



Sauteed Onions

Transparent Associations from Domain Names to Onion Addresses

joint work:

- Rasmus Dahlberg, Karlstad University
- Linus Nordberg, Verkligen Data AB
- Matthew Finkel, Independent

Paul Syverson
Center for High Assurance Computer Systems
(CHACS)
U.S. Naval Research Laboratory
Washington DC

ACM Workshop on Privacy in the
Electronic Society (WPES '22)
Los Angeles and Cyberspace
November 7 02022



Onion Addresses

Tor Project | Anonymity Online



2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion/index.html



[Donate Now](#)

[About](#)

[Support](#)

[Community](#)

[Blog](#)

[Donate](#)

English (en) ▾

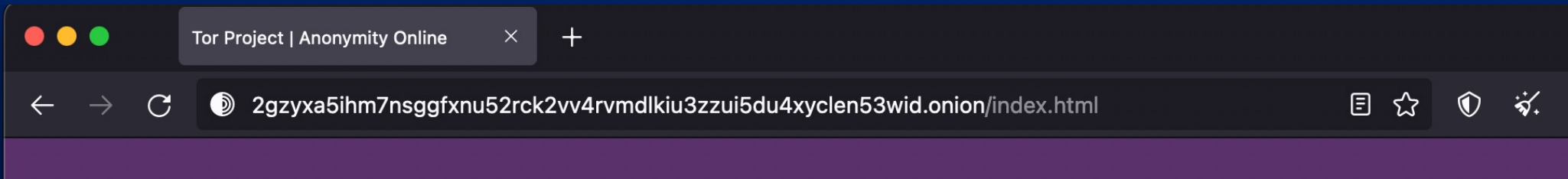
[Download Tor Browser](#) ↓

Browse Privately. Explore Freely.

Defend yourself against tracking and surveillance. Circumvent censorship.



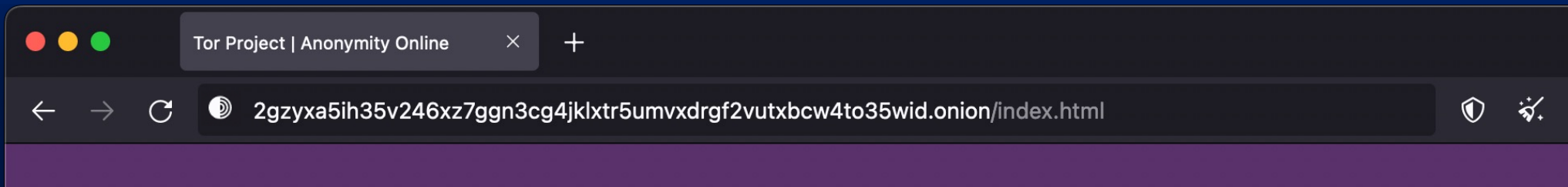
Onion Addresses



- Self-Authenticating: Address encodes ed25519 public key



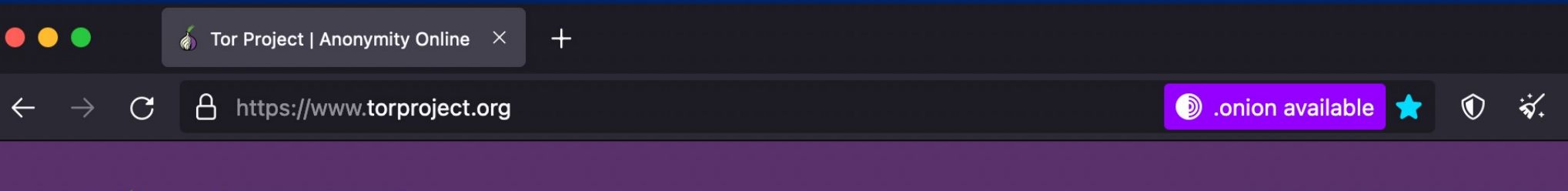
Onion Addresses



- Self-Authenticating: Address encodes ed25519 public key
- Random looking string
 - Hard to discover or recognize
 - Easy to set up doppelganger address for which adversary has key



