Part of The IP Media Group

World Trademark Review Daily

'.ca' and '.uk' registries introduce security measures to prevent domain hijacking

Domain names International - Hogan Lovells LLP

May 16 2014

The Canadian Internet Registration Authority (CIRA), the entity that administers the '.ca' country-code top-level domain (ccTLD), and Nominet, which is responsible for the '.uk' ccTLD, have introduced 'registry lock', a heightened security measure which prevents unauthorised changes, deletions or transfers of ownership of domain names, also commonly known as 'domain hijacking'. Such heightened security measures have been introduced by many registries following a series of high-profile domain hijacking incidents in the past year.

Domain hijacking (or, simply put, domain theft) refers to "the wrongful taking of control of a domain name from the rightful name owner", as defined by the Internet Corporation for Assigned Names and Numbers in its 2005 report entitled "Domain Name Hijacking: Incidents, Threats, Risks, and Remedial Actions". Indeed, domain hijacking dates from the very early days of the Internet and, although originally more pervasive under the '.com' extension, it has now expanded to ccTLDs.

The hijacking of a domain name usually involves some type of fraudulent act, such as impersonation or forgery, on the part of the hijacker which enables unauthorised changes and/or transfer of the domain name. There are other types of hijacking such as the hijacking of the domain name system (DNS) server, also known as 'DNS hijacking' (see "SIDN introduces new security measures").

Once the hijacker takes control over the domain name, it can use the domain name to redirect traffic to another website, such as a phishing website (from which the hijacker can obtain personal and/or financial information and/or inject malware) or a website displaying pornographic material. In some cases, the domain hijackers can also sell the domain name to a third party or to the domain name holder itself for an inflated price.

This can have disastrous consequences for domain name holders and their online businesses, including, but not limited to, denial and theft of electronic mail services, unauthorised disclosure of sensitive information, loss of revenue and/or consumer confidence and damage to the domain name holder's reputation. Furthermore, not only does hijacking affect the domain name holders, it also affects customers who are relying on the services provided and who will see their personal and/or financial information put at risk.

In this context, registry lock provides domain name holders with an additional layer of security that protects their domain names against hijacking. As its name indicates, the domain name is locked at the registry level and any changes to the domain name are not allowed without following rigorous verification and authentication protocols at both the registry and registrar levels.

Some registries, such as DNS Belgium, which operates the '.be' ccTLD, automatically provide the registry lock service for all customers without additional costs, whilst others, such as Nominet, require payment of an additional fee. Regardless, domain name holders are well advised to lock their domain names to protect their customers and online businesses.

For CIRA's press release, see here. For Nominet's press release, see here.

David Taylor and Soraya Camayd, Hogan Lovells LLP, Paris