Lost and Found Certificates

Ian Foster & Dylan Ayrey

Who We Are

Ian

Information Security Engineer

CertGraph

https://dns.coffee

https://lanrat.com

https://github.com/lanrat

@LANRAT

Dylan

truffleHog

WPA2-HalfHandshake-Crack

Pastejacking

Other stuff...

https://github.com/dxa4481

dylanayrey@gmail.com

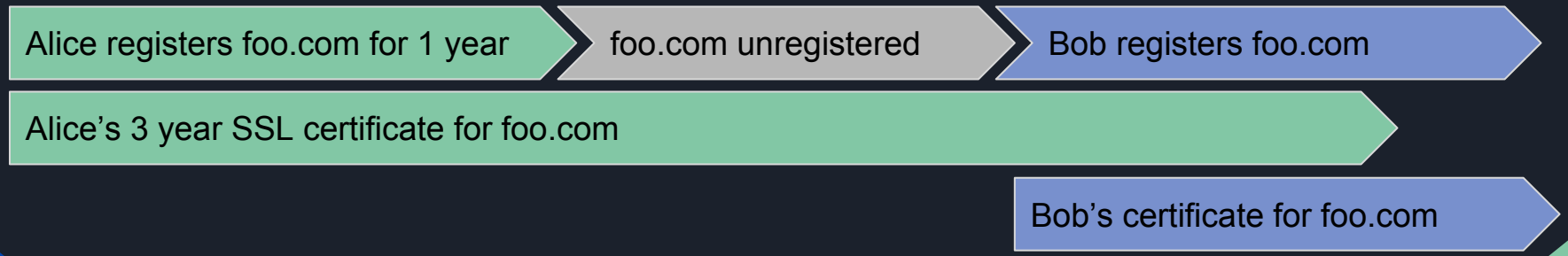
The Problem

A certificate can outlive a the ownership of a domain

This potentially leaves the domain owner with a valid SSL certificate for the next owner

How can you know?

- Buy a new domain… hope for the best?
- In the early 2000's and early 2010's, you'd never know



Certificate Transparency!

- Log of all certificates issued by public Certificate Authorities
- Designed to catch bad or misbehaving Certificate Authorities
- Publicly auditable and searchable
- ½ billion certs and growing

COMODO CA Limited [GB] | https://crt.sh/?q=google.com

crt.sh Identity Search

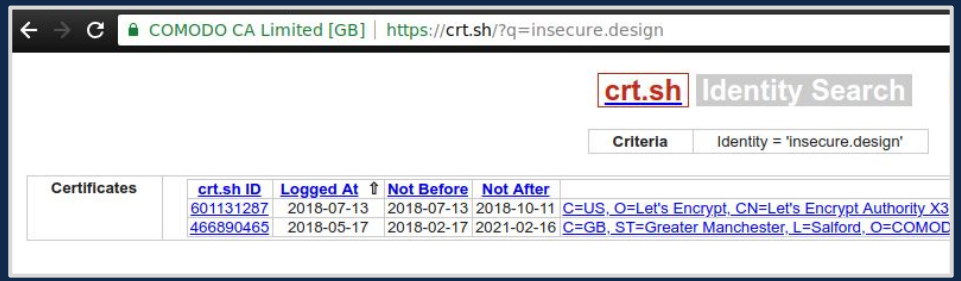
Group by I

Criteria	Identity = 'google.com'

crt.sh ID	Logged At	Not Before	Issuer Name
336351164	2018-02-20	2018-02-20	C=US, O=Google Trust Services, CN=Google Internet Authority G3
336350783	2018-02-20	2018-02-20	C=US, O=Google Trust Services, CN=Google Internet Authority G3
336350306	2018-02-20	2018-02-20	C=US, O=Google Trust Services, CN=Google Internet Authority G3
336346392	2018-02-20	2018-02-20	C=US, O=Google Inc, CN=Google Internet Authority G2
336346028	2018-02-20	2018-02-20	C=US, O=Google Inc, CN=Google Internet Authority G2
336345700	2018-02-20	2018-02-20	C=US, O=Google Inc, CN=Google Internet Authority G2
329172204	2018-02-13	2018-02-13	C=US, O=Google Trust Services, CN=Google Internet Authority G3
329172151	2018-02-13	2018-02-13	C=US, O=Google Trust Services, CN=Google Internet Authority G3
329171802	2018-02-13	2018-02-13	C=US, O=Google Trust Services, CN=Google Internet Authority G3
329166969	2018-02-13	2018-02-13	C=US, O=Google Inc, CN=Google Internet Authority G2

