Investigating the Practicality and Cost of Abusing Memory Errors with DNS

Project Bitfl1p by Luke Young

$ whoami

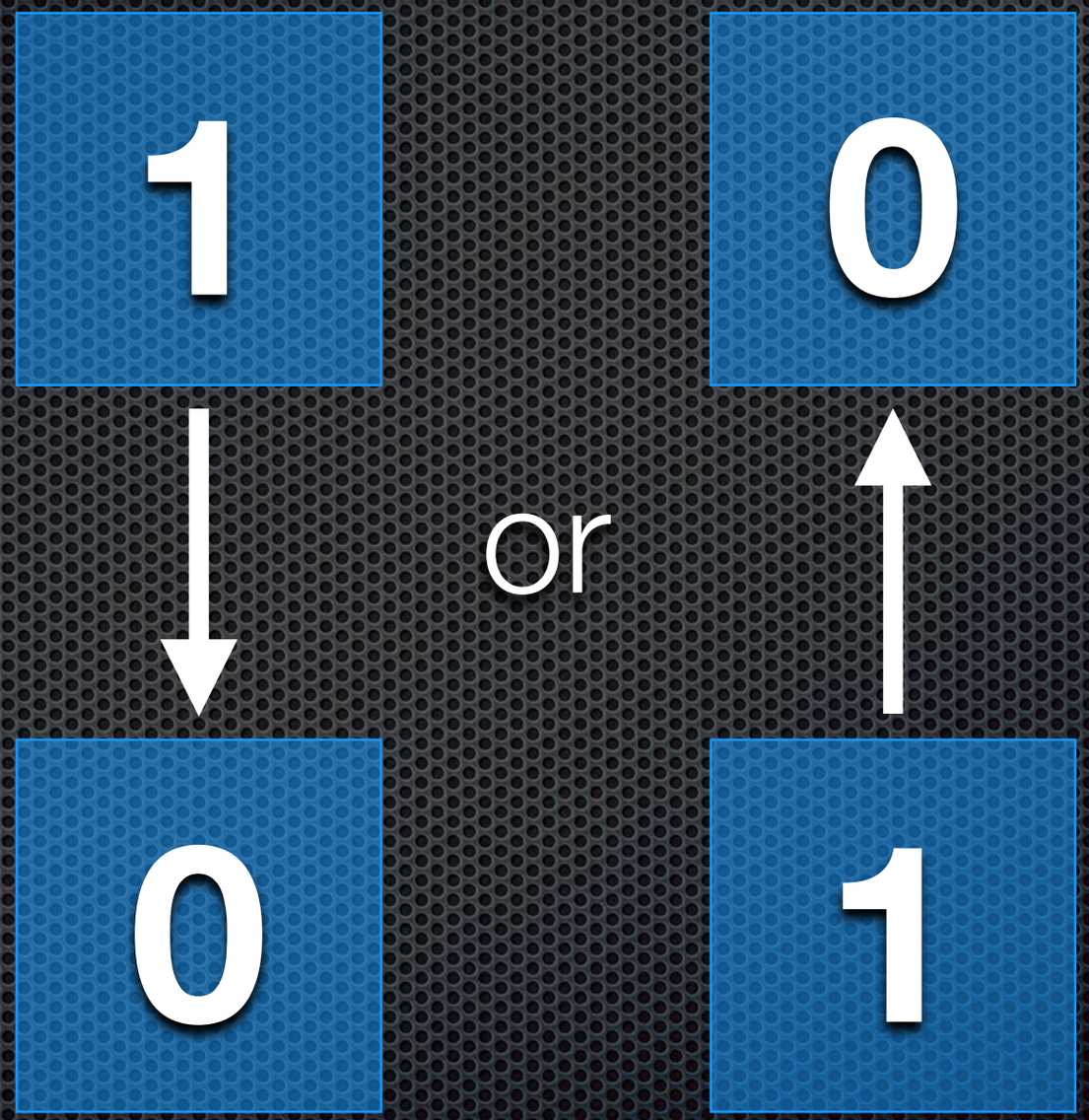
- Undergraduate Student - Sophomore
- Founder of Hydrant Labs, LLC
- This presentation is based upon research conducted as a employee of Hydrant Labs LLC and was not supported or authorized by any previous, current, or future employers with the exception of Hydrant Labs LLC.

- Email: luke@hydrantlabs.org
- LinkedIn: https://www.linkedin.com/in/innoying
- Twitter: @innoying

Agenda

- Bitflips and the history of their exploitation
- Bit-squatting and how it works
- Project Bitfl1p's use of bit-squatting
- Partial data release, other exploitation

What is a bitflip?

