Domain Name Basics
Domain Monitoring

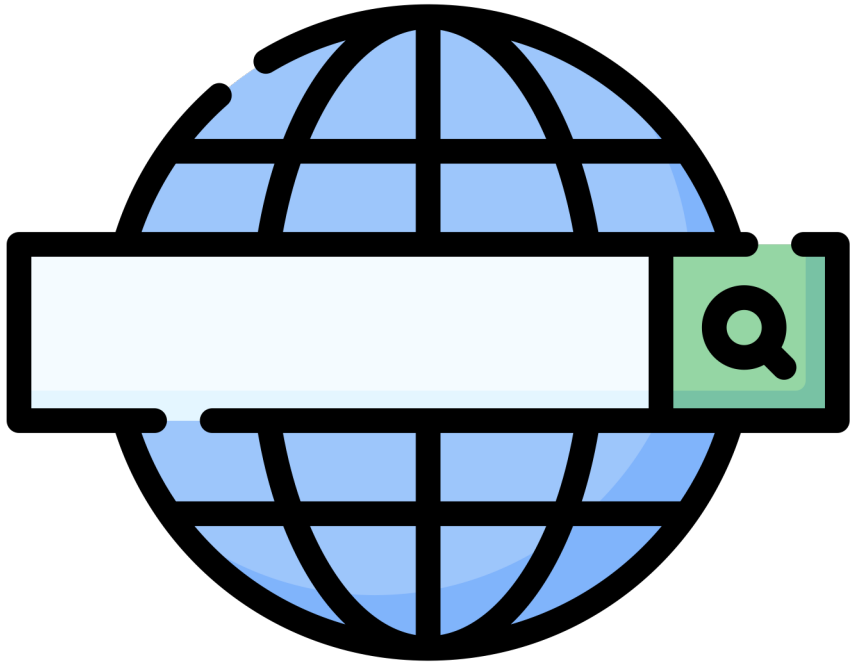
Tobias Sattler
tobiassattler.com

What is Domain Monitoring?

Domain Monitoring allows users to **monitor** domain name **registrations**, usually based on the DNS zone files.

With that, you can keep track of domains to check expiration dates, status or nameserver changes, as well as new registrations.

You can monitor **identical** or **confusingly similar** terms to your brand, corporate name, or trademark by providing a string or domain.



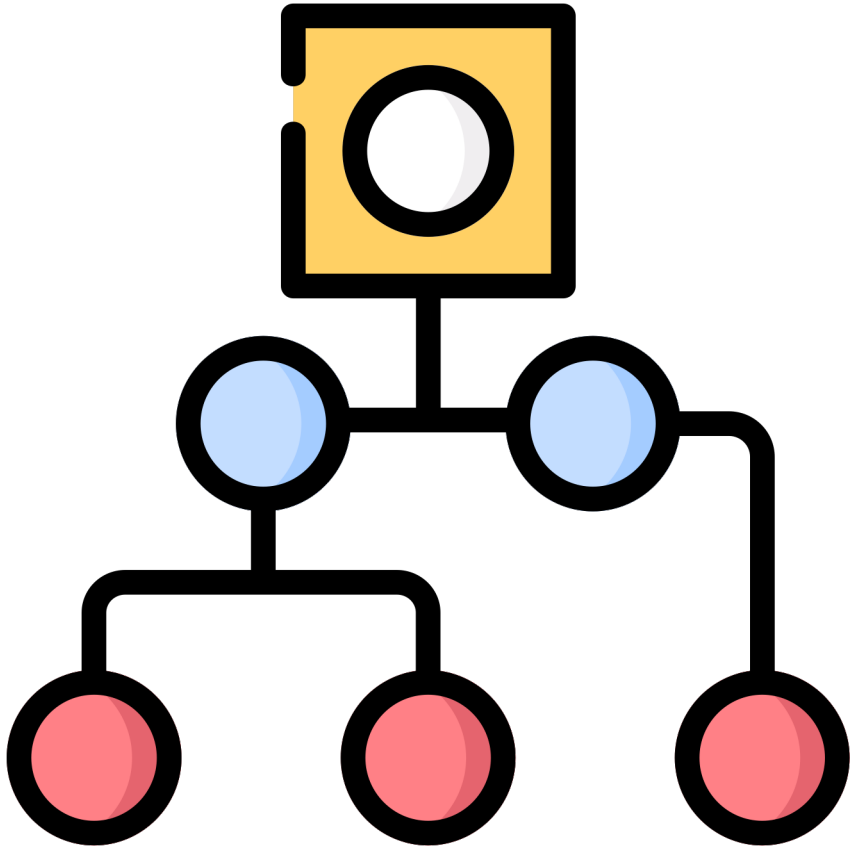
Let’s take a step back: What’s DNS?

