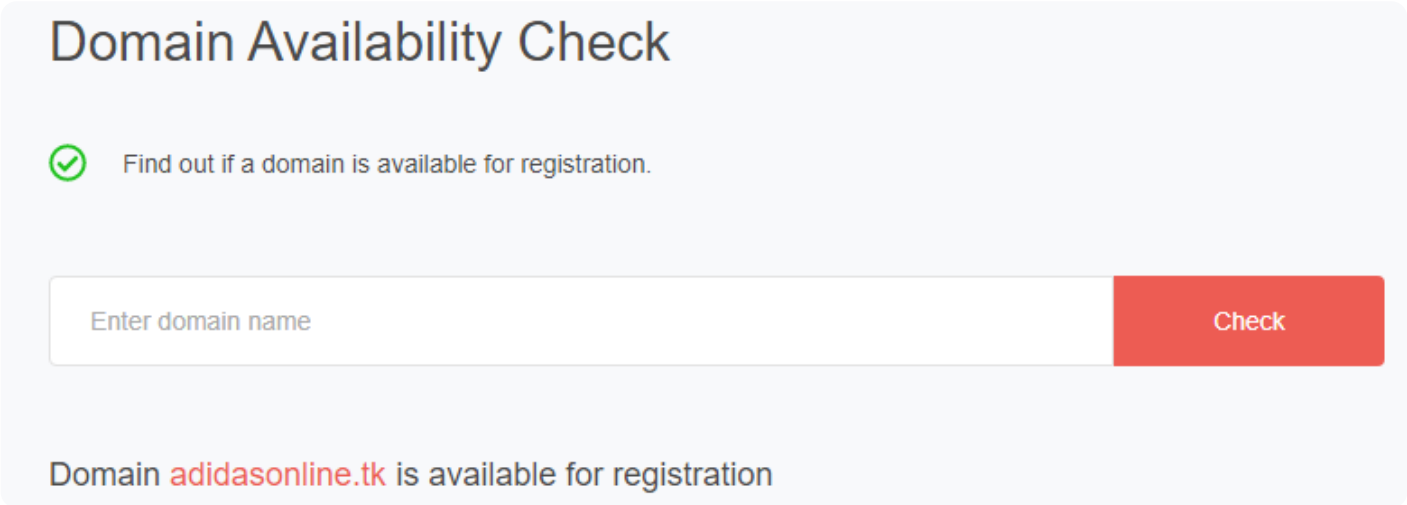
Stop Online Trademark Infringement and Typosquatting with Domain Research Suite (DRS)

Posted on July 2, 2021

One of the tenets of brand protection is ensuring that the brand or company name is used properly and only by the right's owner or its assignee. In domain name disputes and trademark infringement cases, law firms play a vital role and are notably commissioned to help brand owners protect their brands.

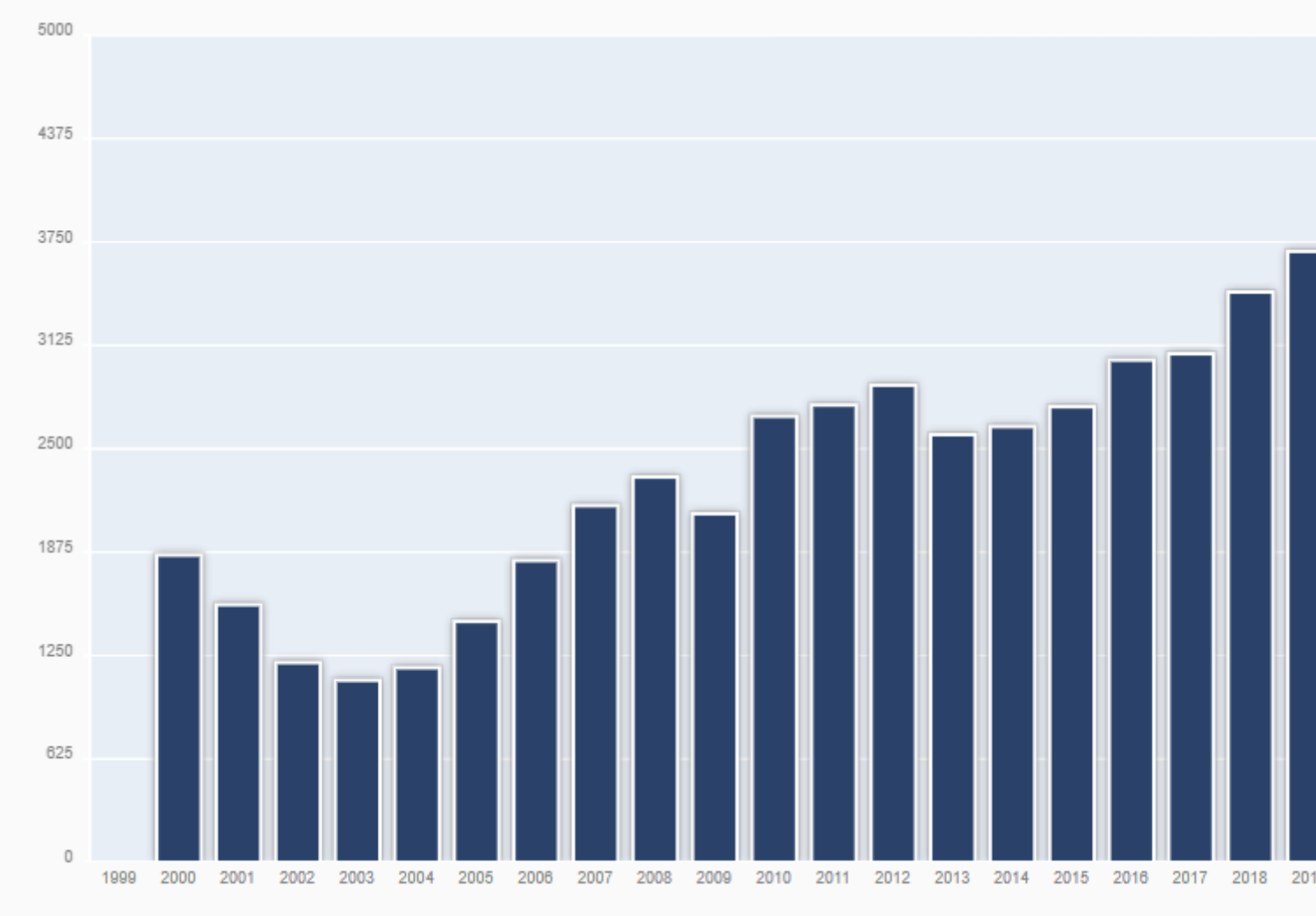
In recent years, these types of brand infringement cases have continued to increase. A branded or trademarked name or variations thereof can easily be used by anyone other than its rightful owner. The prevalence of infringement could have stemmed from the ease at which anyone can register any domain name for as long as it is available.

