fighting counterfeiting and piracy online

BROCHURE

IPTrack is a service provider offering cost effective solutions against online sales of counterfeits.
We work worldwide in almost every language covering standalone websites, sales platforms, social media etc. We also cover m-commerce (tablets, smartphones…).
Our services are designed to enhance legitimate sales while bringing down counterfeiters.
All our services are performed by our trained staff at our premises using our proprietary software.
Our clients are given reports at the pace they set (daily, weekly, monthly etc…) allowing them to monitor and to fine-tune in real time the scope of our services.

IPTrack's references include Christian Dior, Gucci, Tag Heuer, Estée Lauder and many more famous brands

1. Closing single-brand stand-alone websites and search engine cleaning

Objectives

The primary objective of our service is to prevent the simultaneous appearance of websites selling counterfeit products with the official brand websites on search engine results pages. Specifically, our service aims to close and eliminate websites selling counterfeit products and which appear on the first several pages of search engine results.
In practice we find that this is highly effective in eliminating a significant percentage of putative counterfeit sales. Our results show that all but the most determined customer of counterfeit goods is likely to give up at this stage. Certainly, this technology is extremely successful in reducing opportunistic sales in that a potential client carrying out a search on a brand online will not be bombarded with results for counterfeit websites for the brand in question.

Method

Our strategy is based on the mass notification of webhosts demanding that all counterfeit material be removed from the website or that the website be immediately taken offline. This notification is done on the basis of the 1998 DMCA legislation for webhosts in the United States, European Directive 2000/31/EC for the countries of the European Union (and its transposition into national law in the member countries), and national laws in other countries, including China). In the same way, it is possible to send notifications to all of the service providers for these websites: online payment systems, customer service and live help services, etc.

Our action against hosts and third party services has a triple effect on websites selling counterfeits of our clients' products:

- Once the notification is sent, the targeted website becomes inaccessible for a period of time from several hours to more than three days. This is the time necessary for the counterfeiter to contract with a new webhost and bring the website back online: sales stop completely during this period.

- This hosting transfer carries significant costs (deposit, renting server space, cost and time for transfer, IT labor, etc.) and the website is ultimately often hosted by a host of lesser quality. The efficiency – and thus the ranking – of the website suffer as a result.

- While offline, the website is no longer referenced by search engines, which declare the website dead. Website visits fall. Very quickly, its ranking in search results degrades (it appears X pages further back), causing website visits to fall even more, leading to a new decrease in its search engine ranking.

For the counterfeiter, it is a vicious circle of dereferencing.

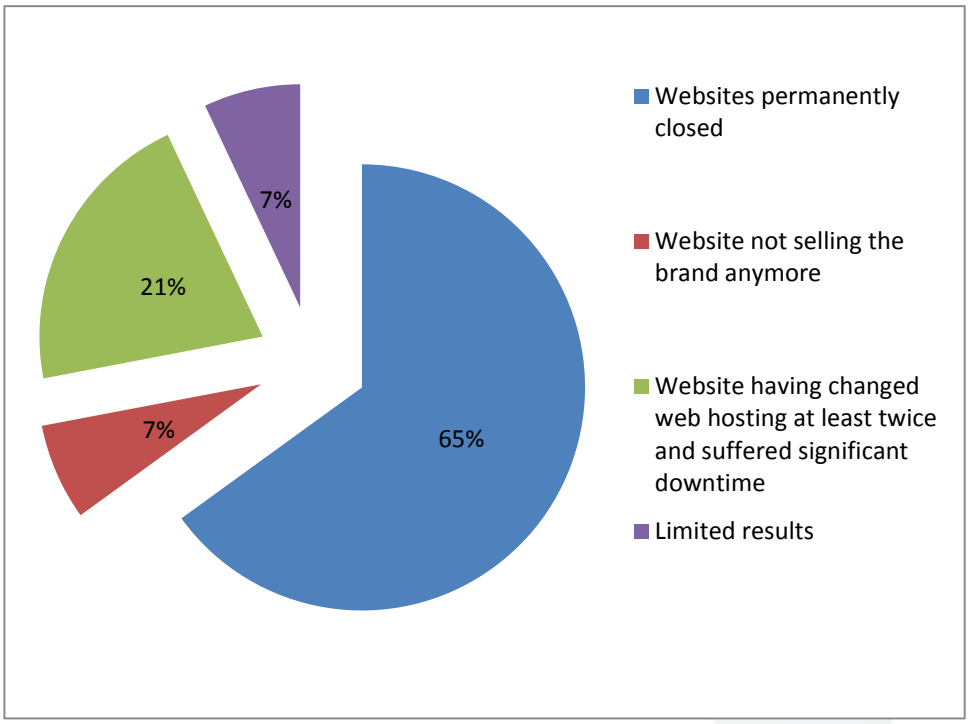
These effects are reinforced by our daily monitoring: as soon as the website goes back online with a new host, we send a new takedown notice to the host, and so on.

