Lost and Found Certificates

Ian Foster & Dylan Ayrey

Who We Are

Ian

CertGraph

https://dns.coffee

https://lanrat.com

https://github.com/lanrat

@LANRAT

Dylan

truffleHog

WPA2-HalfHandshake-Crack

Pastejacking

Other stuff…

https://github.com/dxa4481

bygonessl@insecure.design

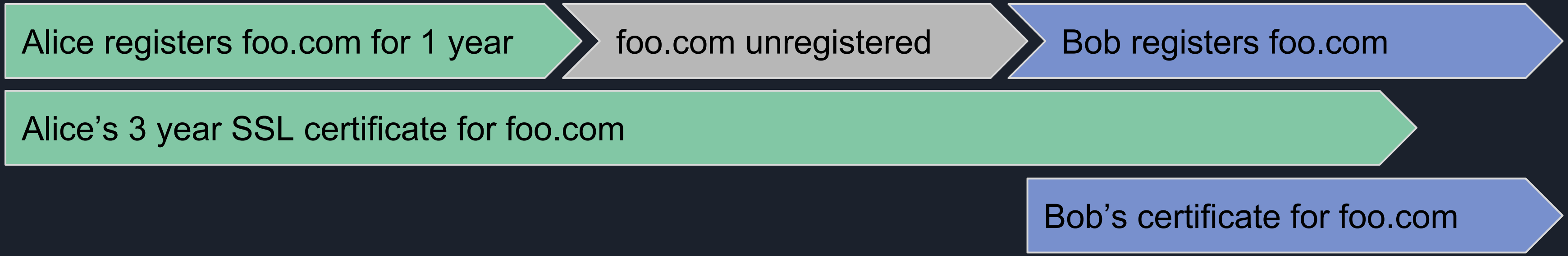
The Problem

Certificates can outlive a domain’s ownership

Old owner retains a valid SSL certificate through the next owner

How can you know?

- Buy a new domain… hope for the best?
- Prior to 2013 no visibility



Alice registers foo.com for 1 year

foo.com unregistered

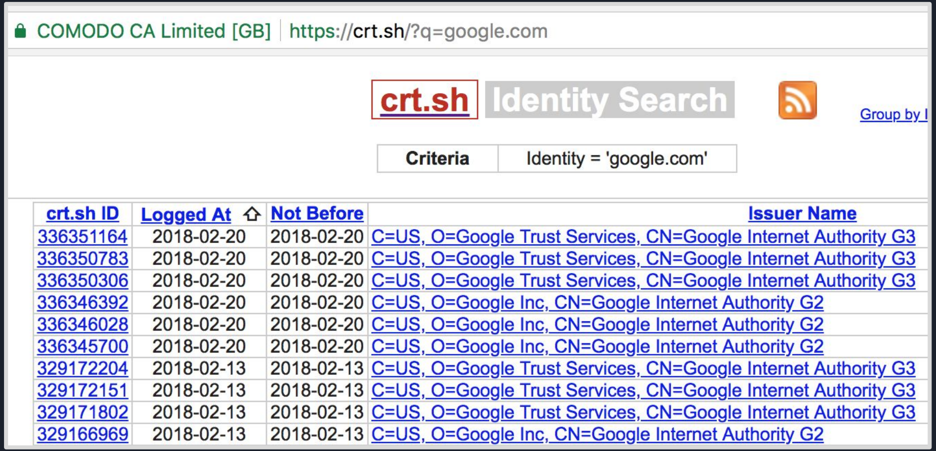
Bob registers foo.com

Alice’s 3 year SSL certificate for foo.com

Bob’s certificate for foo.com

Certificate Transparency!

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



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

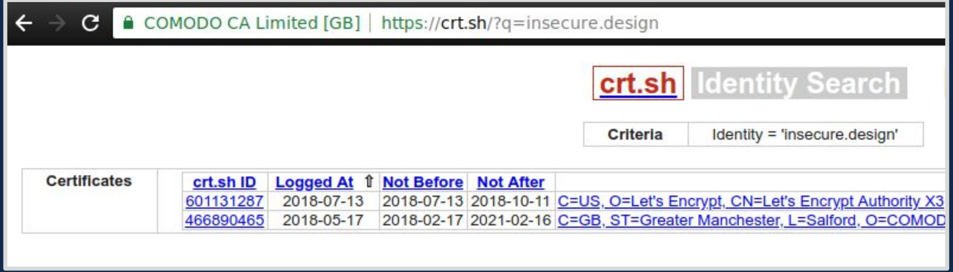
crt.sh Identity Search

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*



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

crt.sh Identity Search

Criteria	Identity = 'insecure.design'

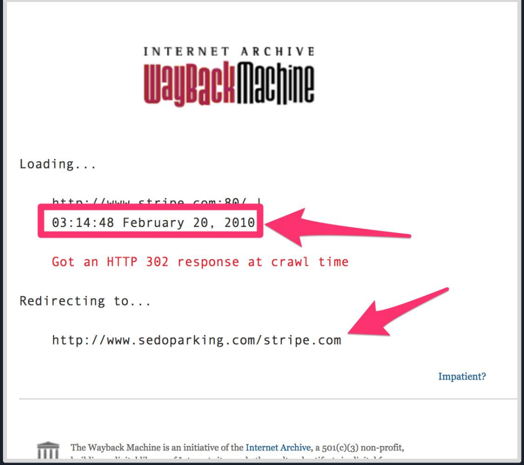
Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	
601131287	2018-07-13	2018-07-13	2018-10-11	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
466890465	2018-05-17	2018-02-17	2021-02-16	C=GB, ST=Greater Manchester, L=Salford, O=COMOD