DNS is a hierarchical distributed naming system to **translate domain names** into **IP addresses**, which makes websites easier to remember, such as

- tobiassattler.com instead of 78.46.19.133

The domain namespace is a tree, and its root is a dot.

- www.tobiassattler.com.



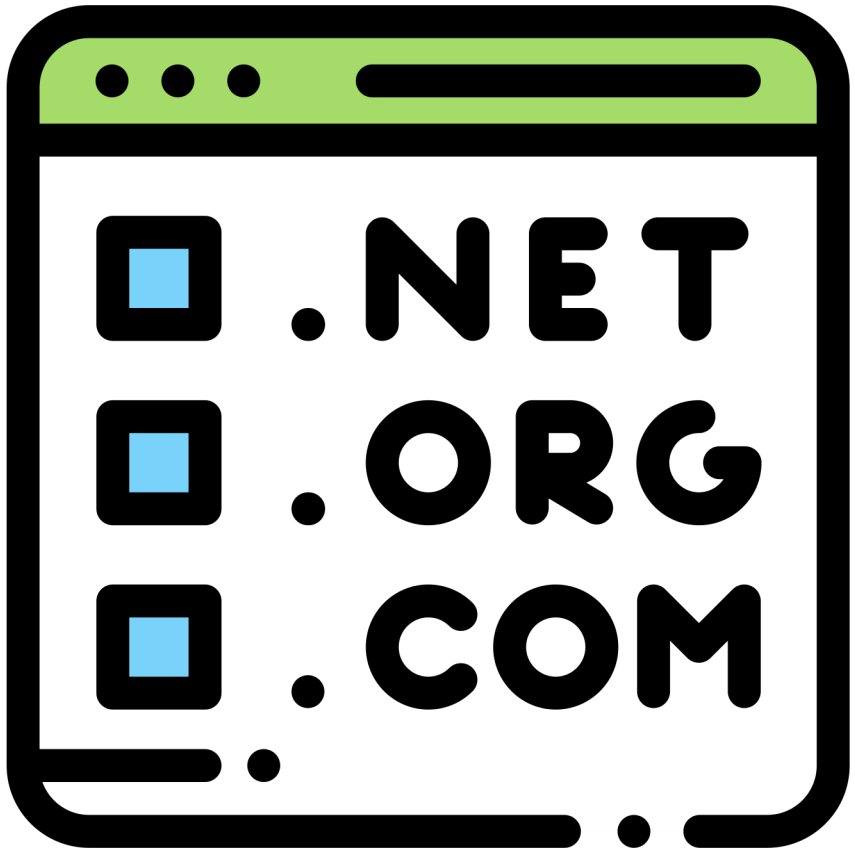
What is a domain name?

It is a **unique string** within the domain name system (DNS). The DNS is a tree, and its root is a dot.

Like browsers and email clients, most programs will ignore the point at the end of a domain name, but it is there.

DNS resolves names; It is a method to **translate** domain names to **IP addresses** to make it easier to remember.

The DNS **zone file** contains **mappings** between domain names and IP addresses, and other resources.



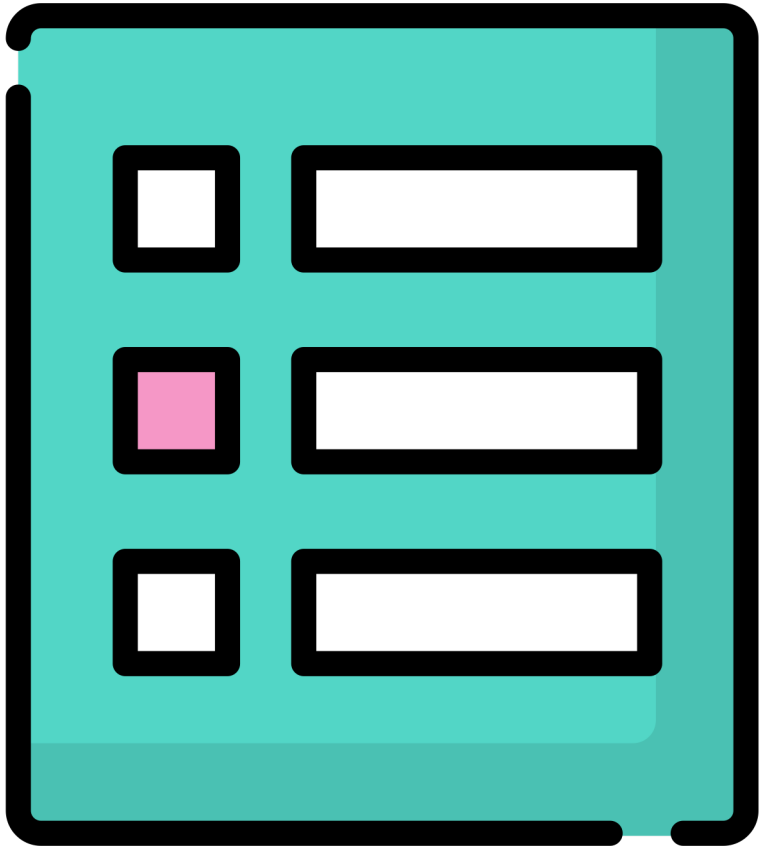
What is a zone file?

