

The Underminer

Abusing CDN Shared Infrastructure

Press Embargo Notice

- The Underminr is scheduled for public release on 21 May 2026 at 9:05am Eastern (Toronto) time.
- As part of responsible disclosure, we are coordinating restricted access to Defenders before public release to the press.
- This session is one of them.
- Our ask: collaborate with us and do not distribute or publicly comment until post-release.



Content Delivery Network

CDN is blind to endpoint's deceptive use of "example.com" DNS resolution to connect to SNI "evilsite.ai" instead



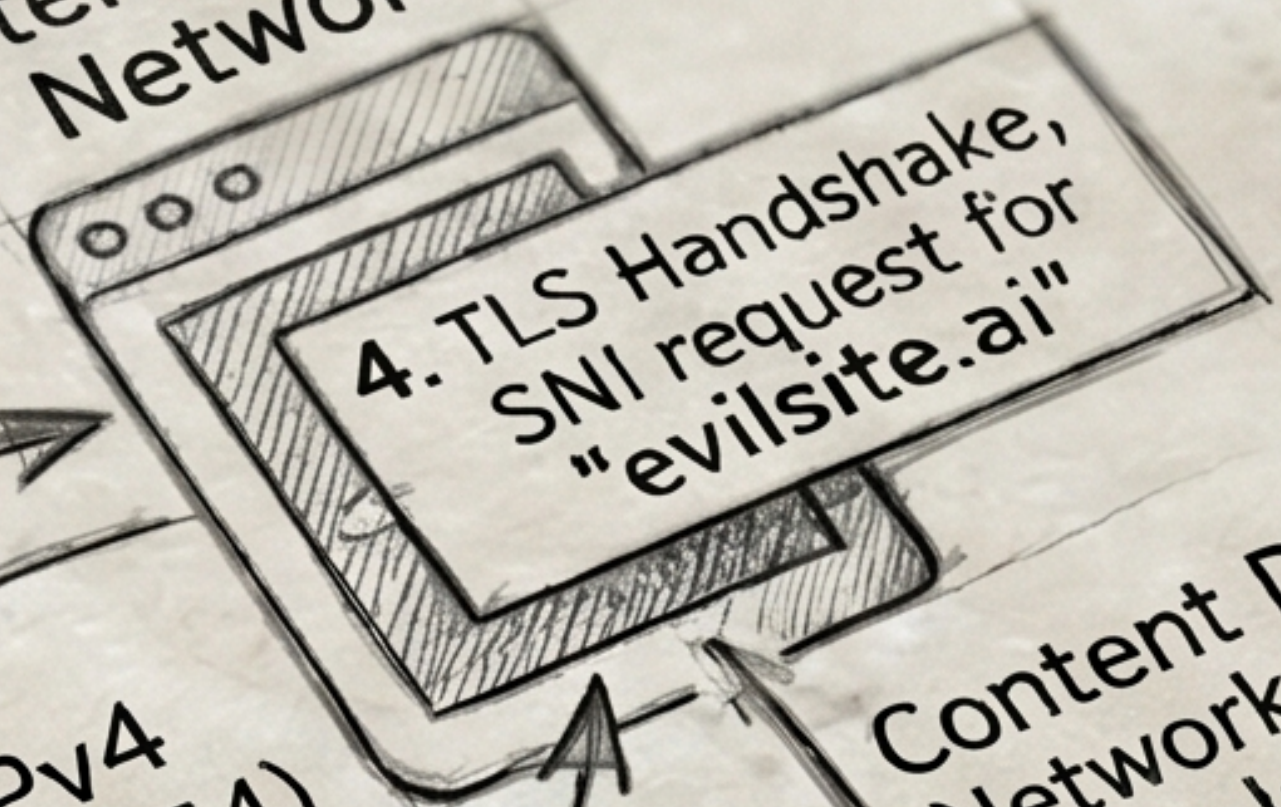
ENDPOINT

1. DNS Query for "example.com"

2. Resulting IPv4 (e.g., 104.20.23.154)

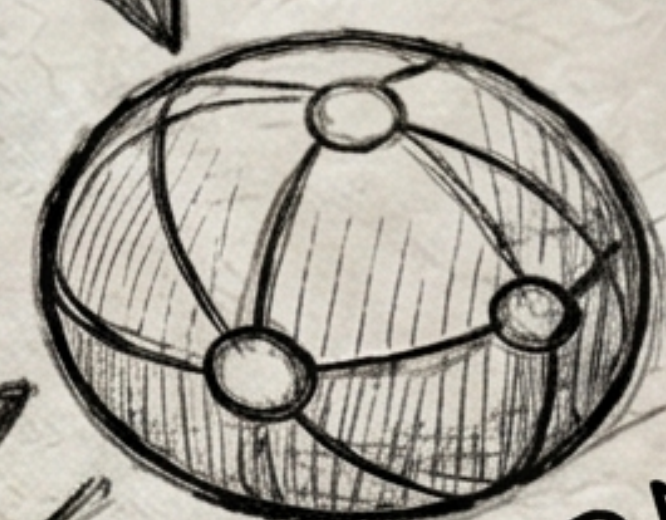
3. TCP Port 443 connection to 104.20.23.154

1. DNS Query for "example.com"



4. TLS Handshake, SNI request for "evilsite.ai"