A significant example

`stripe.com`

Stripe 2010

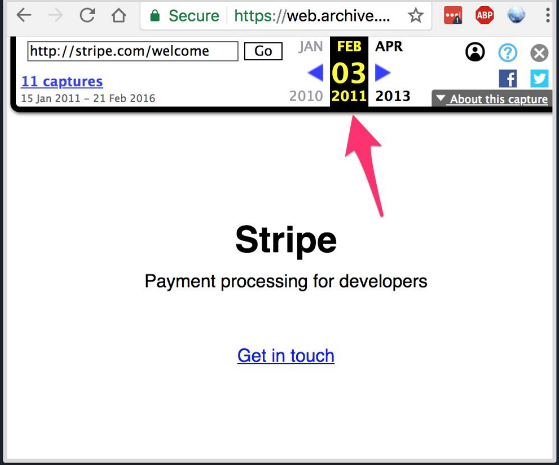


```
Loading...

    http://www.stripe.com:80/ |
    03:14:48 February 20, 2010

    Got an HTTP 302 response at crawl time

Redirecting to...

    http://www.sedoparking.com/stripe.com
```

Impatient?

The Wayback Machine is an initiative of the Internet Archive, a 501(c)(3) non-profit,

Stripe 2011

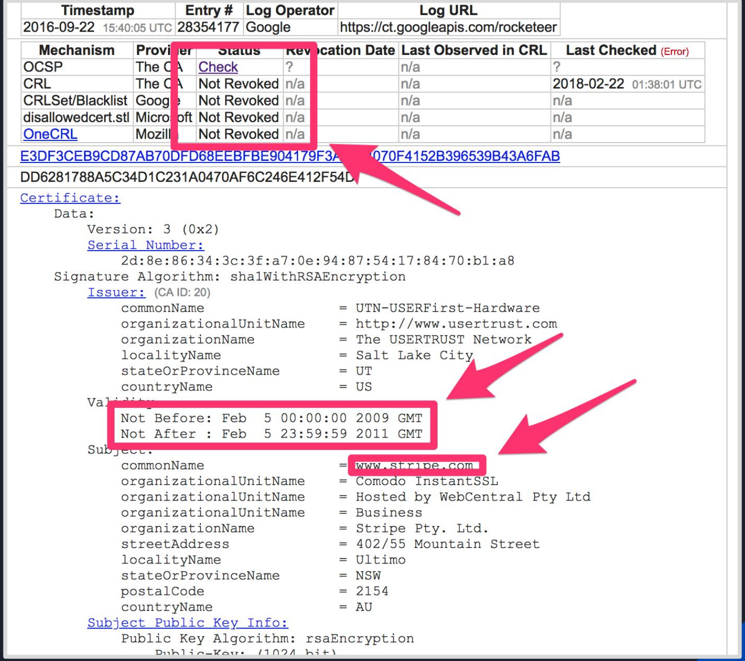


Stripe

Payment processing for developers

Get in touch

Certificate spanning both owners



Timestamp	Entry #	Log Operator	Log URL
2016-09-22 15:40:05 UTC	28354177	Google	https://ct.googleapis.com/rocketeer

Mechanism	Provi er	Status	Rev cation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The C A	Check	?	n/a	?
CRL	The C A	Not Revoked	n/a	n/a	2018-02-22 01:38:01 UTC
CRLSet/Blacklist	Goog e	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Micro oft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozill	Not Revoked	n/a	n/a	n/a

E3DF3CEB9CD87AB70DFD68EEBFBE904179F3A 070F4152B396539B43A6FAB

DD6281788A5C34D1C231A0470AF6C246E412F54D

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2d:8e:86:34:3c:3f:a7:0e:94:87:54:17:84:70:b1:a8
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: (CA ID: 20)
            commonName                = UTN-USERFirst-Hardware
            organizationalUnitName    = http://www.usertrust.com
            organizationName          = The USERTRUST Network
            localityName              = Salt Lake City
            stateOrProvinceName       = UT
            countryName               = US
        Va
            Not Before: Feb  5 00:00:00 2009 GMT
            Not After : Feb  5 23:59:59 2011 GMT
        Sub
            commonName                = www.stripe.com
            organizationalUnitName    = Comodo InstantSSL
            organizationalUnitName    = Hosted by WebCentral Pty Ltd
            organizationalUnitName    = Business
            organizationName          = Stripe Pty. Ltd.
            streetAddress             = 402/55 Mountain Street
            localityName              = Ultimo
            stateOrProvinceName       = NSW
            postalCode                = 2154
            countryName               = AU
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

How big is this issue?

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

Data

- 3 million domains, 7.7 million certs
  - 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

Not perfect: false positives/negatives

1.5M (0.45%)