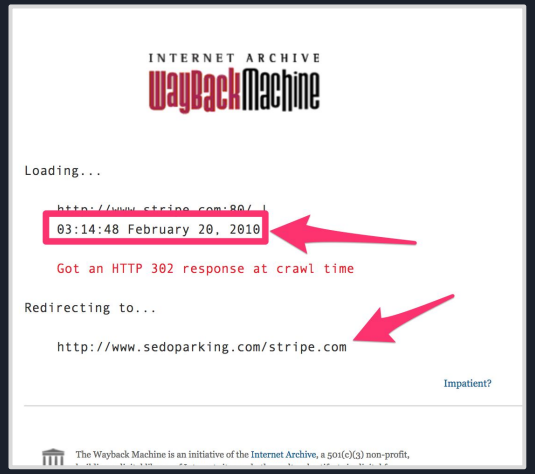
We Can find pre-existing certificates

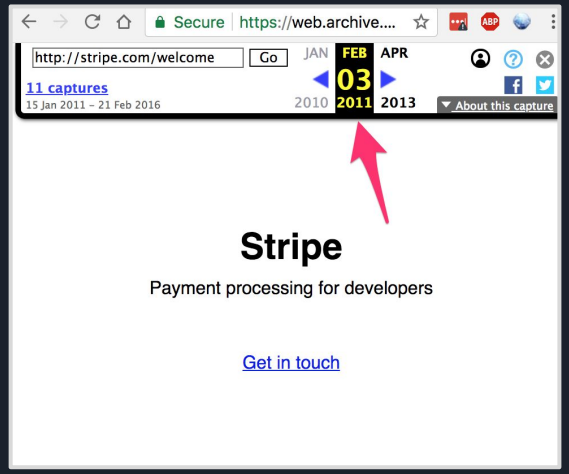
- Note the purchase date of said domain
- Search CT logs for certs pre-dating that date and valid after
- Monitor
  - Old certs may not show up in logs for years, *if ever*

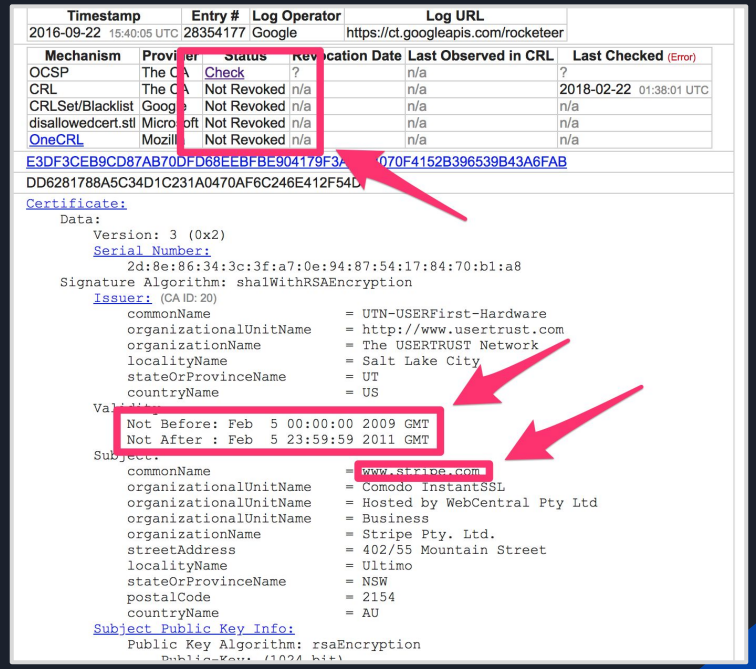


A significant example

stripe.com







How big is this issue?

Searched Certificate Transparency (CT) for certificates that overlap multiple domain registrations

Data

- 3 million domains
  - 1% of internet
- Looked for changes...
  - Expiration date
  - Email contacts
  - Registrar
  - Etc...

