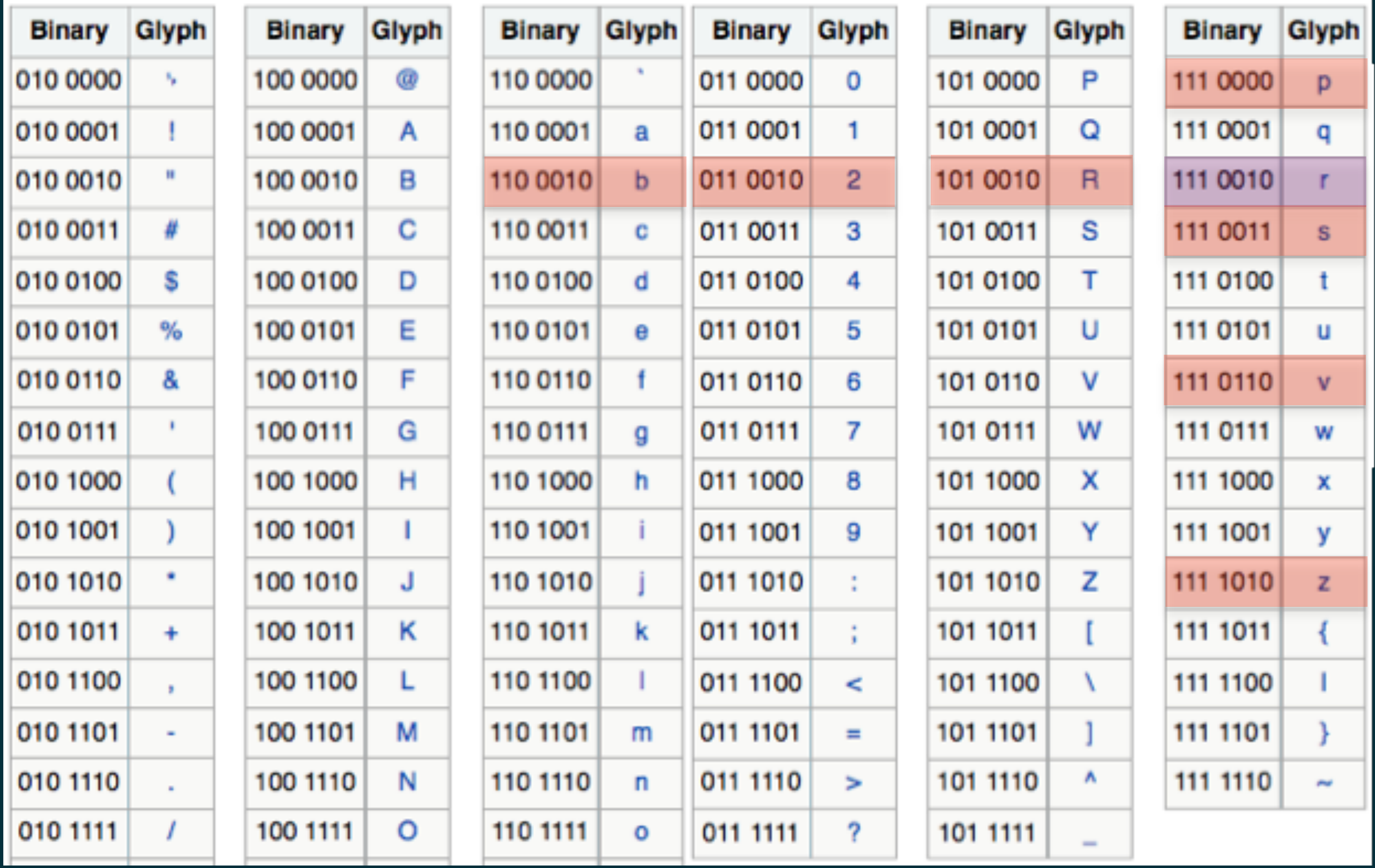
Bitsquatting

Jaeson Schultz
Threat Research Engineer
Cisco Systems
jaeson@cisco.com

ICANN 48
November 18, 2013

Introduction

- Bitsquatting is a form of cybersquatting which specifically targets bit errors in computer memory
- A memory error occurs any time one or more bits being read from memory have changed state from what was previously written
- By changing a single bit, a target domain such as “twitter.com” can become the bitsquat domain “twitte2.com”
- An attacker can simply register a bitsquat domain, wait for a memory error to occur, and afterwards intercept traffic, infect the client, …



Binary	Glyph	Binary	Glyph	Binary	Glyph	Binary	Glyph	Binary	Glyph	Binary	Glyph
010 0000	␠	100 0000	@	110 0000	`	011 0000	0	101 0000	P	111 0000	p
010 0001	!	100 0001	A	110 0001	a	011 0001	1	101 0001	Q	111 0001	q
010 0010	"	100 0010	B	110 0010	b	011 0010	2	101 0010	R	111 0010	r
010 0011	#	100 0011	C	110 0011	c	011 0011	3	101 0011	S	111 0011	s
010 0100	$	100 0100	D	110 0100	d	011 0100	4	101 0100	T	111 0100	t
010 0101	%	100 0101	E	110 0101	e	011 0101	5	101 0101	U	111 0101	u
010 0110	&	100 0110	F	110 0110	f	011 0110	6	101 0110	V	111 0110	v
010 0111	'	100 0111	G	110 0111	g	011 0111	7	101 0111	W	111 0111	w
010 1000	(	100 1000	H	110 1000	h	011 1000	8	101 1000	X	111 1000	x
010 1001	)	100 1001	I	110 1001	i	011 1001	9	101 1001	Y	111 1001	y
010 1010	*	100 1010	J	110 1010	j	011 1010	:	101 1010	Z	111 1010	z
010 1011	+	100 1011	K	110 1011	k	011 1011	;	101 1011	[	111 1011	{
010 1100	,	100 1100	L	110 1100	l	011 1100	<	101 1100	\	111 1100	|
010 1101	-	100 1101	M	110 1101	m	011 1101	=	101 1101	]	111 1101	}
010 1110	.	100 1110	N	110 1110	n	011 1110	>	101 1110	^	111 1110	~
010 1111	/	100 1111	O	110 1111	o	011 1111	?	101 1111	_		

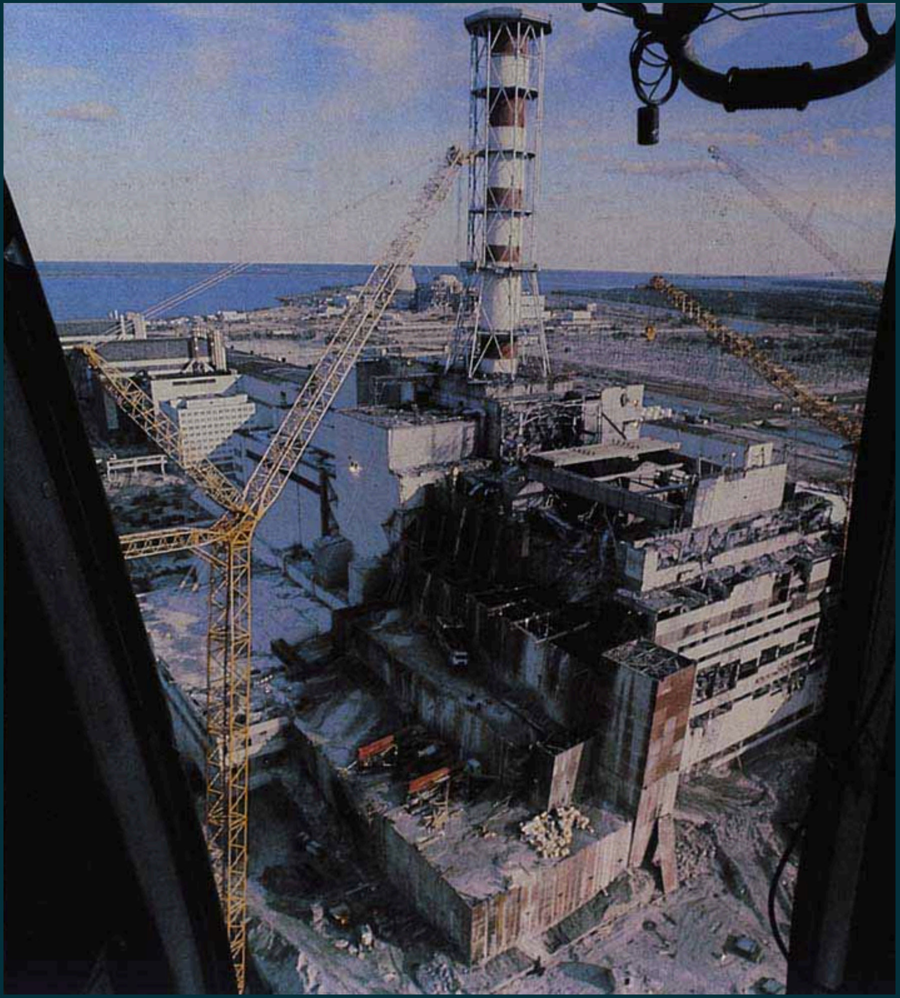
Causes of computer memory errors

- Cosmic Rays
  High energy particles that strike the Earth as frequently as 10,000 per square meter per second

- Heat
  Operating a device outside the recommended operating environment.

- Nuclear Explosions
  Intense neutron emission from low yield nuclear explosions induce a sharp increase in the frequency of bitsquat requests

- Defects in Manufacturing
  Errors in memory have been traced to alpha particle emissions from chip packaging materials.

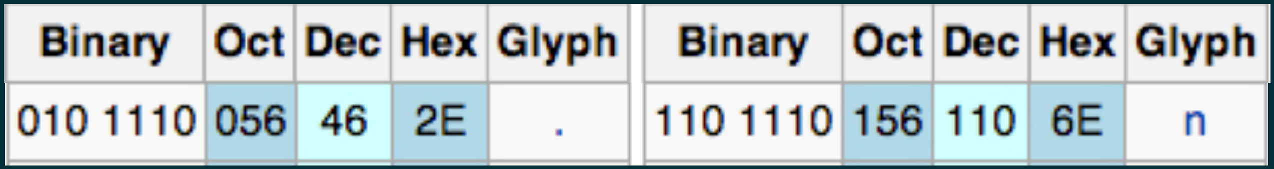


"Cow were alive so the amount of radiation was not immediately deadly for peoples and cockroaches but probably deadly enough for 8" floppy drives, 4k static ram or 16k dynamic ram which were based on capacitive charge... "

RFC1035 declared the valid syntax for domain name labels, which was later refined under RFC1123. According to these RFCs, the only valid characters inside a domain name are:

1. A-Z
2. a-z
3. 0-9
4. - (hyphen)

The lowercase letter “n” can experience a bit error and become a dot “.” and vice versa.

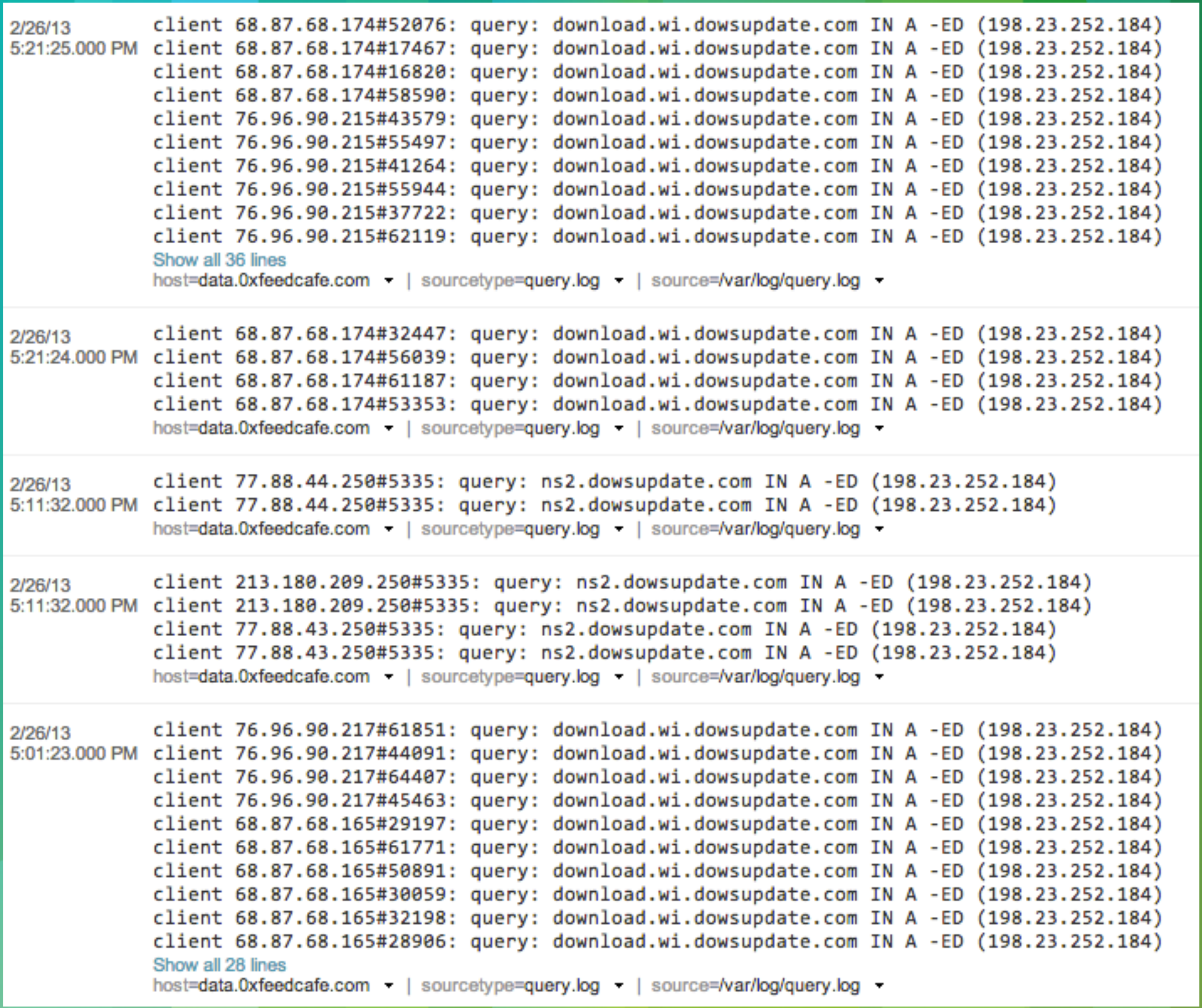


Binary	Oct	Dec	Hex	Glyph	Binary	Oct	Dec	Hex	Glyph
010 1110	056	46	2E	.	110 1110	156	110	6E	n

