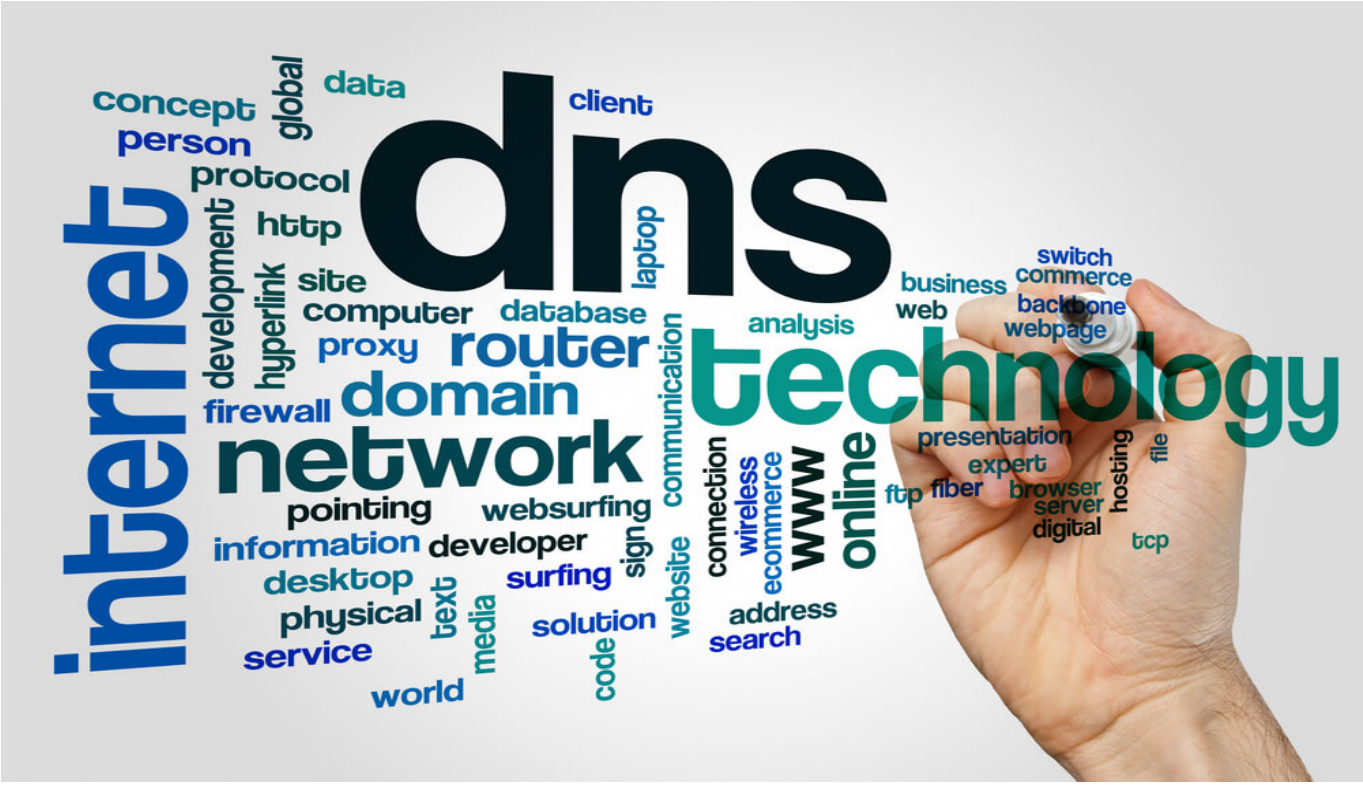

How to Preserve Your Brand Value by Checking the DNS History of Your Domains

Brand trust is the hard currency of any business. In fact, customers cite brand trust as the top reason why they would buy from a retailer, according to a 2018 consumer insights survey. Employees are also most productive when they work for a brand they trust. What's more, in a climate of trust, companies can forge new partnerships and achieve milestones.

