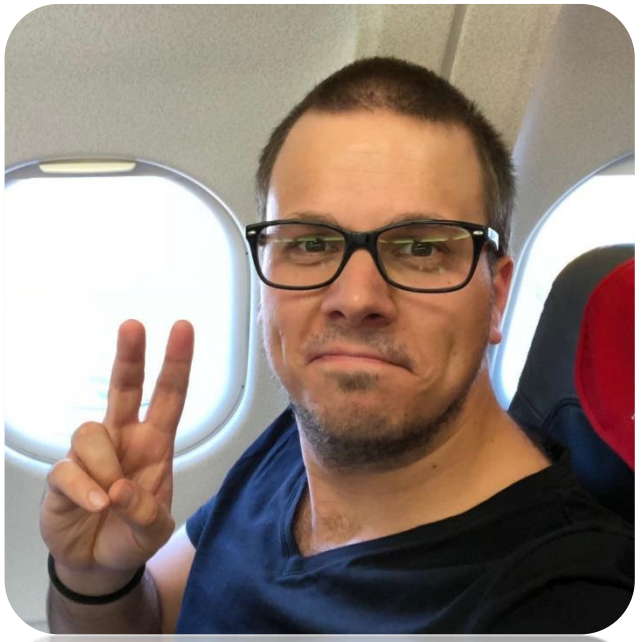
Certificate Transparency Accidental Disclosure

Johannes Weber

Vorstellung

Johannes Weber



- Master IT-Sicherheit
- Berater für Netzwerksicherheit
  - Firewall, Mail, Routing/Switching
  - VPN/Crypto (IPsec, TLS, SSH, …)
- IPv6 & Security
- DNS & Security
- NTP & Security
- Blog: https://weberblog.net
- Twitter: @webernetz

CT Log

Certificate Transparency

https://certificate.transparency.dev/

- „Working together to detect maliciously or mistakenly issued certificates.”
- → Log of all public issued certificates
- Who else issues certificates out of my domains?

Certificate Transparency Log

https://crt.sh/

- Live Demo

Criteria	Type: Identity Match: ILIKE Search: 'ebay.de'

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities
4709554331	2021-06-16	2021-06-16	2022-06-16	ocshelpbotweb.ebay.com	ocshelpbotweb.ebay.de
4709554241	2021-06-16	2021-06-16	2022-06-16	ocshelpbotweb.ebay.com	ocshelpbotweb.ebay.de
4709551025	2021-06-16	2021-06-16	2022-06-16	ocshelpbotweb.ebay.com	ocshelpbotweb.ebay.de
4709550848	2021-06-16	2021-06-16	2022-06-16	ocshelpbotweb.ebay.com	ocshelpbotweb.ebay.de
4709550777	2021-06-16	2021-06-16	2022-06-16	ocshelpbotweb.ebay.com	ocshelpbotweb.ebay.de
4709550796	2021-06-16	2021-06-16	2022-06-16	ocshelpbotweb.ebay.com	ocshelpbotweb.ebay.de
4704953579	2021-06-15	2021-06-15	2022-06-15	reg.ebay.com	origin-reg.ebay.de origin-reg.m.ebay.de reg.ebay.de reg.m.ebay.de
4704953261	2021-06-15	2021-06-15	2022-06-15	reg.ebay.com	origin-reg.ebay.de origin-reg.m.ebay.de reg.ebay.de reg.m.ebay.de
4704948162	2021-06-15	2021-06-15	2022-06-15	reg.ebay.com	origin-reg.ebay.de origin-reg.m.ebay.de reg.ebay.de reg.m.ebay.de
4704944812	2021-06-15	2021-06-15	2022-06-15	reg.ebay.com	origin-reg.ebay.de origin-reg.m.ebay.de reg.ebay.de reg.m.ebay.de
4704282118	2021-06-15	2021-06-15	2022-06-15	rover.intl.ebay.com	metrics.ebay.de rover.ebay.de
4704282061	2021-06-15	2021-06-15	2022-06-15	rover.intl.ebay.com	metrics.ebay.de rover.ebay.de
4704258384	2021-06-15	2021-06-15	2022-06-15	rover.intl.ebay.com	metrics.ebay.de rover.ebay.de
4704258181	2021-06-15	2021-06-15	2022-06-15	rover.intl.ebay.com	metrics.ebay.de rover.ebay.de
4704230682	2021-06-15	2021-06-15	2022-06-15	rover.intl.ebay.com	metrics.ebay.de rover.ebay.de
4704230390	2021-06-15	2021-06-15	2022-06-15	rover.intl.ebay.com	metrics.ebay.de rover.ebay.de

Certificate Transparency

BUT: it leaks all FQDNs to the public!

