

March 2010

Online Piracy and Counterfeiting Overview

For US Chamber of Commerce



GLOBAL
INTELLECTUAL PROPERTY
CENTER

MarkMonitor®

Online Piracy and Counterfeiting Overview

For US Chamber of Commerce

Contents

Introduction	3
Selling counterfeit physical goods: types of sites.....	4
Types of counterfeit and pirated goods sold.....	5
Selling fake digital goods: types of sites	6
Exploit methods	8

In 1993, a now famous *New Yorker* cartoon laughed at anonymity and the Web in its caption, “On the Internet, nobody knows you’re a dog.” Never has that observation been truer than today when it comes to the buying and selling of online goods. Unlike the physical world where shady street corner vendors offering obviously “knocked-off” handbags and other items are easily identified, it is difficult to discern legitimate sellers from illegitimate ones online. Part of the problem is that the market for counterfeit and pirated goods encompasses a wide variety of both physical and digital items. And as the Internet becomes more pervasive, the risk of accidental and intentional consumption of counterfeit and pirated goods increases, attracting more thieves and other opportunists, and escalating the collateral danger to consumers.

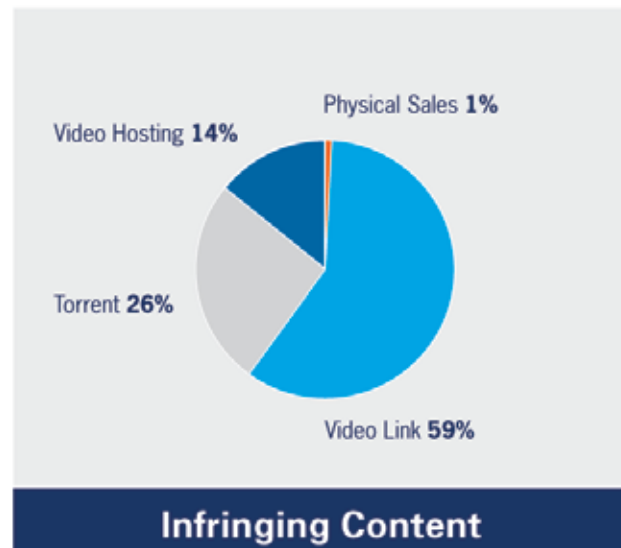
It is a big business too. In 2009, MarkMonitor® estimated \$133 billion of counterfeit goods were sold online worldwide. This is a significant percentage when you consider that the World Customs Organization estimates fake goods are a \$500 billion business annually, about seven percent of total world trade.

It is almost too easy to find counterfeit and pirated goods online. A quick search of the latest popular movie, Top Ten song, designer clothing label, or popular drug can quickly locate a wide variety of illicit merchandise within seconds. And these search results generate traffic rapidly: a few mouse clicks later and these goods are available for purchase or download. A single movie title had more than 140,000 illegal downloads within a few days of its theatrical release in Fall 2009.

In a survey of nearly 4,000 websites that included that same movie title in their content, over a third of them had content that was either illicit or infringing upon the copyrighted movie. See graphic to the right.

The online fakery ecosystem is immense and multi-faceted, involving many players, crossing national borders, and covering many dimensions. Setting up shop is simple, especially these days where the tools to create an eCommerce website can be had cheaply and from hundreds of sources. As the tools improve, piracy is shifting from music to all sorts of digital content, and the thieves are getting more sophisticated in trapping often unwary victims. The cross-border nature of the problem can lead to jurisdictional issues in law enforcement, forcing responsibility for a solution onto brand owners and the relevant industry.

“*On the Internet, nobody knows you’re a dog.*”
 -New Yorker, 1993



Selling counterfeit physical goods: types of sites

When it comes to selling counterfeit physical goods – such as shoes, clothing, luxury items and drugs – there are three different categories of websites that offer a variety of services and play important roles in bringing buyers and sellers together. First are **eCommerce sites**, online storefronts where you can browse, select, shop and purchase the merchandise. Online merchants take great pains to indicate their legitimacy, by using a variety of trusted certifications and using secured websites. However, savvy thieves are adept at following the 'best practices' used by legitimate sites to create their own illicit sites. They even make wholesale copies of the page layouts and brand logos, so to appear at first glance to be legitimate.