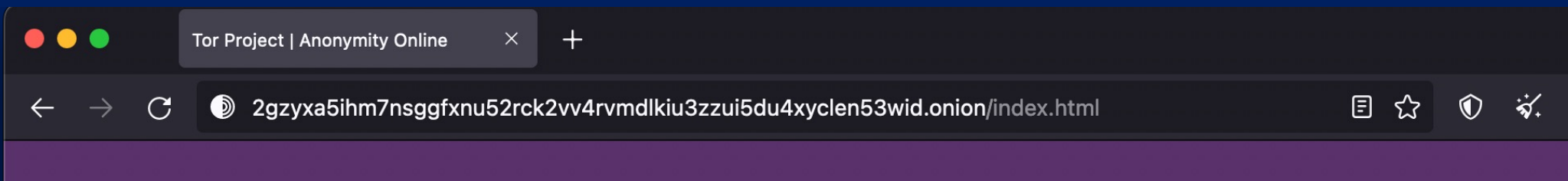
Onion Location



- Self-Authenticating: Address encodes ed25519 public key
- Random looking string
 - Hard to discover or recognize
 - Easy to set up doppelganger address for which adversary has key



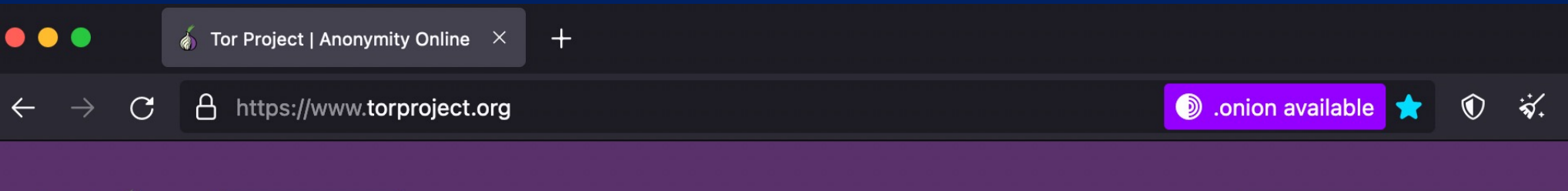
Onion Location



- Self-Authenticating: Address encodes ed25519 public key
- Random looking string
 - Hard to discover or recognize
 - Easy to set up doppelganger address for which adversary has key



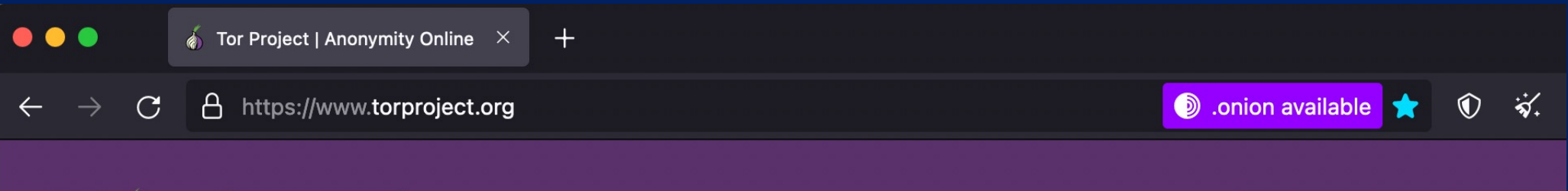
Onion Location makes hijack and other attacks easier



- Self-Authenticating: Address encodes ed25519 public key
- Random looking string
 - Hard to discover or recognize
 - Easy to set up doppelganger address for which adversary has key
 1. Certificate hijack of torproject.org
 2. Set up Onion Location for doppelganger address



Onion Location



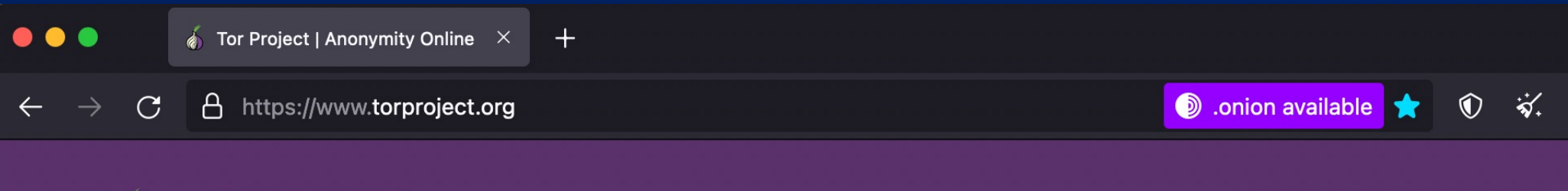
- Hijack and other attacks
 - See our WPES'21 paper "Attack on Onion Discovery and Remedies via Self-Authenticating Traditional Addresses"

Sauteed Onions (this WPES'22 paper)

- Resist Censorship (unlike current Onion Location)