- CT log search for weberlab.de ;D

Not After	Common Name	Matching Identities
2021-09-14	ddiug.weberlab.de	ddiug.weberlab.de ichgruesseeuchrechtherzlich.weberlab.de
2021-09-14	ddiug.weberlab.de	ddiug.weberlab.de ichgruesseeuchrechtherzlich.weberlab.de

A little Experiment

A little Experiment

Cert 1

- Let‘s Encrypt
- random generated hostname
- AAAA to random generated IPv6 IID
- not published anywhere!

- → Logging of DNS queries on the authoritative DNS server
- → Logging of incoming connections to the IPv6 address

Cert 2

- same as cert 1 with different hostname & different IPv6 address
- but CN on my blog for 2,5 months with my blogs hostnames as SAN (Subject Alternative Name)

Cert 2


blog.webernetz.net
Zertifikat
Allgemein
Details
Zertifizierungspfad
Zertifikatsinformationen
Dieses Zertifikat ist für folgende Zwecke beabsichtigt:
• Garantiert die Identität eines Remotecomputers
• Garantiert dem Remotecomputer Ihre Identität
• 2.23.140.1.2.1
• 1.3.6.1.4.1.44947.1.1.1
* Weitere Infos finden Sie in den Angaben der Zertifizierungsstelle.
Ausgestellt für: xd524olksc.ib.weberdns.de
Ausgestellt von: Let's Encrypt Authority X3
Gültig ab 30.10.2019 bis 28.01.2020
Ausstellererklärung
Blog Weber
IT-Security, Networks, IPv6, DNSSEC,
About
IPv6
DNSSEC
NTP
VPN

