
“Domain Name Spying” – The Latest Technique in Domain Name Sabotage

Imagine you own a new business and are finally getting around to selecting a domain name. You are thrilled when you find that the domain name you envision for your company or new product is available for registration. Satisfied, you return a day or two later to purchase the name, only to find out that someone else beat you to the registration. How could this have happened? Is it just a coincidence?

Certainly it is possible that a registrant simply searched the same name and happened to register it before you. However, a more likely and frustrating possibility is that an entity somehow tracked your search and registered the name between the time of your search and your attempted purchase. The entities engaging in this practice, which we have dubbed **domain name spying**, purchase particular domain names only after covertly determining that someone has checked the names’ availability. Domain name spying is not a rare occurrence, as some companies appear to make spying their entire business model.

There is nothing new about companies’ interfering with the good faith acquisition and transfer of domain names. Cybersquatting, which entails registering a domain name confusingly similar to another’s trademark and offering to sell the name at an increased price to the mark’s owner, has long haunted owners of valuable trademarks. Other problematic domain name registration practices include domain name tasting and domain kiting.

Domain name tasting is characterized by short-term registration of many domain names. Domain name tasters take advantage of an Internet Corporation for Assigned Names and Numbers (ICANN) rule called the “add-grace period,” which permits a registrant to obtain a refund of a domain name registration fee by returning the domain name within five days of registration. Why register domain names and return over 90 percent of them within five days? (See Posting of Bob Parsons to Hot Points with Bob Parsons, www.bobparsons.com/DomainKiting.html (May 10, 2006).) A domain name taster registers many domain names in order to generate advertising income from short-term ownership and consider the profitability of paying for long-term ownership of the domain. If the registrant determines over the five-day “tasting” period that a name will not be profitable, the domain name is simply relinquished and the registrant’s fee returned. In short, a domain name taster derives short-term revenue from many websites without cost and efficiently secures numerous domain names that will provide the taster with a return on long-term investment.

Domain kiting takes tasting a step further by further abusing the ICANN grace period. As in the domain name tasting practice, the registrant in a kiting scheme returns domain names at the end of the five-day add-grace period. Upon returning a domain name, however, the kiter quickly reacquires the name. Entities engaged in domain kiting can, therefore, maintain long-term ownership of domain names and never pay an ownership fee.

With an understanding of how domain name tasting and kiting schemes function, one can see that domain name spying is simply a targeted version of these practices. While tasting and kiting involve gathering short-term ownership rights in scores of random domain names, domain name spies specifically pursue domain

names in which others have demonstrated an interest. Spies, like tasters and kitters, may quickly release those names that are unlikely to generate profit, while they permanently register the names with more promising financial returns. What is unknown about the relatively new practice of domain name spying is exactly how the spies determine that someone has researched the availability of a particular domain name.

One company, Chesterton Holdings, makes the following claims on its website (www.chestertonholdings.com):

Domain names are not specifically targeted and are not collected by any untoward methods. Rather, all domain names are lawfully collected in clusters through *highly developed and ground breaking automated technology and modules*. Chesterton does not have special access to public data sources (e.g. the WHOIS database) or personally-identifiable information. [emphasis added]

What no one seems to know is what “highly developed and ground breaking automated technology and modules” are or how they work, or if this is a roundabout way of stating that domain name “spies” hack into vulnerable domain name registrar servers. Even the technical commentators appear to be stumped. See Larry Seltzer, “Whois Hijacking My Domain Research?,” EWEEK, July 19, 2006, at www.eweek.com/article2/0,1895,1991365,00.asp. One commentator for Eweek.com has stated, “All I really know is that there’s no legitimate way to do what Chesterton Holdings is doing, and I hope they finally get called for it.”

Although the methods of domain name spies remain a mystery, some victims of spying may have recourse using trademark and cybersquatting laws. However, only persons or entities with trademark rights obtained by registration or use of a mark can utilize trademark and cybersquatting laws to attempt to acquire a transfer from a spy. If spies do not violate the law by hacking into registrar servers, some spy victims may be left without a remedy. For example, if you are victimized while checking the availability of a domain name for a product you have yet to launch or otherwise protect, you may have to settle for a different domain name or pay the spy a premium for your preferred name.

New methods of illegitimate domain name registration surface frequently. Domain name spying is one of the most recent, but certainly not the last, of such practices. Some groups, including INTA, advocate the elimination of the add-grace period to solve the problems resulting from tasting and kiting. The grace period’s purpose of permitting correction of errors in the domain name registration process, according to these advocates, is better achieved using solutions subject to less abuse. Elimination of the grace period or another amendment to the ICANN rules may best address the problems resulting from tasting, kiting and spying.

However, there may be more simple advice to avoid being a victim of a spy—promptly purchase a domain name upon conducting your initial screening search!

By: Michelle Mancino Marsh and Eric Schreiber, Kenyon & Kenyon LLP, New York, New York; Prepared by the *INTA Bulletin* Features-Policy & Practice Subcommittee