Onion Location



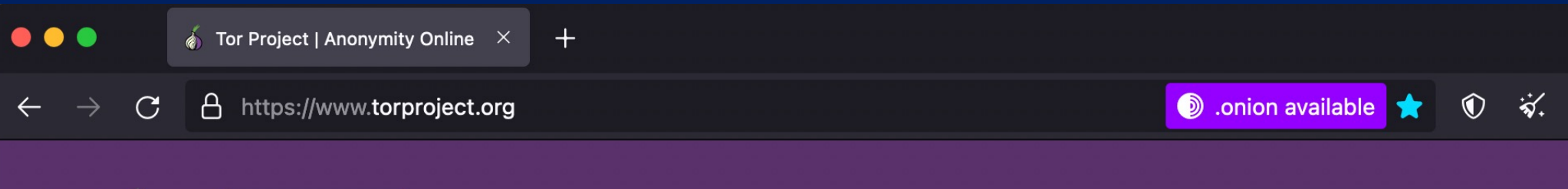
- Hijack and other attacks
 - See our WPES'21 paper "Attack on Onion Discovery and Remedies via Self-Authenticating Traditional Addresses"

Sauteed Onions (this WPES'22 paper)

- Resist Censorship
- Make Onion Association Transparent



Onion Location



- Hijack and other attacks
 - See our WPES'21 paper "Attack on Onion Discovery and Remedies via Self-Authenticating Traditional Addresses"

Sauteed Onions (this WPES'22 paper)

- Resist Censorship
- Make Onion Association Transparent





Sauteed Onions

sauteed-onions.org/

× +

← → ↻ 🔒 https://www.sauteed-onions.org

.onion available

☆

🛡️

🔧

☰

Sauteed Onions

Paper / FAQ / About

Sauteed onions associate registered domain names with onion addresses. These associations are established in TLS certificates, making them publicly enumerable in append-only CT logs.

One of the most prominent use-cases of sauteed onions is to help users defeat censorship of TLS sites: onion sites can be used *if they are discoverable*, which is what sauteed onions help with. This tightens the relation between registered domain names, HTTPS, and onion sites.

Search for onion addresses

You can use any existing certificate search service to check if a registered domain name has an associated onion address. What we will be looking for is a domain name on the form:

<onion addr>onion.www.example.com

Let's give it a go using [crt.sh](#).

What is the onion address of `www.sauteed-onions.org`?

crt.sh | Certificate Search × +

← → ↻ 🔒 https://crt.sh

☆

🛡️

🔧

☰

crt.sh

Certificate Search

Enter an Identity (Domain Name, Organization Name, etc),
a Certificate Fingerprint (SHA-1 or SHA-256) or a crt.sh ID:

www.sauteed-onions.org



Sauteed Onions

A screenshot of a web browser displaying the Mullvad VPN website. The browser's address bar shows 'https://mullvad.net/en/'. The website has a dark blue background. On the left, the text 'You have a right to privacy' is prominently displayed in white. Below it, a paragraph states: 'In a society increasingly determined to erode that right, a fast, trustworthy and easy-to-use VPN is a good first step toward reclaiming it.' There are two buttons: 'What is a VPN?' in a white box and 'Why Mullvad VPN?' in a yellow box. On the right side, there's a green header for 'MULLVAD VPN' with a gear icon. Below this is a map of Europe with a green circle highlighting Sweden. Text on the map says 'SECURE CONNECTION', 'Gothenburg Sweden', and 'se10-wireguard'. At the bottom of the map area are two buttons: 'Switch location' in a grey box and 'Disconnect' in a red box with a refresh icon.



Sauteed Onions

Mullvad VPN - Privacy is a unive X

← → ↻ 🔒 https://mullvad.net/en/

You have a

In a society increasingly determined
fast, trustworthy and easy-to-use V

Why I

Mullvad VPN - Privacy is a unive X

Certificate for mullvad.net

Tor Browser

about:certificate?cert=MIIF5TCCBM2gAwIBAgISAzCrKlcSmrskZV9WCzKx%2FwZdMA0GCSqG

Subject Name	
Common Name	mullvad.net
Issuer Name	
Country	US
Organization	Let's Encrypt
Common Name	R3
Validity	
Not Before	Wed, 02 Nov 2022 07:36:02 GMT
Not After	Tue, 31 Jan 2023 07:36:01 GMT
Subject Alt Names	
DNS Name	mullvad.net
DNS Name	o54hon2e2vj6c7m3aqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.mullvad.net
DNS Name	o54hon2e2vj6c7m3aqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.www.mullvad.net
DNS Name	se-mma-www-101.mullvad.net
DNS Name	www.mullvad.net