Content Delivery Network connection resolution for "evilsite.ai"



DNS INFRASTRUCTURE

[DNS INFRASTRUCTURE is BLIND to actual connection destinat/SNI "evilsite.ai"]

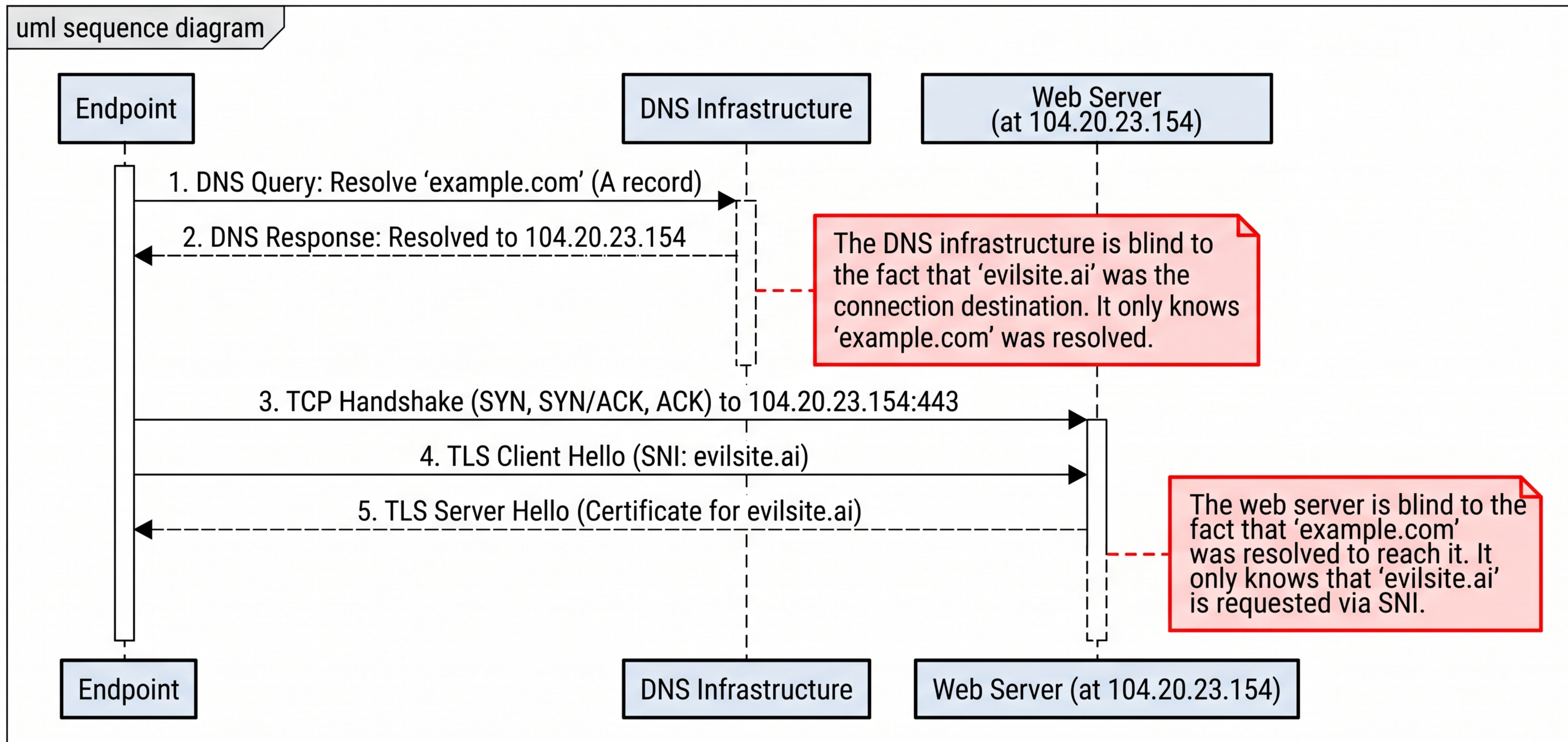


```
% ./underminr.sh example.com evilsite.ai
[*] Target well-known domain: example.com
[*] Hidden destination domain: evilsite.ai
-----
[*] Resolving example.com...
[+] Success: Resolved to IP -> 104.20.23.154
-----
[*] Connecting to 104.20.23.154 but requesting evilsite.ai...
[*] Running curl...
-----
* Added evilsite.ai:443:104.20.23.154 to DNS cache
* Hostname evilsite.ai was found in DNS cache
* Connected to evilsite.ai (104.20.23.154) port 443
* [HTTP/2] [1] OPENED stream for https://evilsite.ai/
* [HTTP/2] [1] [:method: GET]
* [HTTP/2] [1] [:scheme: https]
* [HTTP/2] [1] [:authority: evilsite.ai]
hello world
-----
[*] Demonstration complete.
```