Sources

- CT logs
- Historical WHOIS
- Historical nameservers https://dns.coffee
- WayBack Machine https://archive.org

1.5M (0.45%)

Of domains tested have pre-existing certificates

25% haven't expired yet

BygoneSSL

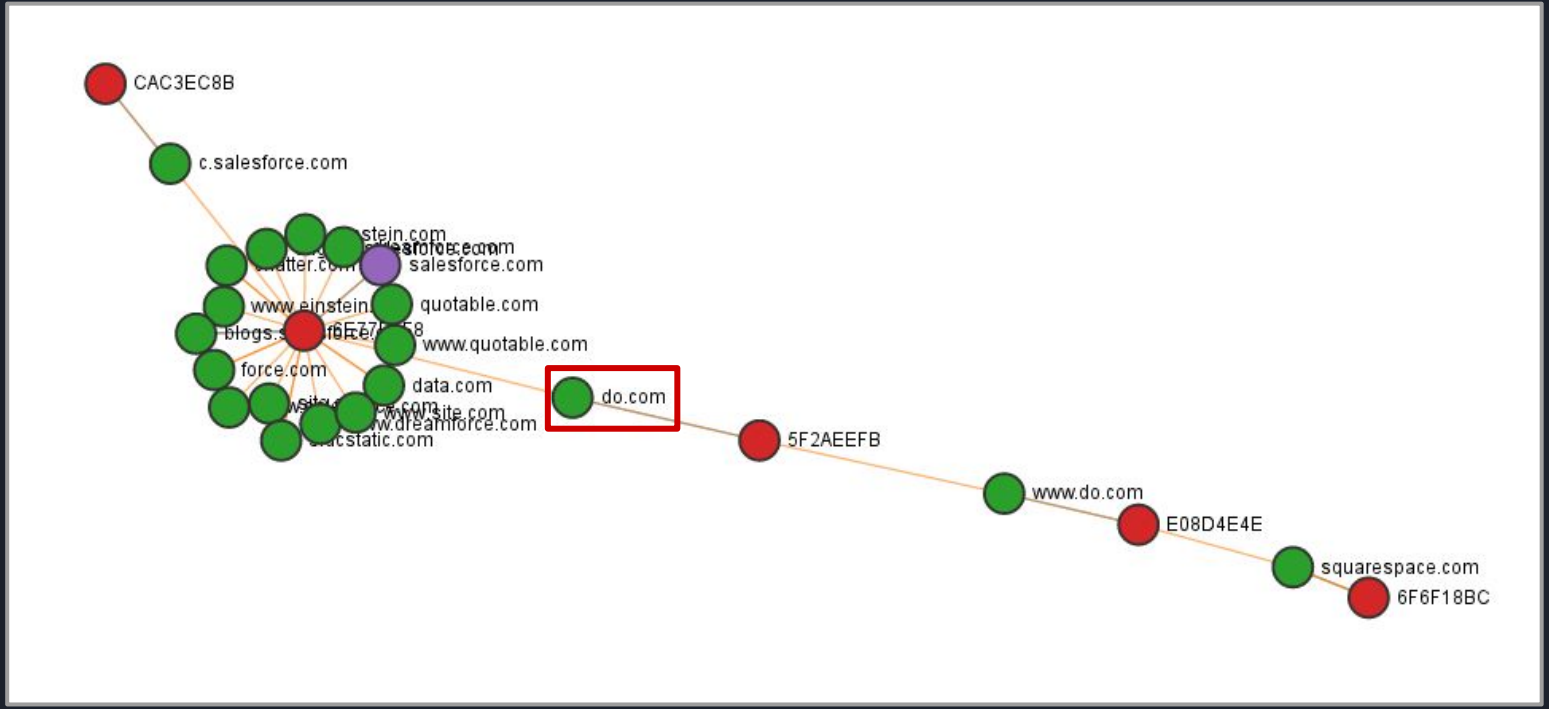
noun

An SSL certificate created before and supersedes its domains' current registration date

Could it be worse?

- Certificates can have many domains
- Certificates can contain some bygone domains and some not

CertGraph Example of BygoneSSL



https://github.com/lanrat/certgraph

Example: do.com

Current Nameservers 4

Name	First Seen
NS2.UNIREGISTRY-DNS.NET	Dec 02, 2017
NS1.UNIREGISTRY-DNS.COM	Dec 02, 2017
NS2.UNIREGISTRY-DNS.COM	Dec 02, 2017
NS1.UNIREGISTRY-DNS.NET	Dec 02, 2017