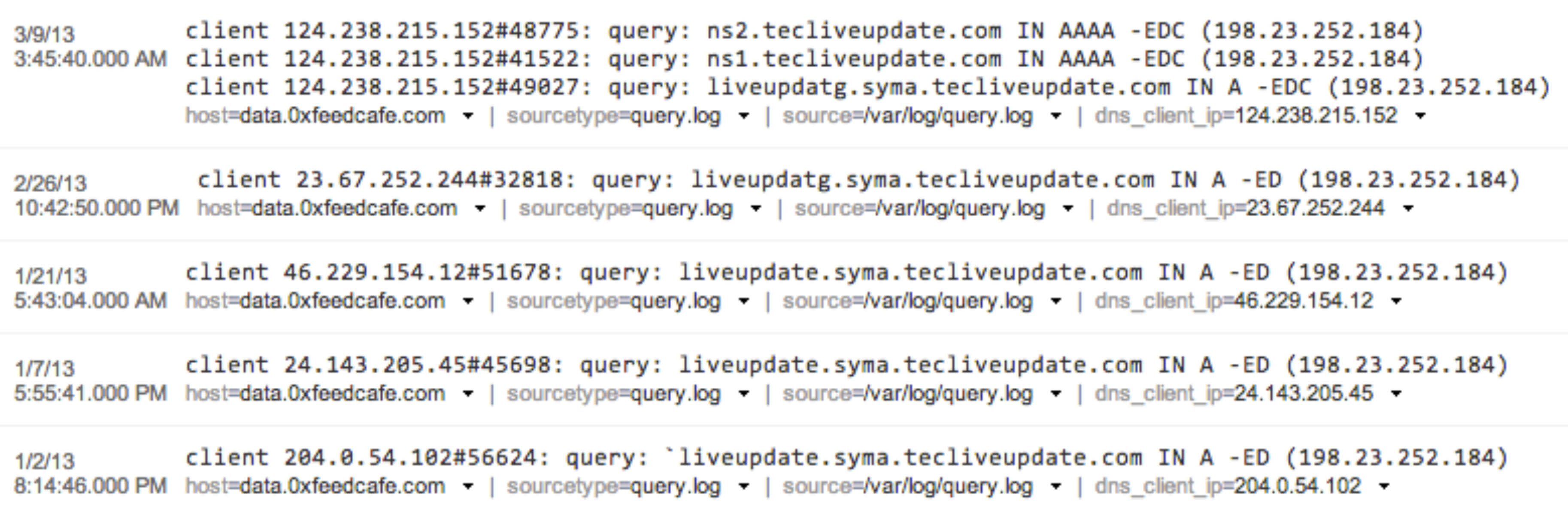
Subdomain Delimiters: “n” flips to “.”

- If a second level domain name contains the letter “n” and there are two or more characters after the letter “n”, then this is a potential bitsquat.
- Examples:

  “windowsupdate.com” has bitsquat “dowsupdate.com”
  “symantecliveupdate.com” has bitsquat “tecliveupdate.com”



```
2/26/13          client 68.87.68.174#52076: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
5:21:25.000 PM   client 68.87.68.174#17467: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 68.87.68.174#16820: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 68.87.68.174#58590: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 76.96.90.215#43579: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 76.96.90.215#55497: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 76.96.90.215#41264: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 76.96.90.215#55944: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 76.96.90.215#37722: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 76.96.90.215#62119: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 Show all 36 lines
                 host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾

2/26/13          client 68.87.68.174#32447: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
5:21:24.000 PM   client 68.87.68.174#56039: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 68.87.68.174#61187: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 68.87.68.174#53353: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾

2/26/13          client 77.88.44.250#5335: query: ns2.dowsupdate.com IN A -ED (198.23.252.184)
5:11:32.000 PM   client 77.88.44.250#5335: query: ns2.dowsupdate.com IN A -ED (198.23.252.184)
                 host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾

2/26/13          client 213.180.209.250#5335: query: ns2.dowsupdate.com IN A -ED (198.23.252.184)
5:11:32.000 PM   client 213.180.209.250#5335: query: ns2.dowsupdate.com IN A -ED (198.23.252.184)
                 client 77.88.43.250#5335: query: ns2.dowsupdate.com IN A -ED (198.23.252.184)
                 client 77.88.43.250#5335: query: ns2.dowsupdate.com IN A -ED (198.23.252.184)
                 host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾

2/26/13          client 76.96.90.217#61851: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
5:01:23.000 PM   client 76.96.90.217#44091: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 76.96.90.217#64407: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 76.96.90.217#45463: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 68.87.68.165#29197: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 68.87.68.165#61771: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 68.87.68.165#50891: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 68.87.68.165#30059: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 68.87.68.165#32198: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 client 68.87.68.165#28906: query: download.wi.dowsupdate.com IN A -ED (198.23.252.184)
                 Show all 28 lines
                 host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾
```

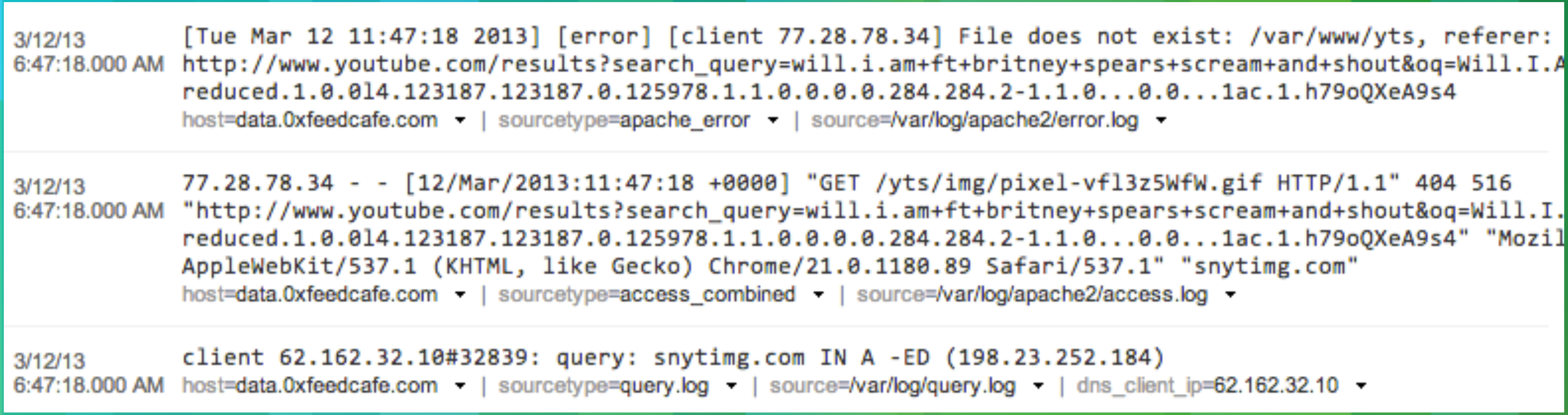


```
3/9/13              client 124.238.215.152#48775: query: ns2.tecliveupdate.com IN AAAA -EDC (198.23.252.184)
3:45:40.000 AM      client 124.238.215.152#41522: query: ns1.tecliveupdate.com IN AAAA -EDC (198.23.252.184)
                    client 124.238.215.152#49027: query: liveupdatg.syma.tecliveupdate.com IN A -EDC (198.23.252.184)
                    host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=124.238.215.152 ▾

2/26/13             client 23.67.252.244#32818: query: liveupdatg.syma.tecliveupdate.com IN A -ED (198.23.252.184)
10:42:50.000 PM     host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=23.67.252.244 ▾

1/21/13             client 46.229.154.12#51678: query: liveupdate.syma.tecliveupdate.com IN A -ED (198.23.252.184)
5:43:04.000 AM      host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=46.229.154.12 ▾

1/7/13              client 24.143.205.45#45698: query: liveupdate.syma.tecliveupdate.com IN A -ED (198.23.252.184)
5:55:41.000 PM      host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=24.143.205.45 ▾

1/2/13              client 204.0.54.102#56624: query: `liveupdate.syma.tecliveupdate.com IN A -ED (198.23.252.184)
8:14:46.000 PM      host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=204.0.54.102 ▾
```

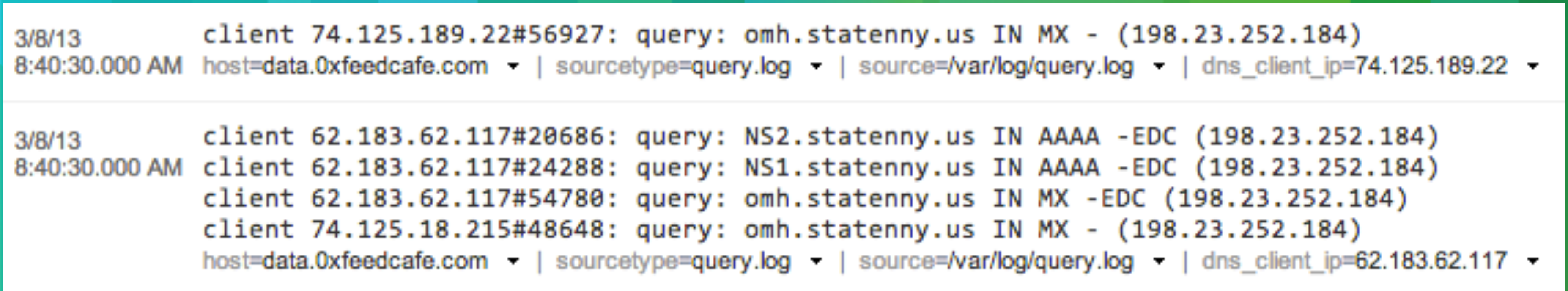
Subdomain Delimiters: “.” flips to “n”

- If a 2nd level domain name uses 3rd level subdomains, these can be leveraged into bitsquat domains.
- Replace the dot separating the 3rd and 2nd level domain labels with the letter “n”.
- Examples:

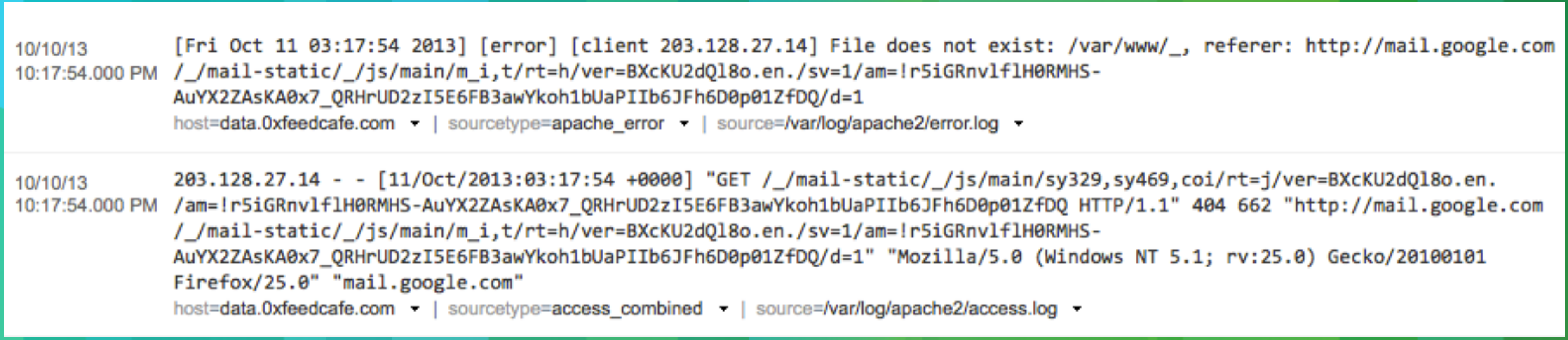
  “s.ytimg.com” has bitsquat “snytimg.com”
  “mail.google.com” has bitsquat “mailngoogle.com”
  “state.ny.us” has bitsquat “statenny.us”



```
3/12/13         [Tue Mar 12 11:47:18 2013] [error] [client 77.28.78.34] File does not exist: /var/www/yts, referer:
6:47:18.000 AM  http://www.youtube.com/results?search_query=will.i.am+ft+britney+spears+scream+and+shout&oq=Will.I.A
                reduced.1.0.0l4.123187.123187.0.125978.1.1.0.0.0.0.284.284.2-1.1.0...0.0...1ac.1.h79oQXeA9s4
                host=data.0xfeedcafe.com ▾ | sourcetype=apache_error ▾ | source=/var/log/apache2/error.log ▾

3/12/13         77.28.78.34 - - [12/Mar/2013:11:47:18 +0000] "GET /yts/img/pixel-vfl3z5WfW.gif HTTP/1.1" 404 516
6:47:18.000 AM  "http://www.youtube.com/results?search_query=will.i.am+ft+britney+spears+scream+and+shout&oq=Will.I.
                reduced.1.0.0l4.123187.123187.0.125978.1.1.0.0.0.0.284.284.2-1.1.0...0.0...1ac.1.h79oQXeA9s4" "Mozil
                AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.89 Safari/537.1" "snytimg.com"
                host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾

3/12/13         client 62.162.32.10#32839: query: snytimg.com IN A -ED (198.23.252.184)
6:47:18.000 AM  host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=62.162.32.10 ▾
```



```
3/8/13         client 74.125.189.22#56927: query: omh.statenny.us IN MX - (198.23.252.184)
8:40:30.000 AM host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=74.125.189.22 ▾

3/8/13         client 62.183.62.117#20686: query: NS2.statenny.us IN AAAA -EDC (198.23.252.184)
8:40:30.000 AM client 62.183.62.117#24288: query: NS1.statenny.us IN AAAA -EDC (198.23.252.184)
               client 62.183.62.117#54780: query: omh.statenny.us IN MX -EDC (198.23.252.184)
               client 74.125.18.215#48648: query: omh.statenny.us IN MX - (198.23.252.184)
               host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=62.183.62.117 ▾
```



```
10/10/13          [Fri Oct 11 03:17:54 2013] [error] [client 203.128.27.14] File does not exist: /var/www/_, referer: http://mail.google.com
10:17:54.000 PM   /_/mail-static/_/js/main/m_i,t/rt=h/ver=BXcKU2dQl8o.en./sv=1/am=!r5iGRnvlflH0RMHS-
                  AuYX2ZAsKA0x7_QRHrUD2zI5E6FB3awYkoh1bUaPIIb6JFh6D0p01ZfDQ/d=1
                  host=data.0xfeedcafe.com ▾ | sourcetype=apache_error ▾ | source=/var/log/apache2/error.log ▾

10/10/13          203.128.27.14 - - [11/Oct/2013:03:17:54 +0000] "GET /_/mail-static/_/js/main/sy329,sy469,coi/rt=j/ver=BXcKU2dQl8o.en.
10:17:54.000 PM   /am=!r5iGRnvlflH0RMHS-AuYX2ZAsKA0x7_QRHrUD2zI5E6FB3awYkoh1bUaPIIb6JFh6D0p01ZfDQ HTTP/1.1" 404 662 "http://mail.google.com
                  /_/mail-static/_/js/main/m_i,t/rt=h/ver=BXcKU2dQl8o.en./sv=1/am=!r5iGRnvlflH0RMHS-
                  AuYX2ZAsKA0x7_QRHrUD2zI5E6FB3awYkoh1bUaPIIb6JFh6D0p01ZfDQ/d=1" "Mozilla/5.0 (Windows NT 5.1; rv:25.0) Gecko/20100101
                  Firefox/25.0" "mail.google.com"
                  host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾
```

