DNS Rebinding Attack: What it is, why it’s risky, and how to block it

Gridinsoft Help Center

What it is

DNS rebinding is a web trick that makes your browser talk to places it normally shouldn’t - like your home router, NAS, or an internal app - by rapidly changing a site’s DNS answer. You think you’re visiting a normal page; your browser is quietly asked to call your private network.

How it works

- You open a booby-trapped website.

- That site’s DNS first points to the attacker’s server, then quickly "rebinds" to an address on your private network (e.g., 192.168.x.x).

- Your browser, which can reach your LAN, is used as a proxy to poke internal devices, steal data, or change settings.

What you might notice

- Router or smart-home settings changed without you doing it

- Admin pages opening without a login prompt (weak devices)

- Odd behavior on internal apps after visiting a sketchy site

If you suspect it

- Close the tab and disconnect from suspicious Wi-Fi.

- Reboot your router; update its firmware and change the admin password.

- Turn off remote admin on routers/IoT and require logins for all internal services.

- Scan PCs/phones for malware; review device logs if available.

Prevent it

- Keep routers, NAS, and IoT updated; disable unauthenticated APIs/admin pages.

- Use a DNS filter that blocks rebinding (many resolvers have anti-rebinding).

- Prefer hostnames with authentication for internal apps; avoid exposing them to the internet.

- Set browser and network CORS/CSRF protections on internal web apps if you run them.

- Segment your network (separate VLAN/Wi-Fi for IoT) so one device can’t see everything.