Sauteed Onions

Subject Alt Names

DNS Name	mullvad.net
DNS Name	o54hon2e2vj6c7m3aqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.mullvad.net
DNS Name	o54hon2e2vj6c7m3aqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.www.mullvad.net
DNS Name	se-mma-www-101.mullvad.net
DNS Name	www.mullvad.net

- Onion Location via Sauteed Onions
 1. Web Extension checks TLS Cert for domain with onion address as subdomain
 2. Redirects to onion address if this is detected
- Performance advantage
 - Header-based Onion Location loads entire page before redirect
 - Cert-based Onion Location redirects after TLS handshake



Sauteed Onions support Transparent Onion Association

Subject Alt Names

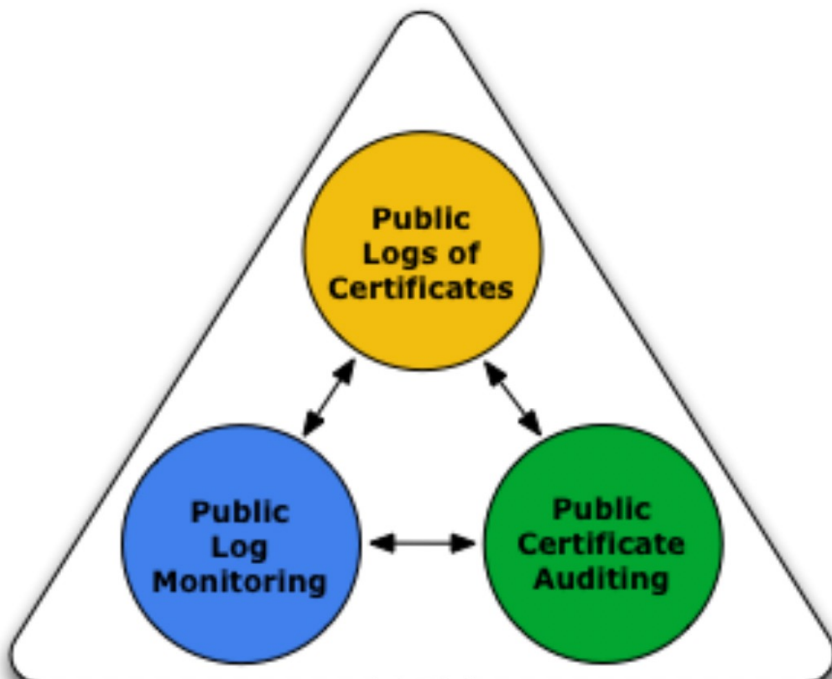
DNS Name	mullvad.net
DNS Name	o54hon2e2vj6c7m3aqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.mullvad.net
DNS Name	o54hon2e2vj6c7m3aqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.www.mullvad.net
DNS Name	se-mma-www-101.mullvad.net
DNS Name	www.mullvad.net

Registered domain and onion address associated in TLS cert
→ Onion association in Certificate Transparency (CT) logs

GlobalSign Blog & News

☐ If you haven't already, please check here to receive email communications about GlobalSign products. You can always update your communication preferences in our [Preference Center](#), and check our [Privacy Policy](#) to see how we handle your data.

☐ I'm not a robot





Sauteed Onions support Transparent Onion Association

Subject Alt Names

DNS Name	mullvad.net
DNS Name	o54hon2e2vj6c7m3aqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.mullvad.net
DNS Name	o54hon2e2vj6c7m3aqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.www.mullvad.net
DNS Name	se-mma-www-101.mullvad.net
DNS Name	www.mullvad.net