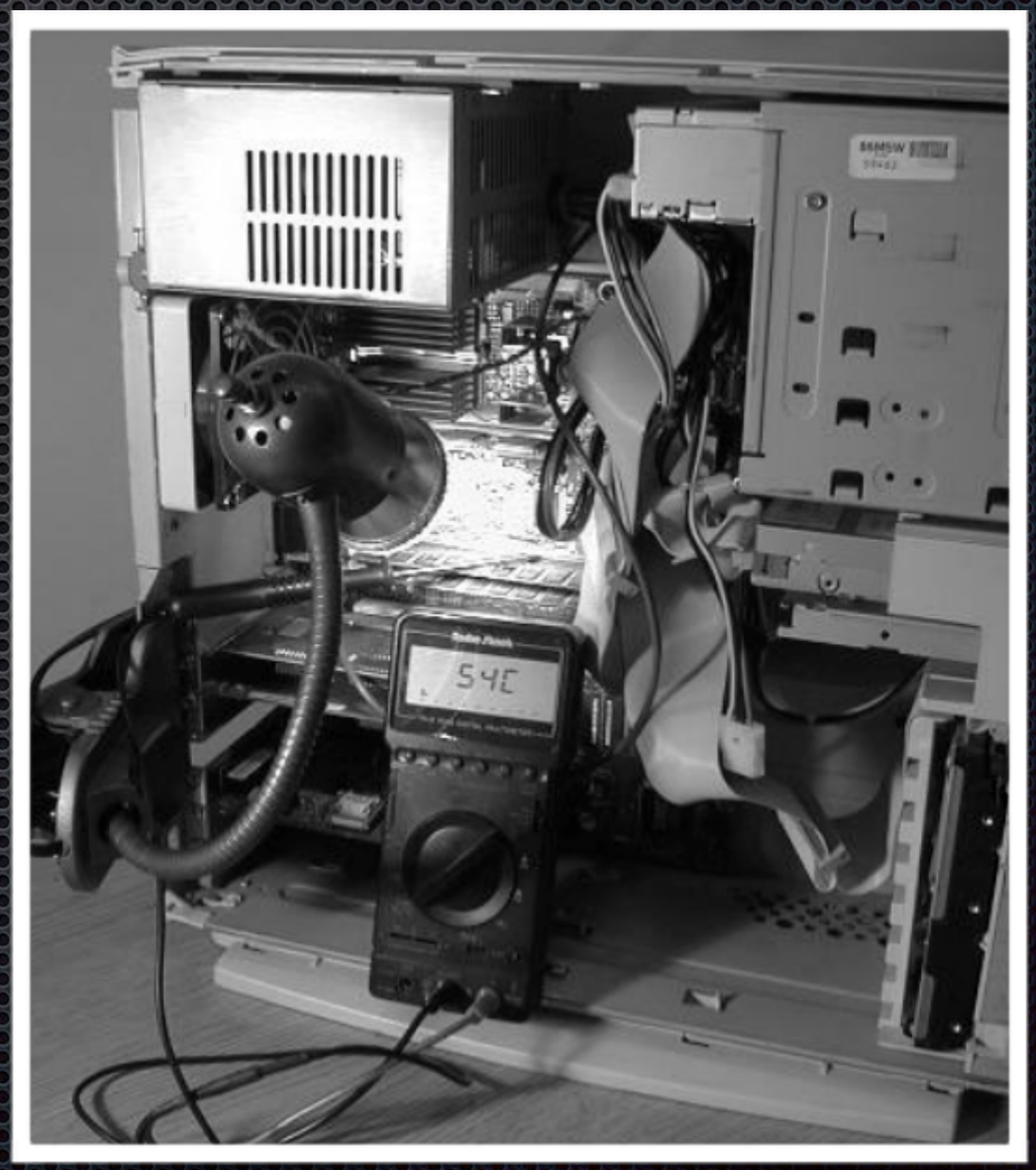


What causes a bitflip?

- Heat
- Electrical Problems
- Radioactive Contamination
- Cosmic Rays

History of bitflips

- “Using Memory Errors to Attack a Virtual Machine” - Princeton University in 2003



Rowhammer

- “Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors” - Carnegie Mellon University in 2014
- “Exploiting the DRAM rowhammer bug to gain kernel privileges” - Google’s Project Zero

What is bit-squatting?

- Named by Artem Dinaburg
- Purchasing of domain names that are one bit away from the legitimate name.

