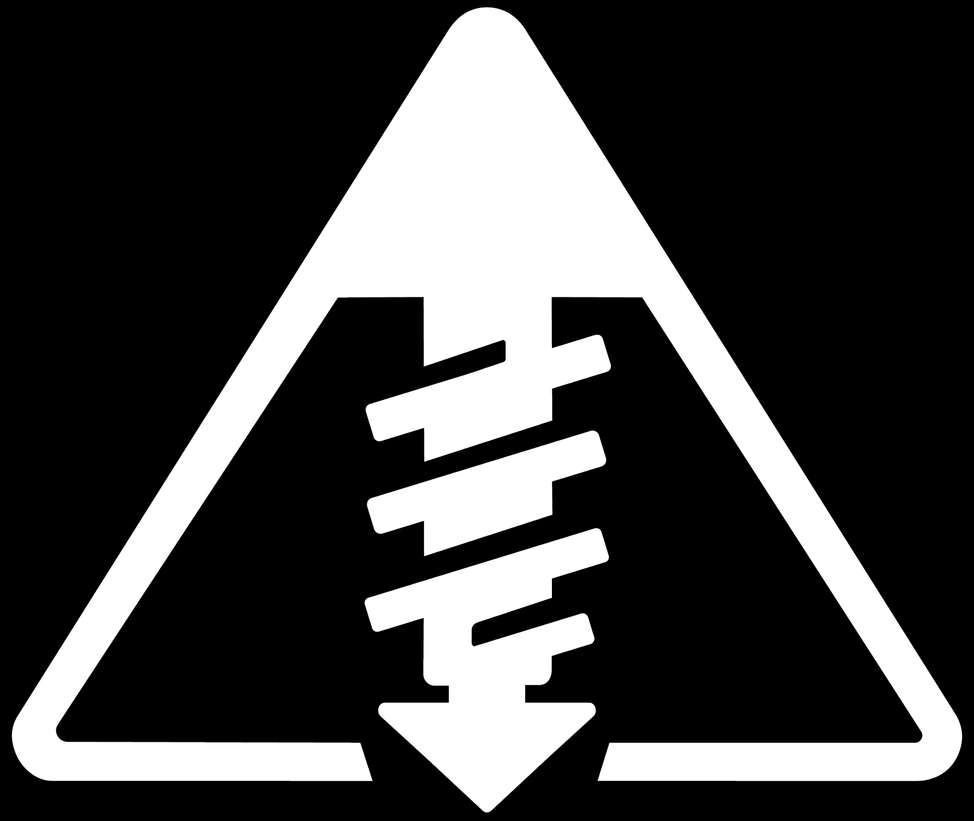


The Underminr

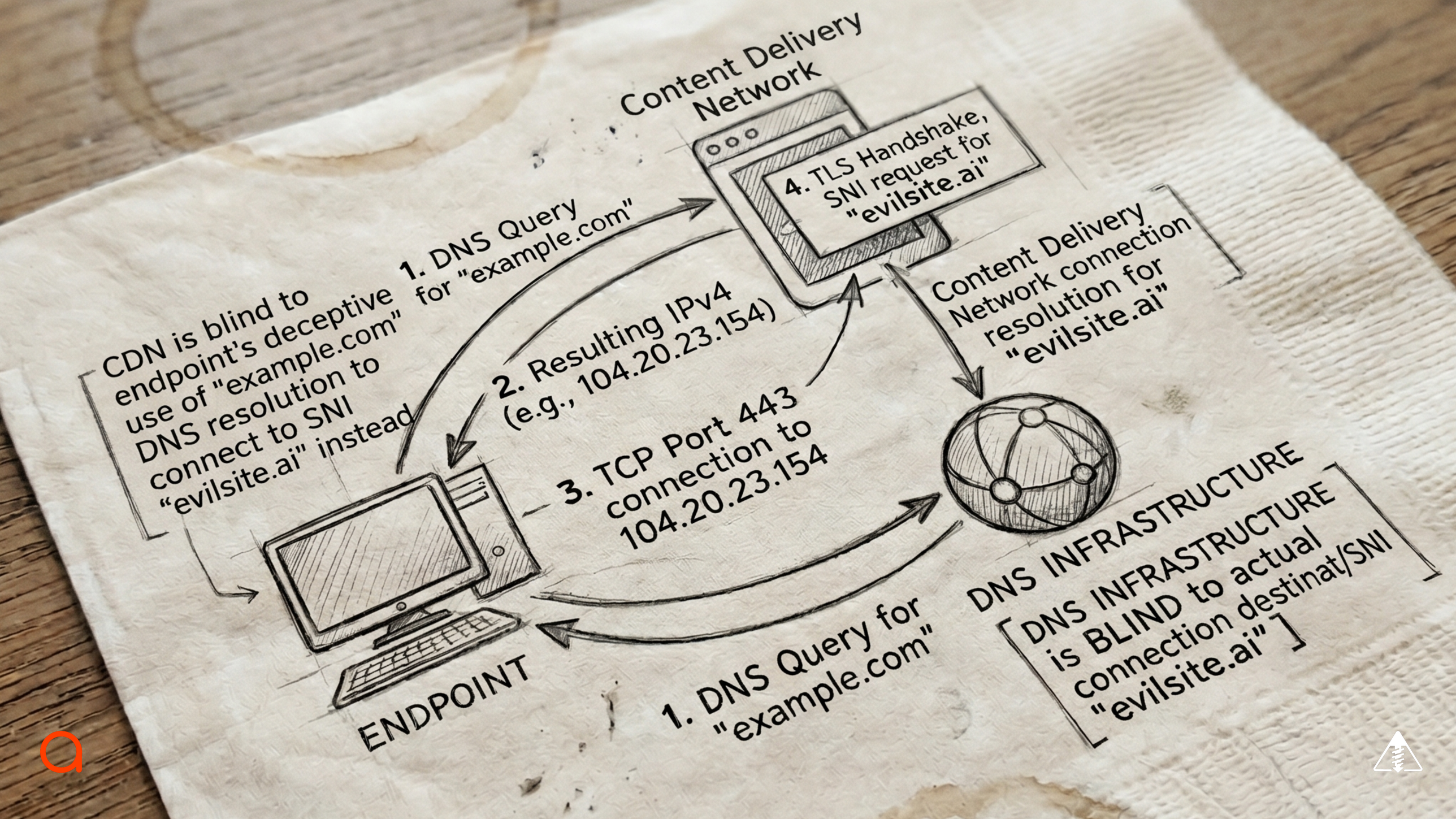
Abusing CDN Shared Infrastructure

David Redekop | ADAMnetworks

DNS-OARC 46 | 2026-05-16

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.