Past Nameservers 17

Name	First Seen	Last Seen
[illegible]	[illegible]	[illegible]
BUY.INTERNETTRAFFIC.COM	Dec 01, 2017	Dec 01, 2017
NS-774.AWSDNS-32.NET	Jul 05, 2014	Nov 30, 2017
NS-1654.AWSDNS-14.CO.UK	Jul 05, 2014	Nov 30, 2017
[illegible]	[illegible]	[illegible]
NS-469.AWSDNS-58.COM	Jul 05, 2014	Nov 30, 2017
NS-1617.AWSDNS-10.CO.UK	Aug 24, 2011	Jul 04, 2014
NS-416.AWSDNS-52.COM	Aug 24, 2011	Jul 04, 2014
NS-881.AWSDNS-46.NET	Aug 24, 2011	Jul 04, 2014
NS-1224.AWSDNS-25.ORG	Aug 24, 2011	Jul 04, 2014
NS1.MARKSMEN.COM	Jun 25, 2011	Aug 23, 2011
NS2.MARKSMEN.COM	Jun 25, 2011	Aug 23, 2011
NS4.MSFT.NET		Jun 23, 2011
NS5.MSFT.NET		Jun 23, 2011
NS1.MSFT.NET		Jun 23, 2011
NS2.MSFT.NET		Jun 23, 2011
NS3.MSFT.NET		Jun 23, 2011

```
Validity
    Not Before: Aug 24 00:00:00 2015 GMT
    Not After : Aug 23 23:59:59 2018 GMT
Subject:
    commonName                = www.salesforce.com
    organizationalUnitName    = Applications
    organizationName          = Salesforce.com, Inc
    localityName              = San Francisco
    stateOrProvinceName       = California
    countryName               = US
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            00:ae:ec:aa:83:1c:39:91:55:ae:9a:53:71:53:f7:
            69:4a:d6:b0:15:b9:bb:26:d4:83:71:d4:c2:74:e6:
            20:4c:33:a1:31:1a:6f:d6:f1:30:6d:29:6c:61:0a:
            cf:06:09:2f:e8:69:40:3f:da:91:8d:88:30:aa:93:
            07:cf:ca:bc:04:85:b0:a5:9d:b7:ab:d8:34:80:e5:
            e0:3b:70:e3:0f:51:17:ba:ed:c4:bc:27:b8:ca:f6:
            c1:2b:70:da:d8:1f:63:44:b0:f6:df:31:d3:e1:3c:
            e2:6f:2a:ae:d4:3d:68:38:eb:de:f1:08:db:cf:6f:
            8b:5c:a5:3a:7a:67:60:89:08:64:c9:15:f8:88:50:
            2a:b8:dc:de:7e:58:e5:03:61:9d:49:89:d8:f8:6d:
            42:9e:a4:44:b2:1f:d7:e3:83:74:6f:27:ba:40:f1:
            38:24:04:02:5e:c3:2a:c9:cb:71:c7:68:54:dc:d2:
            09:45:67:03:ae:e5:a2:19:3c:c3:9c:4a:68:84:b8:
            6f:81:74:c6:98:2c:99:3a:43:dc:27:9a:78:92:ed:
            0d:bb:ff:4c:6d:df:d6:d3:ba:8b:a2:87:4e:25:60:
            bd:30:b5:c7:95:a0:58:96:06:94:40:f0:a2:b2:7c:
            ff:58:f0:78:b0:c4:6f:8a:cb:4e:c1:69:11:d9:33:
            9f:c1
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Subject Alternative Name:
        DNS:www.salesforce.com
        DNS:salesforce.com
        DNS:sfdcstatic.com
        DNS:chatter.com
        DNS:force.com
        DNS:data.com
        DNS:*.sfdcstatic.com
        DNS:*.chatter.com
        DNS:*.force.com
        DNS:*.data.com
        DNS:*.do.com
        DNS:do.com
```

Can we revoke these certs?

If no….

- Spend 10k on a domain, you're screwed for years
- Bad guys could squat on desirable domains
- Cry 😢

If yes…

- You can take down production certs you don't own
- You can DoS companies

Digging deeper....

- Rules that dictate how CA's and browsers operate
- If broken browsers distrust the CA

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

Can revoke if information becomes incorrect

5. **Reporting and Revocation:** An obligation and warranty to: (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.

https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.5.7-29-Apr-2018.pdf

Within 24 hours

4.9.1.1. Reasons for Revoking a Subscriber Certificate

The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. The CA obtains evidence that the Certificate was misused;
5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
6. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;

https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.5.7-29-Apr-2018.pdf

We can DoS production sites

Certificate for `bar.com` can be revoked because it is shared with `foo.com` which has changed ownership during the certificates lifetime

7M (2.05%)

Of domains share a certificate with bygone domains

41% haven't expired yet

Sounds like we can break stuff....