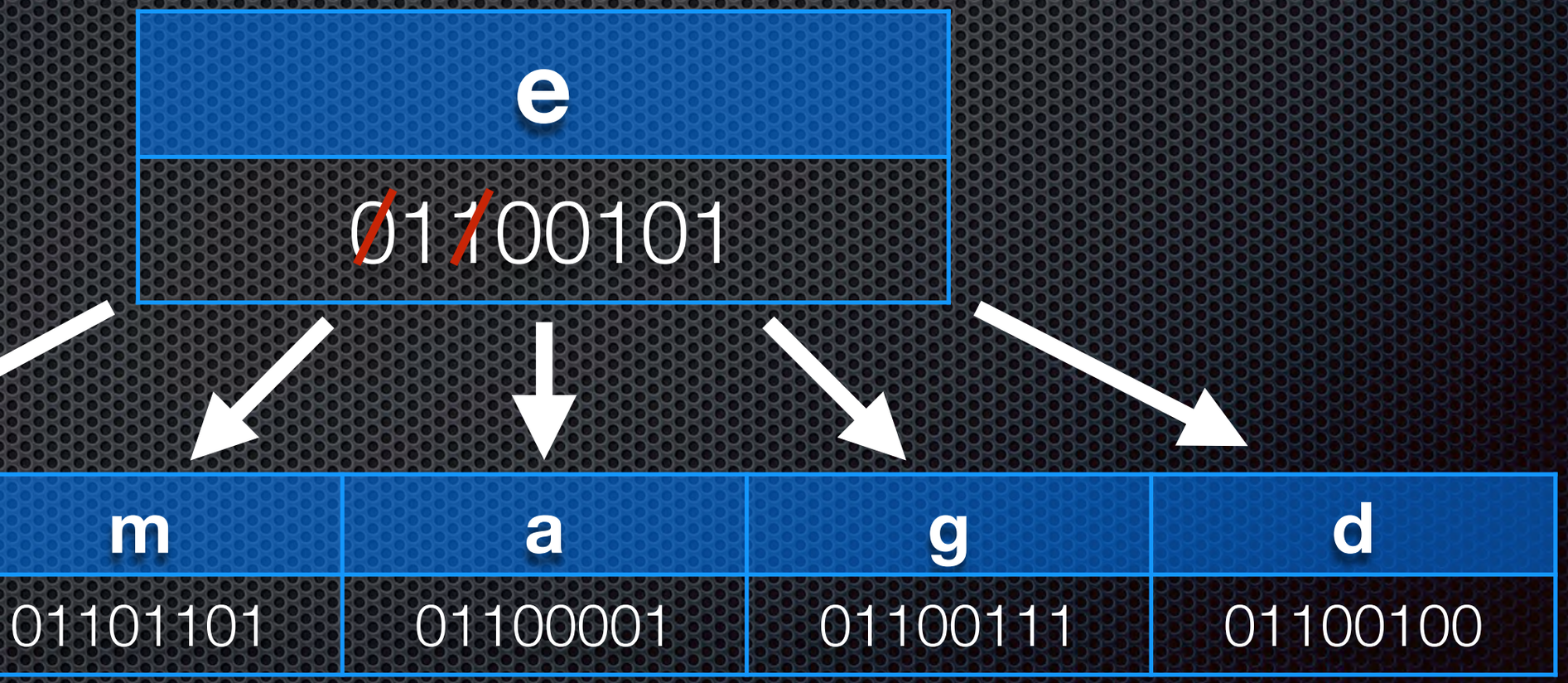
Example of bit-squatting

c	n	n	.	c	o	m
01100011	01101110	01101110	00101110	01100011	01101111	01101101

c	o	n	.	c	o	m
01100011	01101111	01101110	00101110	01100011	01101111	01101101

Generating valid bit-squats

www.defcon.org



Generating valid bit-squats

www.defcon.org

.		n
00101110	⟷	01101110

/		o
00101111	⟷	01101111

$ bf-lookup www.defcon.org

- vww.defcon.org
- uww.defcon.org
- sww.defcon.org
- gww.defcon.org
- 7ww.defcon.org
- wvw.defcon.org
- wuw.defcon.org
- wsw.defcon.org
- wgw.defcon.org
- w7w.defcon.org
- wwv.defcon.org
- wwu.defcon.org
- wws.defcon.org
- wwg.defcon.org
- ww7.defcon.org
- wwwndefcon.org
- www.eefcon.org
- www.fefcon.org
- www.lefcon.org
- www.tefcon.org
- www.ddfcon.org
- www.dgfcon.org
- www.dafcon.org
- www.dmfcon.org
- www.dufcon.org
- www.degcon.org
- www.dedcon.org
- www.debcon.org
- www.dencon.org
- www.devcon.org
- www.defbon.org
- www.defaon.org
- www.defgon.org
- www.defkon.org
- www.defson.org
- www.defcnn.org
- www.defcmn.org
- www.defckn.org
- www.defcgn.org
- www.defcoo.org
- www.defcol.org
- www.defcoj.org
- www.defcof.org

Previous bit-squatting

- Artem Dinaburg - DEF CON 19
- Jaeson Schultz - DEF CON 21
- Robert Stucke - DEF CON 21

Google

google.com

Browser	DNS Resolver	HTTP Server

Typed

Query A Record:
google.com

→

Disk & Memory

Response A Record:
216.58.216.206

←

Memory

HTTP GET /
Host: google.com

→

Disk & Memory

HTTP 200
img (gstatic.com/logo)