Results

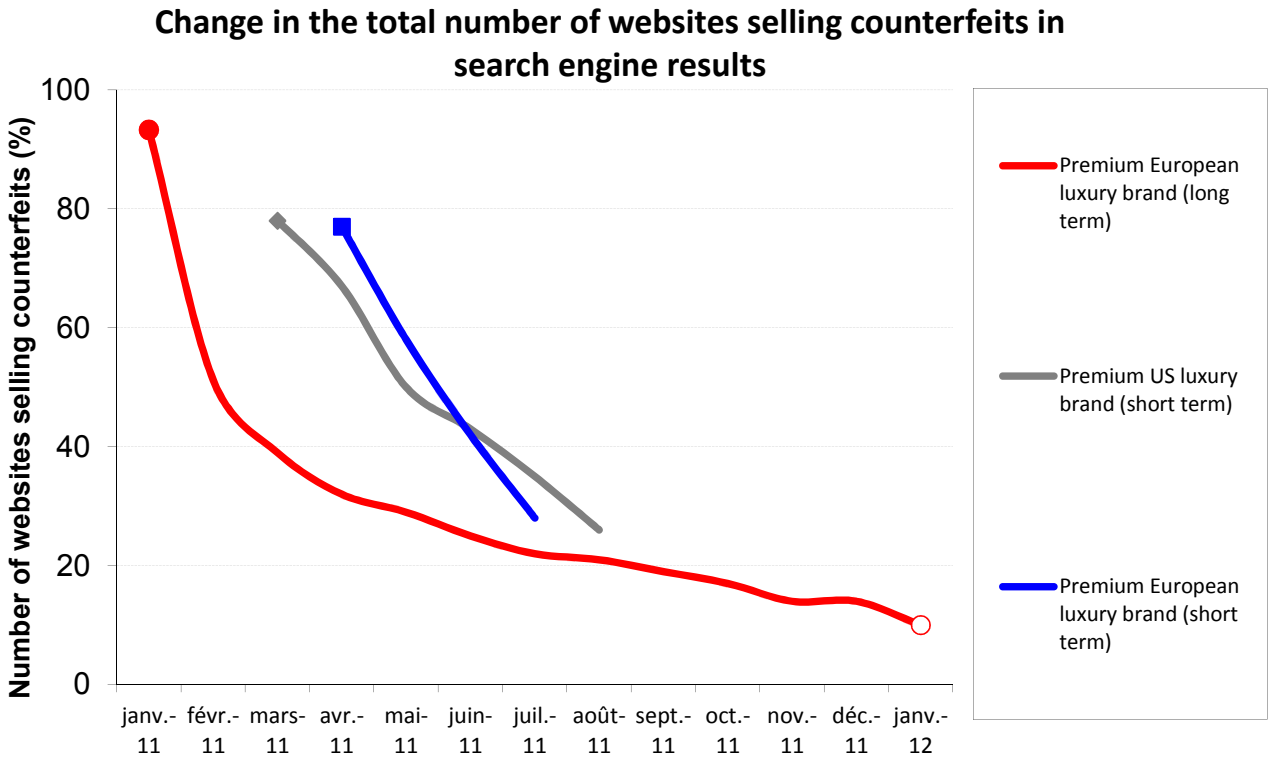
Our clients get a dual result:

Quantitative results: on average, 2/3 of the websites that we process are permanently affected by our actions (closure or cessation of sale of our clients' brands).

