Updated Report – DNS Hijack Investigation

1. Background

Chris previously observed suspicious DNS behavior suggesting a DNS-based man-in-the-middle (MITM). Multiple tests showed queries unexpectedly resolving through Akamai resolvers in the U.S., even when a trusted resolver (e.g. Cloudflare) was specified. This indicated possible DNS interception or manipulation at the router or ISP level.

2. New Findings (August 2025)

a. Home Network (Telmex, No VPN)

- Current router WAN DNS: `187.141.30.237` / `201.144.94.237` (Telmex Business).
- DNS leak test confirms DNS queries are now going only through Telmex servers.
- `nslookup` results match whether specifying Cloudflare (1.1.1.1) or not → no evidence of ongoing DNS MITM.

b. Café Network Test

- Same behavior observed: `nslookup` returned consistent IPs whether forcing Cloudflare or not.
- Confirms anomaly is not present outside the home network either.

c. iPhone Behavior

- Still resolves through Akamai resolvers (Irving/Dallas, U.S.).

- Verified this is due to Apple Private Relay / iCloud DNS routing. It is normal and not attacker-controlled.

d. Change from Earlier Tests

- Previously, DNS leak tests showed multiple Akamai resolvers (not just iPhone).
- Now, only Telmex resolvers are present for router and PC traffic.
- Suggests the malicious DNS interception has been disabled/removed.

3. Assessment

- The attacker likely hijacked DNS temporarily to monitor browsing activity.
- No strong signs of credential theft — activity was consistent with surveillance/traffic monitoring rather than phishing.
- Current configuration is clean: Telmex DNS only, iPhone exceptions explained by Apple.
- Risk remains that attacker could reintroduce the hijack in the future.

4. Recommendations

1. Router Hardening
    - Explicitly configure DNS to Cloudflare (`1.1.1.1` / `1.0.0.1`), Quad9 (`9.9.9.9`), or Google (`8.8.8.8`), rather than relying on ISP defaults.

- Disable remote management, TR-069, and UPnP if possible.
- Change router admin password to a strong, unique one.

2. DNS Integrity Monitoring

Periodically test with:

```
nslookup example.com 1.1.1.1
nslookup example.com
```

- If results differ, it indicates possible manipulation.
- Continue running DNS leak tests for verification.

3. ISP Engagement
   - Ask Telmex:
     - Do they force override to Telmex DNS even if you set a custom one?
     - Are they aware of DNS hijack attempts on customer routers?
4. Device Guidance
   - For iPhone: disable Apple Private Relay if you prefer not to see Akamai DNS in tests.
   - Otherwise, accept Akamai entries as normal iOS behavior.
5. VPN Best Practice
   - Use a trusted VPN when outside your home (cafés, hotels).

    - VPN ensures DNS and traffic cannot be intercepted, even if hijacking reappears.

6. Ongoing Monitoring
    - Save periodic screenshots of DNS test results for reference.
    - Escalate if Akamai resolvers reappear in non-Apple devices.

5. Conclusion

The DNS MITM that previously affected your traffic is no longer active. Current DNS resolution is stable and points only to Telmex servers, with iPhone exceptions explained by Apple infrastructure. The attacker appears to have withdrawn.

Your browsing is no longer being intercepted — but because DNS hijacking can be reintroduced, router hardening, independent DNS checks, and selective VPN use remain important safeguards.

DNS Hardening Checklist

A. Router (Telmex – Huawei/ZTE style interface)

1. **Login to Router Admin Panel** (usually `192.168.1.254` or as shown on sticker).
2. Go to **Internet / WAN Settings** → look for **DNS** field.
3. Replace Telmex DNS with trusted providers, e.g.:
    - Cloudflare: `1.1.1.1` and `1.0.0.1`
    - Quad9: `9.9.9.9` and `149.112.112.112`
    - Google DNS: `8.8.8.8` and `8.8.4.4`
4. **Save & Reboot** router.
5. Disable:
    - **Remote Management / TR-069**
    - **UPnP (Universal Plug & Play)**
    - **WPS** (if present)
6. Change **router admin password** to a long, unique one (not the default).

B. Windows PC

1. Open **Control Panel → Network and Sharing Center → Change Adapter Settings**.

2. Right-click active adapter → **Properties**.

3. Select **Internet Protocol Version 4 (TCP/IPv4)** → **Properties**.

4. Choose **Use the following DNS server addresses** → enter Cloudflare / Quad9 / Google DNS.

5. Repeat for **IPv6** if needed (Cloudflare: `2606:4700:4700::1111`).

6. Open **Command Prompt** and test:

C. VPN Use

- Use a **trusted, no-logs VPN** when on public Wi-Fi or when you want to bypass ISP DNS enforcement.

- Confirm by running **dnsleaktest.com** while VPN is active – only VPN DNS resolvers should appear.

Post-MITM Actions (Now That Attack Is Gone)

1. **Change Passwords (Precautionary)**
    - While there's no sign credentials were stolen, it's best to reset passwords for high-value accounts (email, banking).
    - Enable **MFA** wherever possible.
2. **Firmware Update**
    - Ensure router firmware is **up to date** (older versions are often targeted for DNS hijacks).
3. **Log Monitoring**
    - Keep occasional router log exports — watch for strange admin logins or DNS reconfigurations.
4. **Baseline Tests**
    - Save the current **DNS leak test screenshots** as a baseline.
    - If resolvers suddenly change (to Akamai or other non-Telmex servers), you'll know immediately.
5. **ISP Clarification**
    - Ask Telmex if they *force* DNS routing. Some ISPs override custom DNS, which would explain why `nslookup` gives the same IPs even when forcing Cloudflare.
    - If confirmed, VPN becomes the only reliable way to bypass.
6. **Periodic Re-Tests**

- Every few days, run `nslookup` and dnsleaktest.com.
- This helps ensure attacker hasn’t re-enabled their MITM.