←

Memory

Query A Record:
gstatic.com

→

Disk & Memory

Response A Record:
216.58.216.195

←

Memory

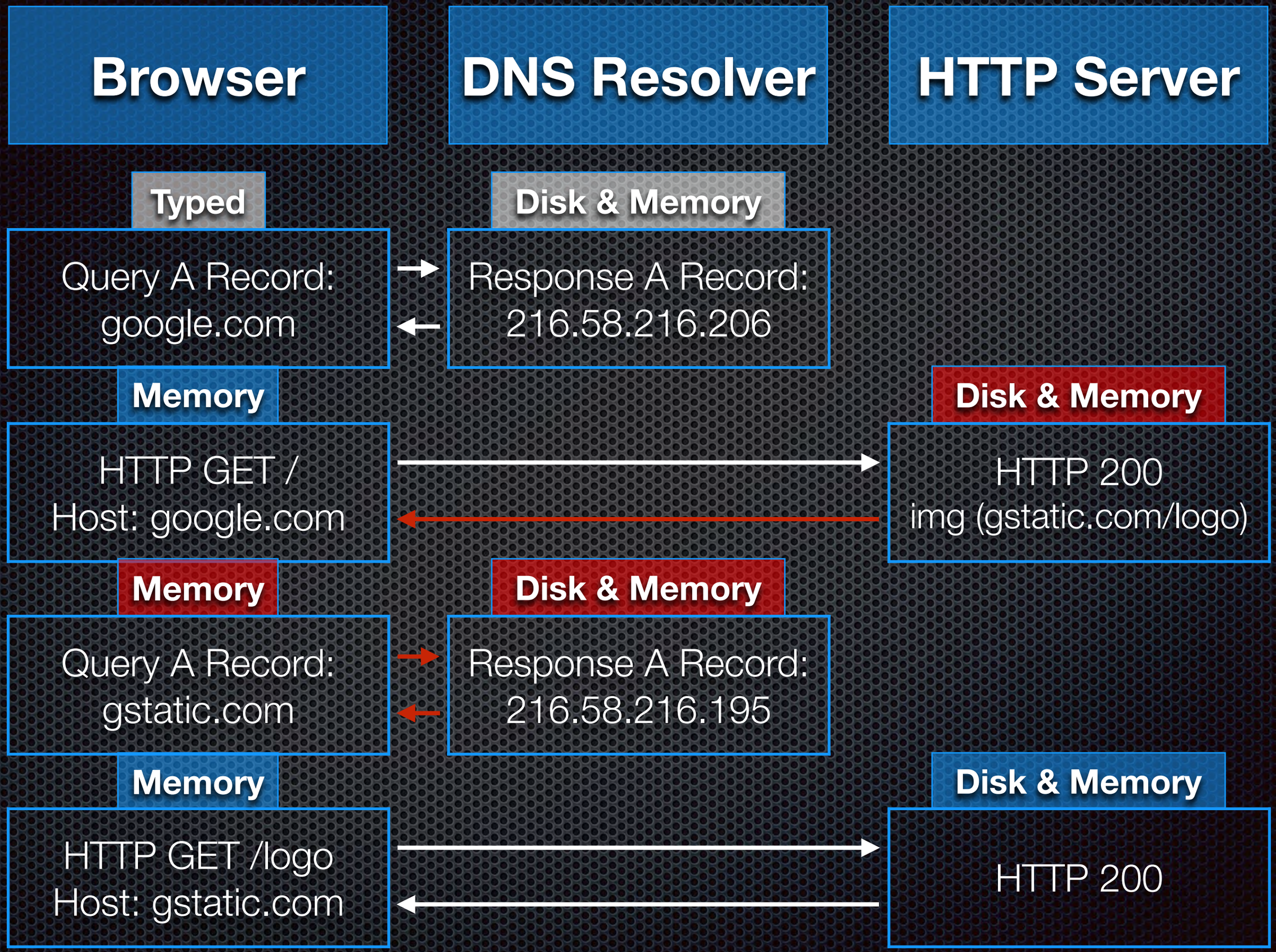
HTTP GET /logo
Host: gstatic.com

→

Disk & Memory

HTTP 200

←


Browser
DNS Resolver
HTTP Server
Typed
Query A Record:
google.com
Disk & Memory
Response A Record:
216.58.216.206
Memory
HTTP GET /
Host: google.com
Disk & Memory
HTTP 200
img (gstatic.com/logo)
Memory
Query A Record:
gstatic.com
Disk & Memory
Response A Record:
216.58.216.195
Memory
HTTP GET /logo
Host: gstatic.com
Disk & Memory
HTTP 200

What is Project Bitfl1p?

- Detect and analyze the frequency of bit flips for an average internet user through the use of bit-squatting
- 336 Domains
- Wildcard SSL certificates
- IPv4 and IPv6 support
- Additional tracking

Selecting a host (Ramnode)

- Multiple IPv4 addresses
- IPv6 support
- Smaller
- High and cheap bandwidth
- Hosted on 2GB RAM, 2 IPv4, a /64 IPv6 addresses, 80GB SSD cached, 3TB bandwidth a month
- Price/Month: $15.50 USD

Selecting domains

- Captured traffic for a day
- Purchased flips of top (interesting) domains

googleusercontent.com

- Chosen because it serves images for Google
- Long name, increases probability of a flip

googleusercontent.com

- coogleusercontent.com
- eoogleusercontent.com
- ggogleusercontent.com
- gkogleusercontent.com
- gmogleusercontent.com
- gnogleusercontent.com
- goggleusercontent.com
- gokgleusercontent.com
- gomgleusercontent.com
- gongleusercontent.com
- goocleusercontent.com
- gooeleusercontent.com
- googdeusercontent.com
- googheusercontent.com
- googlausercontent.com
- googldusercontent.com
- google5sercontent.com
- googleqsercontent.com
- googletsercontent.com
- googleu3ercontent.com
- googleucercontent.com
- googleuqercontent.com
- googleurercontent.com
- googleusdrcontent.com
- googleuse2content.com
- googleusepcontent.com
- googleuseraontent.com
- googleuserbontent.com
- googleusercgntent.com
- googleuserckntent.com
- googleusercmntent.com
- googleusercnntent.com
- googleusercoftent.com
- googleusercojtent.com
- googleusercoltent.com
- googleusercon4ent.com
- googleusercondent.com
- googleuserconpent.com
- googleusercontdnt.com
- googleuserconteft.com
- googleusercontejt.com
- googleusercontelt.com
- googleuserconten4.com
- googleusercontend.com
- googleusercontenp.com
- googleusercontenu.com
- googleusercontenv.com
- googleuserconteot.com
- googleusercontgnt.com
- googleusercontmnt.com
- googleusercontunt.com
- googleuserconuent.com
- googleuserconvent.com
- googleusergontent.com
- googleuserkontent.com
- googleusersontent.com
- googleusescontent.com
- googleusevcontent.com
- googleusezcontent.com
- googleusgrcontent.com
- googleusmrcontent.com
- googleusurcontent.com
- googleuwercontent.com
- googlewsercontent.com
- googlgusercontent.com
- googlmusercontent.com
- googluusercontent.com
- googmeusercontent.com
- googneusercontent.com
- gooooleusercontent.com
- goowleusercontent.com
- woogleusercontent.com