weberjoh@nb15-lx: /var/log/firewalls/2001:470:765b::d031:53/2019/10

```
Last login: Wed Oct 30 13:42:40 2019 from 84.146.144.169
weberjoh@nb15-lx:~$ cd /var/log/firewalls/2001:470:765b::d031:53/2019/10
weberjoh@nb15-lx:/var/log/firewalls/2001:470:765b::d031:53/2019/10$ ls
2001:470:765b::d031:53-2019-10-30.log
weberjoh@nb15-lx:/var/log/firewalls/2001:470:765b::d031:53/2019/10$ tail -f 2001\:470\:765b\:\:d031\:53-2019-10-30.lo
g | grep -e 7qftpqiw5m -e xd524olksc
Oct 30 15:48:51 2001:470:765b::d031:53 named[8781]: zone ib.weberdns.de/IN: ZRQ applied ADD for '_acme-challenge.7qft
pqiw5m': 300 IN TXT "GVCz6pCl3SkbQRDd6nzv7OFfN8XvhiKyEFXxa00M20A" (none).
Oct 30 15:48:51 2001:470:765b::d031:53 named[8781]: zone ib.weberdns.de/IN: ZRQ applied ADD for '_acme-challenge.7qft
pqiw5m': 300 IN RRSIG TXT 10 5 300 20191103144906 20191030134906 26198 ib.weberdns.de. uSAeCn+IWJxLZOGN/QqxcK4sMSFe/8
8v1xlt2u0pktYlXjqE2AKXp0XcnS1788kVcuoUuyV0xpJ0XSnaFqwSSxJfcNXH9N8j060WtT01NarXNgJdYVsm8ci7uXxL6vwT5agbb2xdvgi+7V2h0sK
fNpM3DOfux5qYlK1kxZuV81AF1ImEl6HNTEzhlAdu3rytJkBeIqHuh7TXZSabXQaVWELTuMy6/CfhCkOosL/OFfVL8dFjleeREmYkqmgCwp8iiuh9NiIL
7w+ricf47Ivbz8FvM3nrfaYTWtALcTWilIHn09ypZ8EdDU1FHctgPW/wwEO6kXrF1eACSRuBJRdeUA== (ro ).
Oct 30 15:49:26 2001:470:765b::d031:53 named[8781]: client @0x7fcf080cc9d0 74.63.25.248#59726 (7qftpqiw5m.ib.weberdns
.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (193.24.227.239)
Oct 30 15:49:26 2001:470:765b::d031:53 named[8781]: client @0x7fcf08127b30 2620:171:f9:f0::8#5374 (7qftpqiw5m.ib.webe
rdns.de): query: 7qftpqiw5m.ib.weberdns.de IN AAAA -E(0)DC (2001:470:765b::d031:53)
Oct 30 15:49:59 2001:470:765b::d031:53 named[8781]: client @0x7fcf08118b80 2607:f8b0:4001:c12::10a#63984 (7qftpqiw5m.
ib.weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN AAAA - (2001:470:765b::d031:53)
Oct 30 15:50:05 2001:470:765b::d031:53 named[8781]: client @0x7fcf080cc9d0 5.79.75.66#28583 (7qftpqiw5m.ib.weberdns.d
e): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (193.24.227.239)
Oct 30 15:50:08 2001:470:765b::d031:53 named[8781]: client @0x7fcf080cc9d0 172.253.192.2#48914 (7qftpqiw5m.ib.weberdn
s.de): query: 7qftpqiw5m.ib.weberdns.de IN CAA -E(0)DC (193.24.227.239) [ECS 107.178.232.0/24/0]
Oct 30 15:50:08 2001:470:765b::d031:53 named[8781]: client @0x7fcf080bda20 74.125.113.146#49679 (7qftpqiw5m.ib.weberd
ns.de): query: 7qftpqiw5m.ib.weberdns.de IN MX -E(0)DC (193.24.227.239) [ECS 107.178.232.0/24/0]
Oct 30 15:50:44 2001:470:765b::d031:53 named[8781]: client @0x7fcf08118b80 2620:171:f9:f0::4#43293 (7qftpqiw5m.ib.web
erdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (2001:470:765b::d031:53)
Oct 30 15:50:44 2001:470:765b::d031:53 named[8781]: client @0x7fcf08127b30 2620:171:eb:f0::2#34672 (7qftpqiw5m.ib.web
erdns.de): query: 7qftpqiw5m.ib.weberdns.de IN AAAA -E(0)D (2001:470:765b::d031:53)
Oct 30 15:51:25 2001:470:765b::d031:53 named[8781]: client @0x7fcf08118b80 2001:4ca0:108:42::222#19865 (7qftpqiw5m.ib
.weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (2001:470:765b::d031:53)
Oct 30 15:51:25 2001:470:765b::d031:53 named[8781]: client @0x7fcf080cc9d0 162.158.117.82#59395 (7qftpqiw5m.ib.weberd