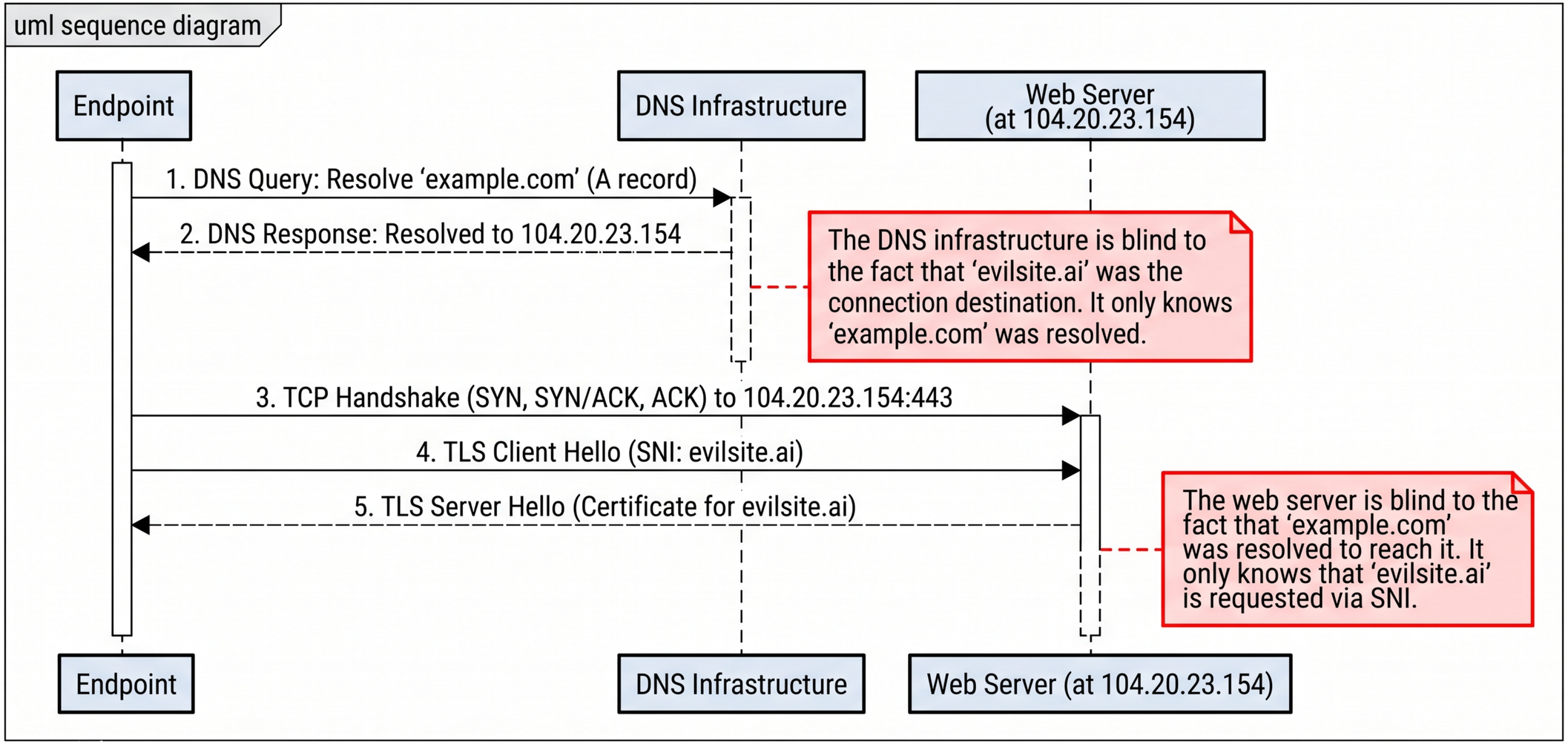

Content Delivery Network
4. TLS Handshake, SNI request for "evilsite.ai"
1. DNS Query for "example.com"
2. Resulting IPv4 (e.g., 104.20.23.154)
3. TCP Port 443 connection to 104.20.23.154
CDN is blind to endpoint's deceptive use of "example.com" DNS