How Subdomain Hijacking Happens in 5 Steps

1

DNS zone points to web hosting server.

A website resolves

2

When web pages reach end of life and are removed, forgetting to purge the A records or CNAMES results in abandoned DNS records.

Abandoned DNS records are known as “dangling DNS”

3

Cybercriminals mine zone data looking for dangling DNS records.

Dangling DNS records are mined

4

Using mined dangling DNS information, cybercriminals can now request the abandoned hostnames from web hosts.

Cybercriminals acquire hostnames from web hosting providers

5

Now cybercriminals can publish illegitimate content to those acquired hostnames on the same server location.

The subdomain is hijacked

Why Subdomain Hijacking is so Difficult to Detect

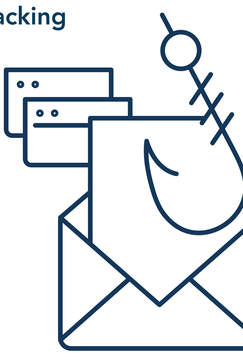
Cybersecurity protocols cannot detect unusual behavior, as the attack uses:

- Legitimate, non-fraudulent subdomains
- Known DNS infrastructure
- Recognized web hosting servers
- No infiltration of the company’s or its vendor’s accounts
- Added SSL certificates to the site to appear authentic

The Impact of Subdomain Hijacking

Illegitimate content hosted by cybercriminals can be used to host fraudulent or phishing content that can:

- Lead to data and security breaches
- Affect consumer confidence
- Tarnish brand reputation



Subdomain Monitoring

Companies are challenged to account for all their digital assets--which ones are critical, functional, or redundant. CSC’s Subdomain Monitoring solution gives you the visibility and contextualized alerts to make informed decisions, and maintain cyber hygiene to prevent a subdomain hijack.

Find out more

We’re ready to talk.

1 800 927 9800

cscdbs.com