You’re Going to Connect to the Wrong Domain

@erbbysam

whoami

@erbbysam

Software Engineer

DC23, DC24 black badge (Badge Challenge, Co9)

The opinions expressed here are my own &

no one was phished in the creation of this presentation

Typosquatting

Humans are not perfect, we mistype domain names. A malicious person can register these mistyped domains.

Only 2 of the 61 1-keyboard letter off variants of americanexpress.com are unregistered.

Example:
qmericanexpress.com
Expires:2018-01-06T00:00:00
Created:2008-01-06T00:00:00
Updated:2017-01-06T00:00:00
Registrar:ABOVE.COMTPTYTLTD.

a	m	e	r	i	c	a	n	e	x	p	r	e	s	s
s	n	w	e	u	x	s	b	w	z	o	e	w	a	a
w	j	r	t	o	v	**w**	m	r	c	l	t	r	d	d
q	k	s	**d**	j	d	q	h	s	s		d	s	e	e
z		d	f	k	f	z	j	d	d		f	d	w	w
													x	x
													z	z

Bitsquatting

A form of typosquating, but one where the computer gets the domain name wrong by flipping a bit.

eoogle-analytics

01100101 01101111 01101111 01100111 01101100 01100101 00101101 01100001 01101110 01100001 01101100 01111001 01110100 01101001 01100011 01110011
01100111 01101111 01101111 01100111 01101100 01100101 00101101 01100001 01101110 01100001 01101100 01111001 01110100 01101001 01100011 01110011