Panic...

```
➜  ~  sudo nc -l 80
GET /attachment/u/0/?ui=2&ik=5c6a36c81d&view=att&th=14b764c34894e1cd&attid=0.1.1&disp=sa
fe&zw&saduie=AG9B_P_1fvIEcxFQKdB_mG4pfaVs&sadet=1424920930164&sads=S1v5A3uDsew-PyFHZd-2J
BxpvEI HTTP/1.1
Host: mail-attachment.googleusercontent.com
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, l
ike Gecko) Chrome/40.0.2214.111 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

➜  ~
```

More panic...

- mail-attachment.googleusercontent.com - Mail Attachments
- oauth.googleusercontent.com - OAuth authentication
- themes.googleusercontent.com - Google fonts
- webcache.googleusercontent.com - Google cached pages
- translate.googleusercontent.com - Google translated webpages

cloudfront.net

- CDN for Amazon CloudFront
- Commonly used to serve JS, CSS, and media
- 43 possible bit-squats, 4 already registered
- Registered 39 of them

cloudfront.net

- aloudfront.net
- bloudfront.net
- cdoudfront.net
- clgudfront.net
- clkudfront.net
- clmudfront.net
- clnudfront.net
- clo5dfront.net
- cloqdfront.net
- choudfront.net
- clotdfront.net
- cloudbront.net
- cloudf2ont.net
- cloudfbont.net
- cloudfpont.net
- cloudfrgnt.net
- cloudfrknt.net
- cloudfrmnt.net
- cloudfrnnt.net
- cloudfroft.net
- cloudfrojt.net
- cloudfrolt.net
- cloudfron4.net
- cloudfrond.net
- cloudfronp.net
- cloudfronu.net
- cloudfronv.net
- cloudfroot.net
- cloudfsont.net
- cloudfvont.net
- cloudfzont.net
- cloudnront.net
- cloudvront.net
- clouefront.net
- cloulfront.net
- cmoudfront.net
- cnoudfront.net
- kloudfront.net
- sloudfront.net

amazonaws.com

- Serves pretty much all AWS services as subdomains excluding CloudFront.
- Includes Amazon S3, ELB, and EC2
- 38 possible bit-squats, 37 were registered
- 33 were already registered by Amazon!

- **amazonass.com**
- s3namazonaws.com
- compute-1namazonaws.com
- compute-2namazonaws.com
- elbnamazonaws.com

doubleclick.net

- Serves Google Ads
- Mainly via JavaScript
- 45 possible bit-squats, 19 already registered

doubleclick.net

- dgubleclick.net
- dkubleclick.net
- dnubleclick.net
- dmubleclick.net
- doqbleclick.net
- dotbleclick.net
- doublecliak.net
- doubleblick.net
- doubleclibk.net
- doublecligk.net
- doubleclicc.net
- doubleclikk.net
- doubleclisk.net
- doubleclmck.net
- doublecnick.net
- doublecmick.net
- doublmclick.net
- doubleglick.net
- doubluclick.net
- doubmeclick.net
- doubneclick.net
- doucleclick.net
- doufleclick.net
- doujleclick.net
- dowbleclick.net
- dourleclick.net

apple.com

- Most apple services are served via subdomains
- 21 possible bit-squats, 1 available: applg.com

icloud.com

- iOS/OSX devices check-in regularly
- Receives emails for icloud.com accounts
- 25 possible bit-squats, 17 registered already
- icdoud.com, iclgud.com, iclkud.com, iclmud.com, iclnud.com, icloqd.com, iclotd.com, icnoud.com

jquery.com

- JavaScript compatibility script
- Used by over 70% of the top 10,000 sites
- 26 possible bit-squats, 9 already registered

jquery.com

- jauery.com
- jqqery.com
- jpuery.com
- jqtery.com
- jqueby.com
- jquepy.com
- jquerq.com
- jquerx.com
- jquesy.com
- jquevy.com
- jqugry.com
- jquezy.com
- jqumry.com
- jsuery.com
- juuery.com

disqus.com

- Blog comment hosting service
- Roughly 750,000 thousand blogs/web-sites use it
- 27 possible bit-squats, 3 already registered

disqus.com

- dhsqus.com
- di3qus.com
- diqqus.com
- dirqus.com
- dis1us.com
- disaus.com
- disqqs.com
- disq5s.com
- disqts.com
- disqu3.com
- disquc.com
- disquq.com
- disqur.com
- disquw.com
- disqws.com
- disuus.com
- diwqus.com
- disyus.com
- dksqus.com
- dmsqus.com
- eisqus.com
- dysqus.com
- tisqus.com
- lisqus.com

google-analytics.com

- The most widely used website statistics service
- 63 possible bit-squats, 53 already registered
- googlm-analytics.com, googlg-analytics.com, googne-analytics.com, gooole-analytics.com, ggogle-analytics.com, gmogle-analytics.com, gomgle-analytics.com, gooele-analytics.com, googde-analytics.com, google-alalytics.com

