Beware in Cyberspace

Private: Stephen Jiew - Senior Associate - Intellectual Property
- Dubai International Financial Centre

April 2015

However, given the degree of domain name scams abound in cyberspace, it is often parodied as the Wild Wild West.

Cybersquatting

Trademark owners understand that domain names can function as trademarks and are often first in line to register their trademarks as domain names. However, they are not the only parties to realise the inherent value of domain names. Domain name registrations are acquired on a first-come, first-served basis. Enter the cybersquatter, a cyber villain who abuses the first come first served system by registering domain names incorporating the often well known trademarks of brand owners before the legitimate trademark owner manages to register the domain name. The cybersquatter registrant then offers the domain name registration to the trademark owner for sale at a ransom price way above the cost of the registration.

Such cyberpirates continue to illegitimately profit on the Internet by hijacking the inherent value of trademarks owned by the brand owners' marks.

Indeed, some cyberpirates register domain names that incorporate valuable trademarks to benefit commercially from Internet traffic that mistakenly arrives at the registrant's website. They misappropriate trademarks for such commercial gain rather than purely for trying to sell on such domain names.

Typosquatting is also another innovative method of trademark misappropriation. In this case, the domain names are registered incorporating misspelled variants of trademarks including nicknames or locally adopted variants thereof. This can be particularly damaging to the brand owner as the locally adopted variant of the trademark could be the term, which has brand recognition and gravitas with the local consumers in the market.

Another egregious form of cybersquatting occurs when competitors register domain names incorporating the trademarks of their rivals in order to deny them use of their own marks as featured addresses in cyberspace.

Cybersquatters are particularly adept at mining the value of trademarks as used in domain names. In such cases, rather than turning a quick buck by on-selling domain names incorporating trademarks at a ransom, cybersquatters are in it for the long haul with the gems, which could potentially make exponential gains due to the inherent trademark value of the domain name.

Thus, for instance, cybersquatters often link the domain name incorporating a trademark to websites featuring pornographic content, since pornographic sites continue to be sources of easy money on the Internet. The registrant of the domain name would then receive a click-through fee whenever an Internet user inadvertently arrived at the pornographic website and clicked on one of the links.

Specific domain name scams examples

Unfortunately, registrants of domain names are easy targets for domain name scams given the fact that most of the details for the registrants of domain names are publicly available on the internet (i.e. company name, contact name, email address and phone number) through websites such as “Whois” (www.whois.com).

As a registrant of a domain name, you may encounter common domain name scams such as the following possibilities:-

- A notification from a domain name company advising you that it has received an application from a third party to register a domain name which has incorporated your trademark. The company says it is alerting you to this fact to provide you with the opportunity to register the domain name first. You are invited to register that domain name with the company as a means of preventing the third party from doing so.
- An email from an authorised domain name registrar in China, informing you that there has been an attempt by an unauthorised entity to register your trademark as a domain name or as an internet keyword in China and from due performance of their internal audit policies, the sender has found out that the trademark actually belongs to you or may be connected to you; the registrar has delayed the registration momentarily to contact you to ascertain whether you might have authorised the third party to register the domain name or internet keyword; if you have not so authorised the third party, the registrar will give you first priority and can register the domain name or internet keyword on your behalf to block the third party from doing so. If you do not, then the registrar will proceed with the third party’s registration.
- a “renewal” notification for a domain name which you do not actually have registered but which is very similar to your actual domain name, with perhaps just a different extension (for example, .net instead of .ae).
- You may be sent a domain name renewal notice by mail or email for your exact domain name, but it has been sent from a different company to the one you registered your domain name with. Paying for and providing your account information to the new company will generally result in a transfer of the domain name to that company.

In order to combat these types of domain name scams, you need to be armed strategically with sound standard operating procedures such as the following:

- Ascertain the identity of your domain name registrar (this is the company you registered your domain name with originally). Only that company will send you legitimate correspondence about your domain name. It is administratively prudent o consolidate your name registrations with a single Registrar.
- Ascertain the expiry date(s) of your domain name registration(s). Usually, your domain name registrar will send you a renewal notification about a month before expiry. A scam entity might send you a renewal notification many months in advance of the expiry date hoping to bait you first.
- Be keenly alert to any correspondence you receive about your domain name, especially with respect to the domain name referred to in the correspondence.
- Legitimate correspondence will not ask you to provide your password for renewal of a domain name. If you are asked for your password, this is usually an indication that the sender is not legitimate.
- Implement strict accounts payable systems to limit the amount of people in your organisation who are authorised to approve and pay invoices so as to minimise the chance of inadvertent payment of a scam invoice.

Any notifications from a domain name registrar informing you that it has received an application from an unauthorised entity to register a domain name which incorporates your trademark are to be treated with great suspicion.

Particularly, you should be wary of Chinese internet keywords. Remember that the internet keywords being offered to you are roman letters rather than Chinese characters and that Chinese websurfers are more likely to enter Chinese characters than English words when looking for your company. In such circumstances, you would really only want to own some Chinese internet keywords if you foresee that your name in roman letters is going to be the identifier for your company in the minds of Chinese consumers rather than a string of Chinese characters and you would be sufficiently disturbed if such Chinese consumers were to be redirected to another's website if they were to type your company's name into the address bar of their internet browser.

The reality is that cybersquatters will continue to register domain names incorporating your trademarks. This is impossible to prevent due to the multitude of available domain names out there especially with the recent proliferation of available domain names such as .money, .party, .wtf, .fund, .legal, .poker, .dad, .cash etc. Practically, it is a near impossibility, not to mention prohibitively costly, to reserve every available domain name out there related to your business. Generally, it is recommended that you register domain names for your core and important brands in the countries of interest to your business.

If you do decide to register a domain name, which has been suggested by a company sending notifications such as those described above, do not use them. You should choose your own domain name registrar, which does not engage in such activities.

In order to combat the multitude of domain name scams out there on the World Wide Web, you need to sit down with your IP lawyers to find out the practical usage of your trade marks on the internet and how best to protect them in this context.