resolution to connect to SNI "evilsite.ai" instead
Content Delivery Network connection resolution for "evilsite.ai"
ENDPOINT
1. DNS Query for "example.com"
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

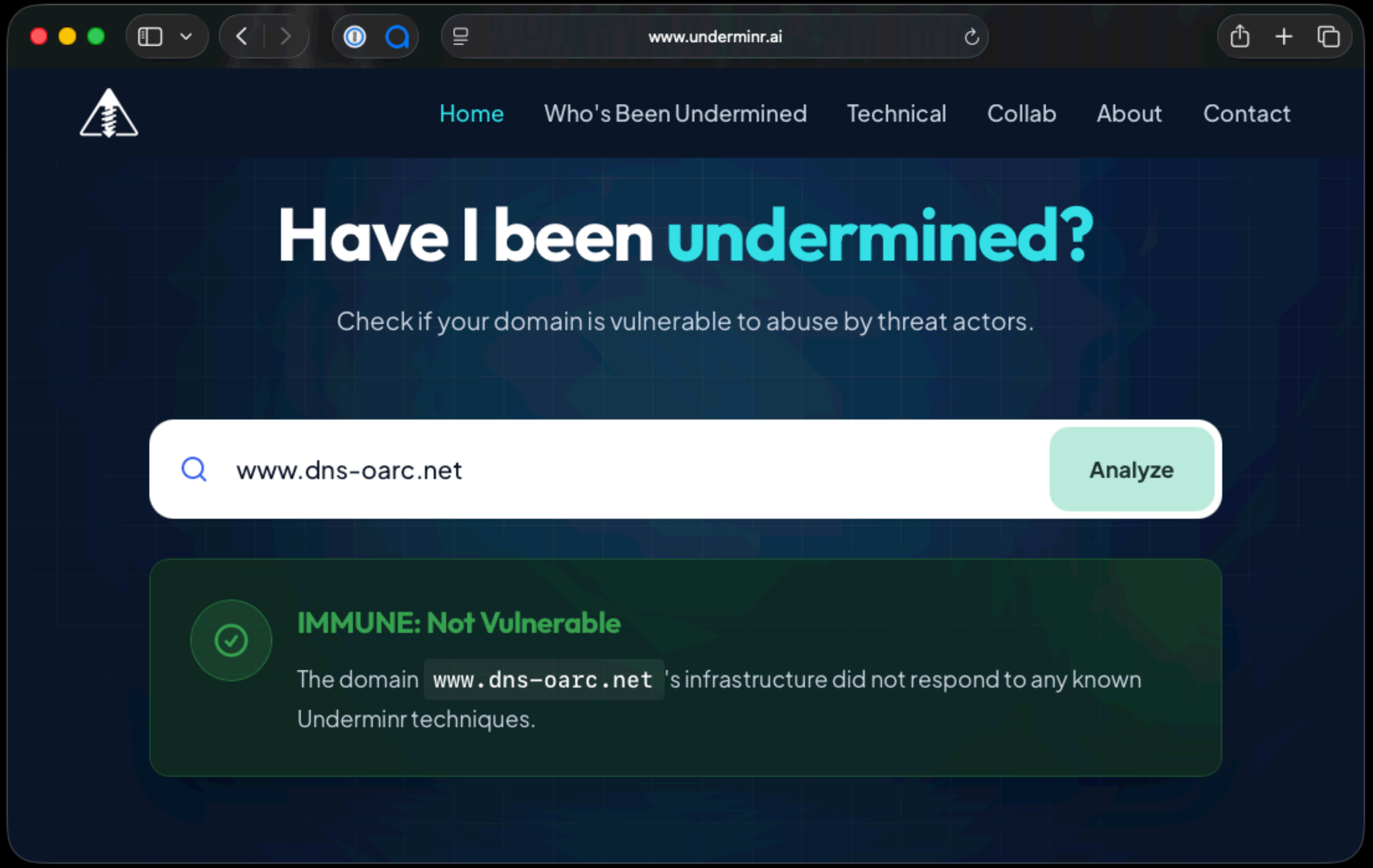
UML SEQUENCE DIAGRAM: NETWORK FLOW AND VISIBILITY