Of domains tested have pre-existing certificates

25% haven't expired yet

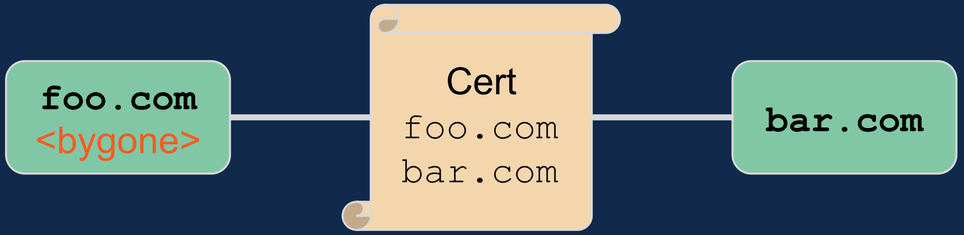
BygoneSSL

noun

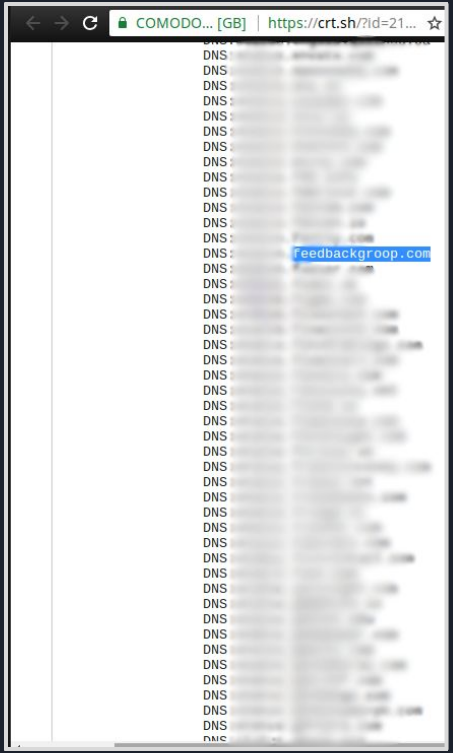
A SSL certificate created before and supersedes its domains’ current registration date

Could it be worse?

- Certificates can have many domains (alt-names)
- Certificates can contain some bygone domains and some not



CDN with 700 domains on one certificate



```
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]feedbackgroop.com
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
DNS:[redacted]
```

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

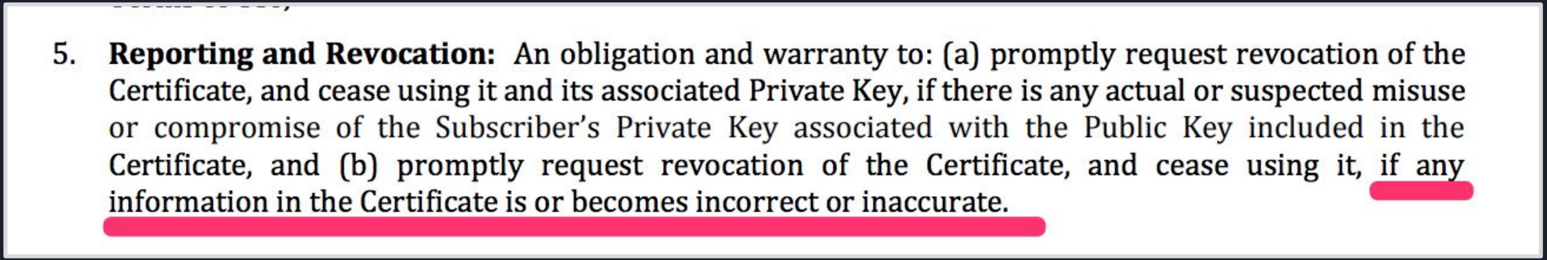
Digging deeper....

CAB CA/BROWSER FORUM

- 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

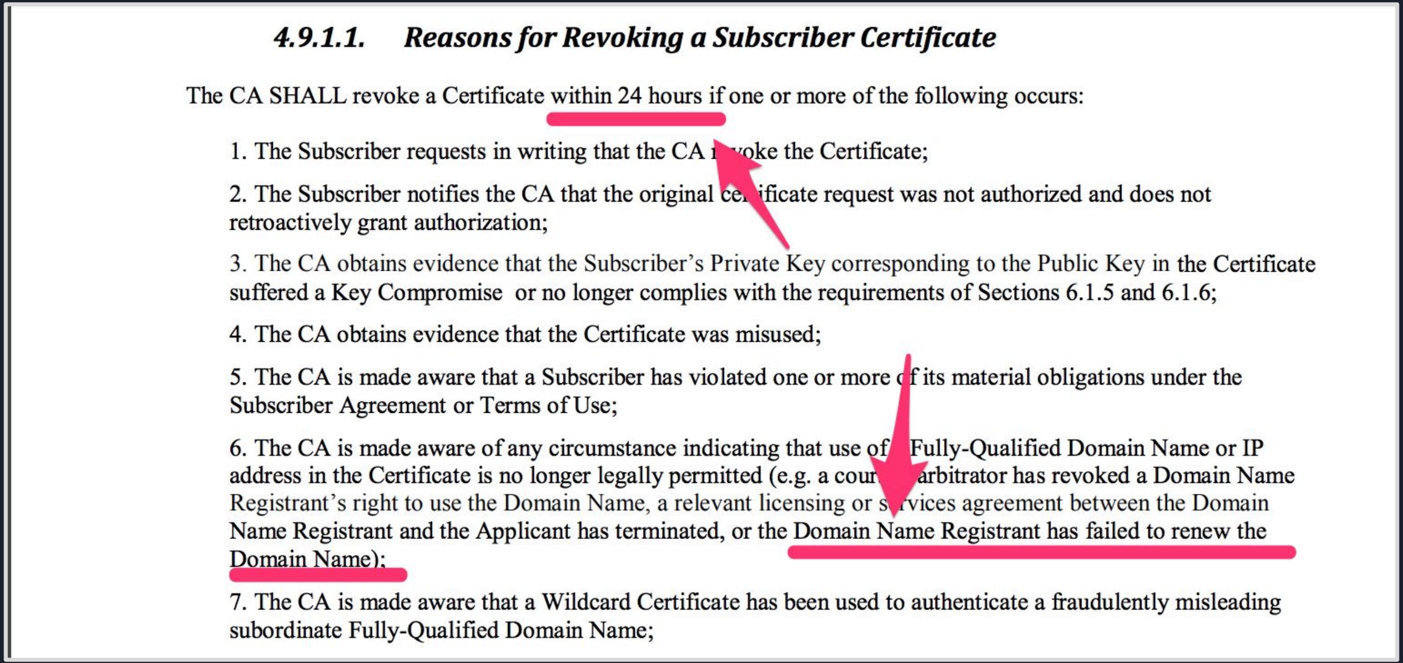
Section 9.6.3



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;