Running the POC script



UML SEQUENCE DIAGRAM: NETWORK FLOW AND VISIBILITY



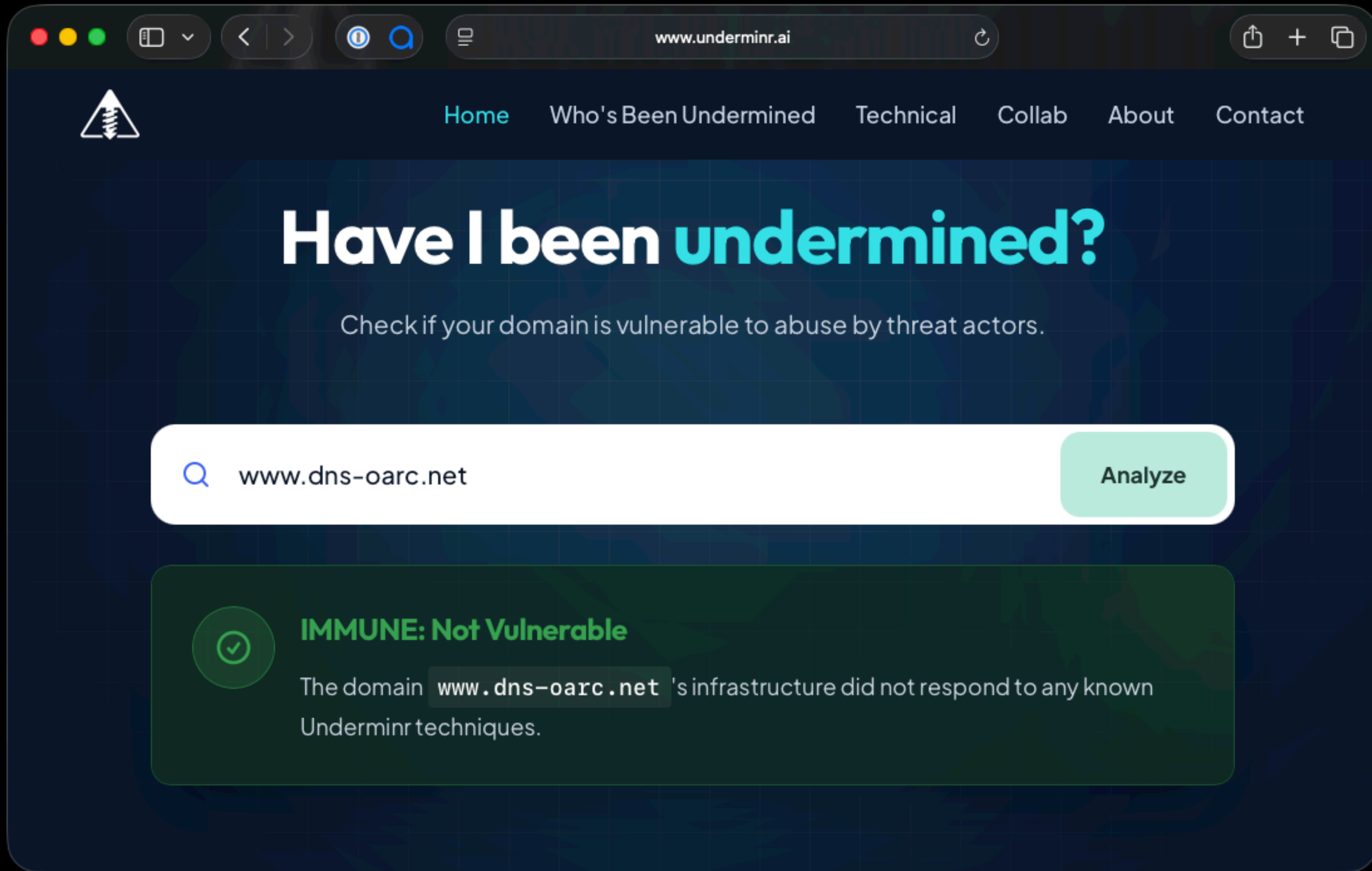
Comparing to Domain Fronting

- Review domain fronting:
 - The bait-and-switch happens inside the CDN
- Compare how Underminr works:
 - The bait-and-switch happens between DNS and SNI/HTTP host header



How bad is it?





The screenshot shows a web browser window with the URL www.underminr.ai. The navigation menu includes [Home](#), [Who's Been Undermined](#), [Technical](#), [Collab](#), [About](#), and [Contact](#). The main heading is "Have I been undermined?" with the subtitle "Check if your domain is vulnerable to abuse by threat actors." A search bar contains the domain `www.dns-oarc.net` and an "Analyze" button. The result is displayed in a green box with a checkmark icon, stating "IMMUNE: Not Vulnerable" and "The domain `www.dns-oarc.net`'s infrastructure did not respond to any known Underminr techniques."



www.underminr.ai

Home Who's Been Undermined Technical Collab About Contact

Have I been undermined?

Check if your domain is vulnerable to abuse by threat actors.

example.com Analyze

VULNERABLE: Potential Abuse

The domain `example.com` is **VULNERABLE**, but has not been seen in reported detections.

The Underminr IP `172.66.147.243` for **Cloudflare** is accepting traffic for deceptive domains at this IP address.



www.underminr.ai

Home Who's Been Undermined Technical Collab About Contact

Have I been undermined?

Check if your domain is vulnerable to abuse by threat actors.

