How Brand and Domain Name Monitoring Can Counteract Cybersquatting

Posted on September 23, 2019

The Web is a huge and unregulated space made up of countless online content locations. There are more than 300 million active websites today with an additional 25 million registered each year. It's only inevitable then that there will be intense competition between registrants and, therefore, demand for domain names, especially for those that use the most recognizable words and identifiers.

In fact, conflicts between trademark holders and domain registrants looking to own the rights to specific domains are common. Numerous disputed domains nowadays are registered either by accident or with the intent to gain money from those who are interested in them. This tactic is known as "cybersquatting," which can have severe consequences for your brand if you don't pay attention to it.

In this article, we'll discuss cybersquatting and how domain name monitoring can protect your business from it.

Why Should I Be Concerned with Cybersquatting?

In essence, cybersquatting refers to registering, selling, or using a domain name to benefit from someone else's trademarked property. It is generally a shady practice of the culprit purchasing domain names that pertain to existing company brands in hope of making a profit.

A cybersquatter is, of course, free to register any domain name — even one that closely resembles a popular trademark — as long as it is available. He is, however, considered a malicious individual because he is infringing on someone else's rights just to benefit from it.

Cybersquatting can take many forms, which include:

- Registering domains that use common English words or phrases for resale later on;
- Registering misspelled variations of well-known website domains;
- Buying domain names that have recently expired;
- Posting disparaging remarks on cybersquatted sites against certain people or companies;
- Publishing affiliated links to monetize content and drive visitors to click them.

These practices can cause the trademark holders significant financial losses and reputational damage. It is, therefore, your responsibility as a brand owner to protect your intellectual property not only when it comes to patents and designs, but also your domain names.

With so much at stake, it's important to know all about cybersquatting and its many forms so you can avoid suffering the consequences.

Types of Cybersquatting

At present, there are four particularly dominant cybersquatting techniques that malicious actors commonly employ and these are:

Typosquatting

Also known as “URL hijacking”, typosquatting involves the creation of fake websites using domain name variations with misspellings or typos in hope that users will inadvertently visit them. Typos can come in the form of misspellings (e.g., goooogle.com), phrasing variations (e.g., googles.com), and TLD extension substitution (e.g., google.co).

More complex typosquatting tactics abuse audio-visual, and hardware similarities in trademarks. For instance, a homograph attack relies on visual likenesses in symbols, letters, or strings. An example would be replacing “w” and “vv” in a domain like “www.walmart.com” (e.g., www.vvalmart.com).

Identity Theft

Another cybersquatting technique requires purchasing a domain that the original owner has forgotten to renew. This uses special applications or algorithms that allow the perpetrator to easily monitor domain expiration dates. Once registered, the cybersquatter can then mimic the real company’s website and trick visitors into believing they are the same domain owner.

Namejacking

This refers to registering domain names associated with a popular individual such as a celebrity or some other public figure. Namejackers stand to benefit from the web traffic that their target individuals’ status typically generates.

Personal names, particularly in the U.S., can be trademarked but only if these have become distinctive enough through long-term use or advertising. Names that do not fulfill this condition cannot be trademarked since many individuals may share them. As such, namejackers that do not reside in the country are outside the scope of the U.S. Anticybersquatting Consumer Protection Act.

Reverse Cybersquatting

In the event of reverse cybersquatting, an attorney can argue that a trademark holder has made false claims of cybersquatting against a supposed “legitimate” domain owner. This practice involves a variety of intimidation tactics used in trademark litigation so the target or real domain owner is pressured to hand over his property to the threat actor.

It is important to note that reverse cybersquatting can be considered a means of exploiting the dispute resolution procedures for domain names. It could even lead to unfair business practices that stay within the confines of the law, as it can enable the “victims” (actually the perpetrators) to receive compensation for damages.

Monetization Practices Related to Cybersquatting

Professional cybersquatters utilize a range of techniques to profit from their illicit activities, including:

- **Ransomware:** Some cybercriminals use cybersquatted domain names to spread ransomware. Victims are often blocked from accessing important files in their systems until

they decide to pay the ransom.