One of the most popular contexts for a domain name to appear is inside of a URL, especially over HTTP. For example, look at the popularity of the bitsquat domains which was originally published by Dinaburg in his 2011 research paper:

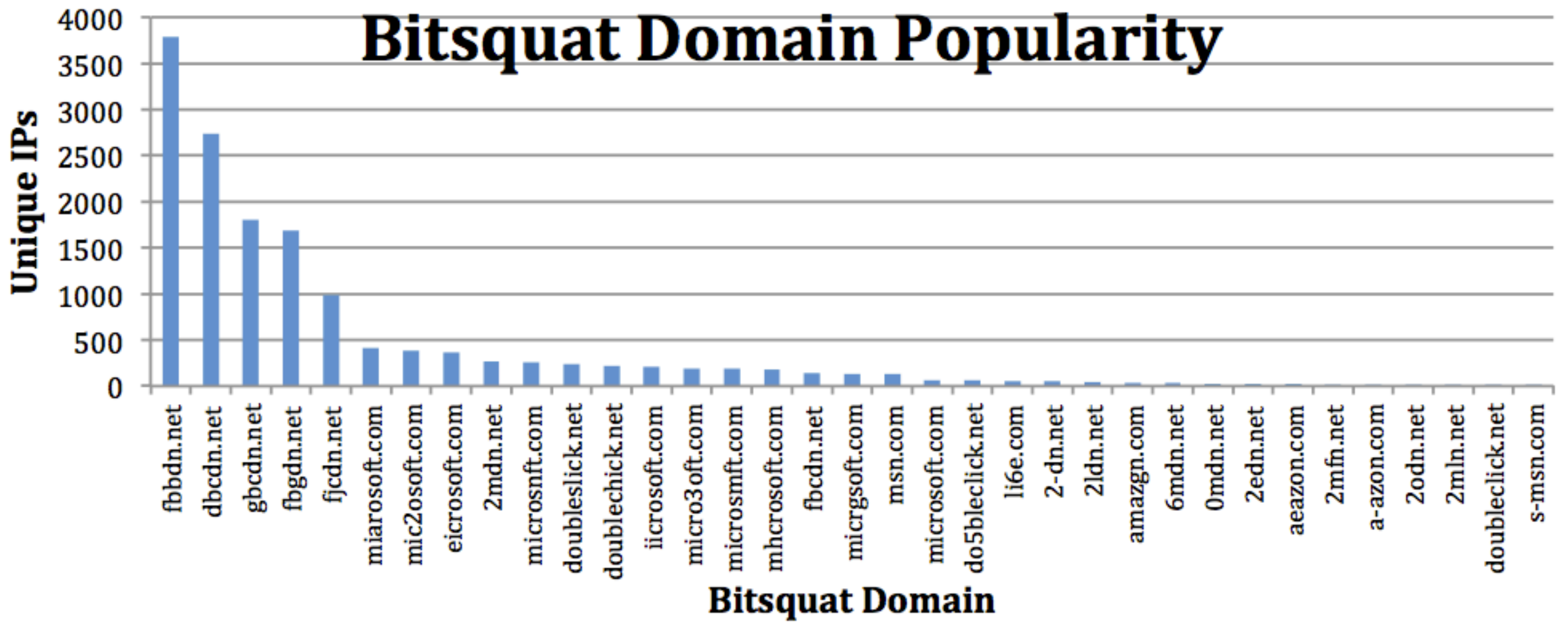
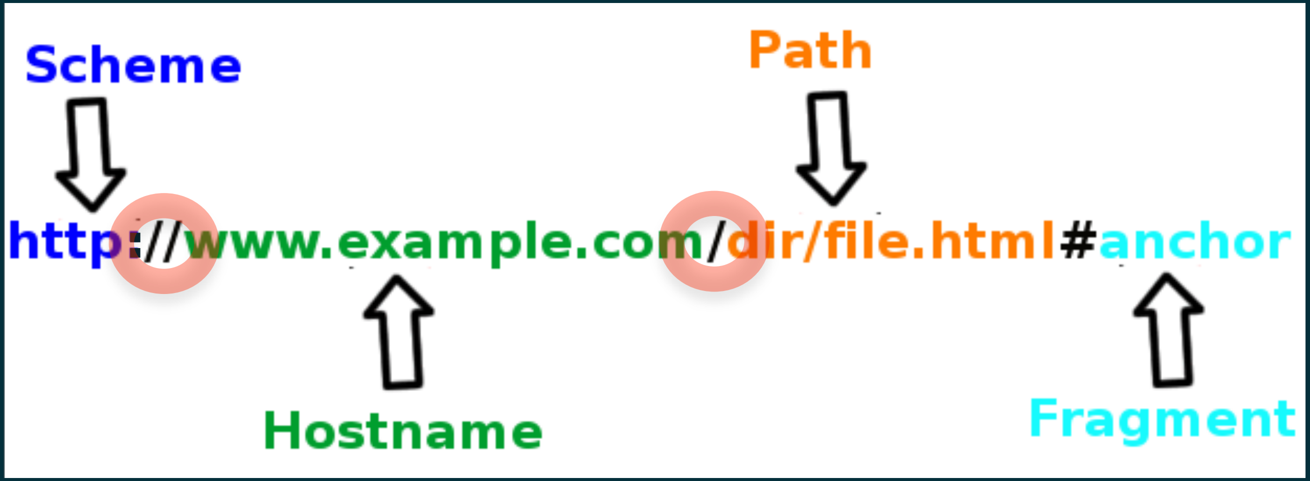


Figure 9: Domain popularity, ordered by the number of unique IPs with the domain in the HTTP `Host` header.

Inside a URL or href, forward slash characters “/” will act as delimiters separating the scheme from the hostname from the path.



Scheme

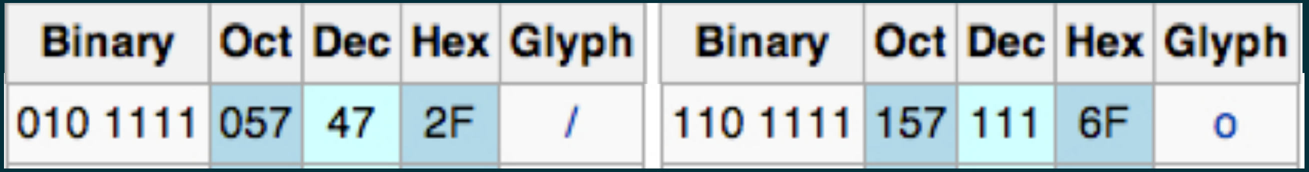
Path

http://www.example.com/dir/file.html#anchor

Hostname

Fragment

The lowercase letter “o” can experience a bit error and become a forward slash “/” and vice versa

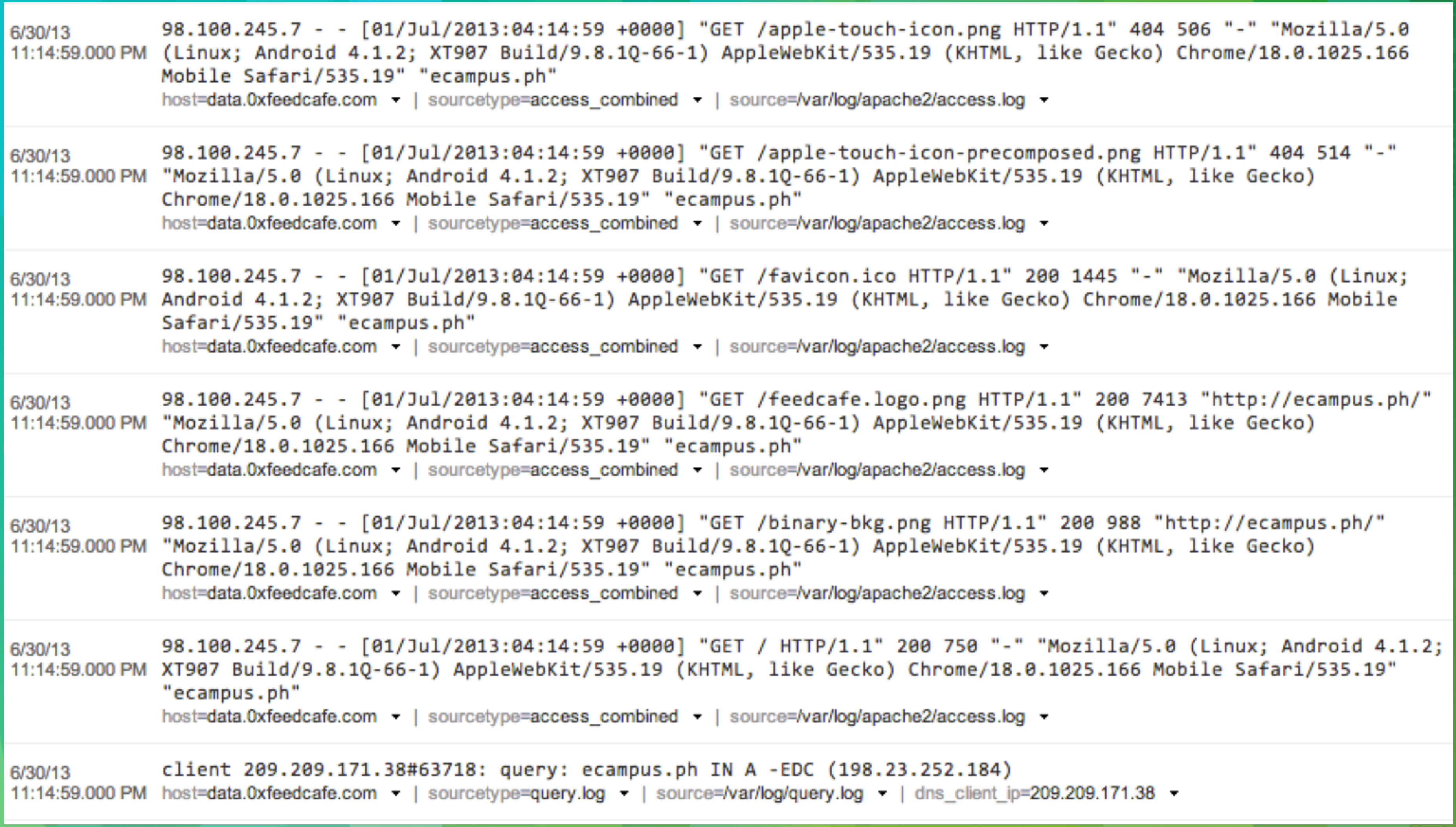


Binary	Oct	Dec	Hex	Glyph	Binary	Oct	Dec	Hex	Glyph
010 1111	057	47	2F	/	110 1111	157	111	6F	o

URL Delimiters: “o” flips to “/”

- Sometimes a fully qualified domain name (FQDN) contains the letter “o” and the preceding characters form a valid second level domain name.
- Most interesting aspect of this method is that domains at non-public Top Level Domains (TLDs) can be targeted.
- Examples:

  “tcoss.scott.af.mil” has bitsquat “tcoss.sc”
  “bop.peostri.army.mil” has bitsquat “bop.pe”
  “ecampus.phoenix.edu” has bitsquat “ecampus.ph”
  “trading.scottrade.com” has bitsquat “trading.sc”



```
6/30/13          98.100.245.7 - - [01/Jul/2013:04:14:59 +0000] "GET /apple-touch-icon.png HTTP/1.1" 404 506 "-" "Mozilla/5.0
11:14:59.000 PM  (Linux; Android 4.1.2; XT907 Build/9.8.1Q-66-1) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.166
                 Mobile Safari/535.19" "ecampus.ph"
                 host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾

6/30/13          98.100.245.7 - - [01/Jul/2013:04:14:59 +0000] "GET /apple-touch-icon-precomposed.png HTTP/1.1" 404 514 "-"
11:14:59.000 PM  "Mozilla/5.0 (Linux; Android 4.1.2; XT907 Build/9.8.1Q-66-1) AppleWebKit/535.19 (KHTML, like Gecko)
                 Chrome/18.0.1025.166 Mobile Safari/535.19" "ecampus.ph"
                 host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾

6/30/13          98.100.245.7 - - [01/Jul/2013:04:14:59 +0000] "GET /favicon.ico HTTP/1.1" 200 1445 "-" "Mozilla/5.0 (Linux;
11:14:59.000 PM  Android 4.1.2; XT907 Build/9.8.1Q-66-1) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.166 Mobile
                 Safari/535.19" "ecampus.ph"
                 host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾

6/30/13          98.100.245.7 - - [01/Jul/2013:04:14:59 +0000] "GET /feedcafe.logo.png HTTP/1.1" 200 7413 "http://ecampus.ph/"
11:14:59.000 PM  "Mozilla/5.0 (Linux; Android 4.1.2; XT907 Build/9.8.1Q-66-1) AppleWebKit/535.19 (KHTML, like Gecko)
                 Chrome/18.0.1025.166 Mobile Safari/535.19" "ecampus.ph"
                 host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾

6/30/13          98.100.245.7 - - [01/Jul/2013:04:14:59 +0000] "GET /binary-bkg.png HTTP/1.1" 200 988 "http://ecampus.ph/"
11:14:59.000 PM  "Mozilla/5.0 (Linux; Android 4.1.2; XT907 Build/9.8.1Q-66-1) AppleWebKit/535.19 (KHTML, like Gecko)
                 Chrome/18.0.1025.166 Mobile Safari/535.19" "ecampus.ph"
                 host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾

6/30/13          98.100.245.7 - - [01/Jul/2013:04:14:59 +0000] "GET / HTTP/1.1" 200 750 "-" "Mozilla/5.0 (Linux; Android 4.1.2;
11:14:59.000 PM  XT907 Build/9.8.1Q-66-1) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.166 Mobile Safari/535.19"
                 "ecampus.ph"
                 host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾

6/30/13          client 209.209.171.38#63718: query: ecampus.ph IN A -EDC (198.23.252.184)
11:14:59.000 PM  host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=209.209.171.38 ▾
```