BygoneSSL

BygoneSSL Man in the Middle

If a company acquires a previously owned domain…

Previous owners could still have valid certificates

MitM the SSL connection with a certificate generated by the previous owner

BygoneSSL Denial of Service

If a certificate has a subject alt-name for a domain no longer owned…

Revoke the certificate with a vulnerable domain and non-vulnerable domain listed in the alternative names

You can DoS the service if the shared certificate is still in use!

Trying to revoke with Let’s Encrypt

- Instant automated turn around
- I emailed security@letsencrypt.org

Let's Encrypt [redacted] (Internet Security Research Group)
Jul 17, 11:14 COT

Thanks for the report. This is actually something that you can do on your end even if you do not have the private key.

The process is outlined in our docs:
https://letsencrypt.org/docs/revoking/

This is the safest and most effective way to revoke certificates, because it proves control of the domain by the person requesting revocation.

All the best,
The Let's Encrypt Team

Trying to revoke with Digicert

- 1 day turn around
- I emailed support@digicert.com

Reply ABOVE THIS LINE to add a note to this request

Thank you,

I just sent an email to the domain owner as listed here https://whois.icann.org/en/lookup?name=a[redacted].

When you receive the email, please reply and we will be happy to revoke the certificate.

Sorry for any confusion.

Thank you for contacting Digicert support and if there is anything else we can help you with, please let us know.

Bryan U.
Technical Support Manager
Digicert Inc.

Trying to revoke with Amazon AWS

- 1 week turn around
- I emailed ec2-abuse@amazon.com

amazon web services™

Hello,

Thank you for following up.Below is the most recent update from our specialist team that handles certificates.

Guidance is as follows:

1. The customer will need to setup the 5 common email addresses.
2. We will re-send the confirmation email.
3. Upon confirmation from the domain owner, we can revoke the certificate.

Regards,
AWS Abuse Team

Trying to revoke with Comodo....

- Still waiting....
- I opened many support chats and emailed security@comodo.com

20:10Edw[redacted]:Unfortunately, without account ownership verification, it is impossible to perform such actions with the certificate.

20:25Mar[redacted]Unfortunately, I cannot revoke the certificate without verifying the account ownership.

Roger9:33 AM

You can forget about this SSL and order a new SSL for : insecure.design

What about resellers? (ssl's)

- 1 week turn around
- I emailed tech@ssls.com

SSLs.com Team via namecheap.com Fri, Jun 22, 5:10 AM (3 days ago)

to me

Dear Dylan,

Thank you for your patience.

We would like to let you know that the certificate for insecure.design has been revoked as requested.

Instantly revoked a cert used in production

crt.sh ID	575907636
Summary	Leaf certificate
Certificate Transparency	

Timestamp	Entry #	Log Operator	Log URL
2018-07-04 05:06:37 UTC	308652682	Google	https://ct.googleapis.com/pilot
2018-07-04 05:16:51 UTC	330152329	Google	https://ct.googleapis.com/rocketeer

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Revoked	2018-07-18 01:35:32 UTC	n/a	2018-07-22 01:25:55 UTC
CRL	The CA	Unknown	n/a	n/a	
CRLSet/Blacklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

SHA-256(Certificate)	D6BA525935FB5963F23E69CC096207594CA6710BCD6278B7A8EDED51C1CD05FB
SHA-1(Certificate)	F3353E20BB7D41F757A419B5F619F02F69C540CB
Certificate | ASN.1	Certificate:

```
    Data:
        Version: 3 (0x2)
```

- I still own and use security.love

```
X509v3 Basic Constraints: critical
    CA:FALSE
X509v3 Subject Key Identifier:
    D9:07:92:D1:0A:FB:AA:22:DE:9A:E9:A2:5C:1F:5F:23:3B:9A:DE:E9
X509v3 Authority Key Identifier:
    keyid:A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:E

Authority Information Access:
    OCSP - URI:http://ocsp.int-x3.letsencrypt.org
    CA Issuers - URI:http://cert.int-x3.letsencrypt.org/

X509v3 Subject Alternative Name:
    DNS:aaaaaaaaaaaaaaaaaaaaaaaaaaaaahkjfdshkjdshfkjdsfh.com
    DNS:security.love
X509v3 Certificate Policies:
    Policy: 2.23.140.1.2.1
    Policy: 1.3.6.1.4.1.44947.1.1.1
```