sfdcstatic.com

- CDN for SalesForce
- SalesForce is one of the largest cloud computing companies in the world
- 42 possible bit-squats

sfdcstatic.com

- 3fdcstatic.com
- cfdcstatic.com
- qfdcstatic.com
- rfdcstatic.com
- sbdcstatic.com
- sfdbstatic.com
- sfdcrtatic.com
- sfdcqtatic.com
- sfdastatic.com
- sfdcctatic.com
- sfdc3tatic.com
- sfdcsdatic.com
- sfdcs4atic.com
- sfdcsta4ic.com
- sfdcstadic.com
- sfdcstatia.com
- sfdcspatic.com
- sfdcstathc.com
- sfdcstapic.com
- sfdcstatib.com
- sfdcstatis.com
- sfdcstavic.com
- sfdcstatyc.com
- sfdcstauic.com
- sfdcstatik.com
- sfdcstatig.com
- sfdcstatkc.com
- sfdcstatmc.com
- sfdcstctic.com
- sfdcstqtic.com
- sfdcsvatic.com
- sfdcsuatic.com
- sfdcwtatic.com
- sfdkstatic.com
- sfdgstatic.com
- sfecstatic.com
- sfdsstatic.com
- sflcstatic.com
- sftcstatic.com
- sndcstatic.com
- svdcstatic.com
- wfdcstatic.com

aspnetcdn.com

- Microsoft's Ajax Content Delivery Network
- Serves Microsoft sites, and many jQuery plugins
- 39 possible bit-squats, 1 registered

aspnetcdn.com

- a3pnetcdn.com
- acpnetcdn.com
- arpnetcdn.com
- aqpnetcdn.com
- as0netcdn.com
- aspfetcdn.com
- aspjetcdn.com
- aspndtcdn.com
- aspletcdn.com
- aspne4cdn.com
- aspnedcdn.com
- aspnepcdn.com
- aspnetadn.com
- aspnetbdn.com
- aspnetcdf.com
- aspnetcdj.com
- aspnetcdl.com
- aspnetcdo.com
- aspnetcen.com
- aspnetcln.com
- aspnetctn.com
- aspnetgdn.com
- aspnetkdn.com
- aspnetsdn.com
- aspneucdn.com
- aspnevcdn.com
- aspngtcdn.com
- aspoetcdn.com
- aspnmtcdn.com
- asqnetcdn.com
- asrnetcdn.com
- astnetcdn.com
- awpnetcdn.com
- asxnetcdn.com
- espnetcdn.com
- cspnetcdn.com
- qspnetcdn.com
- ispnetcdn.com

googleapis.com

- Google's JS Content Delivery Network
- Serves Angular JS, Prototype, etc
- 39 possible bit-squats, 27 registered

googleapis.com

- coogleapis.com
- eoogleapis.com
- ggogleapis.com
- gkogleapis.com
- gmogleapis.com
- gnogleapis.com
- goggleapis.com
- gokgleapis.com
- gomgleapis.com
- goocleapis.com
- gooeleapis.com
- googdeapis.com
- googheapis.com
- googldapis.com
- googlgapis.com
- googlmapis.com
- googmeapis.com
- googneapis.com
- goowleapis.com
- gooooleapis.com
- ooogleapis.com
- woogleapis.com

gstatic.com

- Google static content hosting
- Serves pages like Chrome's connectivity test
- Also purchased by Artem Dinaburg and Robert Stucke
- 30 possible bit-squats, 11 registered

gstatic.com

- gs4atic.com
- gsdatic.com
- gspatic.com
- gsta4ic.com
- gstadic.com
- gstapic.com
- gstathc.com
- gstatia.com
- gstatib.com
- gstatig.com
- gstatkc.com
- gstatmc.com
- gstatyc.com
- gstavic.com
- gstauic.com
- gstctic.com
- gstqtic.com
- gsuatic.com
- gsvatic.com

fbcdn.net

- Facebook's CDN
- 19 possible bit-squats, 3 available
- fbadn.net, fbcdj.net, frcdn.net

ytimg.com

- YouTube's CDN
- 22 possible bit-squats, 3 available
- ytieg.com, yti-g.com, y4img.com

twimg.com

- Twitter's CDN
- 23 possible bit-squats, 9 available
- 4wimg.com, t7img.com, twhmg.com, twi-g.com, twimw.com, twilg.com, twkmg.com, twmmg.com, uwimg.com

Is this even a problem?

- 1.36 Million DNS Queries. Per Day.
- 12,000 SSL connections/day

Purchasing 337 Domains

on a college budget

Coupons!

1&1


Sales: 1 (877) 461-2631
Para español por favor haz clic aquí
US
Partner programs
Help & Contact
Login
1&1
Domain Names
Websites
Web Hosting
Servers
E-Mail & Office
eCommerce
Your search term
.nyc
Starting at
$0.99
first year*
Order now!
1&1 DOMAINS
AT UNBEATABLE PRICES!
Enter your desired web address
MyWebsite
Create your own successful website
Hosting
For developers and professionals
Online Store
Sell successfully online
Virtual Servers
Speed and convenience at a great price

1&1 Internet - Account Authentication <auth@1and1.com>

to me

Dear Luke Young, (Customer ID: [redacted])

You have exceeded the limit of our current special offer.

