offers rewards to users who upload popular content downloaded by other users. The site appears to be owned and operated by a company called FS File Solutions Limited, registered in Nicosia, Cyprus. The Google Transparency Report reveals (as of September 2019) that Google has received notices to delist approximately 26.5 million URLs from its search results. The site has been the subject of litigation in Poland. In September 2017, the Krakow Court of Appeal held that *chomikuj* could not claim safe harbor protection because it was not "passive" and had infringed copyright.

Dbree et al

Domain: dbree.org and related domains noted below
Registrant: Not disclosed
Registrar: Internet Domain Service, BS Corp., The Bahamas
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be Incrediserve LTD (Netherlands)
Traffic: Global Alexa ranking of 27,710, since emerging in April of this year the site has generated 1.8 million visits. The entire network of associated sites has generated 7.4 million visits in the past year.
Revenue Sources: Advertising

Dbree.org is a new locker site that appeared after another notorious locker site, *dbr.ee*, used extensively by pre-release leak networks went down. The new *dbree* is connected with a wide array of other file-hosting locker sites that demonstrate the ease with which these sites appear and disappear as content owners close in on them. In this case, the site is associated with *nippyspace.com, nippyshare.com, nippyfile.com, nippydrive.com, nippybox.com, latestmusic2018.com, xclusivejams.in, xclusivejams.net, etc*. *Dbree* is commonly found to be distributing the pre-release and newly released popular music files linked to from sites like *leakth.is*. *Dbree* and the related nippy sites are completely unresponsive to rights holder notifications of infringement.

Uploaded

Domain: uploaded.net / ul.to
Registrant: Cyando AG
Registrar: Namecheap.com
Hosting Provider: Uploaded-de, Germany
Traffic: Global Alexa ranking of 1412, with over 320.6 million visits in the past year
Revenue Sources: Premium Accounts

Uploaded is another classic cyberlocker which makes available copyright protected content on the Internet without rights holder authorization. Premium accounts and a 'per-premium-sale' rewards scheme generate revenue and incentivize unauthorized making available of copyrighted protected content. The Google Transparency Report reveals (as of September 2019) that Google has received delisting requests relating to over 26.1 million *uploaded* URLs. In October 2012, German authorities successfully criminally prosecuted a previous operator of *uploaded*, but the site was subsequently taken over and continues to operate under the ownership of a Swiss company and is hosted in Germany. Courts in Germany have found the site liable for copyright infringement and issued numerous preliminary decisions against it in actions brought by rights holders. The German FCJ has referred questions in relation to the site's direct liability for copyright infringement to the Court of Justice of the European Union, on which a decision is due, not before the latter half of 2020.

Nitroflare

Domain: nitroflare.com
Registrant: WhoisGuard, Inc., Panama
Registrar: Namecheap.com
Hosting Provider: Global Layer B.V., Netherlands
Traffic: Global Alexa ranking of 3958, with over 106.3 million visits in the past year
Revenue Sources: Premium accounts

Nitroflare is another classic cyberlocker, hosted in the Netherlands, which makes available copyright protected content on the Internet without rights holder authorization, including pre-release content (i.e., content leaked onto the internet prior to its public release date). It offers premium accounts and an affiliate program through which users can "earn money." Despite the infringements detected and notified to the site, the same content re-appears, and/or appears in multiple locations, and there is no effective action being taken by the service to prevent such infringements. Although it offers rights holders a takedown tool, *nitroflare* does nothing to prevent content from being disseminated via links generated by the site in the window *before* rightsholders can intervene to request its removal.

Share-online

Domain: share-online.biz
Registrant: Xlice AG, Panama
Registrar: NameCheap, Inc.
Hosting Provider: Leaseweb, Netherlands
Traffic: Global Alexa ranking of 3214, with over 72.7 million visits in the past year
Revenue Sources: Advertising, premium accounts, and partner programs

Share-online is a classic cyberlocker making available copyright protected content on the Internet without authorization from copyright holders, offering reward schemes and premium accounts, as well as deriving revenue from advertising and partner programs.

Filecrypt (link protector)

Domain: filecrypt.cc
Registrant: Current Whois record shows "REDACTED FOR PRIVACY".
Registrar: Enom, Inc. (U.S.)
Hosting Provider: Virtual Systems LLC, (Ukraine)
Traffic: Global Alexa ranking of 1595, with 141.7 million visits in past year
Revenue Sources: Banner advertisements

Filecrypt is a link protection service designed to protect links to infringing files, such as links to infringing copies of our members' music, from identification and takedown. Essentially, it acts as an encrypted, pirate linking service to infringing files. Filecrypt does not meaningfully apply a DMCA or

copyright policy. Instead it makes a declaration on its abuse page stating that *filecrypt "does **not** host files but offers the users the possibility to provide clearly arranged hyperlinks."*

Registered users can both create containers to encrypt and share links. The "containers" can include multiple mirror links where copies of the infringing file ~~is~~ are hosted. The ability to include mirror links is significant as it makes take downs harder by ensuring that, where possible, the linking container will always contain one or more active links where the file can be accessed. The service is most frequently utilized by sites that engage in the distribution of pre-release leaks where rapid takedown of infringing files is most important.

