Uncover Domain Spoofing Using AI Driven Predictive Monitors

Posted on May 16, 2019

Spoofing is a situation in which an entity (person or software program) successfully impersonates and masquerades as another successful one, with the purpose of gaining an advantage with regards to personal or business information or brand goodwill. Domain spoofing occurs when an attacker appears to use a company's domain to impersonate and masquerade a company and or its products or brands. The domain spoofer may later use the deceived domain name to induce fraudulent practice like phishing i.e. sending deceptive emails pretending to be from a reputed company in order to induce individuals to reveal passwords, credit card numbers or download malicious files.

Sometimes this can also take the form of typosquatting i.e. to emulate someone else's brand or copyright & target Internet users. This typically happens when the user is new to site or fat fingers and types the URL wrongly. An example, instead of “Yahoo” he may type “Yahooo” and still possibly land on a fake website which is similar to the original one.

Domain spoofing/squatting according to US federal law “Anticybersquatting Consumer Protection Act” is related to impersonation of a domain or using an Internet domain name with bad intent (bad faith) to profit from the intangible benefits (goodwill) of products that are trademarked and belonging to someone else. The word ‘intent’ here is very important because in some cases domains with similar names have been found to be genuinely selling a completely different set of product or service. Similar domain names do not always necessarily mean malicious intent but can be due to lack of availability of a name or sincerely not knowing about another brand.

Also, the risk of domain spoofing is not limited to firms who have made it big in their respective fields of excellence (example: Google, Facebook, Amazon, etc.) but the risk is present for any firm which has a great brand or idea with equally good execution capability.

Solution

A possible answer to the above problem would lie in monitoring your brand and trademarks for any existing or new domain registrations containing similar or exact terms. With over 300 million websites, it is not possible to track every domain activity yourself and to that effect, we provide a simplified solution with our Brand Monitor Tool. Our software intelligently and predictively identifies similarly named domains using certain algorithms and statistics, typically based on similarity analysis of data and finds the near matching names.

You can find various typo variations of your brand keywords and monitor them. Any new domain name registered, recently dropped or changes in the Whosis records of the existing domains containing your brand term will be notified in our easy to use tool as well as via email notifications.

Solution Flow

1.0 – Insert your brand/ trademark keyword in the web-tool

1.1 – ADD to monitoring

1.2 – Check for Typo variations in ‘Advance’

1.3 – Add all or relevant misspelling

1.4 – Configure email alerts (optional)

1.5 – Daily changes displayed in the tool

Stakeholders

- New Domain Registrant: A person /company that wants to register a new domain
- Existing Domain Holders: Any person/ company who owns domain name/s for their product/ service
- Domain Investor: A person/ company who invests in domains
- Marketing or Brand Team: A company’s brand custodian
- Brand & Trademark Protection Companies: Company who provide online brand protection services
- Cyber Security Team: Professionals who prevent malicious entities online

Uncovering domain spoofing is extremely helpful to individuals & companies. Proactively

monitoring your brand and trademark can protect your valuable brand online and help you carry out defensive or investigative actions against bad actors. Get started at https://domain-research-monitoring.whoisxmlapi.com/brand-monitor