ns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (193.24.227.239)
Oct 30 15:51:25 2001:470:765b::d031:53 named[8781]: client @0x7fcf080bda20 162.158.117.86#24059 (7qftpqiw5m.ib.weberd
ns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (193.24.227.239)
Oct 30 15:51:25 2001:470:765b::d031:53 named[8781]: client @0x7fcf08118b80 2400:cb00:22:1024::a29e:7552#11832 (7qftpq
iw5m.ib.weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (2001:470:765b::d031:53)
Oct 30 15:51:25 2001:470:765b::d031:53 named[8781]: client @0x7fcf08127b30 2400:cb00:22:1024::a29e:7556#17299 (7qftpq
iw5m.ib.weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (2001:470:765b::d031:53)
Oct 30 15:51:45 2001:470:765b::d031:53 named[8781]: client @0x7fcf080cc9d0 52.215.218.117#61144 (7qftpqiw5m.ib.weberd
ns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (193.24.227.239)
Oct 30 15:51:45 2001:470:765b::d031:53 named[8781]: client @0x7fcf080bda20 34.242.153.179#54564 (7qftpqiw5m.ib.weberd
ns.de): query: 7qftpqiw5m.ib.weberdns.de IN AAAA -E(0)DC (193.24.227.239)
Oct 30 15:51:51 2001:470:765b::d031:53 named[8781]: client @0x7fcf080cc9d0 34.223.37.241#61978 (7qftpqiw5m.ib.weberdn
s.de): query: 7qftpqiw5m.ib.weberdns.de IN NS -E(0)DC (193.24.227.239)
Oct 30 15:51:53 2001:470:765b::d031:53 named[8781]: client @0x7fcf08118b80 2607:f8b0:400e:c01::109#44463 (7qftpqiw5m.
ib.weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN NS -E(0)DC (2001:470:765b::d031:53) [ECS 54.148.165.0/24/0]
Oct 30 15:54:11 2001:470:765b::d031:53 named[8781]: client @0x7fcf080bda20 159.203.199.175#6937 (7qftpqiw5m.ib.weberd
ns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)D (193.24.227.239)
Oct 30 15:54:15 2001:470:765b::d031:53 named[8781]: client @0x7fcf080cc9d0 172.217.33.197#48240 (7qftpqiw5m.ib.weberd
ns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (193.24.227.239) [ECS 206.81.22.0/24/0]
Oct 30 15:54:51 2001:470:765b::d031:53 named[8781]: client @0x7fcf080cc9d0 212.227.22.111#59842 (7qftpqiw5m.ib.weberd
ns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (193.24.227.239)
Oct 30 15:54:51 2001:470:765b::d031:53 named[8781]: client @0x7fcef80b30d0 212.227.22.111#49257 (7qftpqiw5m.ib.weberd
ns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)TDC (193.24.227.239)
Oct 30 15:55:47 2001:470:765b::d031:53 named[8781]: client @0x7fcf080cc9d0 162.158.117.106#44746 (7qftpqiw5m.ib.weber
dns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)D (193.24.227.239)
Oct 30 15:55:47 2001:470:765b::d031:53 named[8781]: client @0x7fcf08118b80 2400:cb00:22:1024::a29e:756a#42440 (7qftpq
iw5m.ib.weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (2001:470:765b::d031:53)
Oct 30 15:56:49 2001:470:765b::d031:53 named[8781]: client @0x7fcf080bda20 212.227.22.111#50532 (7qftpqiw5m.ib.weberd
ns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (193.24.227.239)
Oct 30 16:05:27 2001:470:765b::d031:53 named[8781]: client @0x7fcf080cc9d0 162.158.117.85#56549 (7qftpqiw5m.ib.weberd
ns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)D (193.24.227.239)
```