udemy.com Analyze

ABUSED: Known Abused Domain

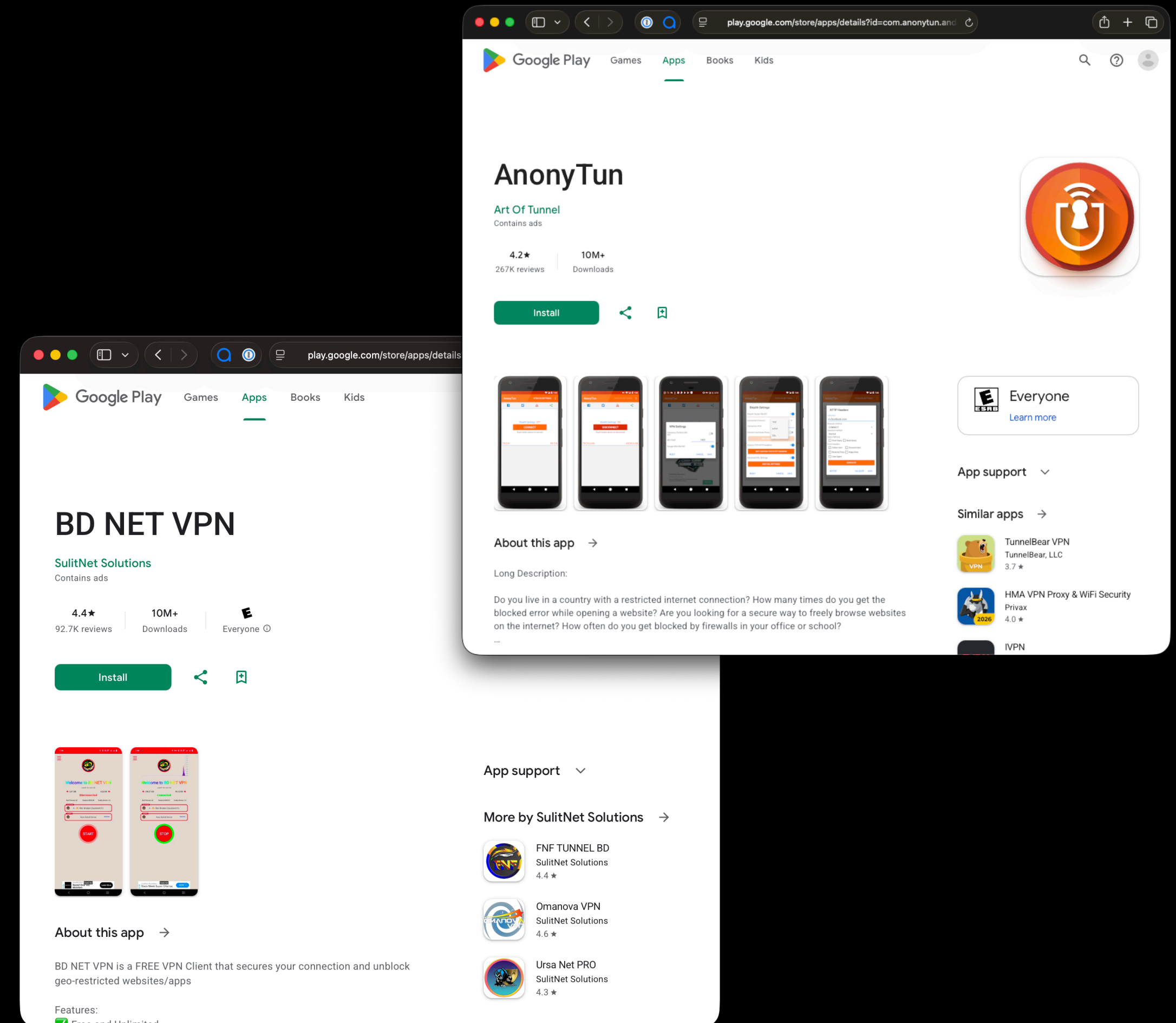
The domain `udemy.com` is **VULNERABLE** and exists in our known abused list.

The Underminr IP `104.16.143.237` for **Cloudflare** is accepting traffic for deceptive domains at this IP address.



Consequences

- Abused by Sketchy VPN apps (BD Net VPN, 10M+ Downloads, AnonyTun, 10M+)
- Malware (including ECH abuse)
- ClickFix (trivial application)



Calling on all defenders...