Unfortunately, most organizations overlook a critical element when building trust — brand protection. Despite the heavy emphasis on marketing strategies, it appears that most companies remain unprepared for attacks on their brand. Intellectual property violations and fraud, for instance, can gravely hurt a company's brand image, reputation, and value. One tool that can help in this area is a DNS database.

How to Use a DNS Database for Brand Protection

A DNS database is essentially a repository of historic Domain Name System (DNS) records. DNS records map IP addresses to domains.

WhoisXML API's DNS Database Download, for instance, is an index of 2 billion hostnames and 500 billion historical DNS records collected over the past 12 years. That makes it an indispensable source of intelligence for brand protection officers to ensure that their digital footprints remain unspoiled. Below are some brand violations that a DNS Database can help prevent.

Website Defacement

The aim of website defacement is to implement an unwanted change of a web page's appearance or functionality. In such an attack, threat actors take control of a website by way of application weaknesses or erroneous statements returned by a HyperText Transfer Protocol (HTTP) response. However, hackers can also easily crack into a website through dangling DNS records.

A web application firewall (WAF) can help you block unwanted HTTP traffic. But you can boost its effectiveness by using a DNS database when possible. A DNS database allows you to identify questionable IP addresses that are requesting access to your website. The database has a vast collection of historical IP addresses and domains, including those that have figured in attacks. You can use it to block not just known malicious domains but also any other connected IP addresses.

Denial-of-Service (DoS) Attacks

DoS attacks aim to overwhelm an Internet host with an influx of junk traffic so that legitimate visitors can't access its services, e.g. the website it is hosting. Highly publicized cases often come in the form of distributed DoS (DDoS) — where the incoming traffic originates from multiple devices or botnets. While 76% of DDoS attacks are below 1 Gbps in size, the worst can generate requests amounting to as

much as 10 Gbps.

High-profile companies are the usual DoS targets, but small businesses are fair game to hackers as well. Whatever the size of an organization, it helps to always be on guard for devastating DoS attacks that can lead to reputational damage and financial loss.

A DNS database can help network analysts spot potentially dangerous IP addresses for blocking. Additionally, website owners can refer to a DNS database to check if their resource record values are correct so they won't figure in DoS attacks.

DNS Hijacking (Cache Poisoning or Redirection)

DNS hijacking is a type of brand attack where users who type a brand's web address in their browsers get redirected to another location. It takes place after a site has been compromised, possibly due to a prior phishing attack or vulnerability exploitation, thus allowing attackers to modify the domain's DNS record. Attackers can also create forged requests, which are then cached by a DNS resolver. Attackers often focus on DNS servers as these are relatively easier to manipulate than a client's host file.

DNS hijacking is, however, only possible if the target site is vulnerable. Victims often have domains pointing to nameservers they no longer use. To ensure that your company doesn't have exposed domains, you can look for your IP address in a DNS database to **check the DNS history of your domains**. As this database contains independent data that are not affected by the current contents of the Domain Name System, from there, you can check if your DNS configurations are correct. If that's not the case, you can update your records to avoid DNS hijacking.

Domain Squatting (URL Hijacking)

Domain squatting perhaps seems like the most benign out of the forms of brand abuse that could result from a DNS-based attack. And yet it's a massive headache for most brand managers. Cybersquatters register a brand's lookalike domain in

bad faith, often to sell counterfeit goods, or dupe customers into booking a fake service. We all know how it ends though. Apart from taking sales away from your company, knock-off merchants will undermine your customer's faith in your brand.

It may seem far-fetched for brand protection agents, but a DNS Database can help in this situation. You can use it to identify all domains that closely resemble yours. From there, you can investigate if they existed before your trademark was approved. If not, then you can start building Uniform Domain-Name Dispute-Resolution (UDRP) cases against offenders — notably with the use of such tools as Brand Monitor and Typosquatting Data Feed.

Brands need to take a proactive stance to protect their domains and trademarks as no one else will do so for them. Knowing the **DNS history of a domain** aided by a DNS database lets organizations gain the trust edge, while ensuring that their brand reputation and assets are abuse-free.