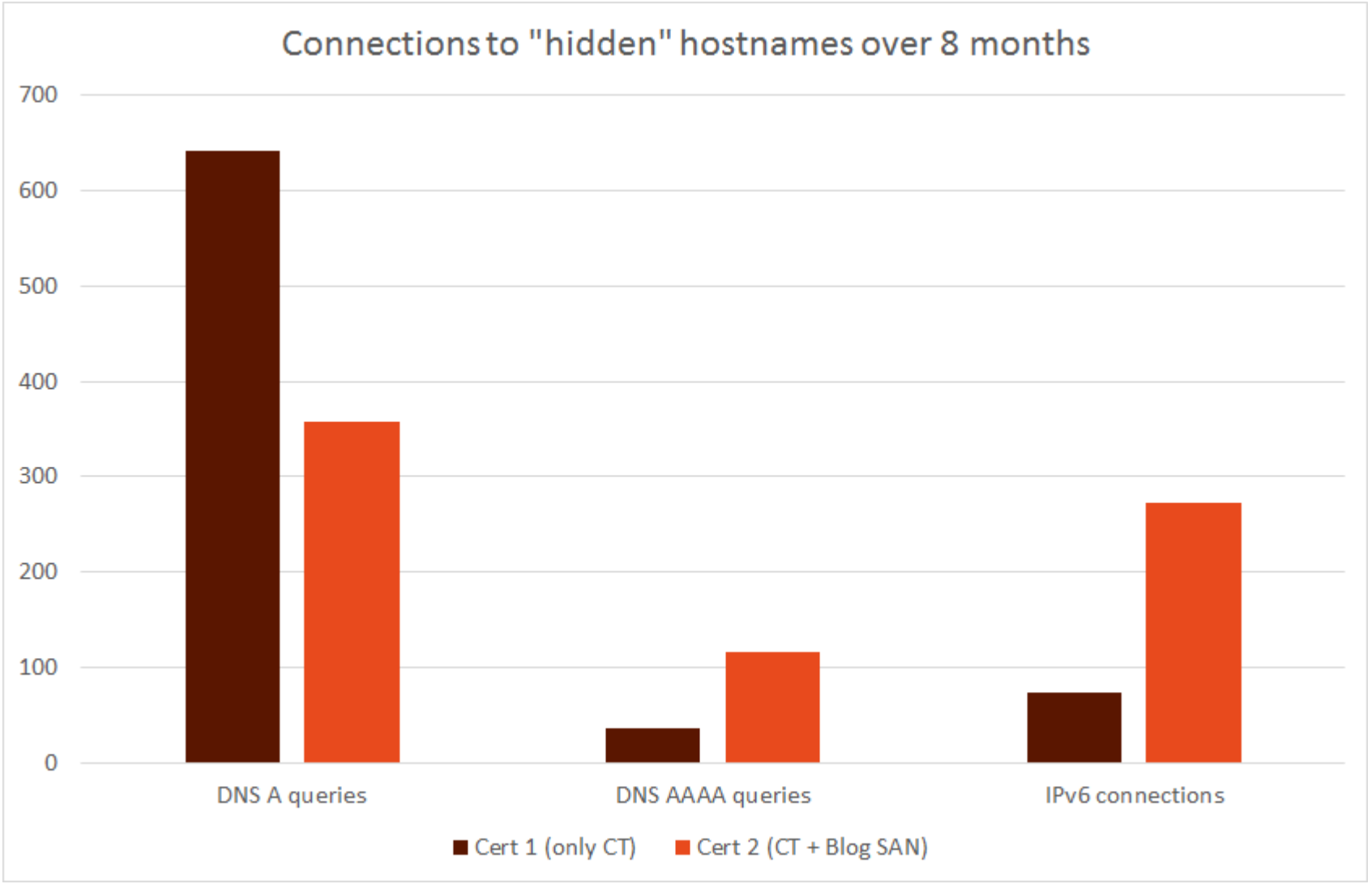
weberjoh@nb15-lx: /var/log/firewalls/2001:470:1f0b:16b0::d032:53/2019/10

```
arpa): query: 1.0.0.127.in-addr.arpa IN PTR +E(0)K (194.247.5.16)
^C
weberjoh@nb15-lx:/var/log/firewalls/2001:470:1f0b:16b0::d032:53/2019/10$ tail -f 2001\:470\:1f0b\:16b0\:\:d032\:53-20
19-10-30.log | grep -e 7qftpqiw5m -e xd524olksc
Oct 30 15:43:11 2001:470:1f0b:16b0::d032:53 named[458]: zone 0.0.0.0.b.5.6.7.0.7.4.0.1.0.0.2.ip6.arpa/IN: ZRQ applied
 ADD for 'b.e.1.9.9.f.d.0.2.6.9.1.2.0.3.d': 300 IN PTR xd524olksc.ib.weberdns.de. (ro host rrpos=0 ).
Oct 30 15:49:06 2001:470:1f0b:16b0::d032:53 named[458]: zone ib.weberdns.de/IN: ZRQ applied ADD for '_acme-challenge
7qftpqiw5m': 300 IN TXT "GVCz6pCl3SkbQRDd6nzv7OFfN8XvhiKyEFXxa00M20A" (none).
Oct 30 15:49:06 2001:470:1f0b:16b0::d032:53 named[458]: zone ib.weberdns.de/IN: ZRQ applied ADD for '_acme-challenge
7qftpqiw5m': 300 IN RRSIG TXT 10 5 300 20191103144906 20191030134906 26198 ib.weberdns.de. uSAeCn+IWJxLZOGN/QqxcK4sMS
Fe/88v1xlt2u0pktYlXjqE2AKXp0XcnS1788kVcuoUuyV0xpJ0XSnaFqwSSxJfcNXH9N8j060WtT01NarXNgJdYVsm8ci7uXxL6vwT5agbb2xdvgi+7V2
h0sKfNpM3DOfux5qYlK1kxZuV81AF1ImEl6HNTEzhlAdu3rytJkBeIqHuh7TXZSabXQaVWELTuMy6/CfhCkOosL/OFfVL8dFjleeREmYkqmgCwp8iiuh9
NiIL7w+ricf47Ivbz8FvM3nrfaYTWtALcTWilIHn09ypZ8EdDU1FHctgPW/wwEO6kXrF1eACSRuBJRdeUA== (ro ).
Oct 30 15:49:42 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900cc9d0 74.63.25.242#4383 (7qftpqiw5m.ib.weber
dns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (194.247.5.16)
Oct 30 15:50:04 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900cc9d0 172.217.34.2#38245 (7qftpqiw5m.ib.webe
rdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (194.247.5.16) [ECS 206.81.22.0/24/0]
Oct 30 15:50:13 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900bda20 91.90.42.154#1098 (7qftpqiw5m.ib.weber
dns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)D (194.247.5.16)
Oct 30 15:50:13 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900cc9d0 91.90.42.154#18832 (7qftpqiw5m.ib.webe
rdns.de): query: 7qftpqiw5m.ib.weberdns.de IN AAAA -E(0)D (194.247.5.16)
Oct 30 15:50:14 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900bda20 74.125.179.10#45562 (7qftpqiw5m.ib.web
erdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A - (194.247.5.16)
Oct 30 15:50:14 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd90118b80 2a00:1450:4001:c02::101#38756 (7qftpqi
w5m.ib.weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (2001:470:1f0b:16b0::d032:53) [ECS 206.81.22.0/24/
0]
Oct 30 15:50:19 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900bda20 74.125.113.129#57073 (7qftpqiw5m.ib.we
berdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (194.247.5.16) [ECS 107.178.232.0/24/0]
Oct 30 15:50:22 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd90118b80 2607:f8b0:4001:c09::10d#40742 (7qftpqi
w5m.ib.weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN SOA -E(0)DC (2001:470:1f0b:16b0::d032:53) [ECS 107.178.232.0
/24/0]
Oct 30 15:50:23 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900bda20 74.125.179.13#53314 (7qftpqiw5m.ib.web
erdns.de): query: 7qftpqiw5m.ib.weberdns.de IN TXT -E(0)DC (194.247.5.16) [ECS 107.178.232.0/24/0]