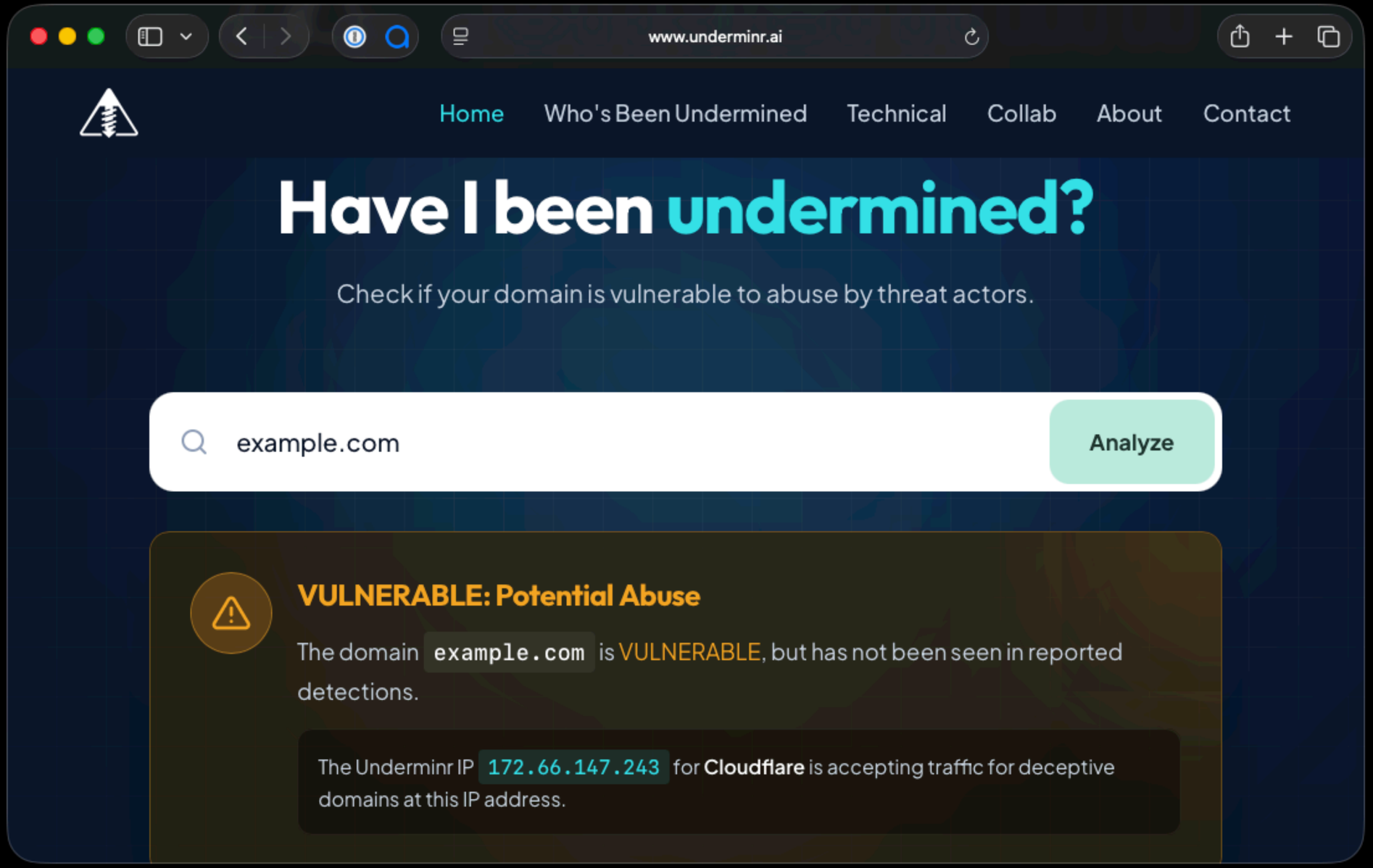


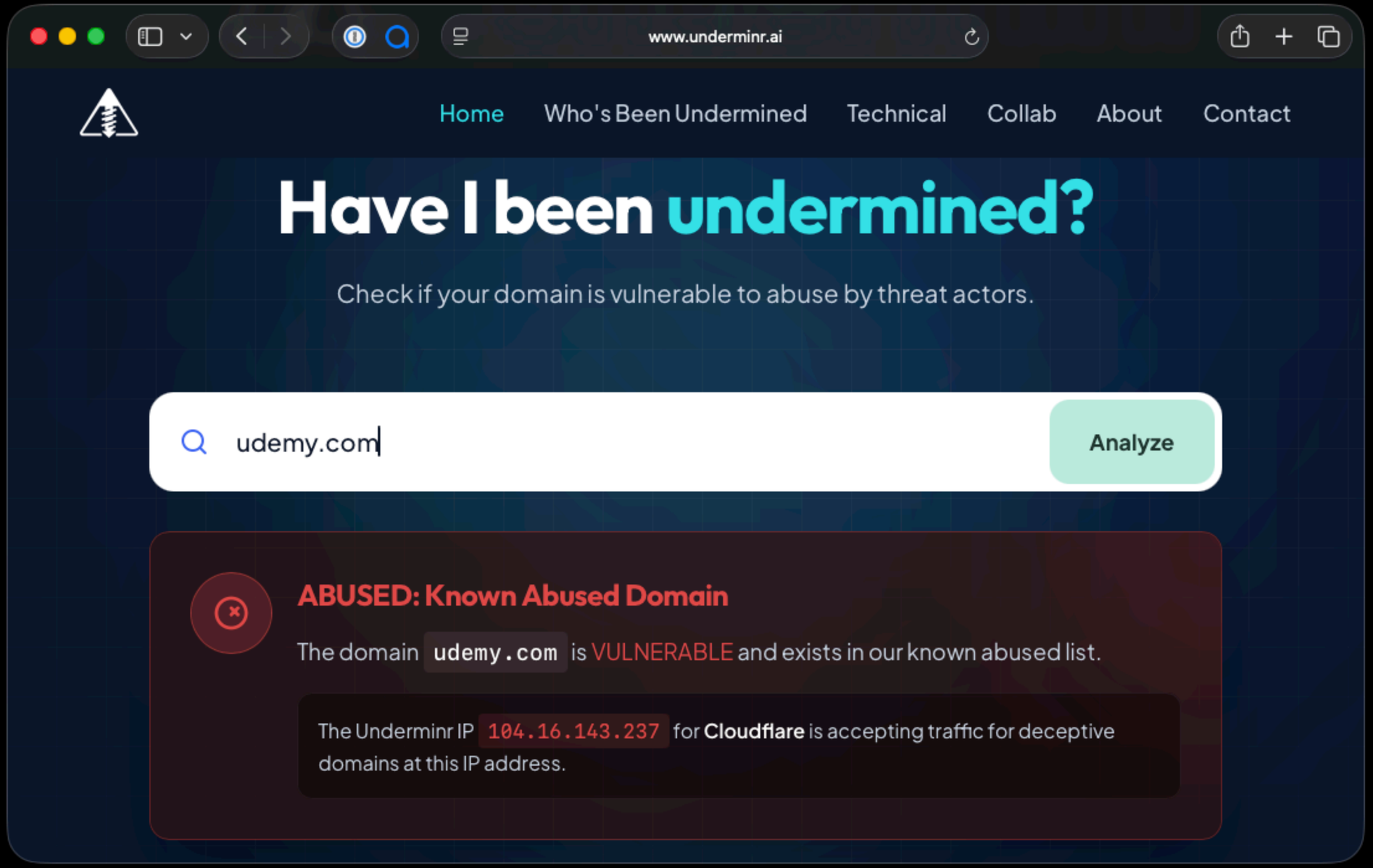
Comparing to Domain Fronting

- 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?