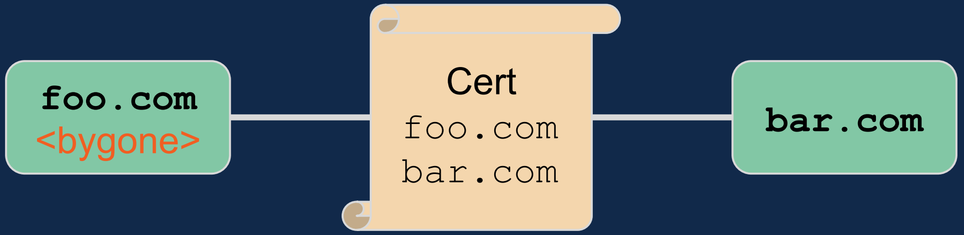
5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;

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

~4x increase!

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

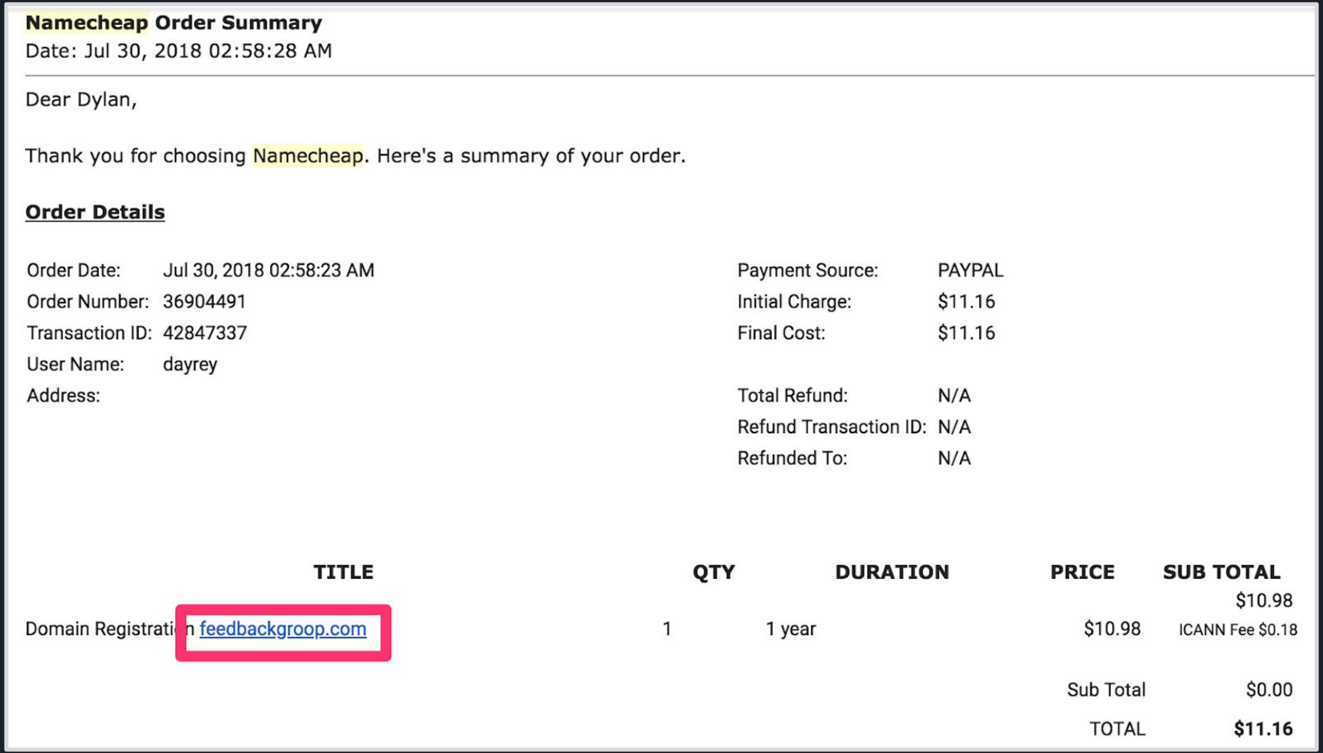
BygoneSSL Denial of Service

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!

Revisiting the CDN... we bought the bygone domain



Namecheap Order Summary
Date: Jul 30, 2018 02:58:28 AM

Dear Dylan,

Thank you for choosing Namecheap. Here's a summary of your order.

Order Details

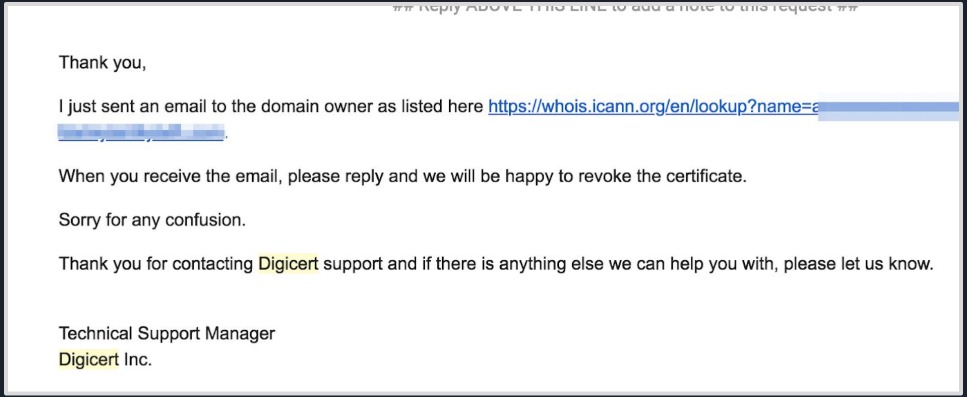
Order Date:	Jul 30, 2018 02:58:23 AM	Payment Source:	PAYPAL
Order Number:	36904491	Initial Charge:	$11.16
Transaction ID:	42847337	Final Cost:	$11.16
User Name:	dayrey		
Address:		Total Refund:	N/A
		Refund Transaction ID:	N/A
		Refunded To:	N/A