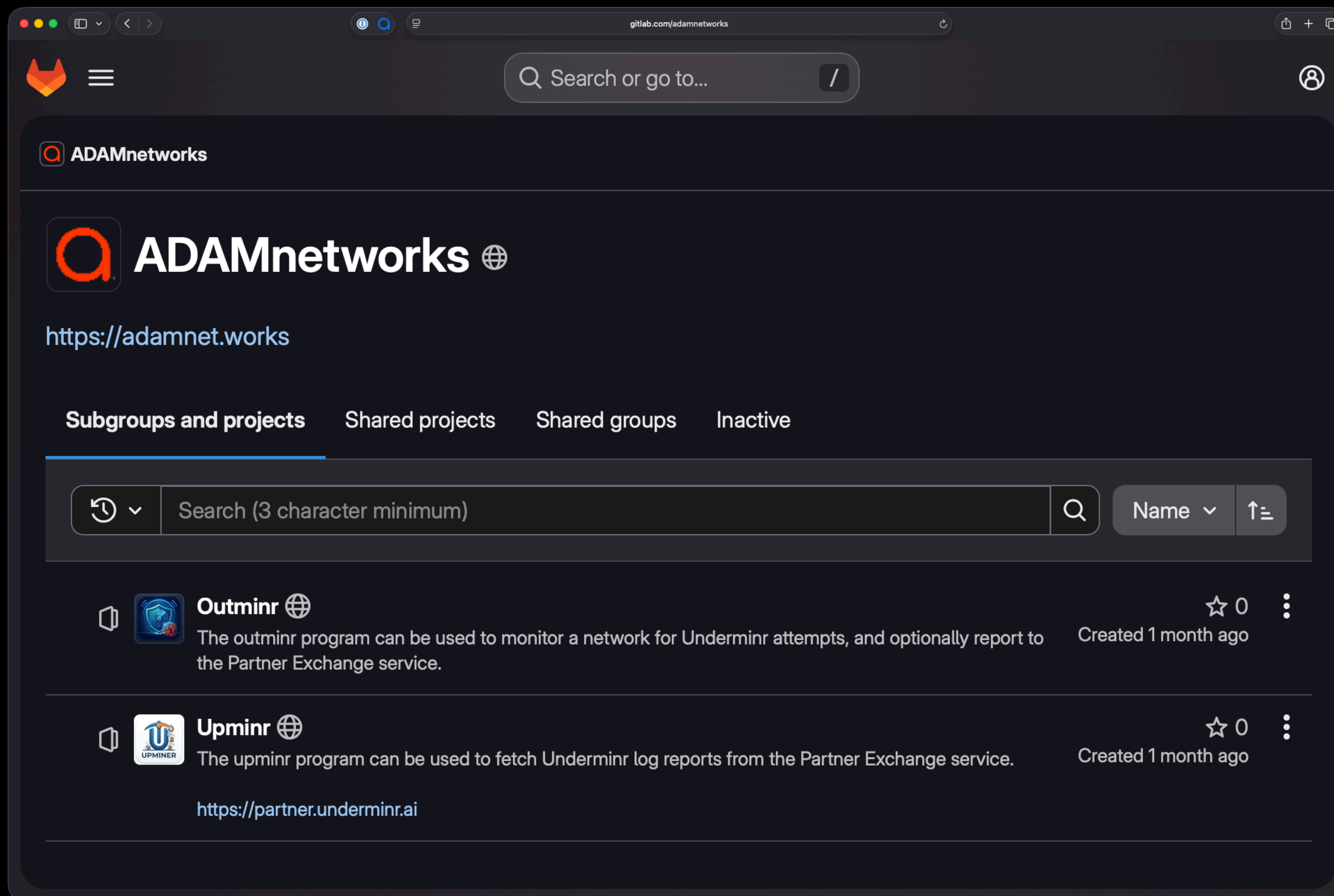


Effective Mitigation

- DNS at root of network trust, hijack/block/log unauthorized Do53
- Don't Talk To Strangers (DTTS) | Zero Trust DNS
- pDNS check on SNI domain
- Strip ECH in responses



Free tools from gitlab.com/ADAMnetworks



The screenshot shows the GitLab profile page for ADAMnetworks. The page header includes the GitLab logo, a search bar, and the user's profile icon. The main content area displays the ADAMnetworks logo and the website URL <https://adamnet.works>. Below this, there are tabs for "Subgroups and projects", "Shared projects", "Shared groups", and "Inactive". The "Subgroups and projects" tab is active, showing a search bar with a filter icon and a search input field. Below the search bar, two projects are listed:

- Outminr** (with a globe icon): The outminr program can be used to monitor a network for Underminr attempts, and optionally report to the Partner Exchange service. Created 1 month ago. 0 stars.
- Upminr** (with a globe icon): The upminr program can be used to fetch Underminr log reports from the Partner Exchange service. Created 1 month ago. 0 stars.