- **Scams:** In cybersquatting, this often translates to credit card fraud and identity theft. Owners of a cybersquatting site may, for instance, inform users that they can win various prizes if they sign up on their website. In truth, the site just collects their personal information so the criminals can steal their identities.

- **Hit stealing:** This refers to the practice of referring visitors who arrive at a cybersquatted domain to a competitor's website. As the name suggests, the main purpose of this activity is to disrupt or inconvenience the victim.

- **Affiliate marketing:** This involves redirecting visitors to web pages that sell products or services in exchange for a commission.

- **Domain parking:** This entails redirecting a domain name's visitors to a website full of ads in order to generate traffic.

Is There a Legal Authority that Works Against Cybersquatting?

One of the ways by which domain name registrars contribute to the fight against cybersquatting is requiring all registrants who own trademarks or copyrights to present their certificates when reporting cases of infringement.

However, the primary entity that counteracts cybersquatting is the ICANN — the same organization responsible for maintaining the entire DNS. It allows cybersquatting victims to resolve

disputes based on the Uniform Domain Name Resolution Policy (UDRP) — a process that is often faster and less costly compared with undergoing a legal proceeding.

Before you can submit a UDRP claim, however, you will need to meet the following criteria:

- 1. The complainant needs to have an unregistered or registered trademark to hand. This evidence will be submitted to the arbitration panel, which will verify the said trademark's existence.
- 2. The complainant needs to explain why or how the trademark he owns is similar to the domain name he is disputing.
- 3. The complainant must prove that the disputed domain name's holder doesn't have the legal right to it.
- 4. Finally, the complainant needs to prove that the disputed domain name was obtained in bad faith.

Once all of these conditions are met and successfully proven, the disputed domain name will be taken down and the right to own it is transferred to the complainant. It is important to note that there are no financial remedies under this process.

Although the UDRP is effective, trademark owners who wish to maintain their good standing shouldn't rely on post-factum solutions in order to remedy the consequences of cybersquatting. Instead, they should start taking measures to prevent it from happening and to minimize the risks as much as possible. One way of doing so is by registering domain names that are similar to your trademarks, which will stop cybersquatters from getting their hands on them.

How Can Domain Name Monitoring Help?

Brand Monitor and domain name monitoring tools in WhoisXML API's Domain Research Suite can protect you from cybersquatting by letting you proactively monitor for intellectual property abuse. It does this by letting you track certain keywords associated with your brand and trademarks. The program will then keep an eye open for it and alert you to the existence of any recently expired or newly registered domain that matches your search terms.

With this capability, you can stay abreast of anything that closely resembles cybersquatting, allowing you to carry out further actions against trademark and domain name hijacking. This could be particularly useful against the various types of cybersquatting tactics cybercriminals are employing these days.

You also get alerted to domain name matches that use other extensions. Normally, users like to register their websites with the .com TLD but some use other TLDs such as .co, .biz, .net, and so on. Although securing these domains even if you don't plan to use them can cost extra, this practice allows you to safeguard your brand from cybersquatters.

Besides keyword tracking, WhoisXML API's brand and **domain name monitoring** tools also come with a "typos" feature that automatically generates misspelled versions of your domain that are added to your list. This not only helps you save time, but it also increases your chances of catching typosquatters even before they can do you any harm.

Concluding Thoughts

Cybersquatting has truly become a lucrative practice in the digital world, which can adversely affect the reputation of even the most well-established brands. It can even pose legal challenges to brand owners, which could be both time-consuming and costly.

And all this is because of the very fine line between the legality and illegality of cybersquatting.

The practice borders on the unlawful but can turn the tables against the real victim, as in cases of reverse cybersquatting.

Although the UDRP can settle disputes related to cybersquatting and similar practices, preventive measures are still recommended to spare trademark owners the hassle and expense which becoming a victim entails. With a software suite that lets you perform advanced brand and domain name monitoring, you get to stay one step ahead of cybersquatters and make the Web a less chaotic space than it currently is.