TITLE	QTY	DURATION	PRICE	SUB TOTAL
Domain Registration feedbackgroop.com	1	1 year	$10.98	$10.98 ICANN Fee $0.18
			Sub Total	$0.00
			TOTAL	**$11.16**

Trying to revoke test cert

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

- Few weeks turn around
- We emailed ec2-abuse@amazon.com



Reply ABOVE THIS LINE to add a note to this request

Thank you,

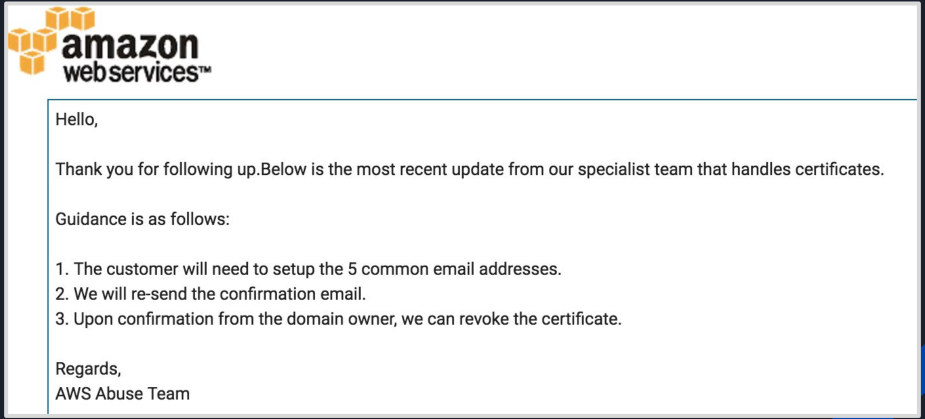
I just sent an email to the domain owner as listed here https://whois.icann.org/en/lookup?name=a[redacted].

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.

Technical Support Manager
Digicert Inc.



Hello,

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

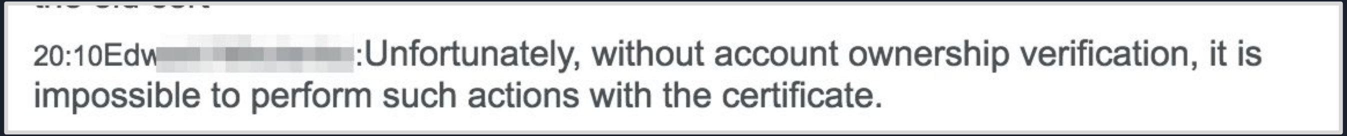
Guidance is as follows:

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

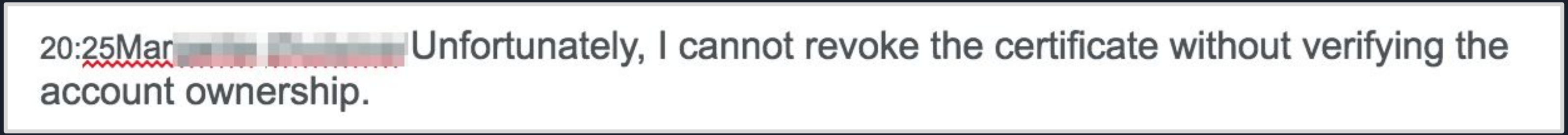
Trying to revoke with Comodo....

