

A **subdomain** is a **child domain** that exists under a main (root) domain. It helps organize and separate different sections, services, or environments of a website.

Ex:blog.raju.com

While organizations invest heavily in securing their primary web properties ([www.raju.com](http://www.raju.com) and raju.com), subdomains often remain the silent entry point for attackers.

Forgotten, misconfigured, or poorly maintained subdomains dramatically expand the attack surface and frequently become the real weakest link during breaches, penetration tests, and bug bounty discoveries.

## The Illusion of Strong Perimeter Security

Most companies focus protection efforts on:

- [www.raju.com](http://www.raju.com)
- raju.com (root domain)

**These flagship assets typically receive:**

- Web Application Firewall (WAF) rules
- Strict Content Security Policy (CSP) & HTTP headers
- Regular patching & vulnerability scanning
- Continuous monitoring & logging**
- Multi-factor authentication (MFA) enforcement

However, the reality is different for subdomains.

Looking them in whois lookup tool

The screenshot shows a web browser displaying a Whois lookup page for the domain `microsoft.com`. The page has a header with navigation links for Domains, Hosting, Servers, Email, Security, Whois, and Deals. A search bar at the top right contains the text "Whois". Below the search bar, there's a link to "Enter Domain or IP". The main content area is titled "Domain information" and lists the following details for `microsoft.com`:

Domain:	<code>microsoft.com</code>
Registered On:	1991-05-02
Expires On:	2026-05-03
Updated On:	2025-04-01
Status:	client delete prohibited client transfer prohibited client update prohibited server delete prohibited server transfer prohibited server update prohibited
Name Servers:	ns1-39.azure-dns.com ns2-39.azure-dns.net ns3-39.azure-dns.org ns4-39.azure-dns.info

Below the domain information, there's a section for "Registrar Information" which shows the registrar as "MarkMonitor Inc.". To the right of the main content, there's a sidebar titled "Interested in similar domains?" with several suggestions like `cashmicrosoft.com`, `smartmicrosoft.com`, etc., each with a "Buy Now" button. At the bottom right, there's a promotional banner for ".space" domains.

## How Organizations Create Hundreds of Subdomains Over Time

**Business needs lead to rapid creation of subdomains for legitimate purposes:**

- Testing & Quality Assurance —• `test.raju.com`
- Development environments •[dev.raju.com](#), `developer.raju.com`
- Staging / Pre-production —• `staging.raju.com`, `uat.raju.com`

- Admin & management panels
  - admin.raju.com, portal.raju.com,
  - manage.raju.com
- Legacy & old projects —• old.raju.com, legacy.raju.com,  
v1.raju.com
- Marketing campaigns & temporary
  - microsites —• summer2025.company.com,
  - blackfriday.raju.com
- VPN & internal tools —• vpn.raju.com, remote.raju.com
- Third-party integrations —•
  - api.partner.raju.com, webhook.raju.com

Many of these are created quickly, used briefly, then forgotten — but never properly decommissioned.

We can find them using subfinder tool

The screenshot shows the Submain Finder web application. At the top, there's a banner with the text "LIVE Israel is committing Genocide in Palestine. Follow the Genocide" and a link to "Consider helping the project, check out our Hall of Fame". Below the banner, there's a search bar labeled "Domain (eg. example.com)" with a "Start Scan" button. A "Private scan" checkbox is checked, with a note explaining it keeps the scan private. The main content area displays the results of a scan for the domain "theroster.com". It shows the "Scan date" as "2026-01-04 16:12:01", "Domain Country" as "Worldwide (COM)", "Subdomains found" as "39", and the "Most used IP" as "148.135.130.115 (5x)". Below this, there's a table with columns for "Subdomain", "IP", and "Cloudflare". The table lists several subdomains, their corresponding IP addresses, and Cloudflare status icons. To the right of the table, there's a "Recent scans:" sidebar listing various domains. At the bottom of the page, there's a navigation bar with links like "Whois Check", "Check Status", "Compare with...", "Copy to clipboard", "Download CSV", "Download JSON", and "Search".

# Why Forgotten Subdomains Are Prime Targets for Attackers

## Dangerous conditions:

- Outdated & unpatched software
  - Running old versions of Apache, WordPress, PHP, Node.js, etc. with known CVEs (e.g., Log4Shell remnants, outdated Laravel, etc.)
- Lack of WAF / monitoring
  - Bypass the main domain's protection entirely; no alerts on suspicious activity
- Weak or default credentials
  - admin:admin, root:toor, no MFA, or exposed .htaccess bypasses
- No regular patching or vulnerability management
  - Years-old vulnerabilities remain exploitable
- Exposed sensitive data
  - Debug modes enabled, .env files, source code backups, database dumps, API keys in javascript
- Dangling DNS records (subdomain takeover risk)
  - CNAME points to deleted cloud resources (AWS S3, Azure Blob, GitHub Pages, Heroku, etc.)
  - attackers claim & control the subdomain

**Result:** While the main website appears "locked down," attackers quietly gain foothold through these forgotten doors.