Further orders placed under this offer will be canceled.

--
Sincerely,
Security Team
1&1 Internet, Inc.

Final statistics

- 89 from GoDaddy
- 255 from 1&1
- Average cost per domain: $1.62
- Total: $545.44

Purchasing SSL Certificates

Wildcard SSL Certificates

- $595 per wildcard certificate from DigiCert
- $595 * 337 domains = $200,000+

StartSSL

- 60$ for Class 2 Identity/Organization verification
- Issued 103 wildcard certificates
- 17 flagged for manual review, all approved

Certificates Issued

- *.aloudfront.net
- *.amazonass.com
- *.applg.com
- *.bloudfront.net
- *.cdoudfront.net
- *.choudfront.net
- *.clgudfront.net
- *.clkudfront.net
- *.clmudfront.net
- *.clnudfront.net
- *.clo5dfront.net
- *.cloqdfront.net
- *.clotdfront.net
- *.cloudbront.net
- *.cloudf2ont.net
- *.cloudfbont.net
- *.cloudfpont.net
- *.cloudfrgnt.net
- *.cloudfrknt.net
- *.cloudfrmnt.net
- *.cloudfrnnt.net
- *.cloudfroft.net
- *.cloudfrojt.net
- *.cloudfrolt.net
- *.cloudfron4.net
- *.cloudfrond.net
- *.cloudfronp.net
- *.cloudfronu.net
- *.cloudfronv.net
- *.cloudfroot.net
- *.cloudfsont.net
- *.cloudfvont.net
- *.cloudfzont.net
- *.cloudnront.net
- *.cloudvront.net
- *.clouefront.net
- *.cloulfront.net
- *.cmoudfront.net
- *.cnoudfront.net
- *.coogleapis.com
- *.dgubleclick.net
- *.dhsqus.com
- *.dkubleclick.net
- *.doubleblick.net
- *.doublecliak.net
- *.doubleclibk.net
- *.doubleclicc.net
- *.doublecligk.net
- *.doubleclikk.net
- *.doubleclisk.net
- *.doubleclmck.net
- *.doublecmick.net
- *.doublecnick.net
- *.doubleglick.net
- *.eoogleapis.com
- *.ggogle-analytics.com
- *.ggogleapis.com
- *.gkogleapis.com
- *.gmogle-analytics.com
- *.gmogleapis.com
- *.goggleapis.com
- *.gokgleapis.com
- *.gomgle-analytics.com
- *.gomgleapis.com
- *.goocleapis.com
- *.gooele-analytics.com
- *.gooeleapis.com
- *.googde-analytics.com
- *.googlm-analytics.com
- *.googne-analytics.com
- *.gooole-analytics.com
- *.goooleapis.com
- *.goowleapis.com
- *.gs4atic.com
- *.gsdatic.com
- *.gspatic.com
- *.gsta4ic.com
- *.gstadic.com
- *.gstapic.com
- *.gstathc.com
- *.gstatia.com
- *.gstatib.com
- *.gstatig.com
- *.gstatkc.com
- *.gstatmc.com
- *.gstatyc.com
- *.gstauic.com
- *.gstavic.com
- *.gstctic.com
- *.gstqtic.com
- *.gsuatic.com
- *.gsvatic.com
- *.icdoud.com
- *.iclgud.com
- *.iclkud.com
- *.iclmud.com
- *.iclnud.com
- *.icloqd.com
- *.iclotd.com
- *.icnoud.com
- *.jsuery.com
- *.kloudfront.net
- *.sloudfront.net

Login Revoked!

StartCom CertMaster (Eddy Nigg) <certmaster@startcom.org> 8/25/14

to me

To Luke Young,

Your certificate with serial number (686611) has been revoked for the following reason(s):

- no reason / see comment below.

The following comment has been added by StartCom's Administration Personnel:

Abuse! Please contact us.

** If you feel, that the reasons above are not correct,
please contact us, by replying to this message, with
your explanation!

StartCom Ltd.
StartSSL™ Certification Authority

StartCom Response

- “Most certificates really shouldn't have been issued to start with” - Eddy Nigg, COO/CTO StartCom Ltd.

Excerpt from StartCom Certificate Policy

- “The StartCom Certification Authority performs additional sanity and fraud prevention checks in order to limit accidental issuing of certificates whose domain names might be misleading and/or might be used to perform an act of fraud, identity theft or infringement of trademarks. For example domain names resembling well known brands and names like PAYPA1.COM and MICR0S0FT.COM, or when well known brands are part of the requested hostnames like FACEBOOK.DOMAIN.COM or WWW.GOOGLEME.COM.”