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

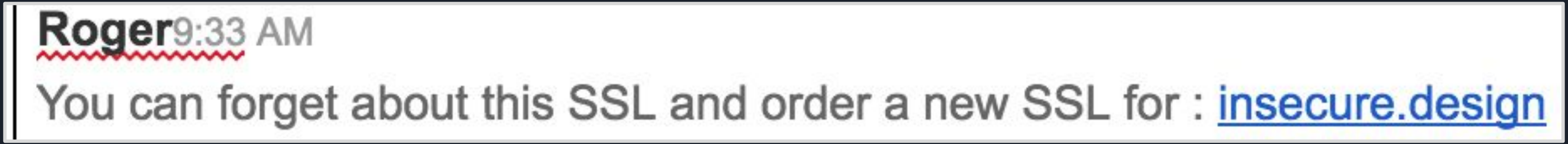


the old cert

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

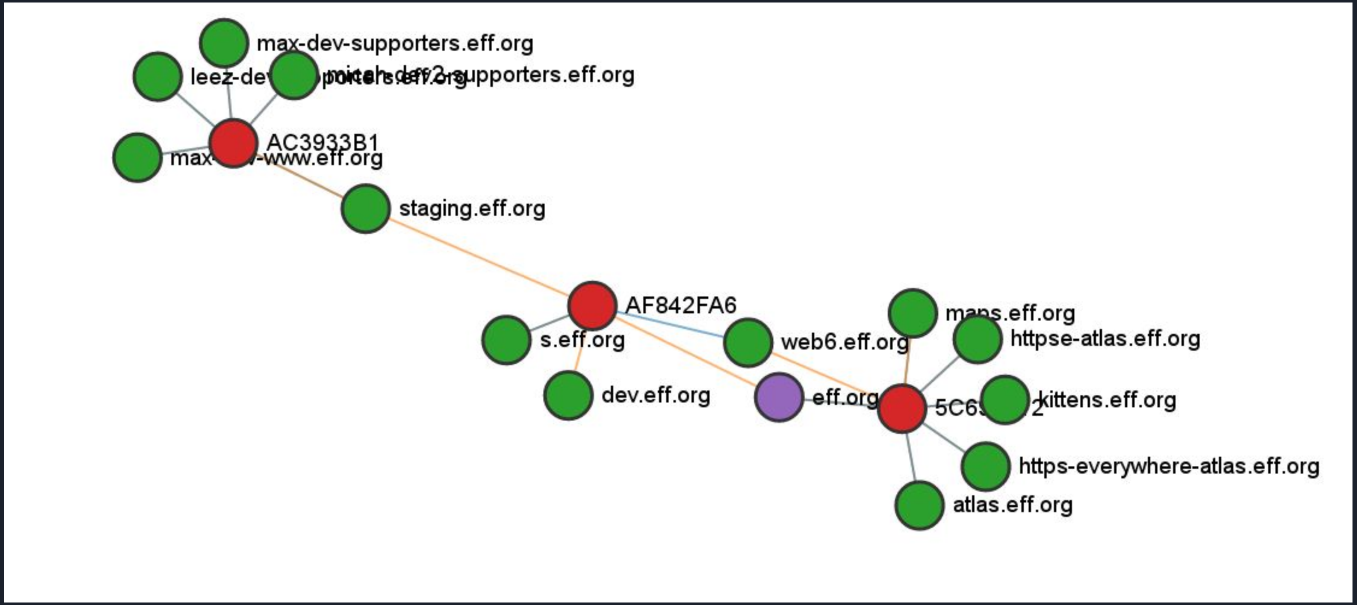
You can forget about this SSL and order a new SSL for : insecure.design

Trying to revoke with Let’s Encrypt

- Current Policy
  - require proving ownership of all domains
- Reached out to CPS Contact
  - Recognized the conflict with CA/B Forum
  - Considering changing the policy

CertGraph

An open source intelligence tool to crawl the graph of certificate alternate names