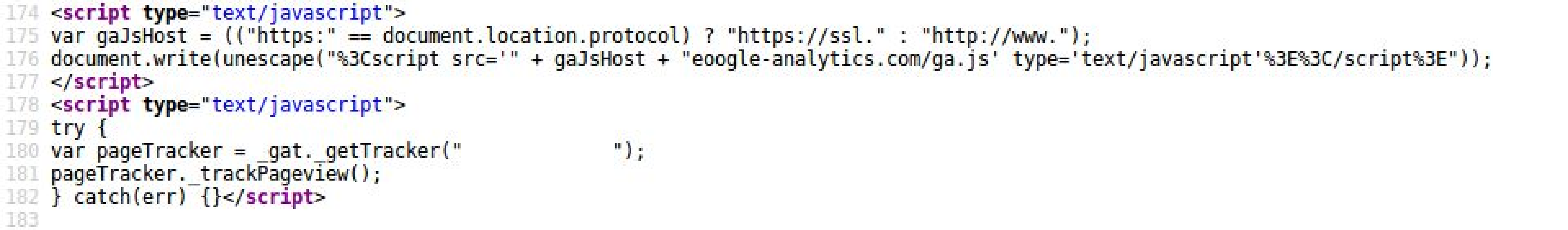
google-analytics

Bitsquatting - Searching for Domains

```
foogle-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
eoogle-analytics.com  no record
coogle-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
ooogle-analytics.com  Expires:2017-12-20T00:00:00 Created:2014-12-20T00:00:00 Updated:2017-03-08T00:00:00 Registrar:ENOM,TINC.
woogle-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
gnogle-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
gmogle-analytics.com  Expires:2018-03-22T00:00:00 Created:2016-03-22T00:00:00 Updated:2017-04-15T00:00:00 Registrar:ENOM,TINC.
gkogle-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
ggogle-analytics.com  Expires:2018-03-22T00:00:00 Created:2016-03-22T00:00:00 Updated:2017-04-15T00:00:00 Registrar:ENOM,TINC.
gongle-analytics.com  Expires:2017-09-13T00:00:00 Created:2011-09-13T00:00:00 Updated:2016-08-12T00:00:00 Registrar:MARKMONITORTINC.
gomgle-analytics.com  Expires:2018-03-22T00:00:00 Created:2016-03-22T00:00:00 Updated:2017-04-15T00:00:00 Registrar:ENOM,TINC.
gokgle-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
goggle-analytics.com  Expires:2017-06-19T00:00:00 Created:2008-06-19T00:00:00 Updated:2016-06-20T00:00:00 Registrar:NAUGUSTLIMITED,TLLC.
goofle-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
gooele-analytics.com  Expires:2018-03-22T00:00:00 Created:2016-03-22T00:00:00 Updated:2017-04-15T00:00:00 Registrar:ENOM,TINC.
goocle-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
gooole-analytics.com  Expires:2018-03-22T00:00:00 Created:2016-03-22T00:00:00 Updated:2017-04-15T00:00:00 Registrar:ENOM,TINC.
goowle-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
googme-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
googne-analytics.com  Expires:2018-03-22T00:00:00 Created:2016-03-22T00:00:00 Updated:2017-04-15T00:00:00 Registrar:ENOM,TINC.
googhe-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
googde-analytics.com  Expires:2018-03-22T00:00:00 Created:2016-03-22T00:00:00 Updated:2017-04-15T00:00:00 Registrar:ENOM,TINC.
googld-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
googlg-analytics.com  Expires:2018-03-22T00:00:00 Created:2016-03-22T00:00:00 Updated:2017-04-15T00:00:00 Registrar:ENOM,TINC.
googla-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
googlm-analytics.com  Expires:2018-03-22T00:00:00 Created:2016-03-22T00:00:00 Updated:2017-04-15T00:00:00 Registrar:ENOM,TINC.
googlu-analytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
googlemanalytics.com  Expires:2017-08-05T00:00:00 Created:2013-08-05T00:00:00 Updated:2016-08-09T00:00:00 Registrar:GODADDY.COM,TLLC
google-cnalytics.com  Expires:2017-11-17T00:00:00 Created:2014-11-17T00:00:00 Updated:2016-11-20T00:00:00 Registrar:DYNADOT,TLLC
google-enalytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