Filecrypt engages in a sophisticated and targeted scheme that encourages copyright infringement by paying out to those who create and distribute links to such content via their service. The music industry has actioned over 15,500 links on filecrypt with only approx. 2,800 removed.

5. Unlicensed Pay-for-Download Sites

A dozen or so websites are based in Russia and the Ukraine that engage in the unlicensed sale of singles and albums at a fraction of the cost found on licensed services. The fact that they pay no royalties to copyright owners allows them to completely undercut legitimate licensed services. The sites look professional, utilizing official album art and selling all the latest releases as well as popular older catalog works.

Mp3va
Domain: mp3va.com
Registrant: Uses privacy/proxy service MyPrivacy.net Ltd. (Canada)
Registrar: easyDNS Technologies, Inc.
Hosting Provider: Filanco LTD (Russia)
Traffic: Global Alexa ranking of 83,770, with 8.7 million visits in the past year
Revenue Sources: Sale of singles and full albums

Mp3va engages in the unlicensed sale of music. The site has the look and feel of a legal music site like Amazon or iTunes; however, it sells single tracks for an average of 15 cents and full albums for about $1.50. Music is sold by the file size, so the cost of singles and albums varies slightly. Users must set up an account and add money to the account, using credit cards or payment intermediaries. Major U.S. credit card and payment processors have terminated support for the site, but offshore intermediaries can still be used. While the operator of the site is currently masked behind a privacy proxy service, older Whois data indicated the site was run by companies in Russia and Cyprus.

Mp3fiesta
Domain: mp3fiesta.com
Registrant: Sergey Novato, Streamusic Ltd (Nicosia, Cyprus)
Registrar: Key-Systems GmbH
Hosting Provider: ASN-AVANTEL-MSK (Russia)
Traffic: Global Alexa ranking of 235,965, with 1.4 million visits in the past year
Revenue Sources: Sale of singles and full albums

Mp3fiesta operates exactly like *mp3va* in its sale of unlicensed music. Like *mp3va,* the site has the look and feel of legal music sites like Amazon or iTunes; however, it sells single tracks for an average of 15 cents and full albums for about $1.50. Music is sold by the file size so the cost of singles and albums varies slightly. Like on *mp3va, mp3fiesta* users must set up an account

and add money to the account, using credit cards or payment intermediaries, and then purchases are made drawing down from funds available in the account.

Music-bazaar

Domain: music-bazaar.com
Registrant: Music-bazaar Co. Ltd. Moscow Russia
Registrar: Regional Network Information Center, JSC dba RU-CENTER
Hosting Provider: Reg.Ru Russia
Traffic: Global Alexa ranking of 245,021, with 1.865 million visits in the past year
Revenue Sources: Sale of singles and full albums

Music-bazaar operates exactly like *mp3va* in its sale of unlicensed music. *Music-bazaar* is a direct download music website, where users can both stream and download copies of unauthorized infringing music content. The site claims to have over 1,500,000 tracks available. Anyone can use the site to browse content; however, only registered account-holders can download or purchase any content from the site.

6. Additional Issues

Piracy within Mobile Apps

Telegram App: Telegram is an instant messaging service which allows users to communicate via text and voice message. As such, the app is of no special concern. However, Telegram users are able to create channels which allow the operator of the channel to distribute messages and content to all members of the channel. Often channels include scripts known as bots which provide some level of interactivity within the channel, sometimes allowing users to request specific content from the channel. Telegram offers many user-created channels which are dedicated to the unauthorized distribution of copyrighted recordings, with some channels focused on particular genres or artists. Telegram itself hosts many of the copyrighted recordings made available through these channels and the RIAA has sent DMCA notices to Telegram containing over 18,000 instances of copyrighted recordings offered without authorization through these channels.

Telegram claims that it forwards our notices to the channel operators who are responsible for removing the infringements listed in our notices. We have found, however, that most channel operators appear to take no action in response to our notices, with nearly all of infringements listed in our notices remaining available. Likewise, Telegram makes no apparent attempt to verify that channel operators have complied with our notices and does not seem to have any kind of repeat infringement policy. Telegram is accessible through various client applications, including popular mobile apps available through the Apple App Store and Google Play.