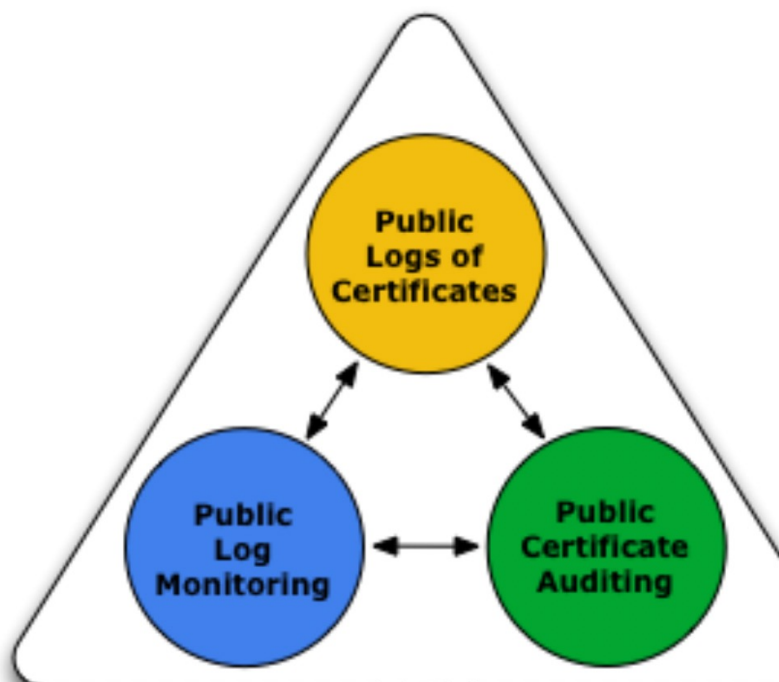
Registered domain and onion address associated in TLS cert
→ Onion association in Certificate Transparency (CT) logs

https://certificate.transparency.dev 67%

Certificate Transparency

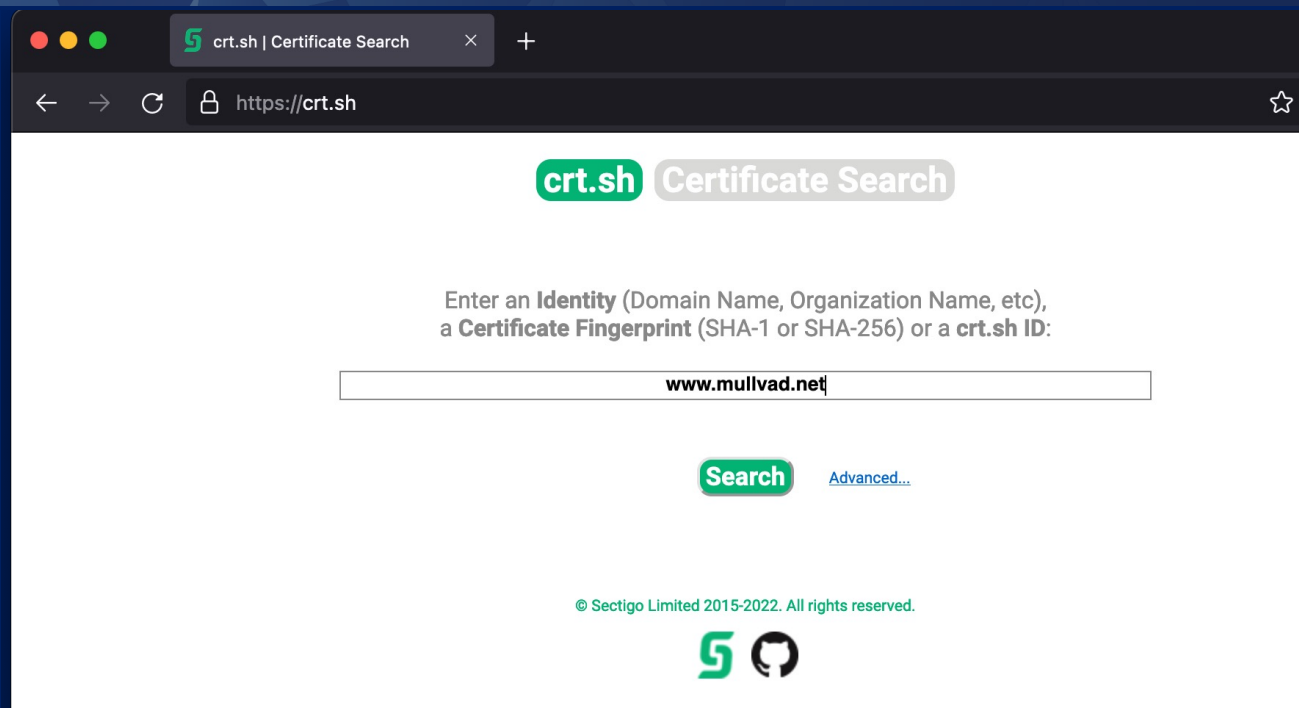
How CT works Actors ▾ Our story GitHub

Working together to detect maliciously or mistakenly issued certificates.