google-inalytics.com  Expires:2018-03-22T00:00:00 Created:2016-03-22T00:00:00 Updated:2017-04-15T00:00:00 Registrar:ENOM,TINC.
google-qnalytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
google-aoalytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
google-alalytics.com  Expires:2018-03-22T00:00:00 Created:2016-03-22T00:00:00 Updated:2017-04-15T00:00:00 Registrar:ENOM,TINC.
google-ajalytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
google-afalytics.com  Expires:2018-03-22T00:00:00 Created:2016-03-22T00:00:00 Updated:2017-04-15T00:00:00 Registrar:ENOM,TINC.
google-anclytics.com  Expires:2017-11-17T00:00:00 Created:2014-11-17T00:00:00 Updated:2016-11-20T00:00:00 Registrar:DYNADOT,TLLC
google-anelytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
google-anilytics.com  Expires:2017-11-17T00:00:00 Created:2014-11-17T00:00:00 Updated:2016-11-20T00:00:00 Registrar:DYNADOT,TLLC
google-anqlytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
google-anamytics.com  Expires:2017-09-14T00:00:00 Created:2011-09-14T00:00:00 Updated:2016-08-13T00:00:00 Registrar:MARKMONITORTINC.
```

Bitsquatting - Example

- **Registered eoogle-analytics.com**
- **Used Let’s Encrypt to get a TLS certificate**
- **Found a misconfigured server, but within 24 hours saw 2 “hits”**



```
<script type="text/javascript">
var gaJsHost = (("https:" == document.location.protocol) ? "https://ssl." : "http://www.");
document.write(unescape("%3Cscript src='" + gaJsHost + "eoogle-analytics.com/ga.js' type='text/javascript'%3E%3C/script%3E"));
</script>
<script type="text/javascript">
try {
var pageTracker = _gat._getTracker("              ");
pageTracker._trackPageview();
} catch(err) {}</script>
```

```
HTTPServerRequest(protocol='http', host='www.eoogle-analytics.com',
method='GET', uri='/r/]_utm.gif?[removed]', version='HTTP/1.1',
remote_ip='[removed]', headers={'Accept-Language': 'ja-JP, en-US;q=0.8',
'Accept-Encoding': 'gzip, deflate', 'X-Wap-Profile':
'http://[removed].com/[removed].xml', 'X-Getzip': 'supported', 'Host':
'www.eoogle-analytics.com', 'User-Agent': '[removed]', 'Accept-Charset': 'utf-8,
iso-8859-1, utf-16, *;q=0.7',  'Connection': 'keep-alive', 'X-Requested-With':
'com.android.browser', 'Referer': 'http://[removed].net/823.html', 'Cache-Control':
'no-cache', 'Cookie': 'VisitorID=[removed]&Exp=11/12/2018 9:13:02 AM'})
```

```
HTTPServerRequest(protocol='https',
host='www.eoogle-analytics.com', method='GET', uri='/analytics.js',
version='HTTP/1.1', remote_ip='[removed]', headers={'Save-Data':
'on', 'Accept-Language': 'en-US,en;q=0.8', 'Accept-Encoding': 'gzip,
deflate, sdch, br', 'Host': 'www.eoogle-analytics.com', 'Accept': '*/*',
'User-Agent': 'Mozilla/5.0 (Linux; Android 5.0.2; P01V
Build/LRX22G) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/58.0.3029.83 Safari/537.36', 'Connection': 'keep-alive',
'Referer': 'http://www.[removed].lk/channel/'})
```