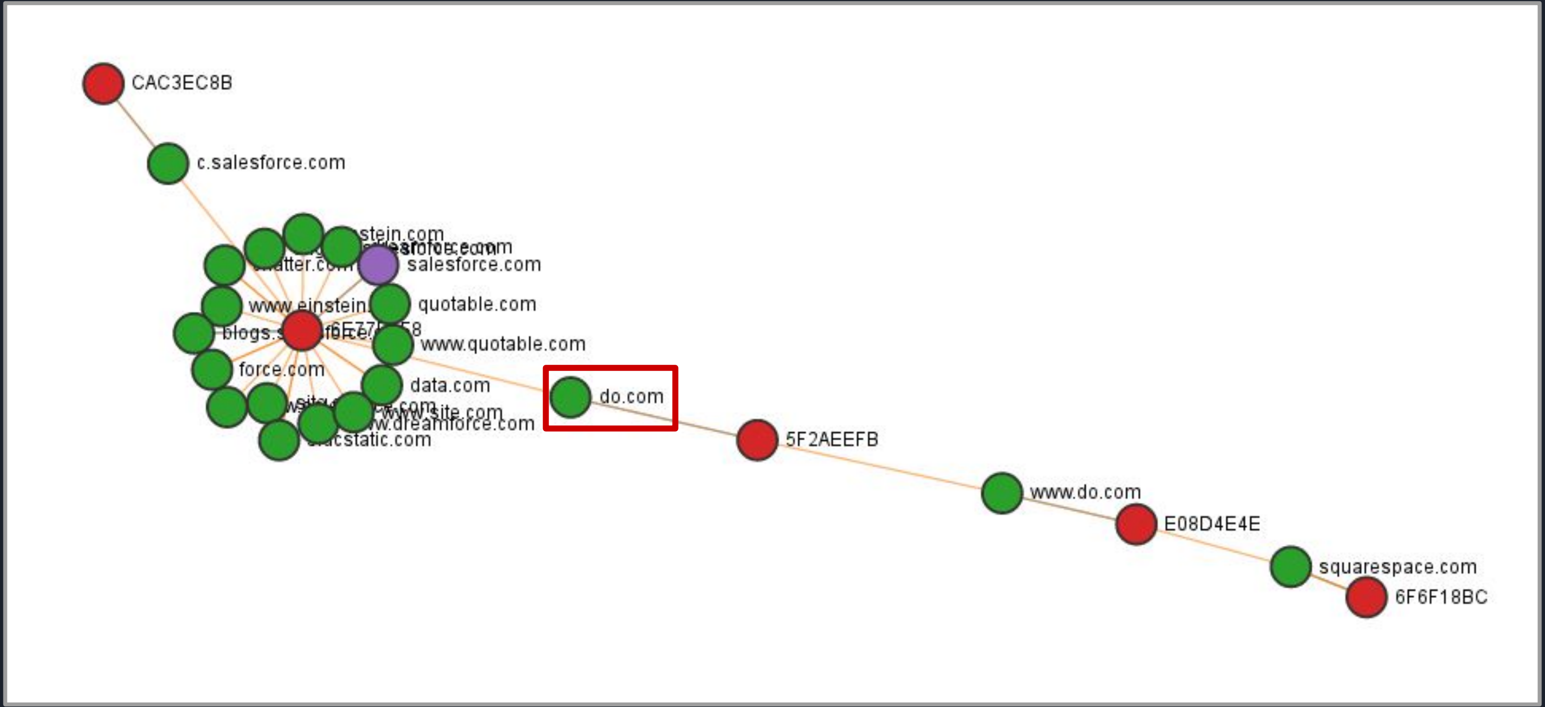


https://github.com/lanrat/certgraph

BygoneSSL DoS Detection

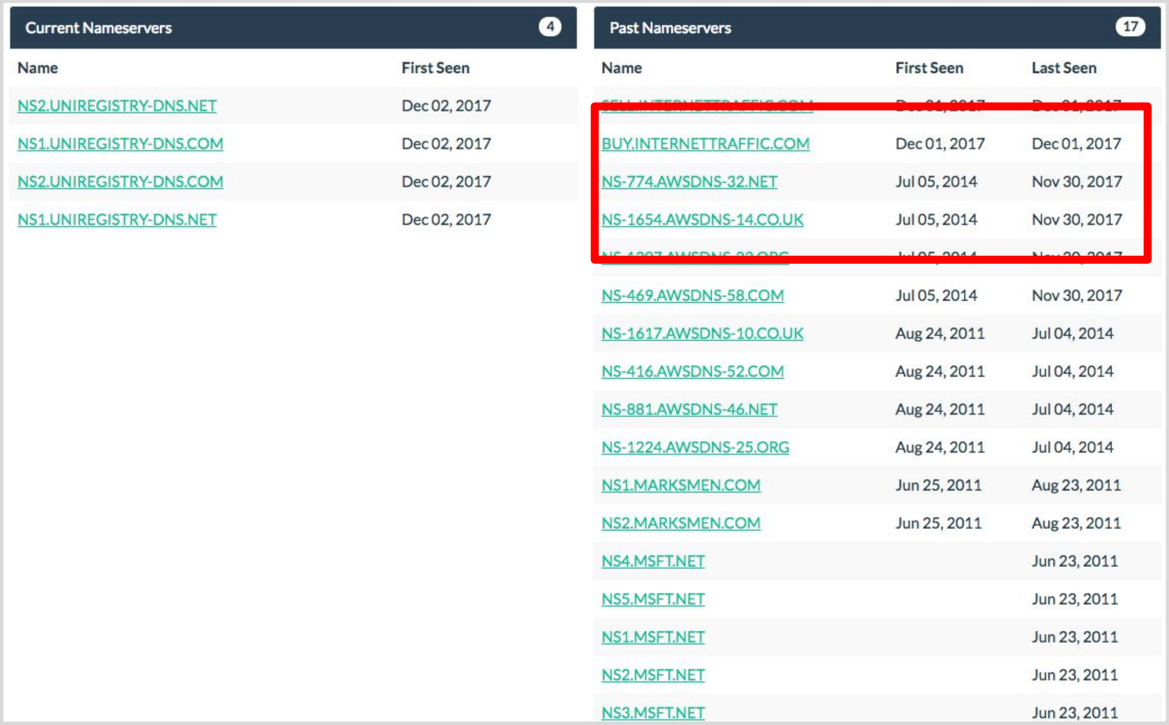
```
certgraph -depth 1 -driver google -ct-subdomains -cdn [DOMAIN]...
```

CertGraph do.com



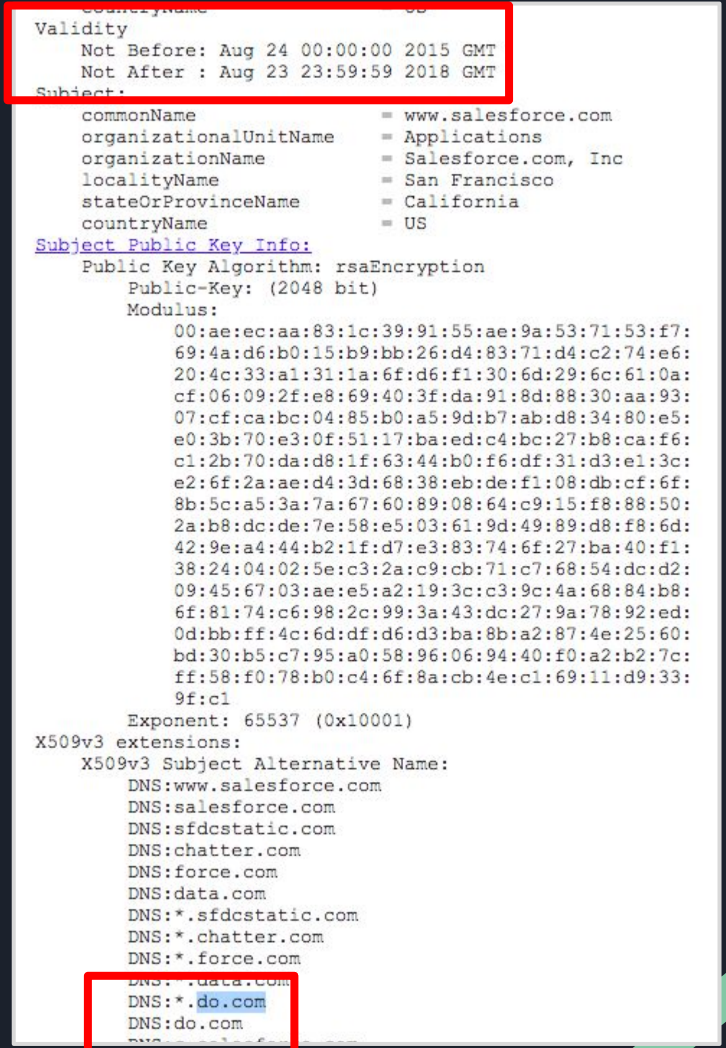
https://github.com/lanrat/certgraph

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
SELL.INTERNETTRAFFIC.COM	Dec 01, 2017	Dec 01, 2017
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
NS-1307.AWSDNS-22.ORG	Jul 05, 2014	Nov 30, 2017
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