For example, for one Paris based premium luxury brand client, in 15 markets throughout the world over six months, we processed 1362 websites selling counterfeits and significantly impacted the operations of 93% of these websites.



Qualitative results: on more than 500 search engine queries processed, the number of websites selling counterfeits fell from an average of three to an average of one or less, and for over 60% of these queries, users no longer find any of these websites on the first three pages.



This curve shows the evolution of the visibility of counterfeits on search engines over one year, for three brands: a premium European luxury brand that we are currently protecting, and premium American and European luxury brands whose protection has ended.

2. Detection and elimination of profiles on social networks and media

Objectives

The primary objective of this service is to fight the multiplication of profiles, pages, groups, videos, etc., on social media that offer counterfeits for sale either directly or indirectly. It also seeks to remove counterfeiters' advertisements, fake official profiles, or those harming the brand's image.

Method

An automatic detection (text and images) is conducted on more than 25 social networks and media. For example, we monitor Facebook, Google+, YouTube, Picasa, Twitter, Tumblr, Vibe, but also VKontatkt in Russia and Weibo in China.
This automatic detection is complemented by human led search techniques and through the implementation of "honey pot" groups and profiles.
Our teams validate the results of the detection before the social networks and media are notified with a request to remove the profiles and accounts.
The service also includes verification that the profiles and accounts have indeed been removed.

Results

The results of this service are immediate: for certain brands, we have several hundred profiles/pages closed per week.

These immediate successes are often the first step for implementing a long-term action. In effect, through our knowledge of social media and the professionalism of our services, we have developed strong relationships with these social media who, for the most part, have no interest in seeing the proliferation of profiles selling illegal products. It is thus possible for us to assist our clients in the proposal and help in setting up filters and proactive measures for these social media and networks.

3. Detection and removal of ads on patforms like Alibaba and eBay

Objectives

The primary objective of this service is to fight against the presence of the sale of counterfeit products on marketplace platforms. Our service can equally target wholesale platforms (business to business "**B2B**" such as dhGate or Alibaba) or marketplace websites for individuals (business to customer "**B2C**", such as eBay or iOffer).

Method

Our service takes a three-pronged approach:

- Detection and removal of ads: Through our proprietary tool, our internal teams – trained and supervised by a project manager – can identify ads and sales of counterfeits. This detection is done based on keywords and image recognition. The infringing ads are then validated by a second team that authorizes the submission of notices requiring the removal of these ads.
- Analysis of the results: This recurring analysis allows us to identify major vendors or platforms experiencing strong growth in counterfeit sales. It can also be used ad-hoc when building cases ahead of meetings with the platforms.
- Reporting: A quantitative and qualitative report is sent monthly to each brand. A consolidated report is sent monthly to the corporate teams.

Scope of service

Our work is focused on a pool of identified platforms. This pool is updated each month and each brand can modify it in accordance with their needs.

This pool currently contains approximately 800 platforms:

- 300 websites in Europe (95% B2C platforms)
- 200 websites in the US and Canada (95% B2C platforms)
- 250 websites in Asia (150 B2B platforms and 100 wholesale platforms)
- 150 websites in the rest of the world (95% B2C platforms)

NB: Unlike other providers:

- We conduct the entire process internally: detection, removal requests, and verification. We do not simply provide a detection tool but manage the entire service for our clients. A detailed report is sent according to a predetermined schedule (monthly, biweekly, etc.)
- You may not be aware that some of our competitors may have some service agreements with a selection of platforms. While these competitors may claim better results on these platforms, they have *de facto* become dependent of the platform which constitutes a conflict of interest with their clients. At IPTrack we pride ourselves in being independent. As a result, we have no side service agreement, no capital interest or any link with any of these platforms.
- We thus must deal with reluctance and intentional delays and evasion from these platforms (bad faith, IP filtering, etc.). However, our independence guarantees that our work is dedicated exclusively to the interests of our clients.