A second type of site is **online auctions**, most familiarly eBay, but hundreds of others exist that are more specialized. While there are measures in place to avoid the sale of fake goods that infringe on trademarks, and the auction administrators will remove these items quickly when requested, there are still many sellers that will attempt to post questionable merchandise.

A final type of site is the **business-to-business exchange**, which sells in quantity at wholesale prices to businesses. These sites are notable because of the sheer volume of suspicious goods that they can move and the wide range of markets that they can touch. In the example below, one seller is advertising the availability of bulk quantities of prescription drugs as well as branded apparel and sunglasses.

To further illustrate this point, the number of exchange listings selling illicit drug compounds continues to grow. In the Summer 2009 Brandjacking Index®, examining the online pharmaceutical industry, MarkMonitor found that business-to-business (B2B) exchange listings for bulk quantities of pills and active pharmaceutical ingredients (APIs) grew by 67 percent from the first study conducted in 2007.

To get a sense of how some of these illicit eCommerce sites drive traffic, MarkMonitor recently investigated how paid search ads led to websites offering counterfeit and pirated goods. The research examined 20 of the top 1,000 product-related searches from 2008 and focused on paid search ads across the three major search engines – Google, Yahoo! and Bing. In total, we analyzed 583 unique websites to which the ads pointed.

The screenshot displays a B2B marketplace interface. At the top, there is a navigation menu with options like 'Home', 'Sell Offers', 'Buy Offers', 'Products', 'Companies', and 'Member Area'. Below this is a search bar and a list of product categories. The main content area features a product listing for '100mg With 4pills-Box' by 'international trade CO., LTD'. The listing includes a 'Free member' badge, a 'Member Since Mar 2008' badge, and a 'Posted Date: April 07, 2008'. There are buttons for 'Send Email', 'Add to Basket', and 'Send Fax'. A 'Products Catalog (7)' overlay is positioned over the product details. At the bottom, two search ads are visible, one for 'Sunglasses' and one for 'New Jersey'.

The findings revealed that approximately 17 percent of the paid search ads for popular consumer products – such as designer handbags and shoes, music, movies, and hi-tech gadgets – led to sites likely offering counterfeit or pirated goods. This number rose for certain categories, such as “designer handbags,” where an eye-opening 32 percent of the paid search ads led to sites appearing to sell fake handbags. When terms like ‘cheap’, ‘discount’ or ‘wholesale’ were added to the searches, additional increases occurred. Across all 20 product searches, for example, the share of paid search ads linking to sites selling possible counterfeits increased from 17 percent to 19 percent when these terms were added. In the designer handbag example, the share of paid search ads linking to suspect counterfeit sites jumped from 32 percent to 49 percent by adding one of these terms.

These results indicate that counterfeiters have mastered the art of targeting buyers looking for unbelievable deals. While consumers need to be more vigilant if they’re seeking authentic products at good prices. Brand owners also need to be cognizant of the paid search strategies employed by fraudsters and monitor not only for the use of their trademarks or product categories as keywords, but also in conjunction with terms that are popular with consumers but may signal counterfeit or pirated products.

“Counterfeiters have mastered the art of targeting buyers looking for unbelievable deals.”

Types of counterfeit and pirated goods sold

Illegitimate copies of a wide variety of both digital and physical goods are available on any number of websites. From aircraft spare parts, weighing several tons, to lighter-weight items like branded sports apparel and footwear, counterfeiters find the Internet a profitable business venue.