BygoneSSL Certificate Transparency Log Monitor

Fork of SSLMate's CertSpotter Log Monitor Tool

https://github.com/lanrat/certspotter

Watchlist file example:

```
insecure.design valid_at:2018-04-18
defcon.org valid_at:1993-06-21
wikipedia.org valid_at:2001-01-13
toorcon.net valid_at:2012-03-13
```

```
4cf5e402bcb5429fe3a83855592cae904c7e91b1f3c6d908e8f7e4d568496acb:
             DNS Name = insecure.design
             DNS Name = www.insecure.design
               Pubkey = ebc1a7c807a20e360aa083cf2bfafcc0468af1de8404a61a2004699cbdc394e6
               Issuer = C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation Secure Server CA
           Not Before = 2018-02-17 00:00:00 +0000 UTC
            Not After = 2021-02-16 23:59:59 +0000 UTC
            BygoneSSL = True
            Log Entry = 3 @ http://ct.example.com:6962 (Certificate)
               crt.sh = https://crt.sh/?sha256=4cf5e402bcb5429fe3a83855592cae904c7e91b1f3c6d908e8f7e4d568496acb
```

BygoneSSL Facebook Search Tool

- Requires auth to Facebook
- Faster!

BygoneSSL Search https://github.com/dxa4481/bygonessl

```
(venv) ➜  tool python bygone.py --config config
BygoneSSL with insecure.design for cert 075ce17f558df97c7e278b89d9ba471c7c845eac5d6510f2f6c8342183ac8315 good until 2018-10-11T15:09:17+0000
BygoneSSL with insecure.design for cert cd469baa874aead524cd5c9b2989c30ccf9eb2123a1119a200595883676a9bc0 good until 2018-10-11T15:09:17+0000
BygoneSSL with insecure.design for cert 4cf5e402bcb5429fe3a83855592cae904c7e91b1f3c6d908e8f7e4d568496acb good until 2021-02-16T23:59:59+0000
BygoneSSL with 0-0.site for cert fcc467c490f0eb4abf664f640cc7b8722e1b9cef2da97cd0bf78ab27a97747df good until 2019-01-05T23:59:59+0000
BygoneSSL with 0-0.site for cert 05e595a211d0c303a27ee50ac8da7bd92381c1ca5bc1fe6e3be3a49665b5b9e8 good until 2019-01-05T23:59:59+0000
BygoneSSL with 0-0.site for cert 7ff8ef22550347550b3654ab56b1164e6f383094ef6c9dcc56232432a471ecbb good until 2019-01-05T23:59:59+0000
BygoneSSL with 0-0.site for cert b8a08d44a56c9ea1084877603a2c0c3fac51dec0248bd4ea0253d6974b4f98f6 good until 2019-01-05T23:59:59+0000
BygoneSSL with 0-0.site for cert 0479c87db202f77a2407b2045fd70514f9d96924c3fe00fb2ff9a148e9cbec6c good until 2018-12-21T23:59:59+0000
```

Unanswered Questions

- How do you give notice when revolving a certificate to its alt-names?
  - How much notice?
- Revocation is broken a best....
  - Our demo certificate has been revoked for months, still works fine

Things you can do to protect your domain

- Use the `Expect-CT` HTTP header with `enforce` to ensure that only CT logged certs will be trusted for your domain
  - If a previous owners certificate is in CT logs, request the CA revoke it
    - Hope user checks CRL lists or OCSP
- We should continuously monitor CT logs for old certs
  - CT has only been required for non-EV since April 2018
    - Only required for certificates issued after April
  - Check currently owned domains as well for older certificates
  - Use CertSpotter with BygoneSSL to monitor logs

Things the internet can do

- Registrars could show pre-existing certificates for domain registrations
  - Include related alt-names
- CAs could only issue short lived certificates
  - Let’s Encrypt!
- CAs should not issue certificates valid for longer than domain registration
- Be careful with subject alt-names
  - If you’re a hosting client domains, check CRL’s and replace certs as needed

Questions?

https://insecure.design

CertSpotter https://github.com/lanrat/certspotter

BygoneSSL Search https://github.com/dxa4481/bygonessl