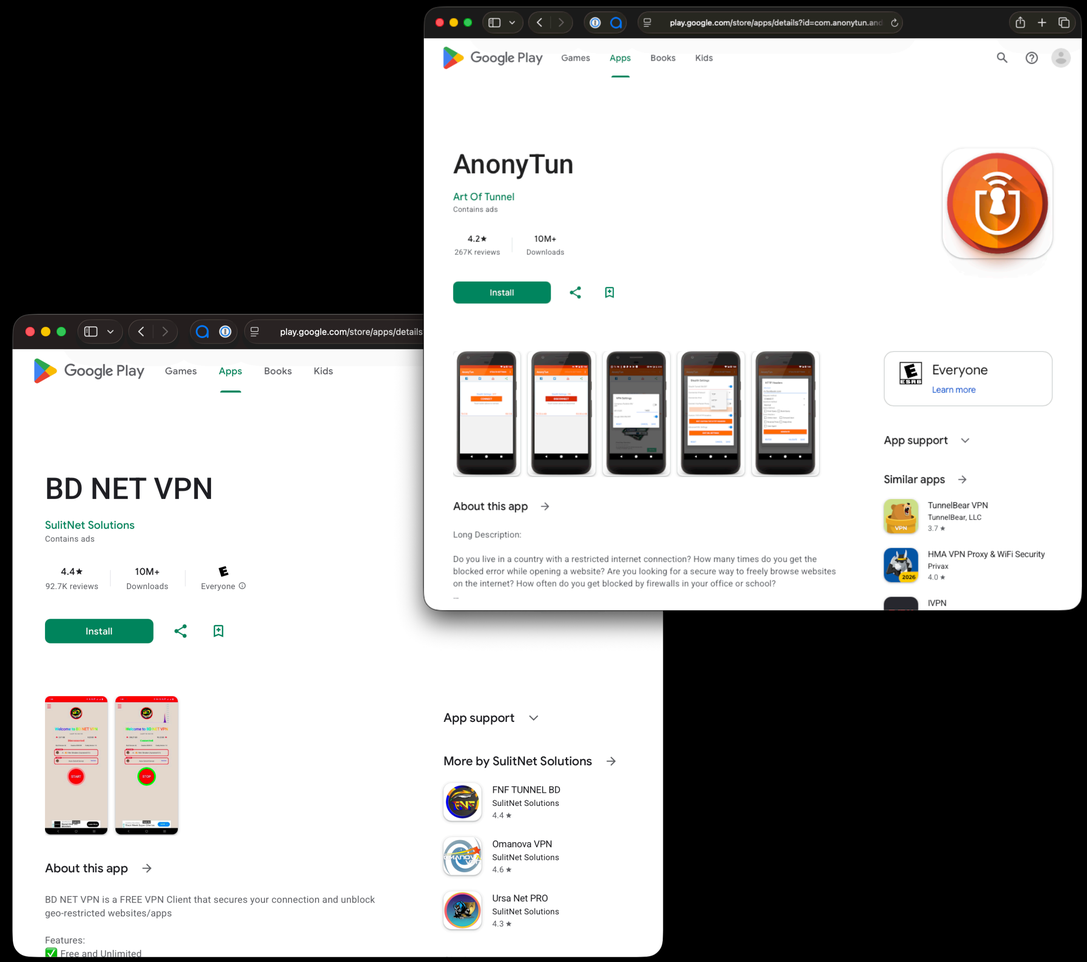

www.underminr.ai
Home
Who's Been Undermined
Technical
Collab
About
Contact
Have I been undermined?
Check if your domain is vulnerable to abuse by threat actors.
www.dns-oarc.net
Analyze
IMMUNE: Not Vulnerable
The domain www.dns-oarc.net 's infrastructure did not respond to any known Underminr techniques.