One of the busiest online marketplaces is pharmaceuticals, where fakes are often available in packaging that closely mimics the original. The price variation in these sites is a valuable tip-off: discounts of 90 percent of the prices at legitimate pharmacies are typical. For example, the Summer 2009 Brandjacking Index identified large pricing discounts as an indication of suspicious prescription drugs. The study found certified pharmacies selling one drug at an average price of \$14 per dose while illicit pharmacies posted prices ranging from 70 cents to less than \$5 per dose. And on the business-to-business exchanges, large quantities of pharmaceuticals were available in bulk for pills as well as for active pharmaceutical ingredients – but not necessarily the true active ingredient.

Because of the potential for large profits, luxury goods such as perfumes, jewelry and designer handbags are also popular targets for counterfeiters. The thieves take advantage of the powerful brands and consumer desire, using them to sell counterfeit versions of their goods.

When it comes to digital goods, the situation is far worse. First-run movies that have yet to make it to the rental market are usually available online within a few hours of appearing in theaters, often copied by an amateur videographer sitting in the audience. Software and music can be downloaded from hundreds, if not thousands of sites. And videogames are the latest digital empire to see widespread copying – in some cases, there are illegal online networks that use pirated copies of popular video games that have been specifically designed by criminals to spread computer viruses while collecting monthly subscription fees!

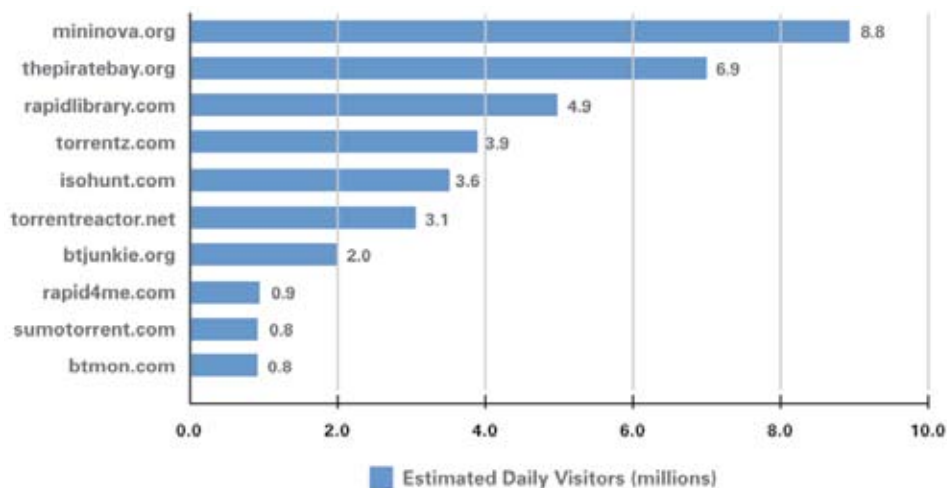
Selling fake digital goods: types of sites

There are several different types of online sources offering digital goods, and often the type and file size of the digital content drives the technology and site that deliver it.

The most common are **peer file sharing sites**, such as Limewire and BitTorrent. Larger files such as software and movies are split into several pieces on users' PCs, and then these files are made available to others on the Internet. When someone is interested in this content, they search the Web to find the location of the files that comprise the desired content, then download the individual files to their own hard drive and re-assemble them to play the movie or run the software on their machine.

While the peer sharing sites were made infamous during the 1990s by the Napster case, they remain very popular outlets for digital goods for many reasons. First, it's all about convenience, selection and speed. Legal sites often play a short commercial before streaming video content and have dramatic geographical limitations. Other legal sites cap the number of downloads for a particular time period. And, more often, legal sites don't offer recently-released content for public viewing without a fee. Illegal sites offer speedier downloads, few restrictions, low- or no-cost downloads, and the most up-to-date—and often pirated—content. In addition, peer-sharing sites are resilient due to multiple copies of the illicit content and fast because they distribute content and bandwidth across many machines and the Internet itself.