Bitsquatting - gTLD

.got

01100111 01101111 011101**0**0

01100111 01101111 011101**1**0

.gov

.bom

0110001**0** 01101111 01101101

0110001**1** 01101111 01101101

.com

IDN Homoglyphs

IDN = “Internationalized domain name”, stored as punycode (xn--*)

Homoglyphs are 2 characters that look the same

Example:

xn--ggle-55da.com = g**оо**gle.com

xn--e1anr4f.com = **тіме**.com

IDN Homoglyphs - Identification

I wanted to conduct a survey of existing IDN homoglyph domains against popular .com domains...

3 options to gather domain names:

1) zone files (hard/impossible to acquire)
2) Certificate Transparency
3) Third party lists ($$$)

Google “pilot” CT log contains ~100 million certificates

- 400GB (compressed)
- searchable (crt.sh)
- A great source of data

IDN Homoglyphs - Identification Continued

Another reason for using Certificate Transparency - if a certificate was registered, the domain was more likely to be used

Let’s build a pipeline:

[Google CT Pilot log] → [parse CN, SAN domains] → [filter punycode .com domains (ex. xn--*.com)]

Cross Reference:

1) Pipeline list, rendered as unicode, passed through the python unidecode package (ex. □ → P)
2) Alexa top 1 million domains

End result:

1,938 CT certificates containing impersonating domains, modified Chromium unit test for punycode display status [TODO - insert github link]

IDN Homoglyphs - Cross Referenced Results

```
ĸ, 22, 0x138, "LATIN SMALL LETTER KRA"
96074858, 1509667199, xn--faceboo-jhb.com, facebooĸ.com , ĸ, facebook.com, 3, 1
86142753, 1507679999, xn--autodes-jhb.com, autodesĸ.com , ĸ, autodesk.com, 697, 1

ł, 5, 0x142, "LATIN SMALL LETTER L WITH STROKE"
94011919, 1524055021, xn--ppe-8ka60c.com, àppłe.com , àł, apple.com, 69, 1
94724468, 1500291180, xn--sack-01a.com, słack.com , ł, slack.com, 205, 1

ı, 100, 0x131, "LATIN SMALL LETTER DOTLESS I"
18331655, 1488327078, xn--reddt-q4a.com, reddıt.com , ı, reddit.com, 7, 1
95900673, 1500493680, xn--t-fka.com, tı.com , ı, ti.com, 3235, 1
84518766, 1497998760, xn--gml-kua34j.com, gmȧıl.com , ȧı, gmail.com, 22463, 1
95900424, 1500493860, xn--fat-jua.com, fıat.com , ı, fiat.com, 54102, 1
94504694, 1509148799, xn--curacao-egamng-hgc.com, curacao-egamıng.com , ı, curacao-egaming.com, 524456, 1
94724500, 1500493920, xn--suzu-kza.com, ısuzu.com , ı, isuzu.com, 866480, 1

ì, 25, 0xec, "LATIN SMALL LETTER I WITH GRAVE"
95900680, 1500670920, xn--twttr-7raz.com, twìttèr.com , ìè, twitter.com, 11, 1
85019386, 1507161599, xn--polonex-3ya.com, polonìex.com , ì, poloniex.com, 1595, 1
83724035, 1497798600, xn--gma-pma40b.com, gmaìĺ.com , ìĺ, gmail.com, 22463, 1
```

