

The “.onion” Special-Use Domain Name

draft-appelbaum-dnsop-onion-tld

Presentation Draft v2.3.1

Outline

- What is a Tor “.onion” address?
- What are “Special Use” names? [RFC6761]
- Why are Tor “.onion” names “Special Use”?
- What is the impact if we do nothing, or delay?

What are
“.onion”
names?

.onion

- Tor Network, est. 2002, ~1m daily users
- “.onion” names label Tor hidden services (est. 2004)
 - [hash-of-public-key].onion
 - “.onion” names are resolved through Tor itself
 - ~30k “.onion” names, ~1% of Tor bandwidth*

* <https://metrics.torproject.org/>

Welcome to Facebook - Log ... x +

https://www.facebookcorewwi.onion

You are connected to **facebookcorewwi.onion** which is run by (unknown) Verified by: DigiCert Inc

The connection to this website is secure.

More Information...

Bitcoin Block Explorer - Bloc... x +

https://blockchainbdgpzk.onion

You are connected to **blockchainbdgpzk.onion** which is run by (unknown) Verified by: DigiCert Inc

The connection to this website is secure.

More Information...

Height	Transactions	Total Sent
348300	< 1 minute	4,808.45 B
348299	3 minutes	16,986.43 B
		17,236.38 B
		9,085.92 B
		6,291.32 B

SecureDrop | Protecting Jou... x +

https://y6xjgkgwj47us5ca.onion

You are connected to **y6xjgkgwj47us5ca.onion** which is run by (unknown) Verified by: DigiCert Inc

The connection to this website is secure.

More Information...

Enabling JavaScript to protect your anonymity: [Learn how to disable it](#), or ignore this warning to continue.

Submit documents for the first time

If this is your first time submitting documents to journalists, start here.

Submit Documents

Already submitted something

If you have already submitted documents in the past, log in to check for responses.

Check for a response

THE//INTERCEPT

What are
“special use”
names?

RFC 6761: Special Use Domain Names

- “if a domain name has **special properties** that **affect the way hardware and software implementations handle the name**, that **apply universally** ..., then **that domain name may be a candidate for** having the IETF declare it to be a **Special-Use Domain Name**”
- Seven categories of special handling that a name might require

“.test”

1. Users are free to use these test names **as they would any other domain names.** ...
2. Application software **SHOULD NOT recognize test names as special**, and SHOULD use test names as they would other domain names.
- ...
5. Authoritative DNS servers SHOULD recognize test names as special and **SHOULD, by default, generate immediate negative responses** for all such queries, unless explicitly configured by the administrator to give positive answers for test names.
6. DNS server operators SHOULD, if they are using test names, **configure their authoritative DNS servers to act as authoritative** for test names.
7. DNS Registries/Registrars **MUST NOT grant requests to register** test names in the normal way to any person or entity. ...

Why is
“.onion”
special use?

.onion = special use

- Substantial & growing **current use** as an pseudo-TLD
- Addresses are cryptographic and self-assigned
 - => **No central authorities** (nor delegated ones)
 - => Unreachable without “**special (software) properties**”
- Not meaningfully resolvable using DNS
 - => **DNS lookups should yield NXDOMAIN**
 - => **Users expect to receive NXDOMAIN**

RFC 6761 Criteria

Class	Special?	Difference
1. User	✓	Different security properties
2. Application	✓✓	Resolve and connect with Tor or fail
3. Libraries	✓	Resolve with Tor or fail
4. Caching Servers	✓	NXDOMAIN
5. Auth'ive Servers	✓	NXDOMAIN
6. Operators	✓	SHOULD NOT configure
7. Registries	✓	MUST NOT register

What if we do nothing or
delay registering “.onion”
as “special use”?

Denying “.onion” degrades applications and the DNS

- Prevents HTTPS for a large number of transactions
 - HTTPS => certificates => registration
- Continued and increasing leakage of potentially private information to the DNS
- Continued and increasing load of bogus queries on DNS resolvers

Growth in ".onion"

- Increasing use of ".onion" for many protocols:
 - "Tor" & "Tor Browser Bundle" - Desktop
"Orbot" & "Orweb" for Android; also iOS, etc...
 - "Mailpile" MUA => SMTP-over-Onion ("SMTorP")
 - "Ricochet" / "invisible.im" => IM-over-Onion
 - Plus: Any TCP service which can use SOCKS
- **Need to fully enable Tor as a secure transport**

Tor needs HTTPS

- HTTPS is more than encryption and authentication
 - Mixed content blocking, secure cookies, etc.
- .onion with HTTP is **vulnerable**
 - Get **some** of the COMSEC through Tor
 - But **none** of the other HTTPS protections

HTTPS needs Certs

- Handful of “.onion” certificates issued through “local names” exception in CA/BF rules
 - Facebook: `https://www.facebookcorewwi.onion/`
 - Blockchain.info: `https://blockchainbdgppzk.onion/`
 - The Intercept: `https://y6xjgkgwj47us5ca.onion/`
- This is not sustainable

October 1st 2015

- **All existing SSL“.onion” certificates MUST be revoked on October 1st 2015 (end of “local name” loophole)**
- CA/B Forum has approved a process for issuing EV certs for “.onion” if (and only if) “.onion” becomes an acknowledged **“public space”** (Ballot 144)
- If “.onion” is not registered by Oct 1st then **all existing SSL .onion sites will be knocked offline**
- Would **shut-down growth in secure communication**
 - cf. RFC7258 “Pervasive Monitoring Is an Attack”

Summary

- “.onion” names are **special**
- ... in **exactly** the sense of RFC 6761
- ... and there are **bad consequences for inaction**
- So let's adopt **draft-appelbaum-dnsop-onion-tld**

Contacts

- **Authors**

- Jake Appelbaum, Tor Project
@ioerror / jacob@appelbaum.net
- Alec Muffett, Facebook
@alecmuffett / alecm@fb.com

- **Points of Contact at IETF 92**

- Richard Barnes
@rlbarnes / rlb@ipv.sx
- Mark Nottingham
@mnot / mnot@mnot.net

APPENDIX

How .onion addresses are made

- Thumbnail sketch:
 - Generate a RSA key pair
Take the public key and hash it
Take the hash and truncate it to a sane length (cur: 80 bits)
Render the hash as a (cur: base-32) ASCII string
Append “.onion”
- Thus: onion addresses are algorithmically-produced bit strings
 - There is no zonefile or registry involved in their use
 - Their existence and reachability is announced to Tor in a dynamic fashion (cf: ARP Announce) and validated cryptographically
 - Some onion addresses are ephemeral, some are long-lived