Oct 30 15:50:23 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900cc9d0 173.194.103.130#42234 (7qftpqiw5m.ib.w
eberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN AAAA -E(0)DC (194.247.5.16) [ECS 107.178.232.0/24/0]
Oct 30 15:50:23 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900bda20 173.194.103.138#58218 (7qftpqiw5m.ib.w
eberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN NS -E(0)DC (194.247.5.16) [ECS 107.178.232.0/24/0]
Oct 30 15:50:55 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd90127b30 2a04:e4c0:12::64#27582 (7qftpqiw5m.ib.
weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0) (2001:470:1f0b:16b0::d032:53)
Oct 30 15:50:55 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd90118b80 2620:0:cc4::66#46354 (7qftpqiw5m.ib.we
berdns.de): query: 7qftpqiw5m.ib.weberdns.de IN AAAA -E(0) (2001:470:1f0b:16b0::d032:53)
Oct 30 15:50:56 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd90127b30 2a00:1450:4001:c00::103#53246 (7qftpqi
w5m.ib.weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (2001:470:1f0b:16b0::d032:53) [ECS 206.81.22.0/24/
0]
Oct 30 15:50:59 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900bda20 66.185.123.242#20823 (7qftpqiw5m.ib.we
berdns.de): query: 7qftpqiw5m.ib.weberdns.de IN DS -E(0)D (194.247.5.16)
Oct 30 15:51:02 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900cc9d0 212.227.22.111#34738 (7qftpqiw5m.ib.we
berdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (194.247.5.16)
Oct 30 15:51:02 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd90582d50 212.227.22.111#55997 (7qftpqiw5m.ib.we
berdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)TDC (194.247.5.16)
Oct 30 15:51:40 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd90118b80 2001:4ca0:108:42::222#59141 (7qftpqiw5
m.ib.weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN CAA -E(0)DC (2001:470:1f0b:16b0::d032:53)
Oct 30 15:51:57 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd90127b30 2400:cb00:65:1024::a29e:8509#40710 (7q
ftpqiw5m.ib.weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (2001:470:1f0b:16b0::d032:53)
Oct 30 15:51:57 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd90118b80 2400:cb00:65:1024::a29e:8509#48363 (7q
ftpqiw5m.ib.weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)D (2001:470:1f0b:16b0::d032:53)
Oct 30 15:52:07 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900bda20 172.217.46.132#63234 (7qftpqiw5m.ib.we
berdns.de): query: 7qftpqiw5m.ib.weberdns.de IN DS -E(0)DC (194.247.5.16) [ECS 54.148.165.0/24/0]
Oct 30 15:52:26 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900bda20 159.203.199.175#58817 (7qftpqiw5m.ib.w
eberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)D (194.247.5.16)
Oct 30 15:53:07 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900bda20 172.253.199.2#65439 (7qftpqiw5m.ib.web
erdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)DC (194.247.5.16) [ECS 176.53.43.0/24/0]
Oct 30 16:05:41 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd90127b30 2400:cb00:22:1024::a29e:7593#14351 (7q
ftpqiw5m.ib.weberdns.de): query: 7qftpqiw5m.ib.weberdns.de IN A -E(0)D (2001:470:1f0b:16b0::d032:53)
Oct 30 16:05:41 2001:470:1f0b:16b0::d032:53 named[458]: client @0x7fdd900bda20 162.158.117.147#33770 (7qftpqiw5m.ib.w
```