IDN Homoglyphs - More Cross Referenced Results

2 interesting domains observed bypasses Chromium checks by using only cyrillic characters:

07022746, 1443571199, xn--80aac5cct.com, таобао.com , таобао, taobao.com, 10, 1

10303999, 1461542399, xn--e1anr4f.com, тіме.com , тіме, time.com, 817, 1

IDN Homoglyphs - Results Contd

A breakdown of the unicode blocks observed:

89 LATIN
25 CYRILLIC
16 HEBREW
14 GREEK
8 KATAKANA
4 ARABIC
3 HANGUL
2 HIRAGANA
1 RUNIC
1 MALAYALAM
1 CANADIAN SYLLABICS

IDN Homoglyphs - Canadian Aboriginal Syllabics

Firefox & Chromium IDN checks were bypassed(punycode value was not displayed) for the following sample domains. Firefox & Chromium security bugs were reported.

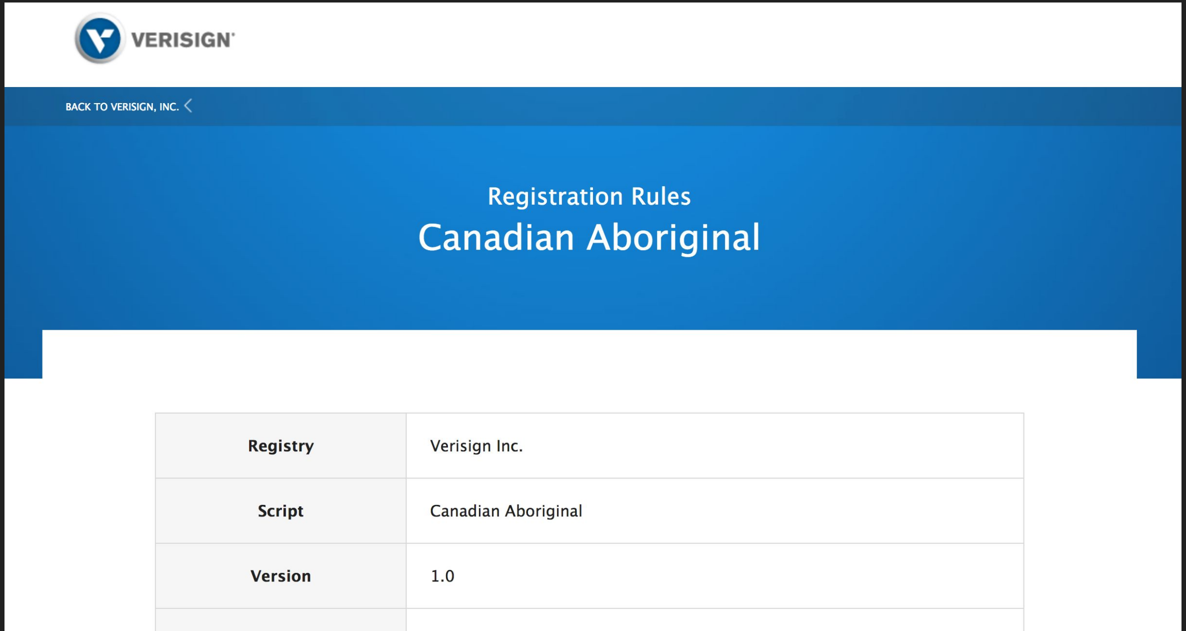
http://xn--youtue-084a.com/ -- youtu□e.com -- example domain
http://xn--youtbe-z72a.com/ -- yout□be.com -- example domain
http://xn--uny-8wq.com/ -- □uny.com -- example domain
http://xn--oor-hxq.com -- □oor.com -- example domain
http://xn--ego-73q.com/ -- □ego.com -- example domain
http://xn--fc-lym.com/ -- fc□.com -- example domain
http://xn--ulu-7sr.com/ -- □ulu.com -- example domain
http://invalid.xn--acebook-yp9a.com/ -- □acebook.com -- example domain

```
Chromium - CVE-2017-5076
Firefox  - CVE-2017-7764
```