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)

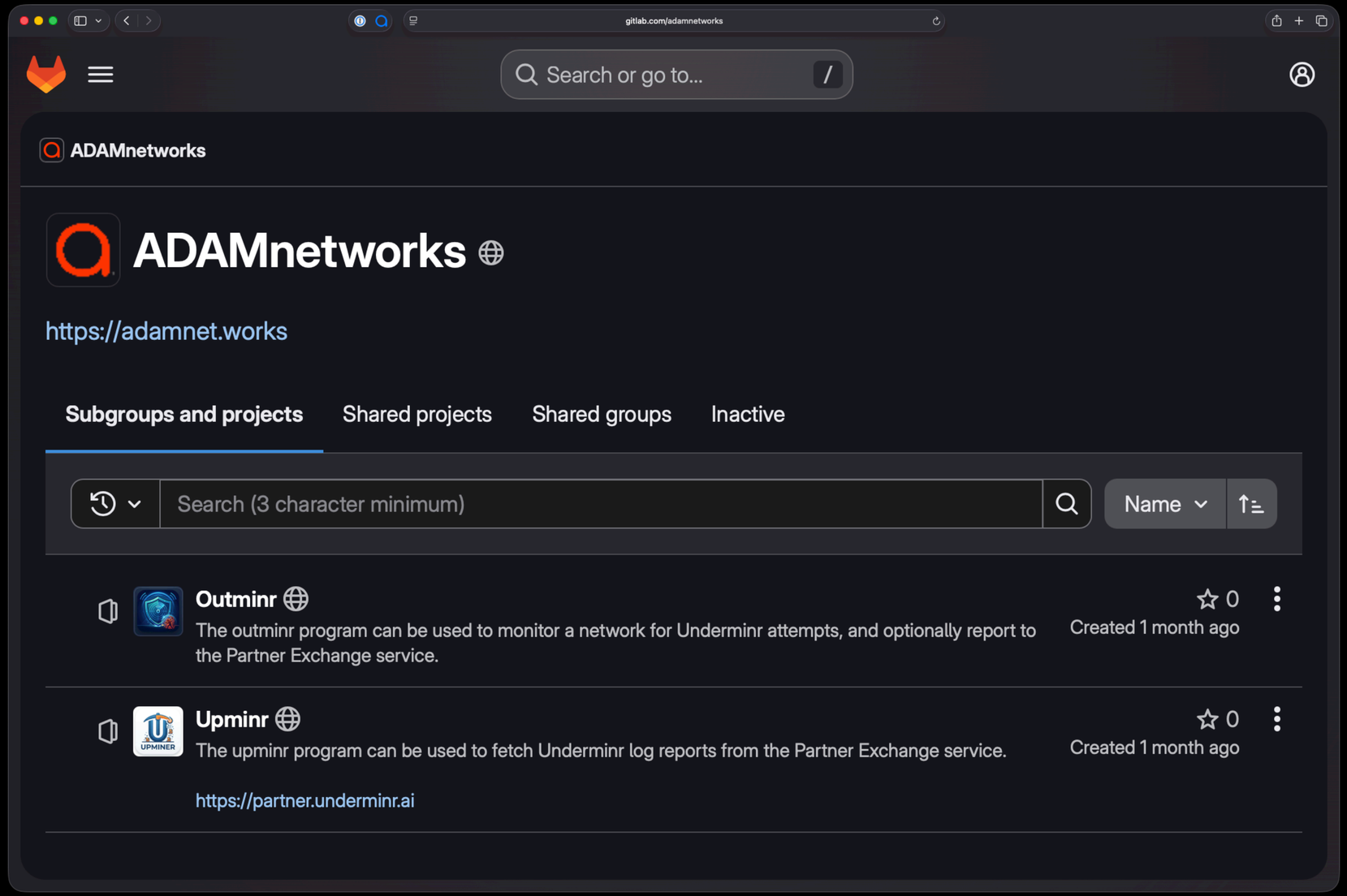


Calling on all defenders...

