Protecting_my_brand.com

Keep Alert's **Jean-François Poussard** takes a look at past cybersquatting cases and how brand owners can detect counterfeit ecommerce sites

The International Chamber of Commerce ("ICC") estimates the economic and social cost of counterfeiting as more than $1,000bn per year[1]. Counterfeiting is a growing problem, most particularly on the internet. Counterfeiters use the name of the brands they are counterfeiting in the domain names of their fraudulent websites.

A white paper[2] on cybersquatting revealed that 59% of abusive domain names contain the actual name of the brand that is the victim of the counterfeiting. The brand is associated with popular search terms such as "buy", (3.3% of Uniform Domain Name Dispute Resolution Policy (UDRP) decisions en 2011), "shop" (3.2 %), "sale" (2.4 %), "store" (2 %) or "outlet" (1.3 %).

The fashion industry, that represents 25% of all World Intellectual Property Organization (WIPO) claimants, is particularly targeted by cybersquatters with a significant increase in counterfeit ecommerce sites such as: calvinklein-boxers.com (D2011-1754), prada-sitoufficiale.org (D2011-2020) or vipcrocs.com (D2011-1493).

"The financial impact of cybersquatting can be substantial, particularly when the counterfeiters succeed in achieving high search engine rankings for their fraudulent websites."

The pharmaceutical industry uses out-of-court procedures to have generic and counterfeit pharmaceutical ecommerce sites shut down, examples include buyambienwithoutaprescription.biz (D2011-0661), and purchase-accutane.com (D2011-1805).

In April 2012, Hermès recovered 74 domain names in a single URDP decision[3] (D2012-0264), these domain names were all being used to sell counterfeit products. In March 2012, at the New York Tribunal, the luxury goods brand also succeeded in recovering 34 abusive domain names that were owned by Chinese individuals, as well as being awarded damages of $100m. The judgment does not of course take into account the solvency of the respondents or mean that the claimant will receive the payment of damages.

UDRP procedures provide a fast means of recovering illicit domain names and stopping counterfeiters (usually around two months). The financial impact of cybersquatting can be substantial, particularly when the counterfeiters succeed in achieving high search engine rankings for their fraudulent websites. These "Black Hat" search engine optimisation techniques are a very real and serious problem for legitimate brand owners. Google search results for "Louboutin", give seven counterfeit ecommerce stores in the top 10 results. This is the same case for Abercrombie & Fitch and Lancel.

These counterfeit ecommerce stores are virtually indistinguishable from the brand's official site: they use the images of brand ambassadors (tennis player Roger Federer's photo is used on wilsontennissale.com, FA1202001430578, and Brad Pitt on tagheuer-watches.com, D2011-1703). The brand's official logos and display secure payment information that give them an air of legitimacy.

In order to effectively combat counterfeit ecommerce sites, it is important to monitor all new and existing domain names that make any reference in whole or in part to your brand name, this can also include minor variations in spelling - a technique known as typosquatting. Prioritise those associated with ecommerce sites. It is also a good idea to identify the other domain names that are hosted under the same IP number. Finally you need to collect evidence of fraudulent activity: abnormally low prices, spelling mistakes, unauthorised use of text and images from the official site and use of dubious domain registrars.

The Keep Alert platform automates the surveillance and monitoring of illicit domain names. The platform covers all top level domains (.COM, .NET, .ORG.), as well as countries (.CN, .DE, .CO.UK.) and their second level domains (eg, .CO.JP). In all, some 750 domain extensions are monitored. Every result contains a timestamped screenshot of the website in question and is categorised by type of website eg, ecommerce, parking page linking to competing sites, registrar waiting page, redirection to third-party site, adult content and inactive.

Brand owners should be aware of domain names that are newly registered, that have been abandoned or that have had changes made to their website content. This last functionality is particularly useful, because as brands are often confronted with literally thousands of suspect domain name registrations, it would not be financially feasible to engage UDRP procedures or legal action for each and every suspicious domain name (waiting page, inactive domains, etc.)

Footnotes

1. http://www.iccwbo.org/bascap/index.html?id=41116.
2. Published by the online brand-monitoring platform Keep Alert http://www.keepalert.com/fr/Case-studies/white-paper-qcybersquatting-in-2011q.html.
3. *Hermes International v Doe*, No 12-civ-1624 (SDNY 30 April 2012).

Author

Jean-François Poussard is a recognised French specialist in cybersquatting and domain names. He is the director of Keep Alert – an online brand-monitoring platform. Jean-François is a regular contributor to specialised industry publications and participates in seminars and professional events, as well as lecturing at business schools.