WHITE PAPER

Unloved subdomains

An unmanaged, uncapped business risk.

Subdomains are the weak link in an organisation's online infrastructure. Networks, users and systems get the security focus, while namespaces sit unmanaged and open. This paper explains how the DNS works, why subdomains go ungoverned, and how to take back control.

THE ADDRESS BOOK OF THE INTERNET

What the DNS is, and why it matters

The internet's Domain Name System (DNS) has been running for over 40 years. It is crucial to the operation of every online service. Without it, the internet would simply stop working. No DNS means no Amazon, Netflix, Google or email.

The rapid expansion of cloud services, and their dependence on the DNS, has produced an explosion of domains and subdomains. Criminals now actively use the DNS and unmanaged subdomains to steal corporate identities, then deploy those identities to attack the owners, employees, users and partners.

The DNS maps a human readable domain name to a machine readable IP address. When a user types a website address such as klarvant.com into a browser, the DNS tells the browser which computer, anywhere in the world, hosts that website.

With something as large as the internet, the DNS is vast. Klarvant, which maps the internet, tracks more than 7 billion identifiers. No single body is responsible for maintaining it or minimising its errors and vulnerabilities. In practice, the DNS is maintained by internet users and domain owners themselves. That is the heart of the problem.

WHAT YOU NEED TO KNOW

- Your corporate identity is at critical risk.
- Subdomains are the weak link of your infrastructure.
- Criminals use subdomains to steal corporate identity.
- All industries are affected and the cost is high.
- In-house teams lack the resources and expertise.
- Most suppliers lack the capabilities to help.

THE DNS IN TWO PARTS

THE DOMAIN NAME

`klarvant.com`

A human readable, memorable set of characters that a user types into a browser.

THE DNS RESOLVES TO →

THE DATA, OFTEN AN IP ADDRESS

`192.168.1.1`

A machine readable set of numbers that tells a browser where to find a resource such as a website.

FIGURE 1 · LIVE INCIDENT

Curve Finance loses about $570k to DNS hijacking

The identity of Curve Finance was targeted by attackers who diverted its users and stole roughly $570,000 (August 2022).

`tronweekly.com/curve-finance-dns-hijacking`

READ A WEB ADDRESS LIKE AN EXPERT

The anatomy of a domain name

A domain name is made of several components separated by punctuation, dots and slashes. Each part has a distinct owner and a distinct job. Understanding the parts is the first step to understanding where the risk sits.