Effective Mitigation

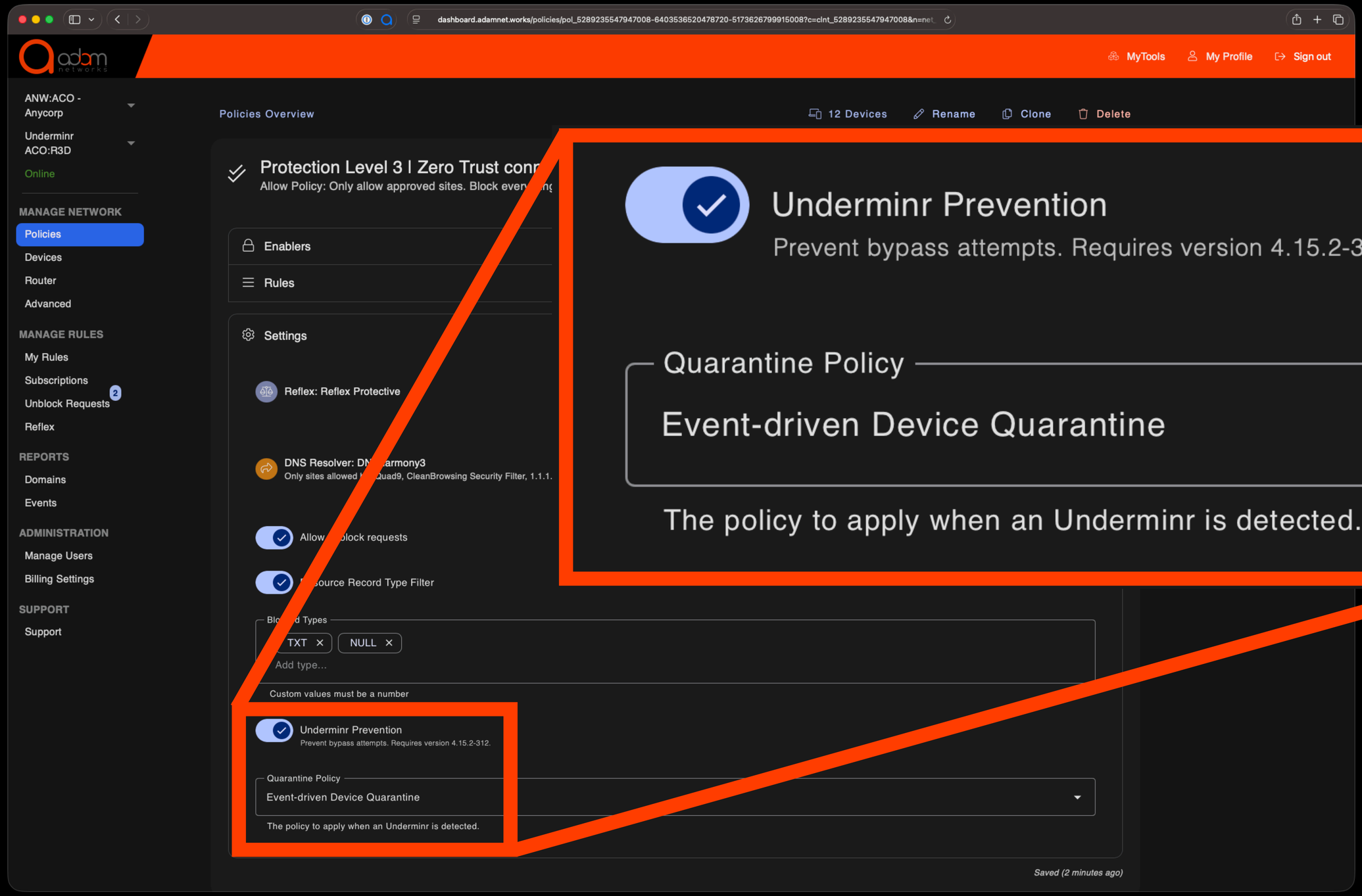
- DNS at root of network trust, hijack/block/log unauthorized Do53
- Don’t Talk To Strangers (DTTS) | Zero Trust DNS
- pDNS check on SNI domain
- Strip ECH in responses

Free tools from gitlab.com/ADAMnetworks



Defense Status

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


MyTools
My Profile
Sign out
ANW:ACO - Anycorp
Underminr ACO:R3D
Online
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
Policies Overview
12 Devices
Rename
Clone
Delete
Protection Level 3 | Zero Trust conn
Allow Policy: Only allow approved sites. Block even
Enablers
Rules
Settings
Reflex: Reflex Protective
DNS Resolver: DN armony3
Only sites allowed Quad9, CleanBrowsing Security Filter, 1.1.1.
Allow block requests
source Record Type Filter
Bl d Types
TXT
NULL
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.
Saved (2 minutes ago)
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