A **zone file** is a text file that describes a DNS zone.

Such a file contains **mappings** between **domain names** and **IP addresses**, and other resources. A TLD zone file contains only domain names **that are resolving**.

The zone file format is defined in RFC 1035 and RFC 1034 and was initially used by the Berkeley Internet Domain Name (BIND) software package.

A zone file is a sequence of entries for resource records (RR).



Risk #1 – Typosquatting

Typosquatting (also called domain squatting) is based on **typos** made by Internet users when **inputting** a website **address** into a browser.

It can be divided into five types, all **similar** to the **victim** site **address** (e.g., example.com):

1. A common misspelling, or foreign language spelling, of the intended site: exemple.com
2. A misspelling based on typos: examlpe.com
3. A differently phrased domain name: examples.com
4. A different top-level domain: example.org
5. Abuse of the ccTLD: example.cm by using .cm, example.co by using .co, or example.om by using .om

Risk #2 – Same name, different TLD

That is relatively simple. You own the domain name example.com, and someone else registers the domain example.net, which per se may not in bad faith.

If example.com is not a trademark but rather a generic term, the registrant of example.net might have other usage intentions.

However, there is also the possibility that someone tries to run a phishing website to **obtain sensitive information** such as usernames, passwords, or credit card information by **disguising** yourself **as another** trustworthy **company** or person.

Risk #3 – Subdomain Hijacking

Subdomain hijacking refers to a technique by which "unused" **subdomains** can be **made** to point to a location of the **attacker's choice**.

You created a subdomain, e.g., subdomain.example.com, and set its DNS record to point to a shared hosting account (AWS, Azure, GitHub, Google Cloud, etc.). Later on, you deleted the service but forgot to remove the DNS entry.

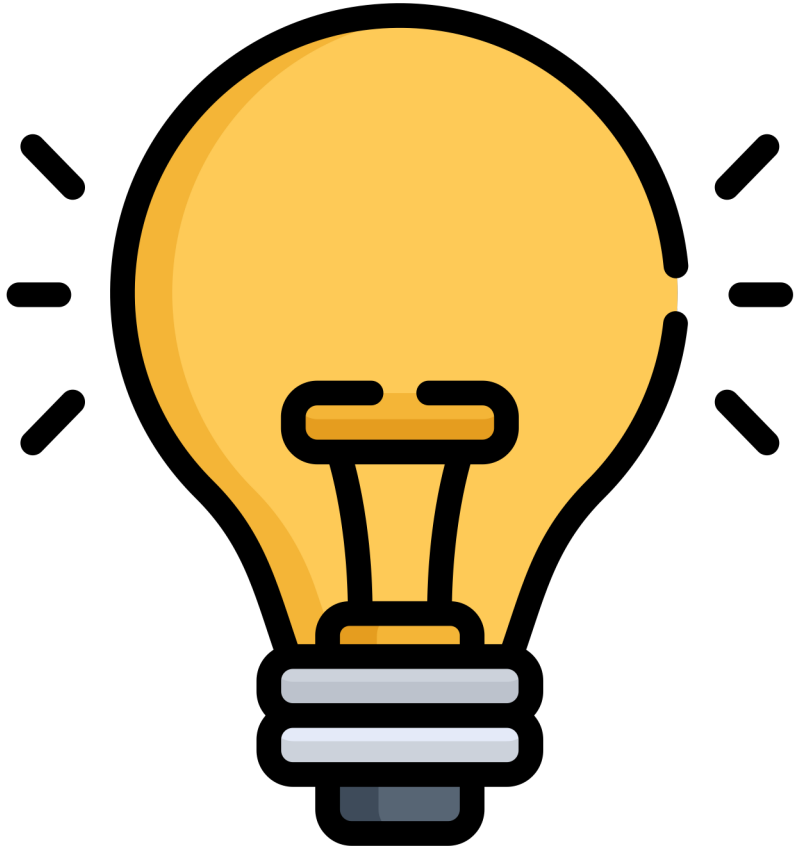
An attacker may add this subdomain to their hosting account on the same IP as your subdomain. Whereas, previously, your subdomain would've been unreachable, accessing it now would show the attacker's landing pages.