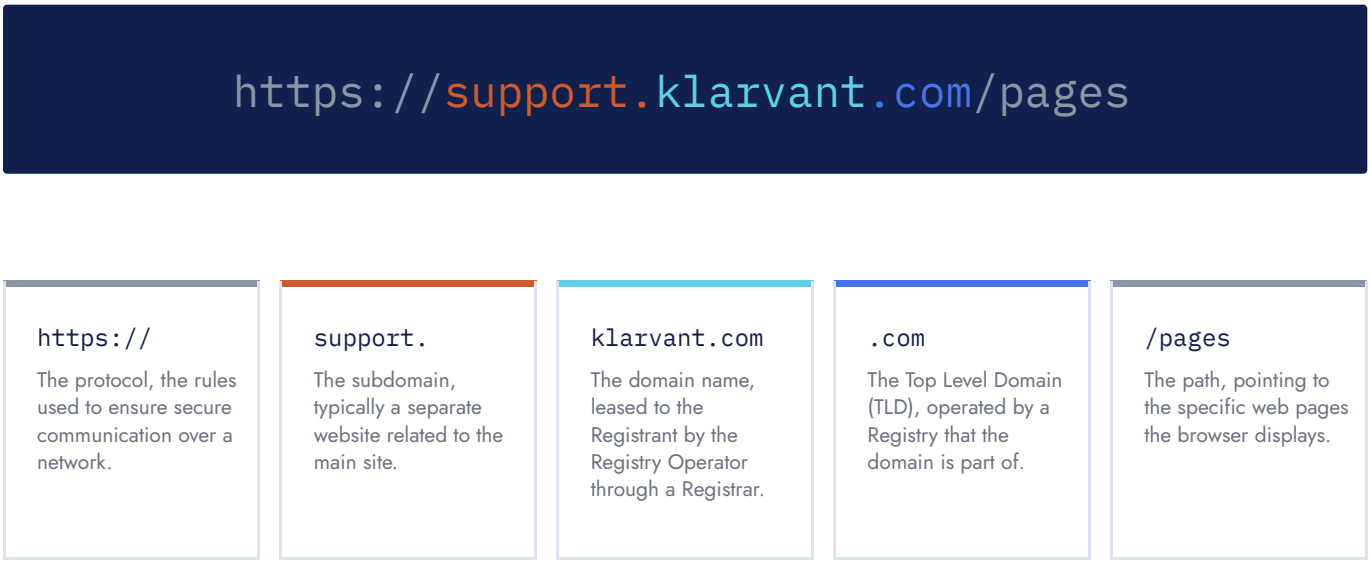


Figure 2: the anatomy of a URL and its parts, including the domain name and subdomain.

FOUR ACTORS, ALL STARTING WITH REG

The 4 REGs of the domain name industry

The way the domain name industry operates has clear parallels with the real estate rental market. There are four main actors, and the regulator of the industry is the Internet Corporation for Assigned Names and Numbers (ICANN). Unlike national real estate regulators, ICANN has global jurisdiction.

Every actor has a commercial interest in keeping domains registered, renewed and reachable. Hold that thought: subdomains break this model entirely.

THE REAL ESTATE ANALOGY

Who is responsible for a domain name?

Registry Operator

≈ LANDLORD

Top Level Domains such as .com are managed by a Registry Operator, the equivalent of a landlord who owns the apartment block. They maintain the integrity of the TLD for all Registrants but do not control individual websites, styles or DNS settings.

Example: Verisign operates and protects the .com TLD.

Registrar

≈ LETTING AGENT

Registrars are assigned the right to market domain names to the public by the Registry Operator. They are the equivalent of a letting agent, and they ensure a Registrant's licence to use a domain remains valid and within terms.

They charge to register and renew, and often host DNS for a fee.

Registrant

≈ TENANT

The Registrant is the ultimate user of the domain name, the equivalent of a tenant. There can be many tenants in one property (Registry), each with their own unique address (domain name). They must go through a Registrar to secure it.

Responsible for correct DNS settings and a secure website.

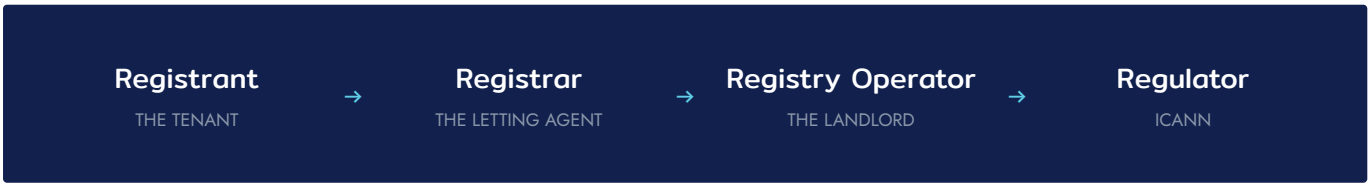
Regulator

≈ TRADING STANDARDS

ICANN is the industry regulator, similar to a national trading standards body but with global jurisdiction. It works to keep the internet stable and takes a keen interest in any Registry or Registrar that may endanger its availability.

Takes a portion of registration fees, plus an annual TLD licence fee.

FOLLOW THE MONEY



The Regulator also takes a share of the registration fee from both the Registrar and the Registry. Every flow here is tied to a parent domain name, so each actor has a commercial interest in keeping domains registered, renewed and reachable. Hold that thought: subdomains break this model entirely.

Figure 3: the main actors in the domain name industry and how fees flow between them. Providers for DNS, cloud and similar services are not shown.

NO FEE, NO OVERSIGHT, NO OWNER

Domain names are governed. Subdomains are not.

The money flows show where the business interests lie for registering and managing a domain name. For subdomains, the same does not hold true. In short: no.

ICANN makes no money from regulating subdomains, so it does not include them in its remit. Because they are not parent domains, Registry Operators and Registrars cannot charge to register them. They have little visibility and assume no responsibility for managing them.

Any Registrant can set up a subdomain such as investors.example.com whenever they want, at no cost. With no cost and no oversight, this has led to the unchecked creation of billions of subdomains.