For instance, the domain name adidasonline[.]tk is available for registration.



Can the domain be owned by any entities other than Adidas? The answer is yes. Because it's available, anyone with an email address and a few dollars can register and own it. Will the domain infringe on the Adidas trademark? Probably, and law firms can help identify such instances, build cases, and often facilitate takedown by using domain data.

The World Intellectual Property Organization (WIPO), in fact, has tallied an increasing number of Uniform Domain-Name Dispute-Resolution Policy (UDRP) complaints over the past years. From only less than 1,500 cases in 2005, the number went up to 4,204 in 2020. Halfway through 2021, WIPO has already reported 2,015 additional cases.



Source: WIPO

As a provider of domain intelligence data, WhoisXML API has also seen its fair share of look-alike domain names, which are commonly referred to as "cybersquatting and typosquatting domains." In

one study, we looked at domains and subdomains that contain the names of 10 of the most spoofed brands and uncovered 177,342 domains and subdomains. About 99.8% of them cannot be publicly attributed to the brand names they contain.

How WhoisXML API's DRS Assists Trademark Professionals

While every retainer arrangement differs when it comes to intellectual property-related services, trademark law firms, large or independent, can detect, monitor, and gather evidence for such cases by using WhoisXML API's Domain Research Suite (DRS).

DRS is a set of tools that provide users with access to one of the largest WHOIS, IP, and DNS data sets through search and monitoring functionalities. DRS has been adopted by many Fortune 500 companies, reputable cybersecurity agencies and LEAs across the globe.

The data in the study cited above, for instance, can also be derived from the Domains & Subdomains Discovery component. In particular, trademark professionals can employ DRS in the following areas involved in intellectual property-related cases, particularly, trademark infringement:

Cybersquatting and Typosquatting Detection

Law firms use DRS to detect domain names that look similar to their client's brand:

- Domains & Subdomains Discovery: Users can look up a list of registered domains and subdomains that contain the brand, company, or trademarked name.
- WHOIS Search: Lookalike domains that the client does not own can be potential cybersquatting domains. Legal firms can build WHOIS reports for each suspicious domain to learn more about its registrant.

Brand and Trademark Infringement Detection

Hundreds of thousands of domains are registered every day. How can law firms keep track of those that potentially infringe on their client's brands? These DRS tools could help:

- Brand Monitor: Law firms can monitor their client's brand, company, or trademarked name, along with its misspelled variations. In addition, Brand Monitor can be set up to send alerts every time a related domain is registered, modified, or dropped.

- Domain Monitor: A potentially infringing domain name can be subjected to observation by being added to Domain Monitor. For instance, if the defendant has promised to let go of the domain after a warning has been served, legal firms can use Domain Monitor to see if he/she follows through.

Evidence Gathering for Legal Cases and UDRP Complaints

The DRS tools previously mentioned can provide data that helps law firms build their cases. In addition, these tools aid in evidence gathering:

- Registrant Monitor: Monitor the name, organization name, or email address of registrants suspected of infringing on a client's brand. The tool can alert users of domain names registered by the monitored registrant.

- WHOIS History Search: Aside from WHOIS Search, law firms can use WHOIS History Search to dig into the historical WHOIS records of a domain name. This can be useful when the latest WHOIS record of a domain has been redacted or to identify possible past domain owners.

- Reverse WHOIS Search: This tool helps uncover other domains associated with a particular registrant's details (i.e., name, email address, etc.), allowing legal firms to help see whether there are other infringements he/she committed.

Cybersquatting and Typosquatting Prevention

Law firms' retainer agreements could include helping clients avoid costly litigation. Filing trademark

infringement cases and UDRP complaints can be seen as a last resort. Thus, among the top uses of DRS is preventing cybersquatting through defensive registration.

Domain Availability Check illustrated in the adidasonline[.]tk example above is a tool that helps law firms and their clients determine if a domain is available for registration. Brand Monitor and Domain Monitor also assist them in identifying and monitoring domains that resemble that of a protected brand.

WhoisXML API's DRS has become an essential part of the legal software community, specializing in intellectual property-related cases and the fight against cybercrime.

Contact us for more information about using DRS in your law firm or practice.