Sauteed Onions support Transparent Onion Association



- publicly usable CT log monitor run by the CA Sectigo



Sauteed Onions support Transparent Onion Association

5 crt.sh | Certificate Search

← → ↺ 🔒 https://crt.sh

Enter an Identity or a Certificate

5 crt.sh | www.mullvad.net

New Tab

← → ↺ 🔒 https://crt.sh/?q=www.mullvad.net

crt.sh Identity Search

Group by Issuer

Criteria Type: Identity Match: ILIKE Search: 'www.mullvad.net'

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities
7885744884	2022-11-02	2022-11-02	2023-01-31	mullvad.net	o54hon2e2vj6c7m3aqqqu6uyece65by3vgoxhqlqsvkmacw6a7m7kiadonion.www.mullvad.net www.mullvad.net
7885736127	2022-11-02	2022-11-02	2023-01-31	mullvad.net	o54hon2e2vj6c7m3aqqqu6uyece65by3vgoxhqlqsvkmacw6a7m7kiadonion.www.mullvad.net www.mullvad.net
7872127660	2022-10-31	2022-10-31	2023-01-29	mullvad.net	o54hon2e2vj6c7m3aqqqu6uyece65by3vgoxhqlqsvkmacw6a7m7kiadonion.www.mullvad.net www.mullvad.net
7872121985	2022-10-31	2022-10-31	2023-01-29	mullvad.net	o54hon2e2vj6c7m3aqqqu6uyece65by3vgoxhqlqsvkmacw6a7m7kiadonion.www.mullvad.net www.mullvad.net
7477887193	2022-09-05	2022-09-05	2022-12-04	mullvad.net	www.mullvad.net
7477876036	2022-09-05	2022-09-05	2022-12-04	mullvad.net	www.mullvad.net
7061866064	2022-07-04	2022-07-04	2022-10-02	mullvad.net	www.mullvad.net
7057856292	2022-07-04	2022-07-04	2022-10-02	mullvad.net	www.mullvad.net
6653661381	2022-05-02	2022-05-02	2022-07-31	mullvad.net	www.mullvad.net
6648851289	2022-05-02	2022-05-02	2022-07-31	mullvad.net	www.mullvad.net
6275457950	2022-03-03	2022-03-03	2022-06-01	mullvad.net	www.mullvad.net
6275459319	2022-03-03	2022-03-03	2022-06-01	mullvad.net	www.mullvad.net
5909385114	2022-01-03	2022-01-03	2022-04-03	mullvad.net	www.mullvad.net
5909386124	2022-01-03	2022-01-03	2022-04-03	mullvad.net	www.mullvad.net
5534656322	2021-11-03	2021-11-03	2022-02-01	mullvad.net	www.mullvad.net
5534650428	2021-11-03	2021-11-03	2022-02-01	mullvad.net	www.mullvad.net
5349823917	2021-10-04	2021-10-04	2022-01-02	mullvad.net	www.mullvad.net
5343640550	2021-10-04	2021-10-04	2022-01-02	mullvad.net	www.mullvad.net
4971263923	2021-08-02	2021-08-02	2021-10-31	mullvad.net	www.mullvad.net
4971260233	2021-08-02	2021-08-02	2021-10-31	mullvad.net	www.mullvad.net
4625733052	2021-06-01	2021-06-01	2021-08-30	mullvad.net	www.mullvad.net
4625737948	2021-06-01	2021-06-01	2021-08-30	mullvad.net	www.mullvad.net
4582367544	2021-05-24	2021-05-24	2021-08-22	mullvad.net	www.mullvad.net
4582362346	2021-05-24	2021-05-24	2021-08-22	mullvad.net	www.mullvad.net
4271715483	2021-03-25	2021-03-25	2021-06-23	mullvad.net	www.mullvad.net
4271715709	2021-03-25	2021-03-25	2021-06-23	mullvad.net	www.mullvad.net
3979725773	2021-01-25	2021-01-25	2021-04-25	mullvad.net	www.mullvad.net
3979726130	2021-01-25	2021-01-25	2021-04-25	mullvad.net	www.mullvad.net
3881286446	2021-01-05	2021-01-05	2021-04-05	mullvad.net	www.mullvad.net
3881283035	2021-01-05	2021-01-05	2021-04-05	mullvad.net	www.mullvad.net



Sauteed Onions support Transparent Onion Association

The screenshot shows a web browser window with the URL `https://crt.sh/?q=www.mullvad.net`. The page displays the 'crt.sh Identity Search' interface. A search bar contains the text 'www.mullvad.net'. Below the search bar, a table lists search results. The table has columns for 'crt.sh ID', 'Logged At', 'Not Before', 'Not After', 'Common Name', and 'Matching Identities'. The results show multiple certificates issued by 'mullvad.net' with various 'Matching Identities' listed.