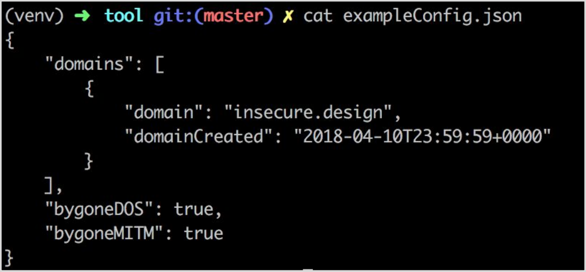


```
    countryName                 = US
Validity
    Not Before: Aug 24 00:00:00 2015 GMT
    Not After : Aug 23 23:59:59 2018 GMT
Subject:
    commonName                  = www.salesforce.com
    organizationalUnitName      = Applications
    organizationName            = Salesforce.com, Inc
    localityName                = 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
```

BygoneSSL Facebook Search Tool

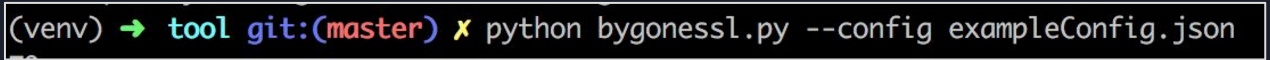
- Requires Facebook developer account
- Detects BygoneSSL DoS
- Detect BygoneSSL MitM certificates instantly
- Rate limited

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

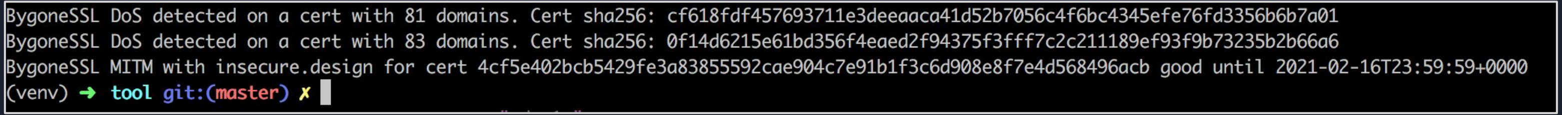


```
(venv) ➜ tool git:(master) ✗ cat exampleConfig.json
{
    "domains": [
        {
            "domain": "insecure.design",
            "domainCreated": "2018-04-10T23:59:59+0000"
        }
    ],
    "bygoneDOS": true,
    "bygoneMITM": true
}
```

facebook for developers



```
(venv) ➜ tool git:(master) ✗ python bygonessl.py --config exampleConfig.json
```



```
BygoneSSL DoS detected on a cert with 81 domains. Cert sha256: cf618fdf457693711e3deeaaca41d52b7056c4f6bc4345efe76fd3356b6b7a01
BygoneSSL DoS detected on a cert with 83 domains. Cert sha256: 0f14d6215e61bd356f4eaed2f94375f3fff7c2c211189ef93f9b73235b2b66a6
BygoneSSL MITM with insecure.design for cert 4cf5e402bcb5429fe3a83855592cae904c7e91b1f3c6d908e8f7e4d568496acb good until 2021-02-16T23:59:59+0000
(venv) ➜ tool git:(master) ✗ █
```

BygoneSSL Certificate Transparency Log Monitor

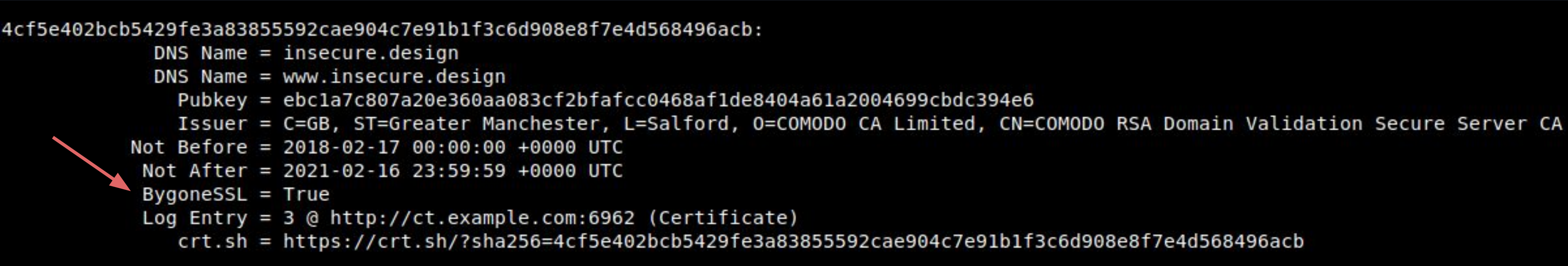
Detect BygoneSSL MitM certificates

Updated SSLMate's CertSpotter Log Monitor Tool

https://github.com/SSLMate/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
```

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 or BygoneSSL to monitor logs for MitM
  - Use CertGraph with bygonessl to monitor for DoS

Things the internet can do

- Registrars could show pre-existing certificates for domain registrations
    - Include related alt-names
- CAs could only issue short lived (90 day) certificates
    - Let’s Encrypt!
- Notify all alt-name owners of revocation
- 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
    - Best to use single certificate for each customer

Thank You

More information https://insecure.design

CertGraph https://github.com/lanrat/certgraph

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

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