URL Delimiters: “/” flips to “o”

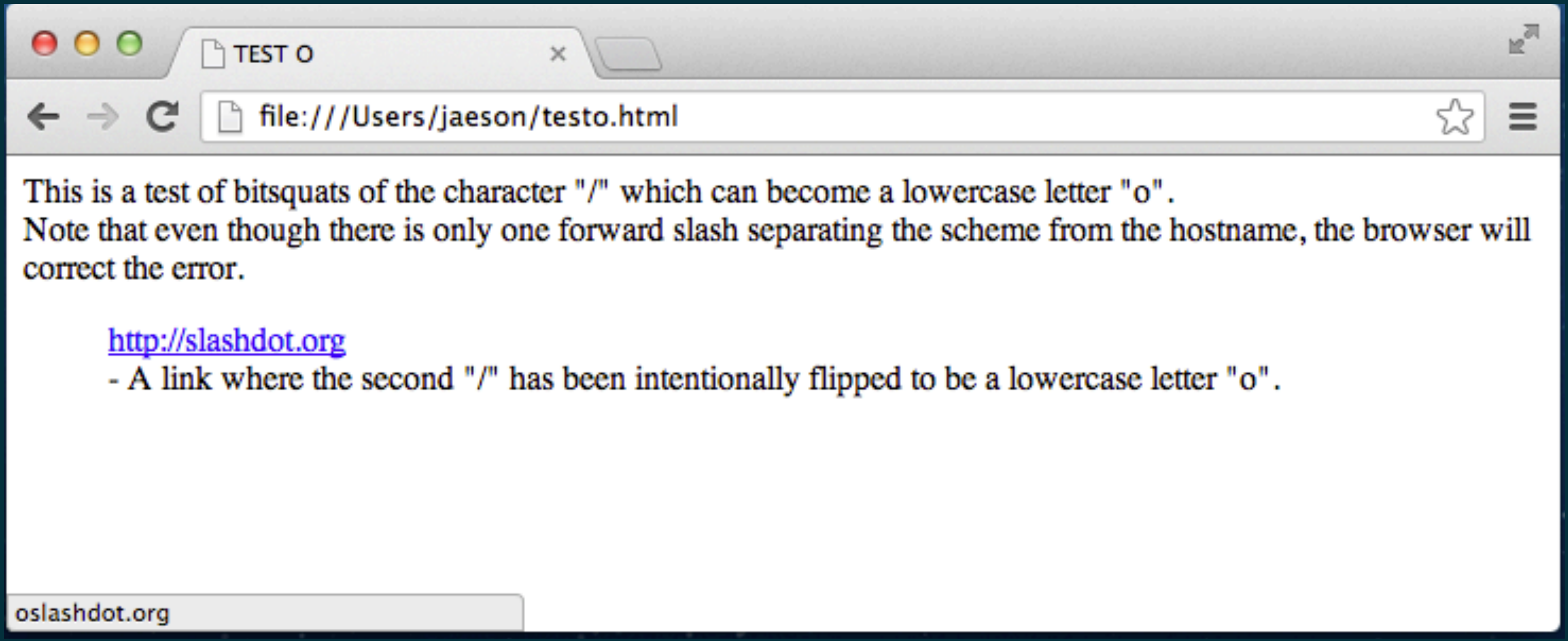
- Sometimes the slashes inside a URL or href can experience a bit error and become a lowercase letter “o”
- Absolute URLs will contain at least 2-3 slashes
- Two slashes separate the scheme from the hostname, and a third slash may separate the hostname from the path. Generally only bit flips of the second slash produce viable bitsquat domains

  http://www.cisco.com/

- Examples:
  “slashdot.org” has bitsquat “oslashdot.org”
  “twitter.com” has bitsquat “otwitter.com”

URL Delimiters: Bad syntax is OK

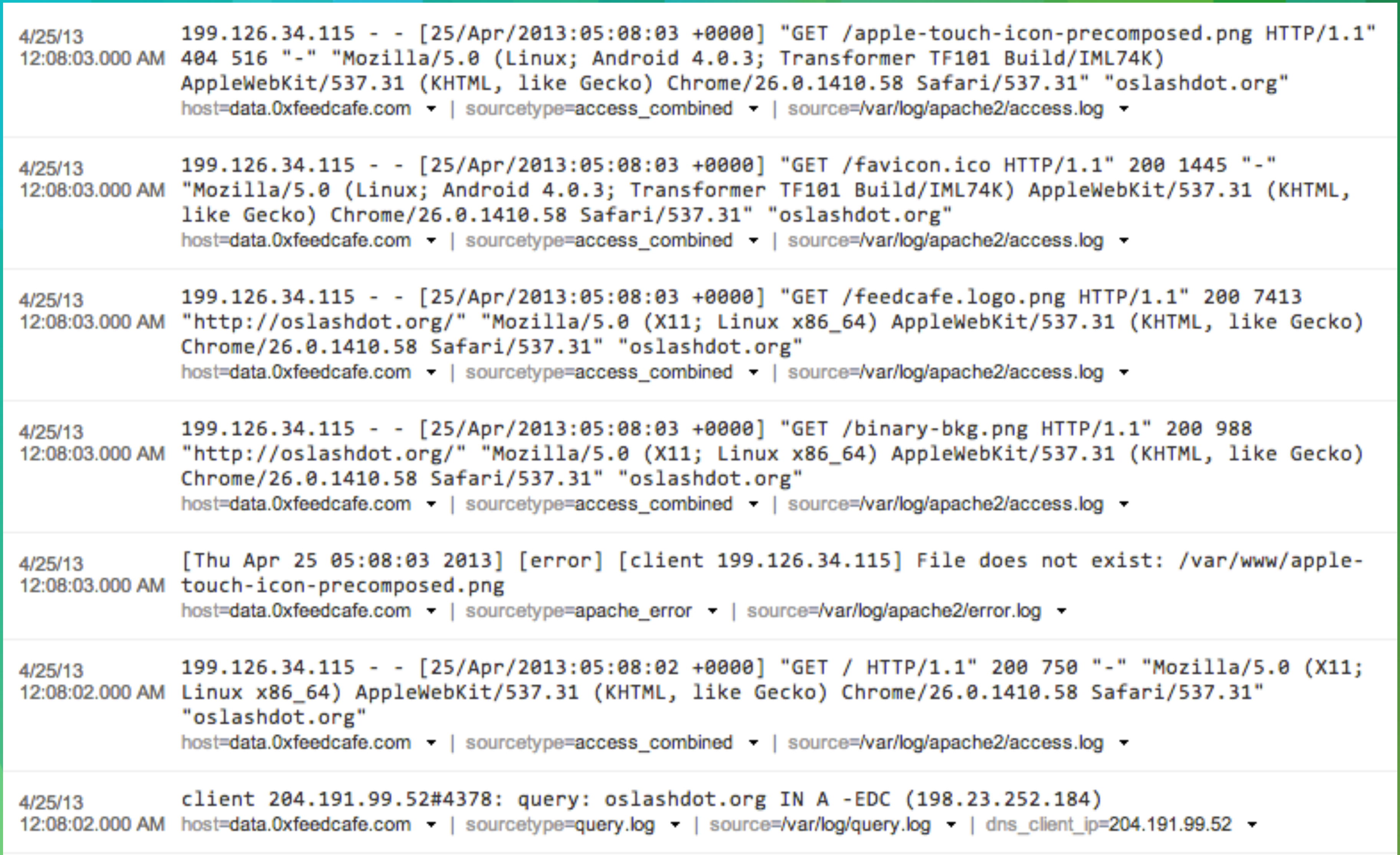
- When the second slash bit flips to become a letter “o”, the URL has only one forward slash separating the scheme from the hostname. The browser allows this bad syntax.



This is a test of bitsquats of the character "/" which can become a lowercase letter "o".
Note that even though there is only one forward slash separating the scheme from the hostname, the browser will correct the error.

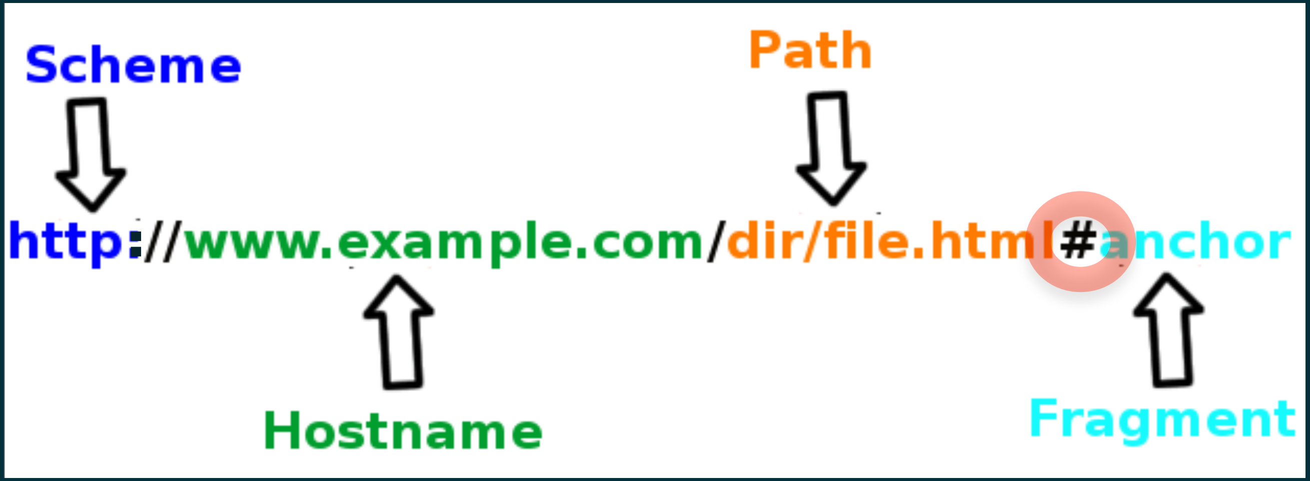
http://slashdot.org
- A link where the second "/" has been intentionally flipped to be a lowercase letter "o".

oslashdot.org

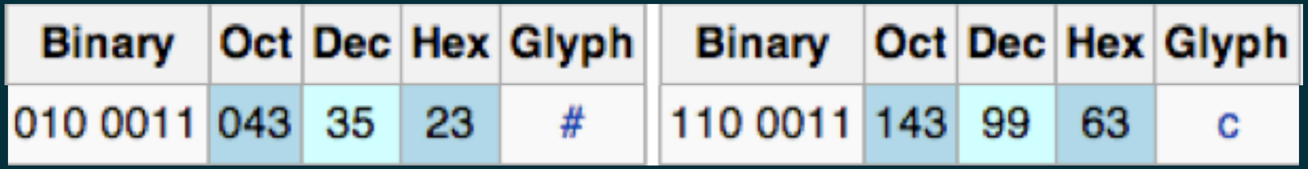


```
4/25/13         199.126.34.115 - - [25/Apr/2013:05:08:03 +0000] "GET /apple-touch-icon-precomposed.png HTTP/1.1"
12:08:03.000 AM 404 516 "-" "Mozilla/5.0 (Linux; Android 4.0.3; Transformer TF101 Build/IML74K)
                AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.58 Safari/537.31" "oslashdot.org"
                host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾

4/25/13         199.126.34.115 - - [25/Apr/2013:05:08:03 +0000] "GET /favicon.ico HTTP/1.1" 200 1445 "-"
12:08:03.000 AM "Mozilla/5.0 (Linux; Android 4.0.3; Transformer TF101 Build/IML74K) AppleWebKit/537.31 (KHTML,
                like Gecko) Chrome/26.0.1410.58 Safari/537.31" "oslashdot.org"
                host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾

4/25/13         199.126.34.115 - - [25/Apr/2013:05:08:03 +0000] "GET /feedcafe.logo.png HTTP/1.1" 200 7413
12:08:03.000 AM "http://oslashdot.org/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.31 (KHTML, like Gecko)
                Chrome/26.0.1410.58 Safari/537.31" "oslashdot.org"
                host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾

4/25/13         199.126.34.115 - - [25/Apr/2013:05:08:03 +0000] "GET /binary-bkg.png HTTP/1.1" 200 988
12:08:03.000 AM "http://oslashdot.org/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.31 (KHTML, like Gecko)
                Chrome/26.0.1410.58 Safari/537.31" "oslashdot.org"
                host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾

4/25/13         [Thu Apr 25 05:08:03 2013] [error] [client 199.126.34.115] File does not exist: /var/www/apple-
12:08:03.000 AM touch-icon-precomposed.png
                host=data.0xfeedcafe.com ▾ | sourcetype=apache_error ▾ | source=/var/log/apache2/error.log ▾

4/25/13         199.126.34.115 - - [25/Apr/2013:05:08:02 +0000] "GET / HTTP/1.1" 200 750 "-" "Mozilla/5.0 (X11;
12:08:02.000 AM Linux x86_64) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.58 Safari/537.31"
                "oslashdot.org"
                host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾

4/25/13         client 204.191.99.52#4378: query: oslashdot.org IN A -EDC (198.23.252.184)
12:08:02.000 AM host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=204.191.99.52 ▾
```

Inside a URL or href, pound/hash characters “#” will act as delimiters separating the the fragment (a.k.a. anchor tag) from the rest of the URL



The lowercase letter “c” can flip a bit and become a pound character “#”



Binary	Oct	Dec	Hex	Glyph	Binary	Oct	Dec	Hex	Glyph
010 0011	043	35	23	#	110 0011	143	99	63	c