The majority of domain owners assume their Registrar or IT provider manages subdomains for them. Almost all are surprised to learn this is not the case, and that the responsibility is theirs. Many discover too late, after revenues and reputation have already been damaged.

ROOT CAUSE

Ultimately, the responsibility for a subdomain lies with the user of the domain name, the Registrant. Unmanaged subdomains are the root cause of major business risks, including Corporate Identity Theft.

THE SCALE OF THE BLIND SPOT

351.5M

registered domain names worldwide

7Bn+

identifiers tracked across the public internet by Klarvant

Subdomains outnumber registered domain names many times over.

CORPORATE IDENTITY THEFT

Ferrari identity stolen in a domain hijack

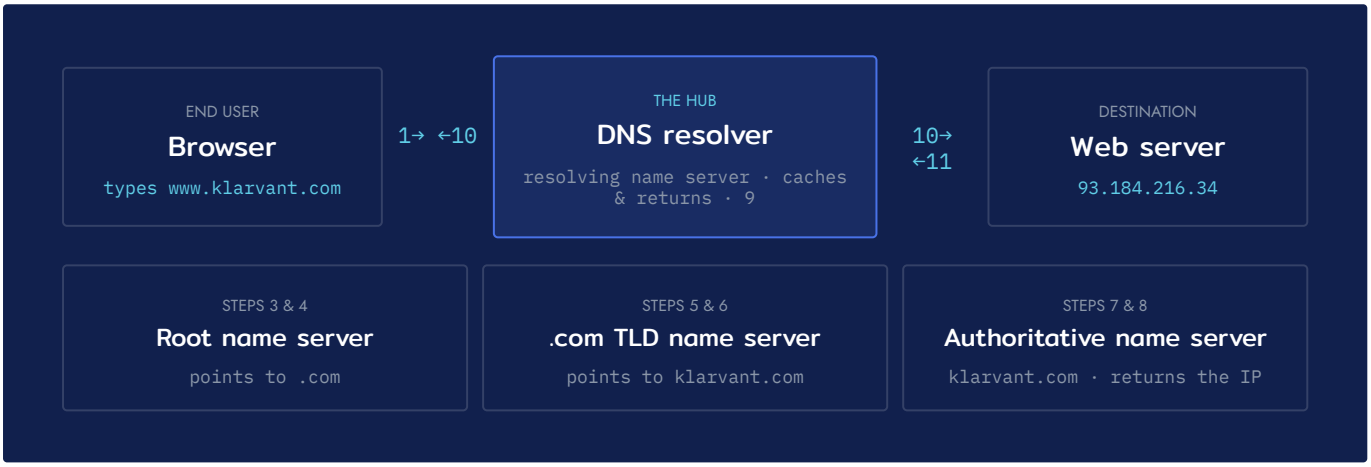
Ferrari had its corporate identity stolen and used to host a fake Ferrari NFT collection. The subdomain forms.ferrari.com was found serving the scam, reported by ethical hacker Sam Curry.

`bleepingcomputer.com · 2022-05-06 · author Ax Sharma`

Sources: registered domains, Verisign DNIB Q2 2022. Identifier figure, Klarvant internet mapping.

FROM WEB ADDRESS TO WEB PAGE

How a DNS lookup works



01 A user types www.klarvant.com into the browser's search bar. The browser checks its local cache to see if it already has this domain stored.

02 If the IP is not in the cache, the browser asks a resolving name server for help finding the IP address of www.klarvant.com.

03 If the resolver has no cached data for klarvant.com or .com, it sends a DNS query to a root name server.

04 The root name server responds and directs the resolver to the relevant Top Level Domain server, in this case .com.

05 The resolver queries the .com TLD name server for the IP address of www.klarvant.com.

06 The TLD name server responds and directs the resolver to the authoritative name servers for klarvant.com.

07 The resolver queries the klarvant.com authoritative name server for the IP address of www.klarvant.com.

08 The klarvant.com authoritative name server responds with the IP address for www.klarvant.com.

09 The resolver puts the data in its cache and sends it to the querying computer and web browser.

10 The web browser uses the IP address to request the web page for www.klarvant.com.

11 The web server at that IP returns the web page data for www.klarvant.com.

While this looks lengthy, the whole process typically takes milliseconds, and many billions of lookups are performed every day.