IDN Homoglyphs - Policy to the Rescue

While a domain name may render in a browser, you may not be able to register it!

https://www.verisign.com/assets/idn/idn-canadian-aboriginal.html

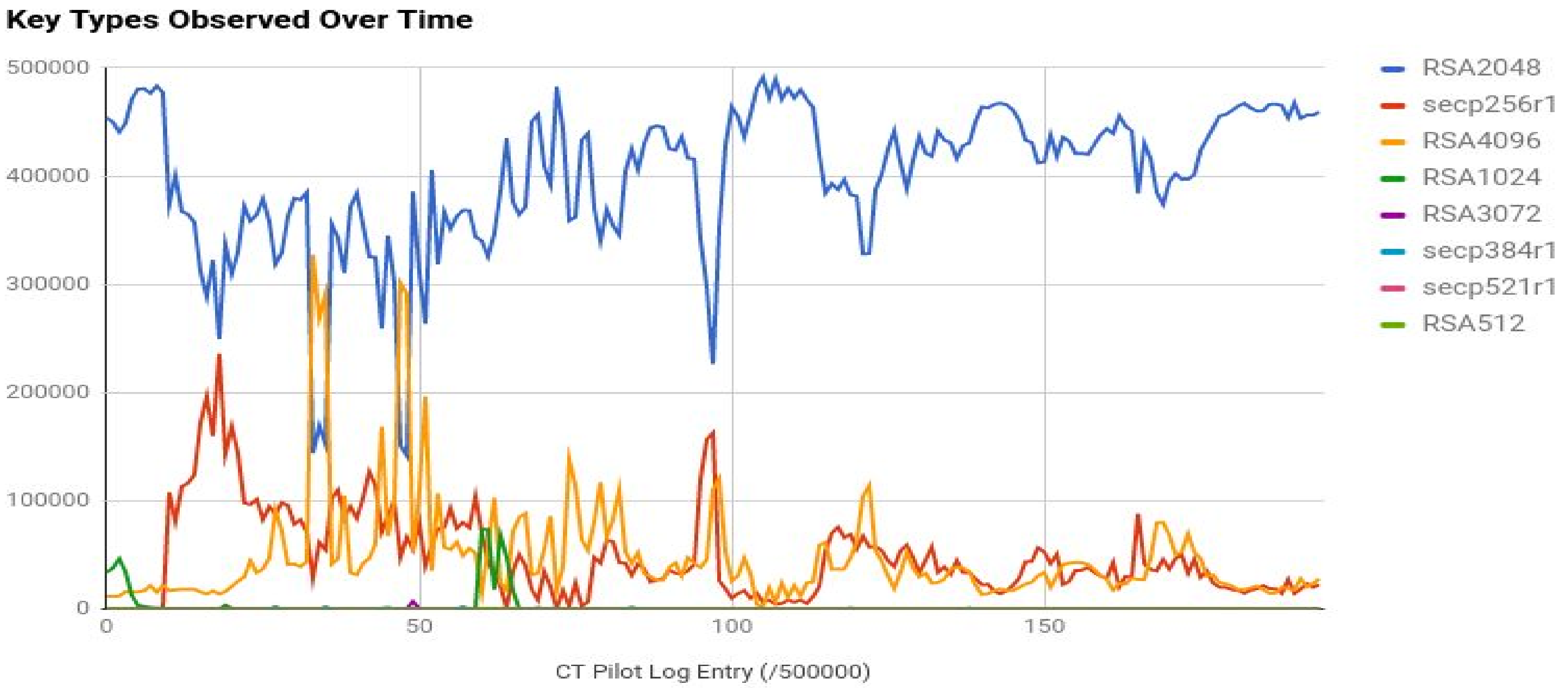


Registration Rules

Canadian Aboriginal

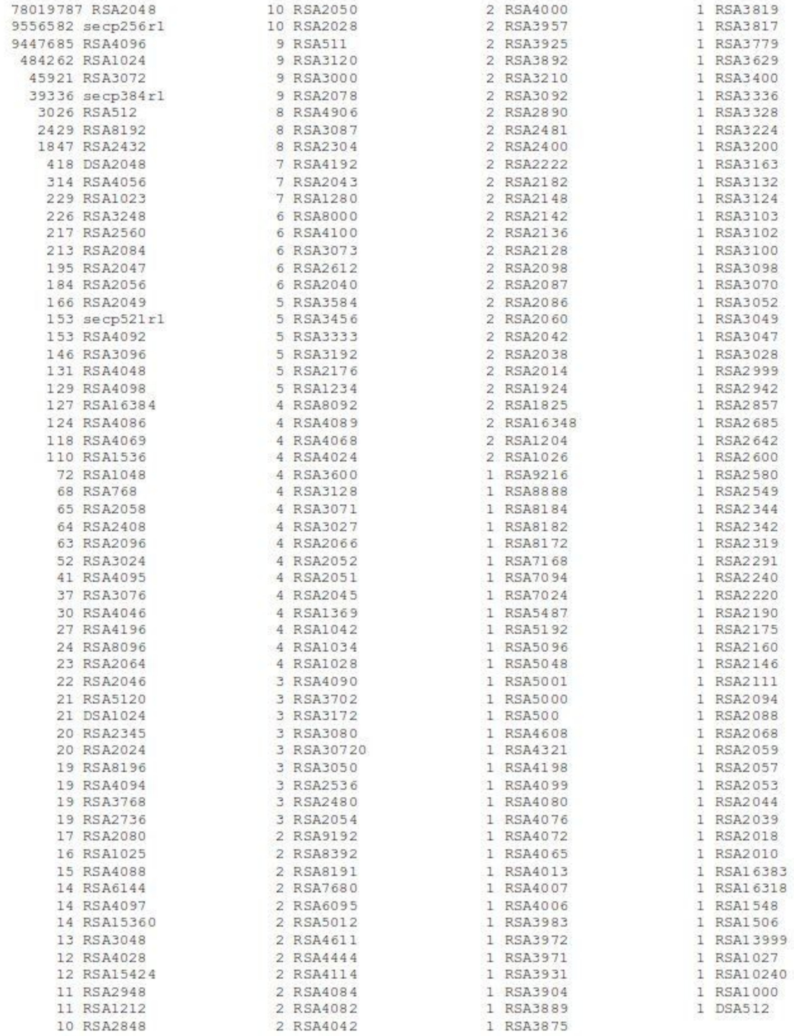
Registry	Verisign Inc.
Script	Canadian Aboriginal
Version	1.0