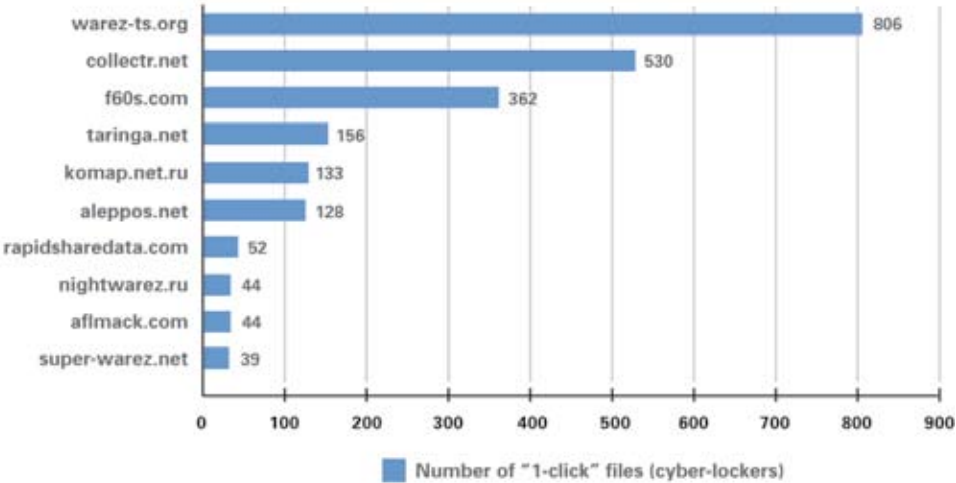
Furthermore, it is easy for anyone to locate the specific content desired. There are specialized search engines that are designed to allow users to find the movie or software program within a few mouse clicks. They go by names such as Mininova.org and RapidLibrary.org. In the chart below, the most popular search sites are shown, including daily visitor counts in the millions:



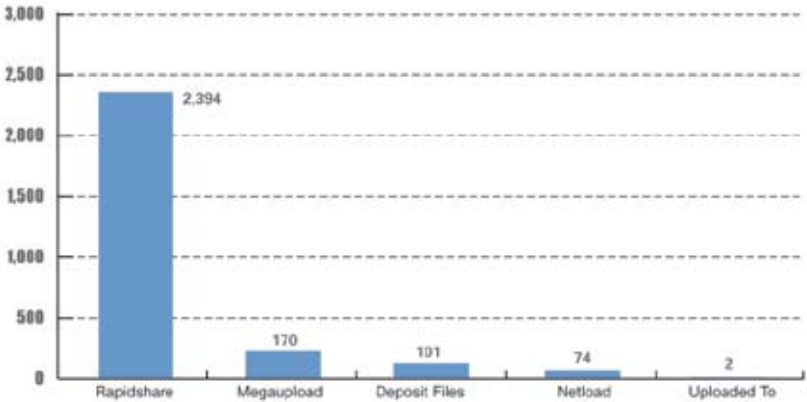
Finally, it is about security by obscurity. Because the files remain on millions of individual computers, they can avoid detection. Because the file-sharing operators have historically been considered "common carriers", there has been a historic reluctance to prosecute individuals. Various court cases and policy changes have altered the landscape: Mininova, for example, state that they will no longer search for illegal content. However, copies of illegal digital files are widespread.

The exchange of files in this manner is not a passing fad; the peer-to-peer sharing site BitTorrent itself has at times been responsible for a large share of Internet traffic over the past several years, including legitimate Web and email traffic, with roughly a third to more than half according to some sources. In contrast, it wasn't all that long ago that simple email traffic had the lion's share of Internet traffic.

A second source of digital content is called **cyberlockers**, where a user uploads files, typically via a Web browser, to a central site that can be shared by others. These services are used for many legitimate purposes, such as online backups of PC files. But there are some that offer potentially pirated and sometimes salacious content, such as Rapidshare, Megaupload, and others. Some of the sites have made it easier to download the dozens of files that make up a movie with a single click, so that even unsophisticated users can copy pirated content.