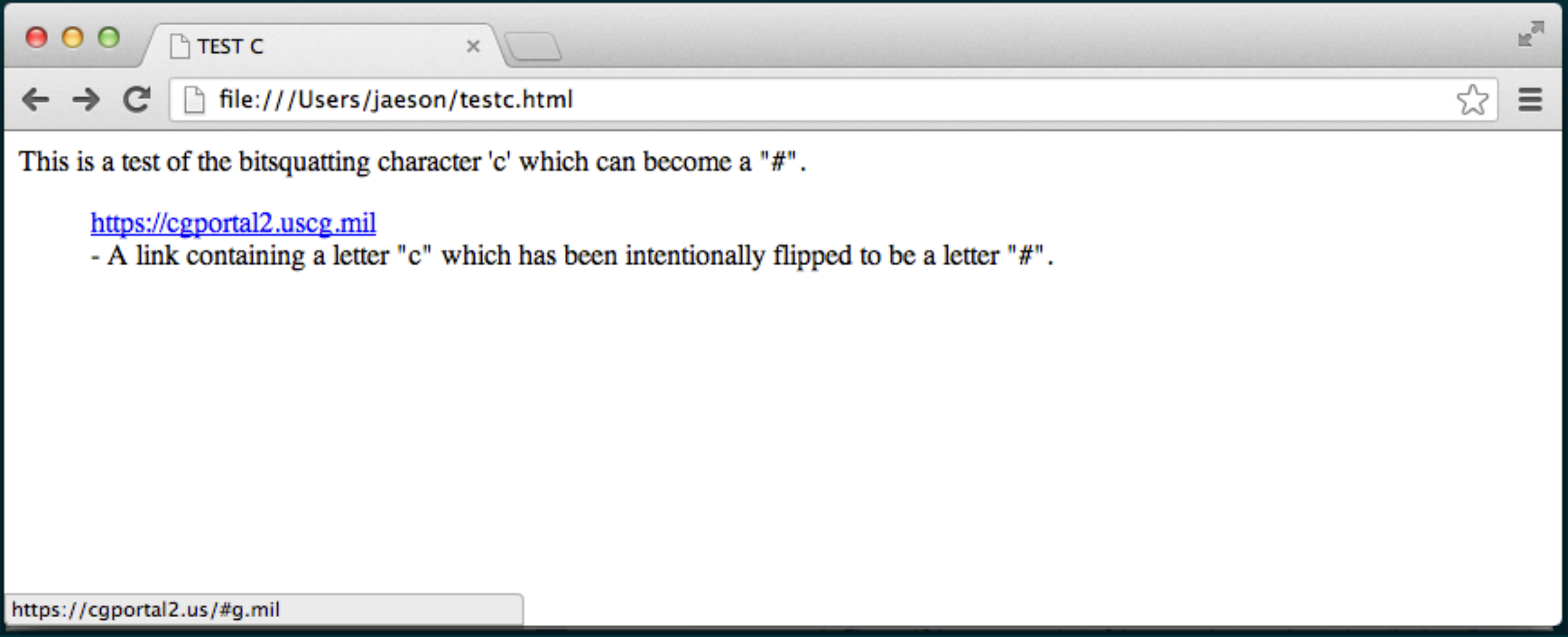
More URL Delimiters: “c” flips to “#”

- Sometimes a fully qualified domain name (FQDN) contains the letter “c” and the preceding characters form a valid second level domain name
- Once again, domains at non-public Top Level Domains (TLDs) can be targeted
- Examples:

  “pki.nrc.gov” has bitsquat “pki.nr”
  “certauth.bechtel.com” has bitsquat “certauth.be”
  “emergency.cdc.gov” has bitsquat “emergency.cd”
  “cgportal2.uscg.mil” has bitsquat “cgportal2.us”

More URL Delimiters: Bad syntax is OK

- When the letter “c” experiences a bit flip and becomes an anchor tag “#”, this causes early termination of the URL.



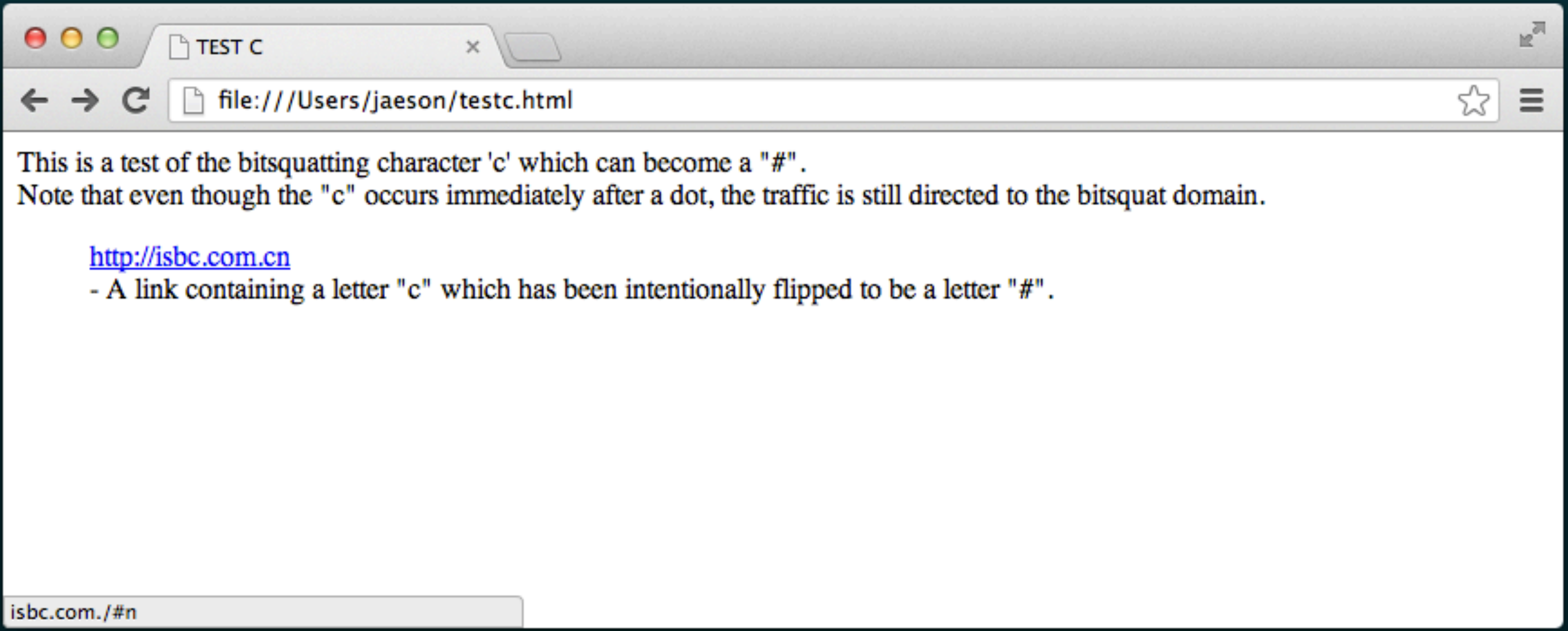
This is a test of the bitsquatting character 'c' which can become a "#".

https://cgportal2.uscg.mil
- A link containing a letter "c" which has been intentionally flipped to be a letter "#".

https://cgportal2.us/#g.mil

More URL Delimiters: Bad syntax is OK

- Even when the letter “c” experiences a bit flip immediately after a dot, the browser still directs traffic to the bitsquat domain.



This is a test of the bitsquatting character 'c' which can become a "#".
Note that even though the "c" occurs immediately after a dot, the traffic is still directed to the bitsquat domain.

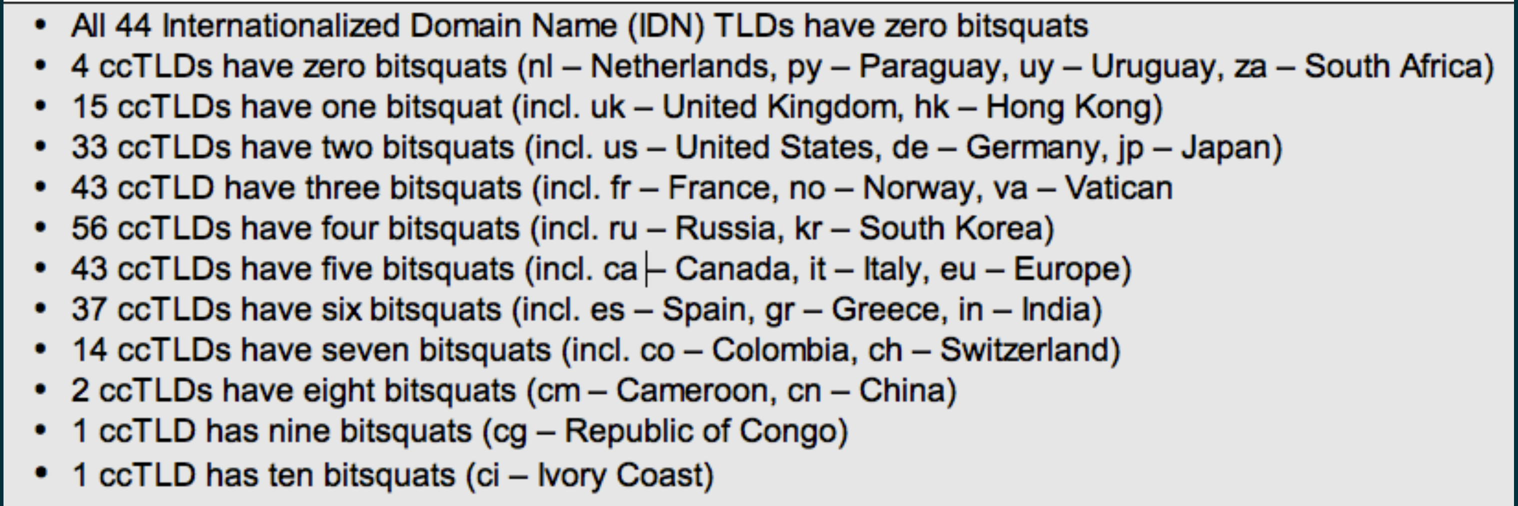
http://isbc.com.cn
- A link containing a letter "c" which has been intentionally flipped to be a letter "#".

Top Level Domain (TLD) Bitsquats

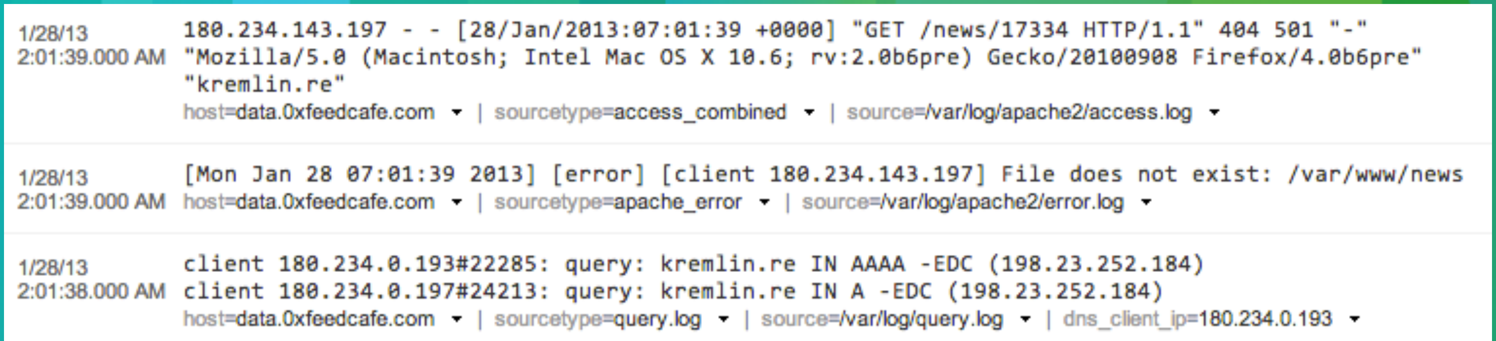
- Bit errors can occur anywhere, so why not in the TLD?
- Most of the generic TLDs (gTLDs) have no bitsquats whatsoever.
- Two gTLDs contain URL Delimiter type bitsquats stemming from the presence of the letter “o”. These are the gTLDs “.pro” and “.coop” with corresponding URL delimiter type bitsquats at the ccTLDs: “.pr” (Puerto Rico) and “.co” (Colombia) respectively

Top Level Domain (ccTLD) Bitsquats

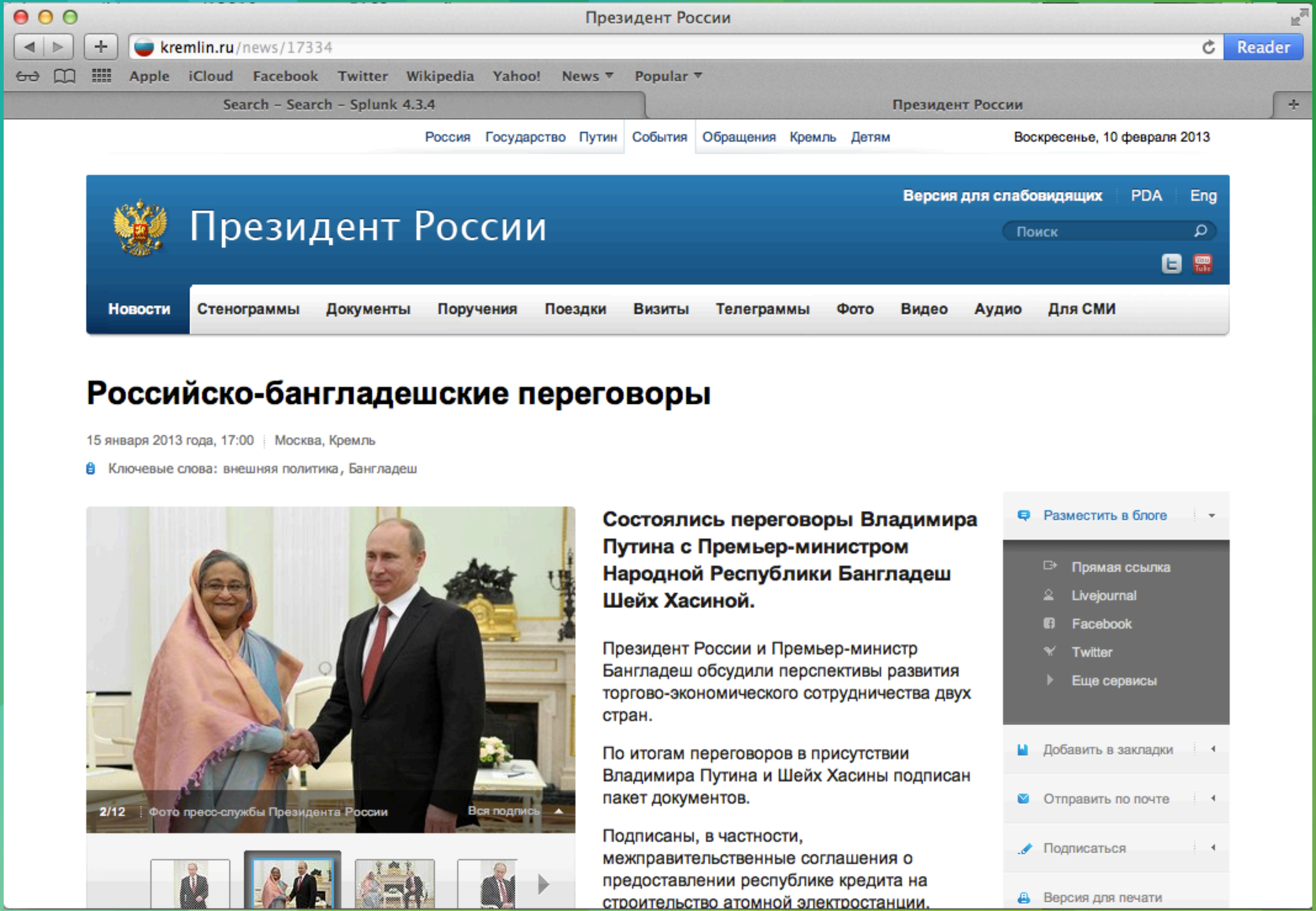
- There happen to be several ccTLDs where bitsquats exist. It is interesting to note that some ccTLDs have no valid bitsquats while other ccTLDs have many. After surveying all valid Internet TLDs and checking the number of possible bitsquats, the following was found:



- All 44 Internationalized Domain Name (IDN) TLDs have zero bitsquats
- 4 ccTLDs have zero bitsquats (nl – Netherlands, py – Paraguay, uy – Uruguay, za – South Africa)
- 15 ccTLDs have one bitsquat (incl. uk – United Kingdom, hk – Hong Kong)
- 33 ccTLDs have two bitsquats (incl. us – United States, de – Germany, jp – Japan)
- 43 ccTLD have three bitsquats (incl. fr – France, no – Norway, va – Vatican
- 56 ccTLDs have four bitsquats (incl. ru – Russia, kr – South Korea)
- 43 ccTLDs have five bitsquats (incl. ca – Canada, it – Italy, eu – Europe)
- 37 ccTLDs have six bitsquats (incl. es – Spain, gr – Greece, in – India)
- 14 ccTLDs have seven bitsquats (incl. co – Colombia, ch – Switzerland)
- 2 ccTLDs have eight bitsquats (cm – Cameroon, cn – China)
- 1 ccTLD has nine bitsquats (cg – Republic of Congo)
- 1 ccTLD has ten bitsquats (ci – Ivory Coast)



```
1/28/13             180.234.143.197 - - [28/Jan/2013:07:01:39 +0000] "GET /news/17334 HTTP/1.1" 404 501 "-"
2:01:39.000 AM      "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:2.0b6pre) Gecko/20100908 Firefox/4.0b6pre"
                    "kremlin.re"
                    host=data.0xfeedcafe.com ▾ | sourcetype=access_combined ▾ | source=/var/log/apache2/access.log ▾

1/28/13             [Mon Jan 28 07:01:39 2013] [error] [client 180.234.143.197] File does not exist: /var/www/news
2:01:39.000 AM      host=data.0xfeedcafe.com ▾ | sourcetype=apache_error ▾ | source=/var/log/apache2/error.log ▾

1/28/13             client 180.234.0.193#22285: query: kremlin.re IN AAAA -EDC (198.23.252.184)
2:01:38.000 AM      client 180.234.0.197#24213: query: kremlin.re IN A -EDC (198.23.252.184)
                    host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=180.234.0.193 ▾
```



Российско-бангладешские переговоры

15 января 2013 года, 17:00 | Москва, Кремль

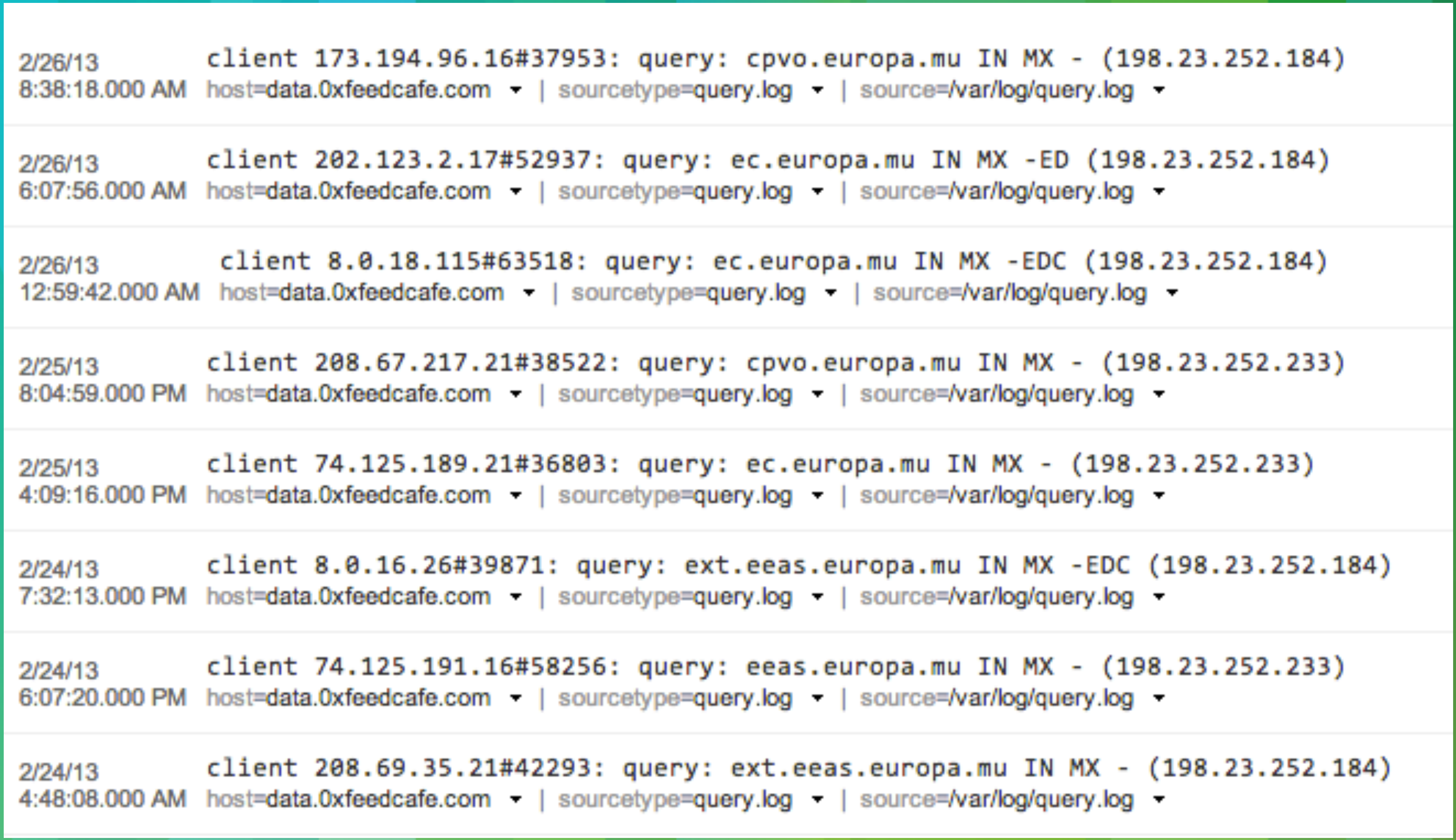
Ключевые слова: внешняя политика, Бангладеш

Состоялись переговоры Владимира Путина с Премьер-министром Народной Республики Бангладеш Шейх Хасиной.

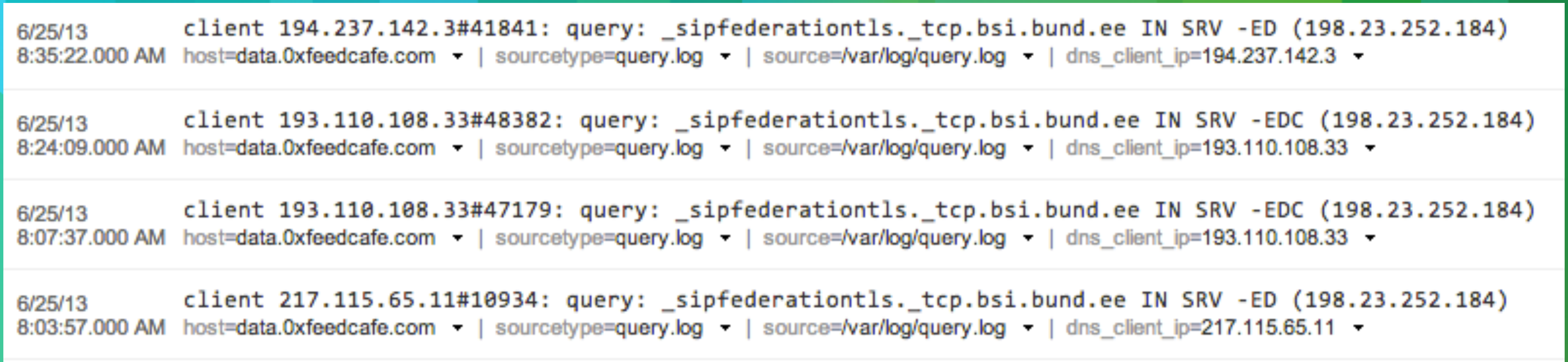
Президент России и Премьер-министр Бангладеш обсудили перспективы развития торгово-экономического сотрудничества двух стран.

По итогам переговоров в присутствии Владимира Путина и Шейх Хасины подписан пакет документов.

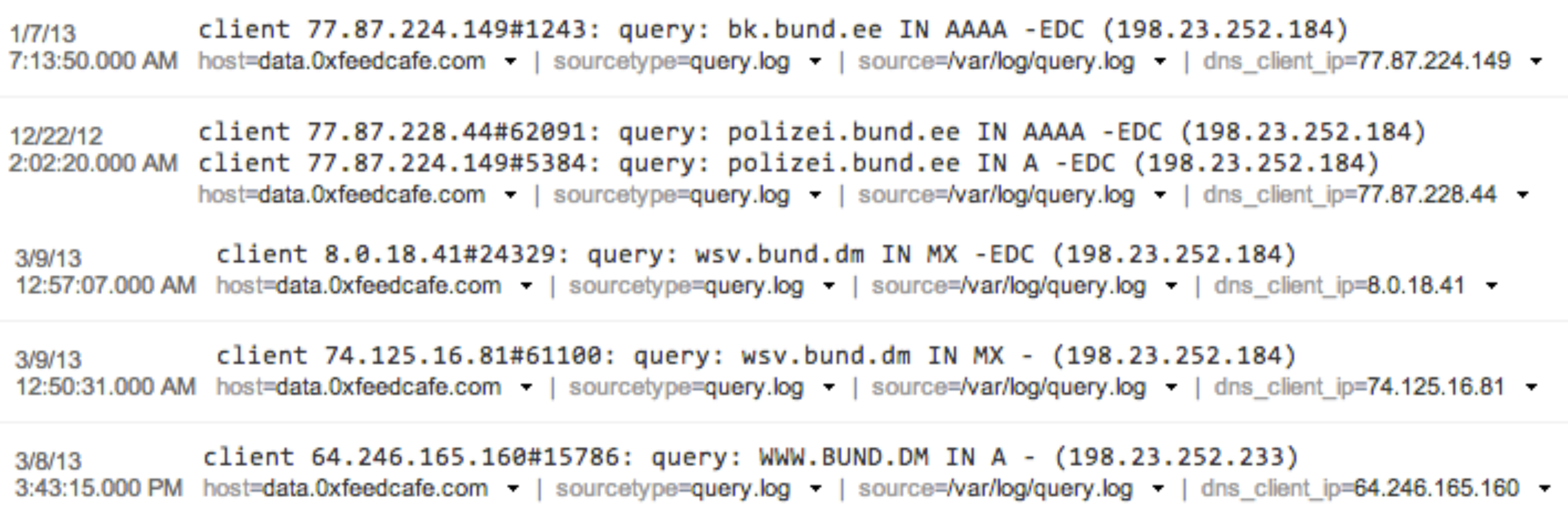
Подписаны, в частности, межправительственные соглашения о предоставлении республике кредита на строительство атомной электростанции.



```
2/26/13          client 173.194.96.16#37953: query: cpvo.europa.mu IN MX - (198.23.252.184)
8:38:18.000 AM   host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾

2/26/13          client 202.123.2.17#52937: query: ec.europa.mu IN MX -ED (198.23.252.184)
6:07:56.000 AM   host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾

2/26/13          client 8.0.18.115#63518: query: ec.europa.mu IN MX -EDC (198.23.252.184)
12:59:42.000 AM  host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾

2/25/13          client 208.67.217.21#38522: query: cpvo.europa.mu IN MX - (198.23.252.233)
8:04:59.000 PM   host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾

2/25/13          client 74.125.189.21#36803: query: ec.europa.mu IN MX - (198.23.252.233)
4:09:16.000 PM   host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾

2/24/13          client 8.0.16.26#39871: query: ext.eeas.europa.mu IN MX -EDC (198.23.252.184)
7:32:13.000 PM   host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾

2/24/13          client 74.125.191.16#58256: query: eeas.europa.mu IN MX - (198.23.252.233)
6:07:20.000 PM   host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾

2/24/13          client 208.69.35.21#42293: query: ext.eeas.europa.mu IN MX - (198.23.252.184)
4:48:08.000 AM   host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾
```