Criteria	Type: Identity	Match: ILIKE	Search: 'www.mullvad.net'		
crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities
7885744884	2022-11-02	2022-11-02	2023-01-31	mullvad.net	o54hon2e2vj6c7m3aqqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.www.mullvad.net www.mullvad.net
7885736127	2022-11-02	2022-11-02	2023-01-31	mullvad.net	o54hon2e2vj6c7m3aqqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.www.mullvad.net www.mullvad.net
7872127660	2022-10-31	2022-10-31	2023-01-29	mullvad.net	o54hon2e2vj6c7m3aqqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.www.mullvad.net www.mullvad.net
7872121985	2022-10-31	2022-10-31	2023-01-29	mullvad.net	o54hon2e2vj6c7m3aqqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.www.mullvad.net www.mullvad.net
7477887193	2022-09-05	2022-09-05	2022-12-04	mullvad.net	www.mullvad.net
7477876036	2022-09-05	2022-09-05	2022-12-04	mullvad.net	www.mullvad.net

- publicly usable CT log monitor run by the CA Sectigo
- Onion Association
 - Censorship resistant (unlike Onion Location)
- easily discoverable without touching original site (`www.mullvad.net`)
- Targeted-attack resistant (unlike Onion Location)
- users verifiably get the same onion association as everyone else
- Legit site owners can check for attacks on their site (unlike Onion Location)



What if crt.sh is blocked or hijacked?

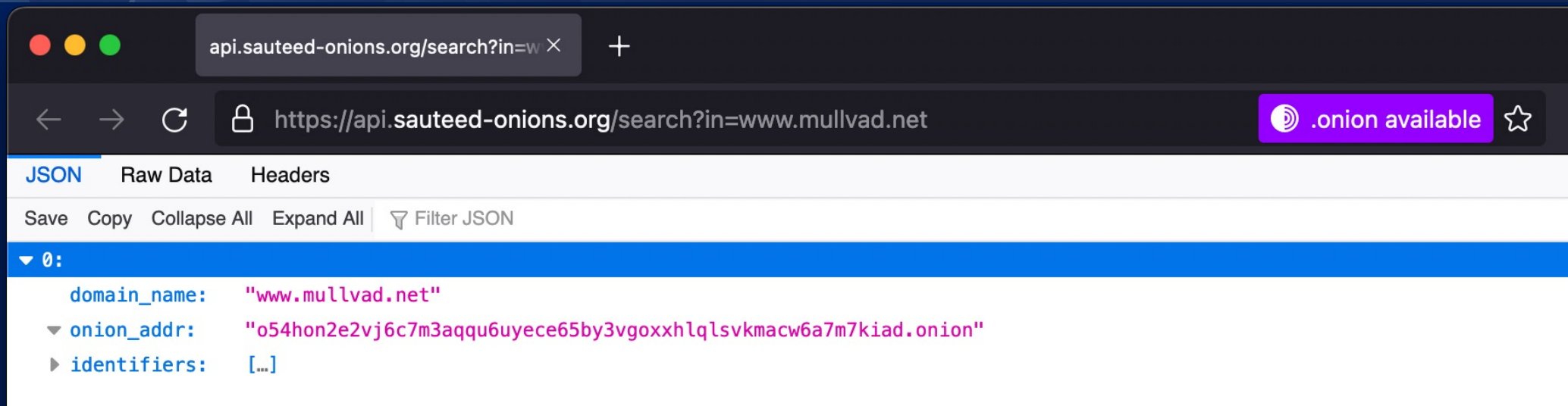
The screenshot shows the crt.sh Identity Search interface. The search criteria are set to 'Identity', 'Match: ILIKE', and 'Search: www.mullvad.net'. The results table lists certificates with their IDs, dates, and common names. The 'Matching Identities' column shows the full certificate path for each entry.