(addr.dst in '2001:470:765b:0:747d:36b6:0d74:f26a') or (addr.dst in '2001:470:765b:0:d302:1962:0df9:91eb')

Receive Time	Type	From Zone	To Zone	Source	Destination	From Port	To Port	Application	Action	Rule	Session End Reason	Bytes Sent	Bytes Received
01/06 09:30:26	drop	untrust	dmz	2604:a880:800:c1::246:e001	2001:470:765b:0:747d:36b6:d74:f26a	38638	443	not-applicable	drop	lets test 1	policy-deny	94	0
01/06 09:30:18	drop	untrust	dmz	2604:a880:800:c1::1a7:3001	2001:470:765b:0:d302:1962:df9:91eb	36302	443	not-applicable	drop	lets test 2	policy-deny	94	0
01/06 09:30:18	drop	untrust	dmz	2604:a880:800:c1::246:e001	2001:470:765b:0:747d:36b6:d74:f26a	38638	443	not-applicable	drop	lets test 1	policy-deny	94	0
01/06 09:30:14	drop	untrust	dmz	2604:a880:800:c1::246:e001	2001:470:765b:0:747d:36b6:d74:f26a	38638	443	not-applicable	drop	lets test 1	policy-deny	94	0
01/06 09:30:12	drop	untrust	dmz	2604:a880:800:c1::246:e001	2001:470:765b:0:747d:36b6:d74:f26a	38638	443	not-applicable	drop	lets test 1	policy-deny	94	0
01/06 09:30:11	drop	untrust	dmz	2604:a880:800:c1::246:e001	2001:470:765b:0:747d:36b6:d74:f26a	38638	443	not-applicable	drop	lets test 1	policy-deny	94	0
01/06 09:30:10	drop	untrust	dmz	2604:a880:800:c1::1a7:3001	2001:470:765b:0:d302:1962:df9:91eb	36302	443	not-applicable	drop	lets test 2	policy-deny	94	0
01/06 09:30:06	drop	untrust	dmz	2604:a880:800:c1::1a7:3001	2001:470:765b:0:d302:1962:df9:91eb	36302	443	not-applicable	drop	lets test 2	policy-deny	94	0
01/06 09:30:04	drop	untrust	dmz	2604:a880:800:c1::1a7:3001	2001:470:765b:0:d302:1962:df9:91eb	36302	443	not-applicable	drop	lets test 2	policy-deny	94	0
01/06 09:30:03	drop	untrust	dmz	2604:a880:800:c1::1a7:3001	2001:470:765b:0:d302:1962:df9:91eb	36302	443	not-applicable	drop	lets test 2	policy-deny	94	0
01/03 22:29:18	drop	untrust	dmz	2600:1900:2000:37:400::11	2001:470:765b:0:d302:1962:df9:91eb	46727	443	not-applicable	drop	lets test 2	policy-deny	94	0
01/03 22:29:16	drop	untrust	dmz	2600:1900:2000:37:400::11	2001:470:765b:0:d302:1962:df9:91eb	46727	443	not-applicable	drop	lets test 2	policy-deny	94	0
01/03 22:29:15	drop	untrust	dmz	2600:1900:2000:37:400::11	2001:470:765b:0:d302:1962:df9:91eb	46727	443	not-applicable	drop	lets test 2	policy-deny	94	0
01/03 05:08:02	drop	untrust	dmz	2604:a880:800:c1::32b:8001	2001:470:765b:0:d302:1962:df9:91eb	33410	443	not-applicable	drop	lets test 2	policy-deny	94	0
01/03 05:07:54	drop	untrust	dmz	2604:a880:800:c1::32b:8001	2001:470:765b:0:d302:1962:df9:91eb	33410	443	not-applicable	drop	lets test 2	policy-deny	94	0
01/03 05:07:49	drop	untrust	dmz	2604:a880:800:c1::32b:8001	2001:470:765b:0:d302:1962:df9:91eb	33410	443	not-applicable	drop	lets test 2	policy-deny	94	0
01/03 05:07:47	drop	untrust	dmz	2604:a880:800:c1::32b:8001	2001:470:765b:0:d302:1962:df9:91eb	33410	443	not-applicable	drop	lets test 2	policy-deny	94	0
01/03 05:07:46	drop	untrust	dmz	2604:a880:800:c1::32b:8001	2001:470:765b:0:d302:1962:df9:91eb	33410	443	not-applicable	drop	lets test 2	policy-deny	94	0
01/03 04:41:57	drop	untrust	dmz	2604:a880:800:c1::251:d001	2001:470:765b:0:747d:36b6:d74:f26a	34946	443	not-applicable	drop	lets test 1	policy-deny	94	0
01/03 04:41:49	drop	untrust	dmz	2604:a880:800:c1::251:d001	2001:470:765b:0:747d:36b6:d74:f26a	34946	443	not-applicable	drop	lets test 1	policy-deny	94	0
01/03 04:41:45	drop	untrust	dmz	2604:a880:800:c1::251:d001	2001:470:765b:0:747d:36b6:d74:f26a	34946	443	not-applicable	drop	lets test 1	policy-deny	94	0
01/03 04:41:43	drop	untrust	dmz	2604:a880:800:c1::251:d001	2001:470:765b:0:747d:36b6:d74:f26a	34946	443	not-applicable	drop	lets test 1	policy-deny	94	0
01/03 04:41:42	drop	untrust	dmz	2604:a880:800:c1::251:d001	2001:470:765b:0:747d:36b6:d74:f26a	34946	443	not-applicable	drop	lets test 1	policy-deny	94	0