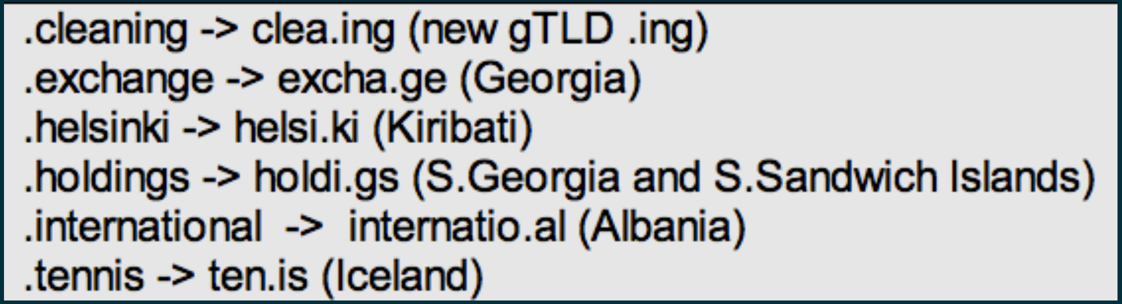
```
6/25/13         client 194.237.142.3#41841: query: _sipfederationtls._tcp.bsi.bund.ee IN SRV -ED (198.23.252.184)
8:35:22.000 AM  host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=194.237.142.3 ▾

6/25/13         client 193.110.108.33#48382: query: _sipfederationtls._tcp.bsi.bund.ee IN SRV -EDC (198.23.252.184)
8:24:09.000 AM  host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=193.110.108.33 ▾

6/25/13         client 193.110.108.33#47179: query: _sipfederationtls._tcp.bsi.bund.ee IN SRV -EDC (198.23.252.184)
8:07:37.000 AM  host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=193.110.108.33 ▾

6/25/13         client 217.115.65.11#10934: query: _sipfederationtls._tcp.bsi.bund.ee IN SRV -ED (198.23.252.184)
8:03:57.000 AM  host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=217.115.65.11 ▾
```



```
1/7/13          client 77.87.224.149#1243: query: bk.bund.ee IN AAAA -EDC (198.23.252.184)
7:13:50.000 AM  host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=77.87.224.149 ▾

12/22/12        client 77.87.228.44#62091: query: polizei.bund.ee IN AAAA -EDC (198.23.252.184)
2:02:20.000 AM  client 77.87.224.149#5384: query: polizei.bund.ee IN A -EDC (198.23.252.184)
                host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=77.87.228.44 ▾

3/9/13          client 8.0.18.41#24329: query: wsv.bund.dm IN MX -EDC (198.23.252.184)
12:57:07.000 AM host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=8.0.18.41 ▾

3/9/13          client 74.125.16.81#61100: query: wsv.bund.dm IN MX - (198.23.252.184)
12:50:31.000 AM host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=74.125.16.81 ▾

3/8/13          client 64.246.165.160#15786: query: WWW.BUND.DM IN A - (198.23.252.233)
3:43:15.000 PM  host=data.0xfeedcafe.com ▾ | sourcetype=query.log ▾ | source=/var/log/query.log ▾ | dns_client_ip=64.246.165.160 ▾
```

New Generic TLD (gTLD) Bitsquats

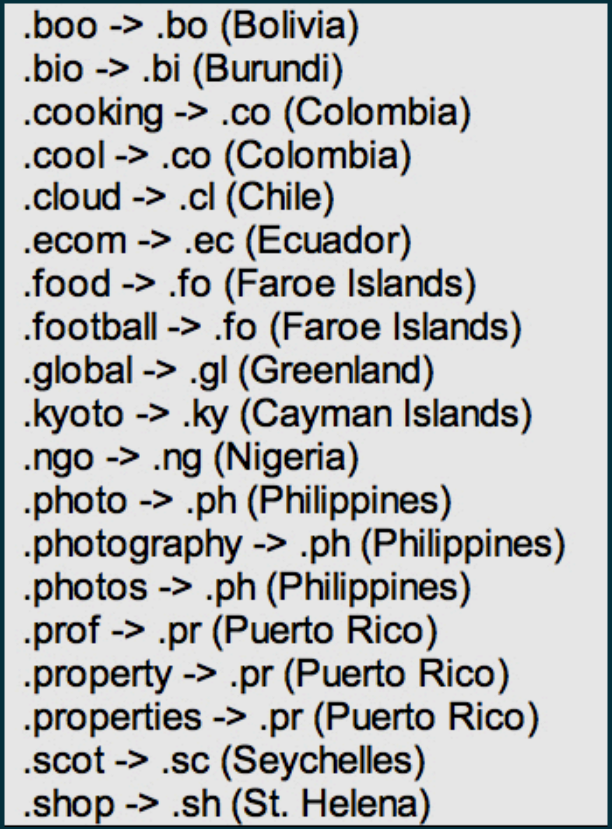
- In 2013 ICANN is approving a number of new gTLDs. Some of these proposed new gTLDs contain subdomain delimiter bitsquats for the entire TLD. Possessing one of these would allow the attacker to mount a bitsquat attack against all domains registered under the target gTLD.



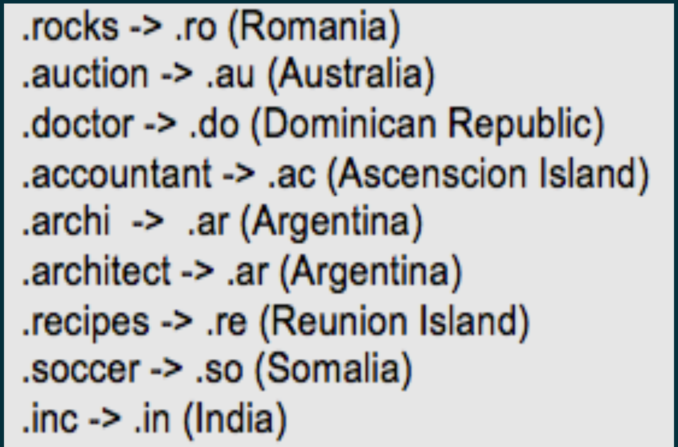
.cleaning -> clea.ing (new gTLD .ing)
.exchange -> excha.ge (Georgia)
.helsinki -> helsi.ki (Kiribati)
.holdings -> holdi.gs (S.Georgia and S.Sandwich Islands)
.international -> internatio.al (Albania)
.tennis -> ten.is (Iceland)

New Generic TLD (gTLD) Bitsquats

- Several of the proposed new gTLDs will have URL delimiter bitsquats in ccTLD space



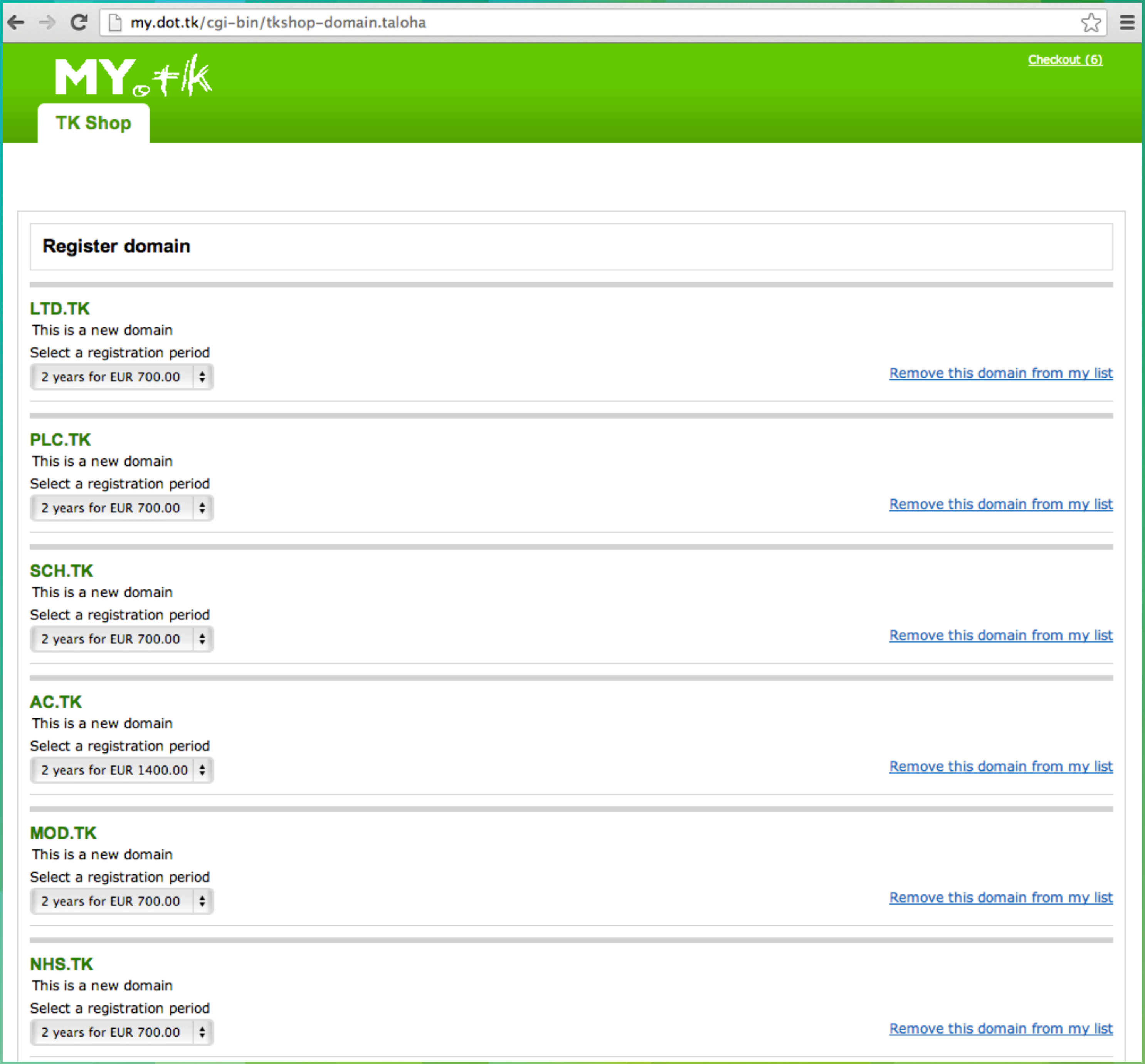
.boo -> .bo (Bolivia)
.bio -> .bi (Burundi)
.cooking -> .co (Colombia)
.cool -> .co (Colombia)
.cloud -> .cl (Chile)
.ecom -> .ec (Ecuador)
.food -> .fo (Faroe Islands)
.football -> .fo (Faroe Islands)
.global -> .gl (Greenland)
.kyoto -> .ky (Cayman Islands)
.ngo -> .ng (Nigeria)
.photo -> .ph (Philippines)
.photography -> .ph (Philippines)
.photos -> .ph (Philippines)
.prof -> .pr (Puerto Rico)
.property -> .pr (Puerto Rico)
.properties -> .pr (Puerto Rico)
.scot -> .sc (Seychelles)
.shop -> .sh (St. Helena)



.rocks -> .ro (Romania)
.auction -> .au (Australia)
.doctor -> .do (Dominican Republic)
.accountant -> .ac (Ascenscion Island)
.archi -> .ar (Argentina)
.architect -> .ar (Argentina)
.recipes -> .re (Reunion Island)
.soccer -> .so (Somalia)
.inc -> .in (India)

More ccTLD Bitsquats

- The ".uk" (United Kingdom) ccTLD has one ccTLD bitsquat.
- The bitsquat ccTLD is ".tk" (Tokelau)
- The .uk domain registrar Nominet restricts ".uk" domain names to one of several canned 2nd level domain prefixes. For example, co.uk, net.uk, org.uk, and so on
- Several of the same 2nd level ".tk" domains are available. By registering one of these domains, a bitsquatter would receive bitsquats for ***any*** domain underneath the corresponding 2nd level domain in ".uk"



my.dot.tk/cgi-bin/tkshop-domain.taloha

Register domain

LTD.TK
This is a new domain
Select a registration period
2 years for EUR 700.00
Remove this domain from my list

PLC.TK
This is a new domain
Select a registration period
2 years for EUR 700.00
Remove this domain from my list

SCH.TK
This is a new domain
Select a registration period
2 years for EUR 700.00
Remove this domain from my list

AC.TK
This is a new domain
Select a registration period
2 years for EUR 1400.00
Remove this domain from my list

MOD.TK
This is a new domain
Select a registration period
2 years for EUR 700.00
Remove this domain from my list

NHS.TK
This is a new domain
Select a registration period
2 years for EUR 700.00
Remove this domain from my list

Current Bitsquatting Mitigations

- Use Error Correcting (ECC) memory.

  Needs to happen simultaneously, and world-wide to be an effective solution.

- Register the bitsquat domain so that no third party can register it.

  This is not always possible, as many popular bitsquat domains have already been registered. Depending on the length of the domain, this can also be a costly endeavor.

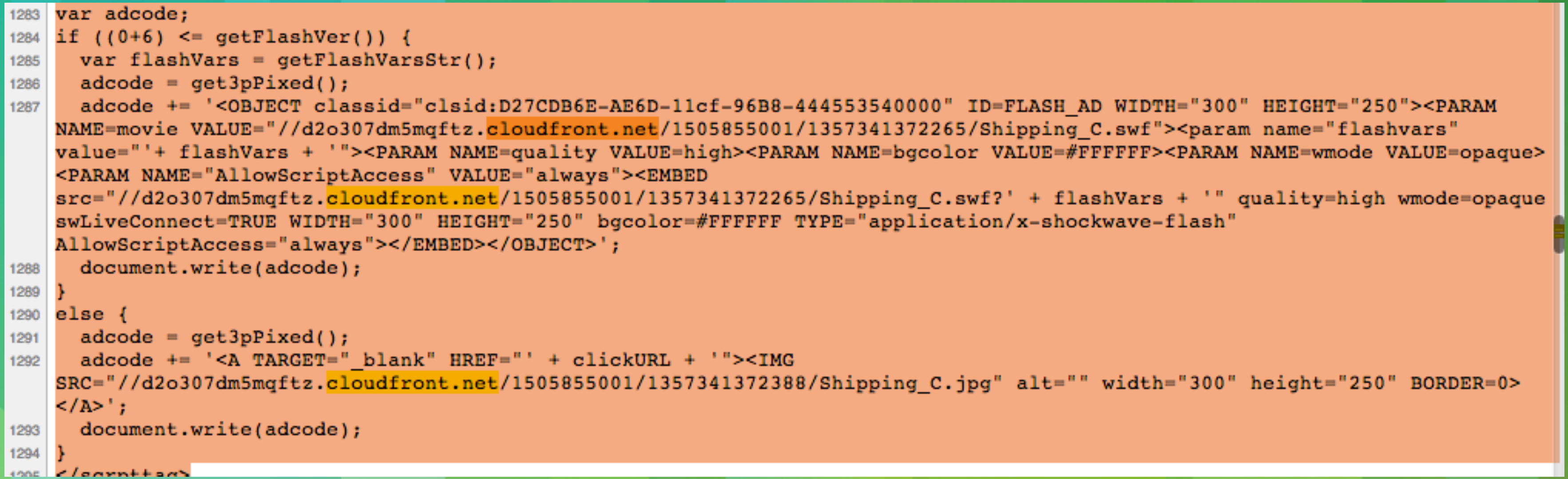
- We can do better than this…

New Mitigation for Bitsquatting #1

- Because some of these new bitsquatting techniques rely on 3rd level domain names to work, then a careful strategy around their selection and use can help avoid the possibility of bitsquats
- Simply subdivide 2nd level domain traffic among a large number of 3rd level domains. Each subdomain takes on a small slice of the overall potential bitsquat traffic and therefore becomes much less likely to result in a successful bitsquat attack.
- If those subdomains are changed or updated with any frequency, a bitsquatter will have practically no chance at a successful attack.