A search for a recent first-run movie found the following results, with the number of copies of the movie found on each service:



The good news about many of these peer sharing and cyberlocker sites is that they can be responsive to effective enforcement strategies, as was the case for Mininova. The bad news is that there are so many people uploading new content daily, as you can see from our chart, that constant vigilance is required. More bad news is that often the digital files are either poor copies, or contain viruses or other infections that can turn 'victims' PCs into a dangerous mess, as described in the next section.

Exploit methods

Just as the types of sites offering stolen content vary, so too are the tools of the online fakery trade. What is worse is that the criminals are getting better at using them to produce results. Let's look at just a few of these methods.

One of the best-known forms of Internet fraud is **phishing**, which is the act of sending out plausible email or social media communications that direct the victim to an illegitimate site that collects identity data, passwords, and account information in order to exploit it. Phishers are getting more sophisticated, targeting their victims more carefully, and still seeing tremendous success as witnessed by the rising number of attacks.

The fastest growing form of fraud is **malware** – or malicious software – which is increasingly deposited on as many PCs as possible, usually without the victim's knowledge. These PCs are then used to coordinate attacks on others, in effect assembling a gigantic army of digital demons, or 'bot nets', that can invade corporations and steal additional information. These digital infections are often downloaded via peer file sharing networks that have posted the malware posing as the required player for a first-run movie, a pop tune or an infected version of a commercial software program.

Search engines have become the main navigation aid for Internet users, but sadly many listings point to sites offering counterfeit or pirated goods. The operators of these sites understand best practices in search engine marketing (SEM) as well as they understand best practices in eCommerce site design. These shady characters utilize search engine optimization (SEO) to make sure their sites are listed near the top of the results for natural, or organic, search. They also invest in paid search advertising, often purchasing legitimate brand names as keywords to point Web surfers to illicit sites. For example, in a recent examination of paid search ads promoting one popular drug brand, only 25 out of 186 results were for legitimate sellers of this drug. The purchase of the keyword may have been within the rules established by the search engines, but certainly the illicit results displayed to Web surfers are not.

And the cyber-criminals are learning how to harness the Web 2.0 revolution including **new communications platforms** like Twitter, virtual worlds and social networks, and widening their scope to include online computer gaming for their fraudulent activities. Phishers are creating copycat sites to collect passwords and to perform identity theft on members of these sites. And because of the networked nature of these sites, once someone's identity is compromised it is easy to capture other "friends" on one's network, too.

The universe of fakery is extensive, ever-changing, and both wide and deep. There are a variety of exploits, opportunities, and operators. These criminals do not hesitate to invest marketing dollars in paid search, search engine optimization and eCommerce sites using industry best practices in navigation and layout. It's the cyber-equivalent of having shadowy sellers hawking their suspicious goods on every street corner and in front of every residence in every city or town, taking advantage of the public's trust and the inherent anonymity of the Internet to reap profits at the expense of both consumers and legitimate businesses.

“*Cyber-criminals are learning how to harness the Web 2.0 revolution.*”

About the U.S. Chamber and the Global Intellectual Property Center

The Global Intellectual Property Center, an affiliate of the U.S. Chamber of Commerce, is working around the world to champion intellectual property as vital to creating jobs, saving lives, advancing global economic growth, and generating breakthrough solutions to global challenges. The U.S. Chamber of Commerce is the world's largest business federation representing more than 3 million businesses and organizations of every size, sector, and region. For more information, please visit www.theglobalipcenter.com.

About MarkMonitor

MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks. With end-to-end solutions that address the growing threats of online fraud, brand abuse and unauthorized channels, MarkMonitor enables a secure Internet for businesses and their customers. The company's exclusive access to data combined with its patented real-time prevention, detection and response capabilities provide wide-ranging protection to the ever-changing online risks faced by brands today. For more information, please visit www.markmonitor.com.

More than half the Fortune 100 trust MarkMonitor to protect their brands online.
See what we can do for you.

MarkMonitor, Inc.
U.S. (800) 745-9229
Europe: +44 (0) 207 840 1300
www.markmonitor.com

Boise | San Francisco | Washington D.C. | New York | London | Frankfurt

MarkMonitor®