Bulletproof ISPs

As noted above, infringing sites are turning more towards offshore hosting ISPs that support the sites' infringing activities. These "Bulletproof" ISPs support various types of criminality through considerable leniency in the kinds of materials they permit to be uploaded and distributed via their networks. These ISPs do not respond to notices of infringement or warning letters that the ISP is hosting and supporting known infringing sites. The two most problematic bulletproof ISPs that support infringing activity relating to music are:

- **Ecatel/Quasi Networks (Novogara LTD and Incrediserve LTD) – Seychelles / Amsterdam.** Ecatel is a Dutch hosting provider founded in 2005, registered in the UK, and headquartered in The Hague. It offers offshore hosting options and, over the last decade, has consistently hosted criminal and toxic content, and generated spam and DDoS traffic from its IP space. Ecatel is known to law enforcement, has been shut down by its peers at least once (in 2008), and was subject in 2012 to DDoS attacks by Anonymous for hosting child pornography. In 2017, BREIN raised an action against Ecatel and its associated hosting companies for the hosting of, and failure to remove, infringing and illegal content. One such associated hosting company is Quasi Networks (http://www.quasinetworks.com/) operated from Mahe, Seychelles with the infrastructure located in the Netherlands. Quasi Networks is responsible for hosting various sites engaged in the transmission of pre-release works, including *dbree.org*, and the series of "*nippy" prefixed locker sites*, *xclusivejams*, *mp3monkey.net*, *gosongs*, and *leakth.is*. With little recourse to remove infringements, both Ecatel and Quasi represent a significant danger to our member companies.

- **FlokiNET – Romania/Iceland/Finland.** FlokiNET (https://flokinet.is/) is a web hosting service that prides itself on allowing the completely anonymous hosting of content across its three server locations: Romania, Iceland, and Finland. In a recent case involving pre-release music piracy for a site known as *musicmafia.to*, FlokiNET was listed as the registrant of the domain. FlokiNET advertises quite openly, "We do not require any personal details or identification; any valid e-mail address is enough information to be a client." As a result, many different types of websites hosted on the ISP host bestiality pornography and fraudulent sites, amongst others. Other infringing sites hosted on FlokiNet include *avxhome.se*, *djnotorioussam.com*, and *x1337.to*. The operator of FlokiNET is known to the authorities and resides in Romania but, to date, no action has been taken to close the service.

Nigerian-Operated Infringing Sites

We have continued to see a significant growth in the number of Nigerian-operated sites that are distributing direct download links for pre-release and newly released music affecting our member companies. The number of such infringing sites with a Nigerian operator stands at over 400. These sites are a great cause for concern to the industry as they generally disregard infringement notices and refuse to disable access to content. They are particularly damaging as they prevent the growth of legitimate services in emerging markets. The sites' primary method of promotion is via Twitter, and most sites make use of the Nigerian-operated ISP speedhost247.com.

PHYSICAL MARKETS

In 2018, physical CD and vinyl album sales continued to generate considerable revenue for U.S. record companies. Prominent ecommerce platforms have become the ideal outlet for counterfeit physical products being produced in Russia and China. In some cases, Russian and Chinese sellers will sell directly on retail platforms, shipping the goods to consumers from Russia or China. In other cases, the principals behind the Chinese and Russian counterfeits sell to third-party sellers on platforms that may or may not know they are buying and reselling counterfeits.

Chinese and Russian Counterfeit CD Manufacturing and Distribution

Counterfeit CDs and vinyl albums being manufactured and sold out of China and Russia are high quality products made to closely resemble authentic ones. These counterfeits can be readily identified by our experts even though the tell-tale signs of counterfeits are not apparent to casual

observers. The outside packaging copies pull tabs, security seals, and shrink-wrap, while the insert booklets will mirror the legitimate versions of the product, printed on high-grade commercial printing machinery. In addition to straight-up counterfeit copies of legitimate album releases, we have also seen a rise in the manufacture of compilation "Best of" and "Greatest Hits" albums that were never released by the record labels. Finally, we are finding vinyl versions of albums released only in CD format (i.e., that were never released on vinyl).

Test purchases have established that massive quantities of these counterfeits were finding their way into the legitimate market principally through various ecommerce platforms like Amazon, eBay, and AliExpress. Consumers are paying full price for counterfeit offerings appearing alongside legitimate offerings, resulting in a one-for-one displacement of a legitimate sale.

An essential element for these platforms in protecting their customers and copyright owners from these Chinese and Russian counterfeits lies first and foremost in pre-screening sellers to ensure they have legitimate sources of supply. Amazon has initiated such a program, but the other major platforms have not. Each of these platforms has established processes by which counterfeit offerings can be reported and removed; however, there appears to be inconsistent action against repeat infringers. In addition, titles identified as infringing because there is no legal version of the title (e.g., "greatest hits", vinyl albums) are not being removed from platforms across the board. More can be done by ecommerce platforms to prevent counterfeit products illegally being manufactured and sold from Russia and China from infiltrating the legitimate marketplace here and around the world.