Potential problem domains

- *.eoogleapis.com
- *.ggogleapis.com
- *.gkogleapis.com
- *.gmogleapis.com
- *.goggleapis.com
- *.gokgleapis.com
- *.gomgleapis.com
- *.goocleapis.com
- *.gooeleapis.com
- *.goooleapis.com
- *.goowleapis.com

- *.ggogle-analytics.com
- *.gmogle-analytics.com
- *.gomgle-analytics.com
- *.gooele-analytics.com
- *.googde-analytics.com
- *.googlm-analytics.com
- *.googne-analytics.com
- *.gooole-analytics.com

Timeline

- 7/29/14 - Identity/Organization verification completed
- 8/14/14 - Certificate requests started
- 8/25/14 - Login certificate revoked
- 10/16/14 - Certificates revoked

Mass revocation

Inbox	StartSSL Certificate revoked, 17 Oct 2014 03:26 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 03:25 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 02:58 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 02:57 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 02:56 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 02:55 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 02:54 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 02:53 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 02:52 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 02:39 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 02:38 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 02:37 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 02:36 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 02:35 - has been revoked for the following re	10/16/14
Inbox	StartSSL Certificate revoked, 17 Oct 2014 02:34 - has been revoked for the following re	10/16/14

Remaining certificates

- *.applg.com
- *.jsuery.com
- *.dhsqus.com
- *.gsta4ic.com
- *.gstatig.com
- *.gs4atic.com
- *.gsdatic.com
- *.gstatib.com
- *.gspatic.com
- *.gstavic.com
- *.gsvatic.com
- *.gstctic.com
- *.gstauic.com
- *.gstatyc.com
- *.gstathc.com
- *.gsuatic.com
- *.gstqtic.com
- *.gstapic.com
- *.gstadic.com
- *.gstatmc.com
- *.gstatkc.com
- *.gstatia.com

“Everything we haven't revoked so far was considered not so problematic and hence we left them to expire naturally.”

The Future

- EFF's Let's Encrypt CA
- Other vendors

Getting noticed

- “One example would be in the gstatic.com domain that was used in the demonstrations and presentations:

  gstatic.com – October 2013 – 26 squats unregistered

  gstatic.com – October 2014 – 0 squats unregistered

  This reduction in availability was observed in other domains too, interestingly most of the gstatic squats and some of the other domains appear to have been registered by the same individual with the name servers at bitfl1p.com so at least some one is having fun :)” - x8x.net

Uh oh...

This webpage is not available

Hide details

Reload

The server at **bitfl1p.com** can't be found, because the DNS lookup failed. DNS is the network service that translates a website's name to its Internet address. This error is most often caused by having no connection to the Internet or a misconfigured network. It can also be caused by an unresponsive DNS server or a firewall preventing Google Chrome from accessing the network.

Error code: DNS_PROBE_FINISHED_NXDOMAIN

Uh oh...

```
➜ ~  dig bitfl1p.com @8.8.8.8

; <<>> DiG 9.8.3-P1 <<>> bitfl1p.com @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52382
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;bitfl1p.com.                   IN      A

;; ANSWER SECTION:
bitfl1p.com.            21440   IN      A       168.235.68.45
bitfl1p.com.            21440   IN      A       168.235.68.44

;; Query time: 43 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Mar 10 18:34:19 2015
;; MSG SIZE  rcvd: 61
```

Uh oh...

```
➜ ~  dig bitfl1p.com @75.75.75.75

; <<>> DiG 9.8.3-P1 <<>> bitfl1p.com @75.75.75.75
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 33561
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;bitfl1p.com.                   IN      A

;; Query time: 53 msec
;; SERVER: 75.75.75.75#53(75.75.75.75)
;; WHEN: Tue Mar 10 18:36:38 2015
;; MSG SIZE  rcvd: 29
```

Payment Issues (Stripe)

- Wells Fargo says they're approving the transaction
- "I had a look at that charge and we have reason to believe that that card has been associated with fraudulent activity."
- "We are indeed blocking it on our end due to a level of risk on this card that we're not willing to take. I know this a very vague reason, but for security purposes I'm limited in how much information I am able to give out."

Vendor Responses

Salesforce

- 42 domains
- Response time under 2 hours
- Transfer initiated in under 24

Amazon AWS

- 44 domains
- Timeline:
  - 6/15 - Reported
  - 6/15 - Vendor initial ACK
  - 6/18, 6/19, 6/23 - Vendor requests conference call to discuss issue, further correspondence planning
  - 6/25 - Conference Call
  - 6/30 - Domains unlocked and transfer process initiated

Apple

- 9 domains
- Timeline:
  - 6/15 - Reported
  - 6/15 - Vendor initial ACK
  - 6/17 - Domains unlocked and transfer process initiated

Facebook

- 3 domains
- Timeline:
  - 6/15 - Reported
  - 6/15 - Vendor initial ACK
  - 7/1 - Vendor requests transfer codes
  - 7/6 - Domains unlocked and transfer process initiated

Twitter

- 9 domains
- Timeline:
  - 6/15 - Reported
  - 6/17 - Vendor declines domain transfer

Google

- 152 domains
- Timeline:
  - 6/15 - Reported
  - 6/15 - Vendor initial ACK
  - 6/29 - Attempted vendor contact
  - 7/4 - Attempted vendor contact
  - 7/6 - Vendor declines domain transfer

Microsoft

- 38 domains
- Timeline:
  - 6/15 - Reported
  - 6/15 - Vendor initial ACK
  - 6/29 - Attempted vendor contact
  - 7/6 - Attempted vendor contact
  - 7/16 - Attempted vendor contact

The Data

Data Release

- 32 GB of JSON DNS logs
- Curated HTTP/HTTPS logs
- Curated SMTP logs
- Curated API logs
- More logs available on request

Project Bitfl1p - Luke Young

- Email: luke@hydrantlabs.org
- LinkedIn: https://www.linkedin.com/in/innoying
- Website (with Code & Data Dumps): www.bitfl1p.com