Results

In 2012, 27 different brands used our services.

In total, we have had over **1 million ads removed**, on 500 platforms throughout the world.

Moreover, we have opened **negotiations with over 100 platforms** seeking to establish upstream filters or to prepare legal action against professional counterfeit vendors.

4. Specific Actions

a- Custom online threats audit

While the majority of counterfeiters choose to operate multiple websites with short life expectancies, some prefer to rely on a significant investment in IT security. This choice allows them to defeat the take down notice "**TDN**" system by hiding the location where their server is actually hosted. The TDNs are then ineffective because the server is not located at the host to whom the TDN is sent. The website can then flourish undisturbed.

In this situation IP Track can carry out a custom online threat audit.

The primary objective of this service is to carry out a technical and strategic audit of online entities (websites, servers, relays, etc.) that seek to facilitate the sale of counterfeits. In the vast majority of cases, these entities use advanced anonymization techniques that make TDNs unsuccessful. One must thus determine who operates the entity. What is the precise geographic location of the machine? Who hosts it? How is the anonymization done? And finally, is it possible to obtain information on the machine's users? The results of the audit then allow the newly revealed host to be served with TDNs.

Unlike volume actions, this audit requires a specialized approach led by our team of IT security specialists. In strict compliance with the law, they will organize the conditions required to obtain the necessary information.

Following the audit, we prepare a report detailing all of the information obtained, the actions that can follow, and the state of the situation in progress.

To date, our teams have achieved a **100% success rate** and all of the targeted websites have been located and deactivated.

b- Ground investigations

In certain major cases, it may be desirable to use a team of private investigators to validate certain hypotheses or to make seizures.

It is often difficult to find the right provider in each country and monitoring the investigation generally takes a lot of time. It is equally important to know the specific legal requirements for each country.

This is why IP Track offers its clients its network of private investigators with whom we have a track record guaranteeing their reliability, their integrity and their efficiency.

In addition to the selection, IP Track can also manage these investigators for you.

This saves you a great deal of time and is also more efficient. In effect, our teams have experience working with these investigators and know the specifics of the countries in which they work.

Unlike many companies, we work with complete transparence, since the investigator's quote is submitted directly to you; IP Track charges only a markup for managing the investigation.

c- Fight against parallel sales – legitimate networks

We are currently working on a service for the fight against parallel sales online (unauthorized reseller, heavy discount shops, 2nd hand stock…). This service, currently in beta, is based on our proprietary IP Track tool.

The distribution channels under surveillance are private or grouped sales[1]. This scope can be adapted with respect to regions and priorities.

The surveillance takes place on the basis of keywords (brand, model name, customer product codes, etc.) and image search tools. Human operators verify the results of this automatic detection. In addition to this direct detection on the websites, a "human" search is regularly carried out via newsletters, metasearch engines and forums dedicated to these sales channels, in order to identify the most confidential sales as well as "flash" sales.

Each week, the client receives a report: for each sale detected, we identify the website, the products for sale, the sale expiration date, and the contact information for the website. Screenshots are also annexed to the report.

In addition, it is possible to detect the sale of stolen products on ad platforms.

d- Fight against parallel sales – sale of stolen goods

Marketplace platforms allow a very precise geolocation of sellers. This « visible » geolocation can be complemented by EXIF metadata. These EXIF metadata contain very precise information, sometimes even geolocation by GPS.

If a production and/or logistics unit has a high product theft rate, it may be interesting to put the main sales platforms of the unit's country under surveillance (e.g. Craigslist and iOffer).

By analyzing the product advertisements and photos over several weeks within the geolocation parameters of the targeted unit (e.g. the city of the production location or logistics depot + a 50km perimeter), it is possible to identify sellers regularly offering genuine new products. From there, it is often possible to make a direct or indirect link with employees of the unit in question.

NB. This detection method can also be used to detect the resale of products stolen by employees from the stores, or to detect the resale of products given to employees for a specific occasion (end of year parties, etc.) or obtained through restricted sales.

[1] Example list of monitored websites in annex.