How Domain Monitoring helps you

Domain Monitoring can help you **keep track** of domain names that an identical or confusingly similar to your brand, corporate name, or trademark.

You will **receive** a **report** with identified domain names, which poses a threat to you.

Experts will **advise** and **recommend** when infringement is confirmed and help you act against it and enforce your rights.



Rights Protection Mechanism

It is essential to **defend** your **intellectual property** (IP) and to know what possibilities are there. The Rights Protection Mechanism (RPM) is such a mechanism that helps to safeguard your rights.

These include the Uniform Domain Name Dispute Resolution Policy (**UDRP**), Uniform Rapid Suspension (**URS**), and Trademark Post-Delegation Dispute Resolution Procedure (Trademark PDDRP).

Some ccTLDs have also adopted UDRP or have a similar dispute mechanism.

UDRP

The Uniform Domain Name Dispute Resolution Policy (**UDRP**) is a process established in 1999 by the Internet Corporation for Assigned Names and Numbers (ICANN) for **resolving disputes** regarding the registration of **domain** names.

There are five dispute resolution providers approved by ICANN:

1. The Asian Domain Name Dispute Resolution Centre (ADNDRC)
2. National Arbitration Forum (NAF)
3. World Intellectual Property Organization (WIPO)
4. Czech Arbitration Court, Arbitration Center for Internet Disputes
5. The Arab Center for Dispute Resolution (ACDR)

URS

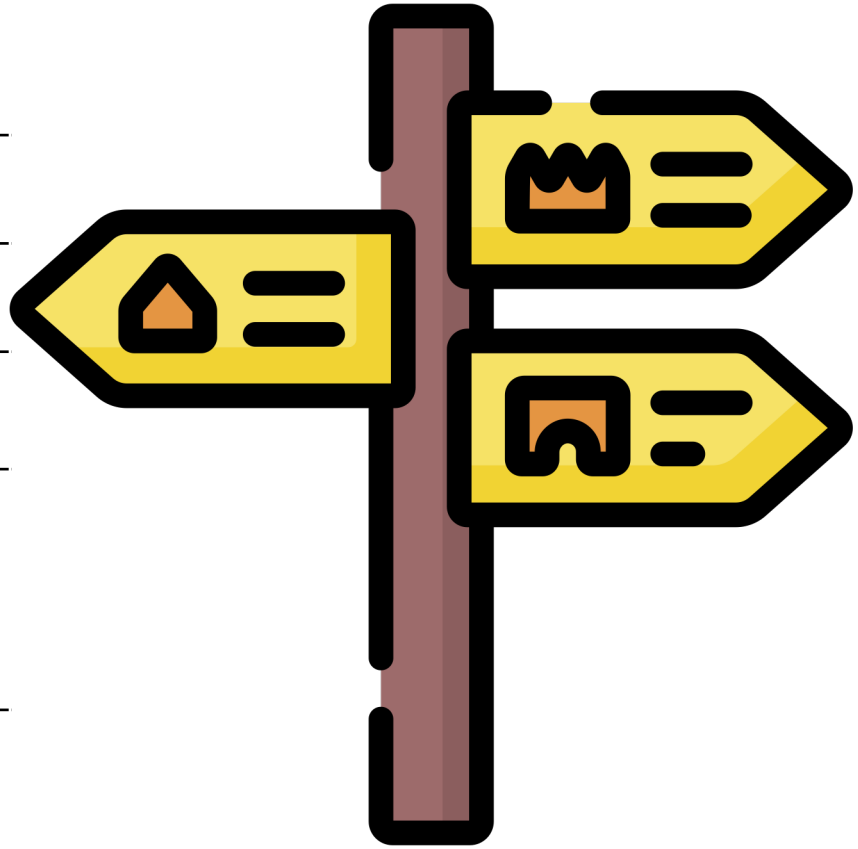
ICANN designed the Uniform Rapid Suspension System (**URS**) exclusively to provide trademark owners with a **quicker** and more **low-cost** process compared to UDRP to **take down** websites infringing on their intellectual property rights.

There are three dispute resolution providers approved by ICANN:

1. The Asian Domain Name Dispute Resolution Centre (ADNDRC)
2. MFSD Srl
3. National Arbitration Forum (NAF)

Comparing UDRP and URS

UDRP	URS
All domains	Mostly new gTLDs
Average of 2 months	Average of 17 days
Starting at $1,000	Starting at $375
“Clear and convincing evidence” and “no genuine issue of material facts”	“A preponderance of the evidence”
Transfer or cancellation	Suspension



Thank you!