Results


Connections to "hidden" hostnames over 8 months
700
600
500
400
300
200
100
0
DNS A queries
DNS AAAA queries
IPv6 connections
Cert 1 (only CT)
Cert 2 (CT + Blog SAN)

Results

	Cert 1 only CT	Cert 2 CT + Blog SAN
DNS queries for A (unique sources)	642 (307)	357 (228)
DNS queries for AAAA (unique sources)	37 (32)	117 (99)
DNS queries for CAA (unique sources)	3 (3)	24 (14)
All queried RRs	642 A 37 AAAA 22 MX 6 DS 5 NS 3 TXT 3 SOA 3 CAA 2 CNAME	357 A 117 AAAA 29 MX 24 CAA 8 TXT 8 NS 7 SOA 4 DS 3 CNAME 2 DNSKEY

Results

	Cert 1 only CT	Cert 2 CT + Blog SAN
IPv6 connections (unique sources) [unique /32]	73 (15) [2]	273 (46) [14]
Destination Ports	73x 443	154x 80 122x 443
Sourcing ASes	14 DigitalOcean, LLC 1 Google LLC	14 DigitalOcean, LLC 8 Quintex Alliance Consulting 6 Emerald Onion 4 Google LLC 4 F3 Netze e.V. 2 Zwiebelfreunde e.V. 2 Nexeon Technologies, Inc. 1 OVH Ltd 1 Keyweb AG 1 Joey Julian Koenig 1 Hydra Communications Ltd 1 Hurricane Electric LLC

Conclusion

- Don’t expect you can receive valid X.509 certificates on the Internet for private use cases.
- **Every single FQDN is immediately publicized in the CT logs and will be scanned!**

Discussion: Usage of wildcard certificates

Pros:

- hostnames are „hidden“ from CT log

Cons:

- distribution of the private key among different machines
- note: there are other methods of finding hostnames anyway

Jetzt ist aber Schluss

Vielen Dank fürs Zuhören…
Fragen?

johannes@webernetz.net