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
- >1 billion certificates and growing
- Thanks Sectigo/Comodo for crt.sh!
We can find pre-existing certificates

- Note the purchase date of a given domain
- Search CT logs for certificates pre-dating registration date and valid after
- Monitor
  - Old certs may not show up in logs for years, *if ever*
A significant example: stripe.com

Certificate spanning both owners

Stripe 2010

Stripe 2011
How big is this issue?

Searched Certificate Transparency (CT) for certificates that overlap multiple domain registrations (July 2018)

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](https://dns.coffee)
Methodology: Data Flow

Processing App
- Get Certificates
- Get Timelines
- Affected Check

Database
- CT Cache
- Domain Timeline
- Results DB

Sources:
- Domain List
- CT Servers
- Historical WHOIS
Methodology: Domain Timeline

Goal: given historical whois, determine when a domain was:

- Registered
- Transferred
- Updated
- Edited
- Etc...

Not perfect: false positives/negatives

Pseudo-Code logic for determining if a domain has transferred ownership or not:

- If the expiration field has changed
  - If expiration has increased
    - If Increased by more than 2 days
      - If only year has changed to (oldDate + n years +-(1 day)): (renew)
        - If emails differ
          - Protection changes
            - Renew + protection
          - Protection unchanged
            - Does registrar change?
              - Transfer
            - Same registrar
              - Updated info.
        - Emails same
          - renew
          - Expiration is new date with no relation to previous date
            - Transfer
          - Increased by less than 2 days
            - Unknown, likely glitch
          - If expiration has decreased
            - by more than 2 days
              - Transfer
            - Decreased by < 2 days
              - Registrar glitch
  - Expiration unchanged
    - No change or change I don’t care about
1.5M (0.45%)

Of domains tested have pre-existing certificates

25% haven’t expired yet (at time of research)
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
Can we revoke these certs?

If we can’t...

- Spend $$$ on a domain, you’re screwed for years
- Bad guys could squat on desirable domains
- Cry 😞

If we can revoke...

- You can take down production certs you don’t own
- You can DoS websites
Digging deeper....

- Rules that attempt to capture minimum requirements how CA's operate
- If broken user-agents 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.

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
4. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

The CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. The CA obtains evidence that the Certificate was misused;
3. 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;
4. 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);
5. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. The CA is made aware of a material change in the information contained in the Certificate;

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

If revoked, may cause DoS for bar.com if still in use.
7M (2.05%)

Of domains share a certificate with bygone domains

~4x increase!

41% haven't expired yet (at time of research)
Sounds like we can break stuff....
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 an in use 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
Order Number: 36904491
Transaction ID: 42847337
User Name: dayrey
Address:

<table>
<thead>
<tr>
<th>TITLE</th>
<th>QTY</th>
<th>DURATION</th>
<th>PRICE</th>
<th>SUB TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Registrant: feedbackroop.com</td>
<td>1</td>
<td>1 year</td>
<td>$10.98</td>
<td>$10.98</td>
</tr>
</tbody>
</table>

Sub Total: $0.00
TOTAL: $11.16
Attempting to Revoke a BygoneSSL Certificate

- Not all CA’s have a way to contact them if you are not the certificate customer for revocation
  - email/CPS/support form/web form/etc.?  
- Tested revoking our certificate on 4 different CA’s
  - Revocation took from a day to a few weeks, some never revoked...
  - One CA refused to revoke and a support representative tried to sell us a new certificate instead.
  - ACME powered CA’s require proving ownership of all domains in a certificate.
    - ACME: at the time of testing

In many cases, the current state of revocation is broken :(  

CertGraph

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

Example graph of eff.org using only HTTPS

BygoneSSL DoS Detection

certgraph -depth 1 -driver google -ct-subdomains -cdn -dns -tldplus1 [DOMAIN]...
CertGraph salesforce -> squarespace

https://github.com/lanrat/certgraph
Example: do.com
BygoneSSL Facebook Search Tool

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

- Requires Facebook developer account
- Detects BygoneSSL DoS
- Detect BygoneSSL MitM certificates instantly
- Rate limited
BygoneSSL Certificate Transparency Log Monitor

Detect BygoneSSL MitM certificates (not DoS)
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
Things site owners can do to protect their domain

- 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 2018
  - 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

- If a previous owners certificate is in CT logs, request the CA revoke it
  - Hope user checks CRL lists or OCSP

- Use the `Expect-CT` HTTP header with `enforce` to ensure that only CT logged certs will be trusted for your domain
  - Useful for User-Agents that are CT aware but do not enforce
Suggestions for the internet and CA/B Forum:

- Registrars could show pre-existing certificates for domain registrations
  - Include related alt-names & sub-domains
  - Offer automatic revocation
- The shorter lived certificate the better
  - Reduces the impact and feasibility of BygoneSSL
  - Let’s Encrypt! (90 days)
- If revoking: notify all alt-name owners of revocation
- CAs should not issue certificates valid for longer than domain registration
- Be very careful with subject alt-names
  - If you’re a hosting client domains (CDN), check CRL’s and replace certs as needed
  - Best to use single certificate for each customer/domain
- Standardize & automate revocation
  - ACME does this but requires verification of all domains on certificate
Examples of how others fixed BygoneSSL

- **Cloudflare**
  - Rotates certificates so frequently the attack window is minimized
  - Does not bother to revoke older certificates

- **Google/Firebase**
  - Added automated detection for affected certificates

- **Fastly**
  - Identified affected customers and notified them to update certificates

- **GitHub Pages**
  - Each custom domain has its own certificate
  - *Was never vulnerable!
Thank You
bygonessl@insecure.design

More information https://insecure.design

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

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

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