Certificate Transparency Fun - Graph of Key Types



Certificate Transparency Fun - Most Common Key Types

RSA2048	78019787
secp256r1	9556582
RSA4096	9447685
RSA1024	484262
RSA3072	45921
secp384r1	39336
RSA512	3026



```
78019787 RSA2048
 9556582 secp256r1
 9447685 RSA4096
  484262 RSA1024
   45921 RSA3072
   39336 secp384r1
    3026 RSA512
    2429 RSA8192
    1847 RSA2432
     418 DSA2048
     314 RSA4056
     229 RSA1023
     226 RSA3248
     217 RSA2560
     213 RSA2084
     195 RSA2047
     184 RSA2056
     166 RSA2049
     153 secp521r1
     153 RSA4092
     146 RSA3096
     131 RSA4048
     129 RSA4098
     127 RSA16384
     124 RSA4086
     118 RSA4069
     110 RSA1536
      72 RSA1048
      68 RSA768
      65 RSA2058
      64 RSA2408
      63 RSA2096
      52 RSA3024
      41 RSA4095
      37 RSA3076
      30 RSA4046
      27 RSA4196
      24 RSA8096
      23 RSA2064
      22 RSA2046
      21 RSA5120
      21 DSA1024
      20 RSA2345
      20 RSA2024
      19 RSA8196
      19 RSA4094
      19 RSA3768
      19 RSA2736
      17 RSA2080
      16 RSA1025
      15 RSA4088
      14 RSA6144
      14 RSA4097
      14 RSA15360
      13 RSA3048
      12 RSA4028
      12 RSA15424
      11 RSA2948
      11 RSA1212
      10 RSA2848
```

```
      10 RSA2050
      10 RSA2028
       9 RSA511
       9 RSA3120
       9 RSA3000
       9 RSA2078
       8 RSA4906
       8 RSA3087
       8 RSA2304
       7 RSA4192
       7 RSA2043
       7 RSA1280
       6 RSA8000
       6 RSA4100
       6 RSA3073
       6 RSA2612
       6 RSA2040
       5 RSA3584
       5 RSA3456
       5 RSA3333
       5 RSA3192
       5 RSA2176
       5 RSA1234
       4 RSA8092
       4 RSA4089
       4 RSA4068
       4 RSA4024
       4 RSA3600
       4 RSA3128
       4 RSA3071
       4 RSA3027
       4 RSA2066
       4 RSA2052
       4 RSA2051
       4 RSA2045
       4 RSA1369
       4 RSA1042
       4 RSA1034
       4 RSA1028
       3 RSA4090
       3 RSA3702
       3 RSA3172
       3 RSA3080
       3 RSA30720
       3 RSA3050
       3 RSA2536
       3 RSA2480
       3 RSA2054
       2 RSA9192
       2 RSA8392
       2 RSA8191
       2 RSA7680
       2 RSA6095
       2 RSA5012
       2 RSA4611
       2 RSA4444
       2 RSA4114
       2 RSA4084
       2 RSA4082
       2 RSA4042
```

```
       2 RSA4000
       2 RSA3957
       2 RSA3925
       2 RSA3892
       2 RSA3210
       2 RSA3092
       2 RSA2890
       2 RSA2481
       2 RSA2400
       2 RSA2222
       2 RSA2182
       2 RSA2148
       2 RSA2142
       2 RSA2136
       2 RSA2128
       2 RSA2098
       2 RSA2087
       2 RSA2086
       2 RSA2060
       2 RSA2042
       2 RSA2038
       2 RSA2014
       2 RSA1924
       2 RSA1825
       2 RSA16348
       2 RSA1204
       2 RSA1026
       1 RSA9216
       1 RSA8888
       1 RSA8184
       1 RSA8182
       1 RSA8172
       1 RSA7168
       1 RSA7094
       1 RSA7024
       1 RSA5487
       1 RSA5192
       1 RSA5096
       1 RSA5048
       1 RSA5001
       1 RSA5000
       1 RSA500
       1 RSA4608
       1 RSA4321
       1 RSA4198
       1 RSA4099
       1 RSA4080
       1 RSA4076
       1 RSA4072
       1 RSA4065
       1 RSA4013
       1 RSA4007
       1 RSA4006
       1 RSA3983
       1 RSA3972
       1 RSA3971
       1 RSA3931
       1 RSA3904
       1 RSA3889
       1 RSA3875
```

```
       1 RSA3819
       1 RSA3817
       1 RSA3779
       1 RSA3629
       1 RSA3400
       1 RSA3336
       1 RSA3328
       1 RSA3224
       1 RSA3200
       1 RSA3163
       1 RSA3132
       1 RSA3124
       1 RSA3103
       1 RSA3102
       1 RSA3100
       1 RSA3098
       1 RSA3070
       1 RSA3052
       1 RSA3049
       1 RSA3047
       1 RSA3028
       1 RSA2999
       1 RSA2942
       1 RSA2857
       1 RSA2685
       1 RSA2642
       1 RSA2600
       1 RSA2580
       1 RSA2549
       1 RSA2344
       1 RSA2342
       1 RSA2319
       1 RSA2291
       1 RSA2240
       1 RSA2220
       1 RSA2190
       1 RSA2175
       1 RSA2160
       1 RSA2146
       1 RSA2111
       1 RSA2094
       1 RSA2088
       1 RSA2068
       1 RSA2059
       1 RSA2057
       1 RSA2053
       1 RSA2044
       1 RSA2039
       1 RSA2018
       1 RSA2010
       1 RSA16383
       1 RSA16318
       1 RSA1548
       1 RSA1506
       1 RSA13999
       1 RSA1027
       1 RSA10240
       1 RSA1000
       1 DSA512
```

Questions?

Contact:

@erbbysam

very@busy.business