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities
7885744884	2022-11-02	2022-11-02	2023-01-31	mullvad.net	o54hon2e2vj6c7m3aqqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.www.mullvad.net www.mullvad.net
7885736127	2022-11-02	2022-11-02	2023-01-31	mullvad.net	o54hon2e2vj6c7m3aqqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.www.mullvad.net www.mullvad.net
7872127660	2022-10-31	2022-10-31	2023-01-29	mullvad.net	o54hon2e2vj6c7m3aqqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.www.mullvad.net www.mullvad.net
7872121985	2022-10-31	2022-10-31	2023-01-29	mullvad.net	o54hon2e2vj6c7m3aqqqu6uyece65by3vgoxhqlsvkmacw6a7m7kiadonion.www.mullvad.net www.mullvad.net
7477887193	2022-09-05	2022-09-05	2022-12-04	mullvad.net	www.mullvad.net
7477876036	2022-09-05	2022-09-05	2022-12-04	mullvad.net	www.mullvad.net

- publicly usable CT log monitor run by the CA Sectigo
- Onion Association
 - Censorship resistant (unlike Onion Location)
- easily discoverable without touching original site (www.mullvad.net)
- Targeted-attack resistant (unlike Onion Location)
- users verifiably get the same onion association as everyone else
- Legit site owners can check for attacks on their site (unlike Onion Location)



What if crt.sh is blocked or hijacked?

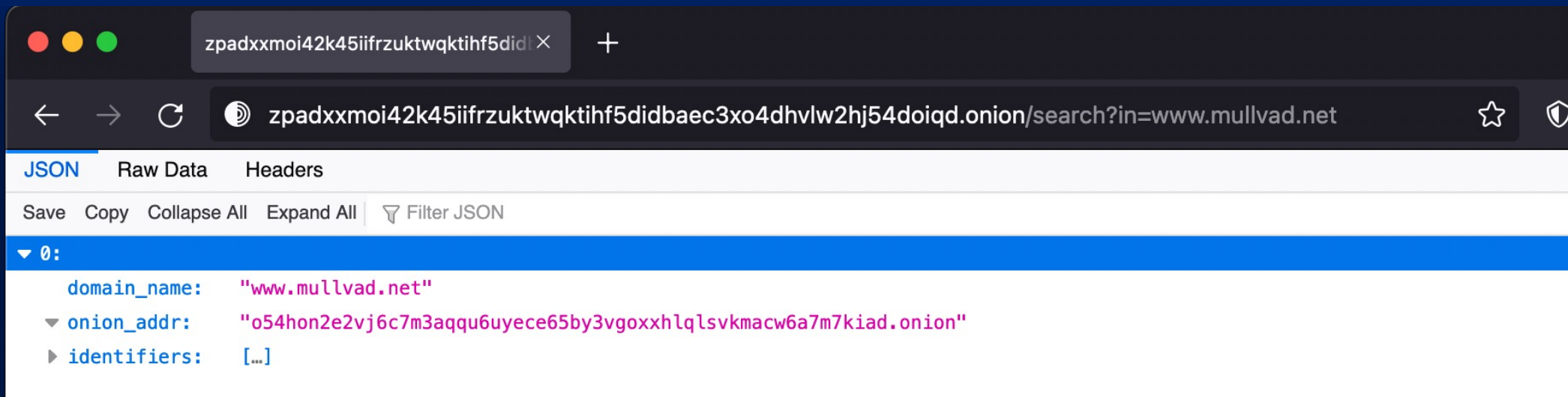


• REST API

- search on domain names for onion association
- additional info, e.g., specific cert, index of cert in specific CT log
- even if CT log gets blocked, onion assocs already in DB still available & validatable (also true of log data at crt.sh)



What if crt.sh is blocked or hijacked?



• REST API

- search on domain names for onion association
- additional info, e.g., specific cert, index of cert in specific CT log
- even if CT log gets blocked, onion assocs already in DB still available & validatable (also true of log data at crt.sh)
- available at onion address (resists being blocked or hijacked)
- source code available

<https://gitlab.torproject.org/tpo/onion-services/sauteed-onions>

<https://gitlab.torproject.org/rhatto/sauteed-week/-/blob/main/docs/api.md>



Summary/Future Work/Questions

- Onion Location (header-based) facilitates attacks and is blockable
- Curated lists/search engines for onion association not retroactively accountable
- Sauteed Onions (set up your own! See www.sauteed-onions.org)
 - transparent, consistent, accountable
 - REST API
 - available at onion address (resists blocking)
 - source available for inspection/independent implementation
 - WebExtension
 - redirects to onion address after TLS handshake
- Future Work:
 - auto load onion associations from REST API datasets for local association
 - like HTTPS Everywhere but with ruleset transparency/accountability
 - replace header-based Onion Location with sauteed Onion Location
 - replace subdomain-onion SAN with X.509 extension
 - build onion association info into onion services DHT