The URL <https://partner.underminr.ai> is displayed below the Upminr project description.



Defense Status

- Microsoft ZT DNS - vulnerable
- DiscrimiNAT - not vulnerable
- pDNS-only sites - vulnerable



MANAGE NETWORK

- Policies
- Devices
- Router
- Advanced

MANAGE RULES

- My Rules
- Subscriptions
- Unblock Requests ²
- Reflex

REPORTS

- Domains
- Events

ADMINISTRATION

- Manage Users
- Billing Settings

SUPPORT

- Support

Protection Level 3 | Zero Trust con...
Allow Policy: Only allow approved sites. Block every...

Enablers

Rules

Settings

Reflex: Reflex Protective

DNS Resolver: DNS Harmony3
Only sites allowed through Quad9, CleanBrowsing Security Filter, 1.1.1.

Allow block requests

Resource Record Type Filter

Blocked Types
TXT x NULL x

Add type...

Custom values must be a number

Underminr Prevention
Prevent bypass attempts. Requires version 4.15.2-312.

Quarantine Policy
Event-driven Device Quarantine

The policy to apply when an Underminr is detected.



Underminr Prevention

Prevent bypass attempts. Requires version 4.15.2-312.

Quarantine Policy

Event-driven Device Quarantine

The policy to apply when an Underminr is detected.



Contributions

infoblox  quad9

SOPHOS  Microsoft