TWO CATEGORIES, SIX COMMON TECHNIQUES

Types of DNS attack

Attackers take advantage of vulnerabilities in the DNS to reach organisations and their wider ecosystem. Attacks come in two main forms.

AVAILABILITY ATTACKS

Aim to take a service offline by overwhelming or disrupting the DNS infrastructure that users depend on.

INTEGRITY ATTACKS

Aim to corrupt or subvert DNS data so that legitimate names resolve to attacker controlled destinations.

DNS flood attacks

A DoS or DDoS attack where DNS servers are flooded with traffic to real or random domains until they become overloaded.

DNS amplification

Takes advantage of a DNS server permitting recursive lookups to amplify and spread an attack to other DNS servers.

DNS tunnelling

Uses the DNS to encode and transport commands or data in and out of an organisation, often to exfiltrate data unnoticed.

Cache poisoning

A legitimate record in a DNS server, often a cache, is replaced by the attacker. It can affect any record type in the DNS.

DNS hijacking

Subverts the resolution of DNS queries by taking control of domains or subdomains at namespace, Registry, Registrar or host level.

Domain shadowing

Hijacks the DNS of a legitimate domain to operate subdomains for malicious activity, without changing the existing entries.

FUN FACTS ABOUT THE DNS

1983

The DNS is almost 40 years old. It traces its roots to 1983, from two papers published by Paul Mockapetris.

1 file

Before DNS servers, all internet addresses were stored in a single file called hosts.txt.

1985

The first commercial .com domain, symbolics.com, was registered on 15 March 1985 by Symbolics Inc.

509 hrs

The longest known sustained DDoS attack ran for 509 hours, more than 21 days.

2 ways

Lookups run in two directions: forward, from URL to IP address, and reverse, from IP address to URL.

7Bn+

Klarvant tracks more than 7 billion identifiers; subdomains are the vast unmanaged majority of the namespace.

A SIMPLE, REPEATABLE METHOD

How to regain control of your subdomains

Follow three simple steps to reduce your risk and protect your business. The work is continuous, not a one off, because the namespace keeps changing.

Step 01

Find

Understand how many subdomains you have by performing a subdomain inventory check, then identify the assets at risk through a subdomain audit.

Step 02

Fix

Take immediate action to fix the critical and high risk subdomain configuration issues that the audit surfaces.

Step 03

Follow

Continue to monitor subdomains over time to maintain a low risk profile as your namespace grows and changes.

'Most subdomains are unmanaged, forgotten and ignored. They are the weak link, a proliferating risk used to steal corporate identities.'

KLARVANT · DIGITAL GOVERNANCE INTELLIGENCE

Not sure where to start?

If you are unsure how to take any of these steps, talk to Klarvant. We will help you get started in the right direction with independent advice from an expert, through a free, no obligation call. No integration is required.

BOOK A SUBDOMAIN REVIEW

sales@klarvant.com

IN SUMMARY

Your corporate identity is at critical risk

With the growth of cloud services, subdomain use is soaring. Most subdomains are unmanaged, forgotten and ignored. They are the weak link, and a proliferating risk used to steal corporate identities. Teams lack resources and experience, while suppliers lack the capabilities to help. This is widespread, affecting organisations of all sizes across all industries.

It does not have to be this way. Klarvant maps and analyses the internet to protect businesses from Corporate Identity Theft, with no integration required.

Most

subdomains are unmanaged, forgotten and ignored.

About Klarvant

Klarvant specialises in mapping, monitoring and securing large and complex internet namespaces. We help corporations and governments understand, sanitise and protect their vulnerable DNS networks across the globe. Klarvant is a UK company.

Contact: sales@klarvant.com

REFERENCES

IDC 2022 Global DNS Threat Report, average cost of a DNS attack: $942k.

Curve Finance DNS hijacking, tronweekly.com.

ICANN, what the regulator does, icann.org.

Verisign Domain Name Industry Brief, Q2 2022, registered domain totals.

Ferrari subdomain hijack, bleepingcomputer.com, May 2022.

DNS history, Paul Mockapetris, 1983, en.wikipedia.org.

Take back control of your namespace

Book a free, no obligation subdomain review and see your exposure across the domains, subdomains and identifiers that make up your public footprint.

BOOK A SUBDOMAIN REVIEW

sales@klarvant.com