Amazon includes in their web pages content from a domain named cloudfront.com. The 3rd level domain names here normally would make great URL delimiter bitsquats because the “o” in cloudfront yields a valid ccTLD in .cl (Chile)… EXCEPT

Amazon changes the subdomain at cloudfront.com frequently enough that this thwarts attempts to capitalize on bitsquat traffic. By changing the 3rd level domain name frequently, Amazon leaves too small a window of time in which to set-up and collect bitsquat traffic.

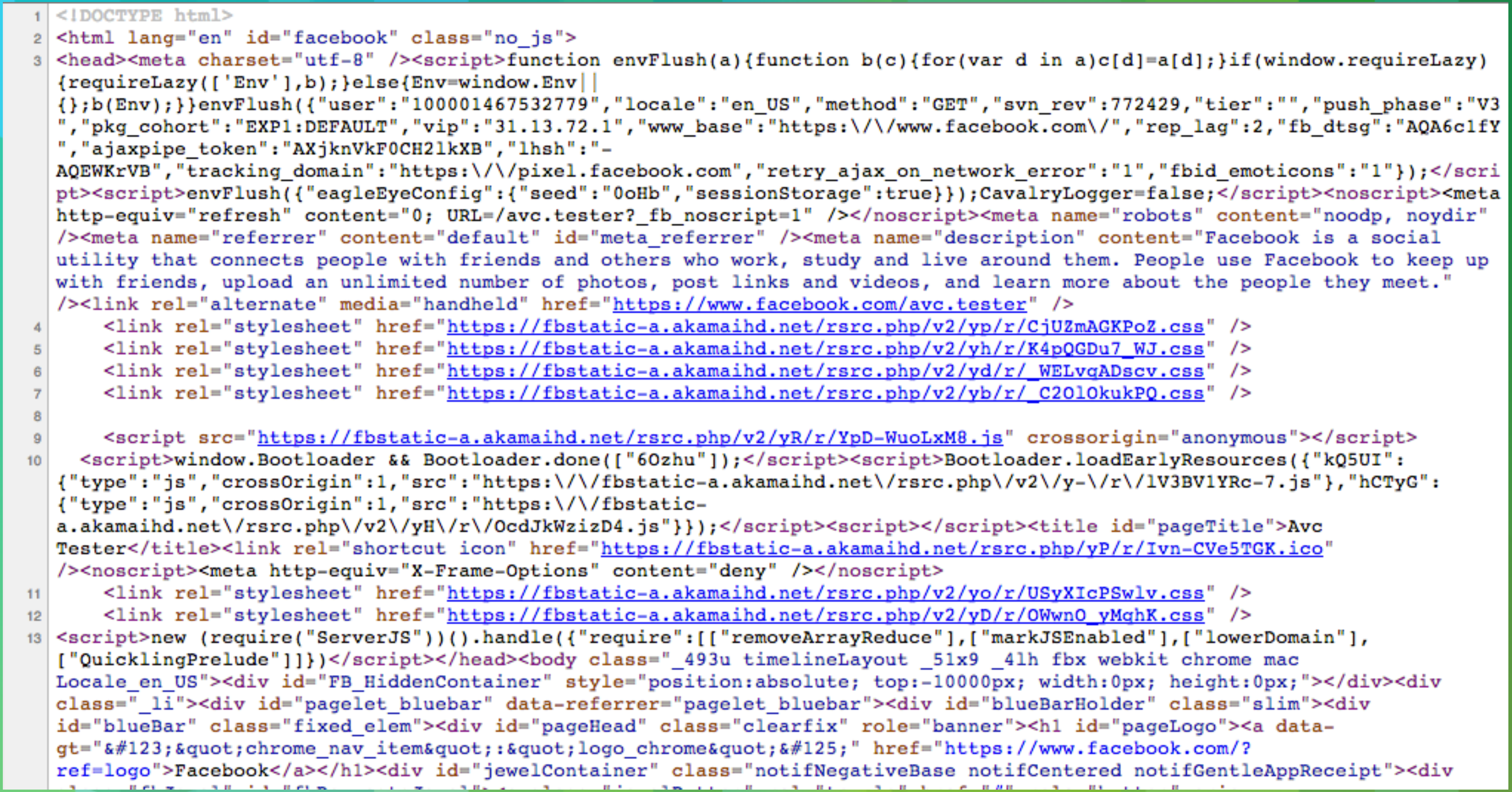


```
var adcode;
if ((0+6) <= getFlashVer()) {
  var flashVars = getFlashVarsStr();
  adcode = get3pPixed();
  adcode += '<OBJECT classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" ID=FLASH_AD WIDTH="300" HEIGHT="250"><PARAM
NAME=movie VALUE="//d2o307dm5mqftz.cloudfront.net/1505855001/1357341372265/Shipping_C.swf"><param name="flashvars"
value="'+ flashVars + '"><PARAM NAME=quality VALUE=high><PARAM NAME=bgcolor VALUE=#FFFFFF><PARAM NAME=wmode VALUE=opaque>
<PARAM NAME="AllowScriptAccess" VALUE="always"><EMBED
src="//d2o307dm5mqftz.cloudfront.net/1505855001/1357341372265/Shipping_C.swf?' + flashVars + '" quality=high wmode=opaque
swLiveConnect=TRUE WIDTH="300" HEIGHT="250" bgcolor=#FFFFFF TYPE="application/x-shockwave-flash"
AllowScriptAccess="always"></EMBED></OBJECT>';
  document.write(adcode);
}
else {
  adcode = get3pPixed();
  adcode += '<A TARGET="_blank" HREF="' + clickURL + '"><IMG
SRC="//d2o307dm5mqftz.cloudfront.net/1505855001/1357341372388/Shipping_C.jpg" alt="" width="300" height="250" BORDER=0>
</A>';
  document.write(adcode);
}
</scripttag>
```

New Mitigation for Bitsquatting #2

- The majority of the bitsquat requests that Dinaburg received during his original bitsquatting research came from domain variants of Facebook’s content delivery network fbcdn.net. Facebook is a web application.
- The web application design can be changed to help reduce the number of times the domain name appears in memory, thus reducing the number of opportunities for a bitsquat request.
- Using relative links inside of HTML instead of absolute links reduces the number of appearances of the domain name.
- With a base href, the domain name will appear at most once per HTML page. The downside is that if a bit error does occur in the base href, then all links in the document would go to the same bitsquat domain.

Notice the prevalence of absolute URLs used by Facebook



```
<!DOCTYPE html>
<html lang="en" id="facebook" class="no_js">
<head><meta charset="utf-8" /><script>function envFlush(a){function b(c){for(var d in a)c[d]=a[d];}if(window.requireLazy)
{requireLazy(['Env'],b);}else{Env=window.Env||
{};b(Env);}}envFlush({"user":"100001467532779","locale":"en_US","method":"GET","svn_rev":772429,"tier":"","push_phase":"V3
","pkg_cohort":"EXP1:DEFAULT","vip":"31.13.72.1","www_base":"https:\/\/www.facebook.com\/","rep_lag":2,"fb_dtsg":"AQA6c1fY
","ajaxpipe_token":"AXjknVkF0CH21kXB","lhsh":"-
AQEWKrVB","tracking_domain":"https:\/\/pixel.facebook.com","retry_ajax_on_network_error":"1","fbid_emoticons":"1"});</scri
pt><script>envFlush({"eagleEyeConfig":{"seed":"0oHb","sessionStorage":true}});CavalryLogger=false;</script><noscript><meta
http-equiv="refresh" content="0; URL=/avc.tester?_fb_noscript=1" /></noscript><meta name="robots" content="noodp, noydir"
/><meta name="referrer" content="default" id="meta_referrer" /><meta name="description" content="Facebook is a social
utility that connects people with friends and others who work, study and live around them. People use Facebook to keep up
with friends, upload an unlimited number of photos, post links and videos, and learn more about the people they meet."
/><link rel="alternate" media="handheld" href="https://www.facebook.com/avc.tester" />
    <link rel="stylesheet" href="https://fbstatic-a.akamaihd.net/rsrc.php/v2/yp/r/CjUZmAGKPoZ.css" />
    <link rel="stylesheet" href="https://fbstatic-a.akamaihd.net/rsrc.php/v2/yh/r/K4pQGDu7_WJ.css" />
    <link rel="stylesheet" href="https://fbstatic-a.akamaihd.net/rsrc.php/v2/yd/r/_WELvqADscv.css" />
    <link rel="stylesheet" href="https://fbstatic-a.akamaihd.net/rsrc.php/v2/yb/r/_C2OlOkukPQ.css" />

    <script src="https://fbstatic-a.akamaihd.net/rsrc.php/v2/yR/r/YpD-WuoLxM8.js" crossorigin="anonymous"></script>
  <script>window.Bootloader && Bootloader.done(["6Ozhu"]);</script><script>Bootloader.loadEarlyResources({"kQ5UI":
{"type":"js","crossOrigin":1,"src":"https:\/\/fbstatic-a.akamaihd.net\/rsrc.php\/v2\/y-\/r\/1V3BV1YRc-7.js"},"hCTyG":
{"type":"js","crossOrigin":1,"src":"https:\/\/fbstatic-
a.akamaihd.net\/rsrc.php\/v2\/yH\/r\/OcdJkWzizD4.js"}});</script><script></script><title id="pageTitle">Avc
Tester</title><link rel="shortcut icon" href="https://fbstatic-a.akamaihd.net/rsrc.php/yP/r/Ivn-CVe5TGK.ico"
/><noscript><meta http-equiv="X-Frame-Options" content="deny" /></noscript>
    <link rel="stylesheet" href="https://fbstatic-a.akamaihd.net/rsrc.php/v2/yo/r/USyXIcPSwlv.css" />
    <link rel="stylesheet" href="https://fbstatic-a.akamaihd.net/rsrc.php/v2/yD/r/OWwnO_yMqhK.css" />
<script>new (require("ServerJS"))().handle({"require":[["removeArrayReduce"],["markJSEnabled"],["lowerDomain"],
["QuicklingPrelude"]]})</script></head><body class="_493u timelineLayout _51x9 _4lh fbx webkit chrome mac
Locale_en_US"><div id="FB_HiddenContainer" style="position:absolute; top:-10000px; width:0px; height:0px;"></div><div
class="_li"><div id="pagelet_bluebar" data-referrer="pagelet_bluebar"><div id="blueBarHolder" class="slim"><div
id="blueBar" class="fixed_elem"><div id="pageHead" class="clearfix" role="banner"><h1 id="pageLogo"><a data-
gt="&#123;&quot;chrome_nav_item&quot;:&quot;logo_chrome&quot;&#125;" href="https://www.facebook.com/?
ref=logo">Facebook</a></h1><div id="jewelContainer" class="notifNegativeBase notifCentered notifGentleAppReceipt"><div
```

New Mitigation for Bitsquatting #3

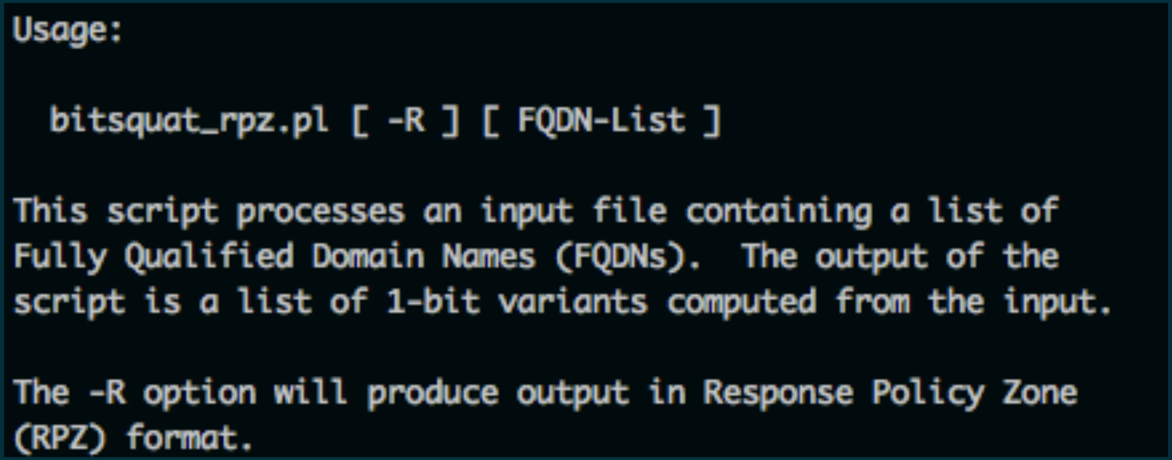
- Capital ASCII characters are equivalent for DNS and URL hostname purposes, but possess fewer bits error variants
- There are no bit error variants of capital letters in the range 0-9
- The "." is not a bit error variant of the capital letter "N", only the lowercase "n"
- The "/" is not a bit error variant of the capital letter "O", only the lowercase "o"
- The "#" is not a bit error variant of the capital letter "C", only the lowercase "c"
- By simply substituting capital letters whenever lowercase letters "c", and "m" through "y" appear in a domain name, several bitsquat variants can be avoided.

New Mitigation for Bitsquatting #4

- Create an RP zone containing bitsquats of popular domains. These bitsquat domains can be configured with CNAMEs that point at the real domain, silently "correcting" bit errors without any work on the part of the client experiencing the bit error.
- There is a bitsquat domain of "paypal.com" called "raypal.com". It is a real site, and not affiliated with PayPal, but it would be much more likely for a network's users to be going to paypal.com instead. Therefore, some of these legitimate sites could either be whitelisted or just be counted as acceptable FPs.

bitsquat_rpz.pl

- A Perl script which accepts Fully Qualified Domain Names (FQDNs) as input. The output is a list of all the 1-bit variants. Output may also be written as a Response Policy Zone (RPZ)
- http://blogs.cisco.com/wp-content/uploads/bitsquat_rpz.pl_.zip



```
Usage:

  bitsquat_rpz.pl [ -R ] [ FQDN-List ]

This script processes an input file containing a list of
Fully Qualified Domain Names (FQDNs).  The output of the
script is a list of 1-bit variants computed from the input.

The -R option will produce output in Response Policy Zone
(RPZ) format.
```

Conclusion

- Bitsquatting is easier than it ever has been given the number of devices attached to the internet that lack error correcting memory. Bitsquatting will become easier to do over time.
- Bitsquatting affects less popular sites too, even sites registered at “protected” TLDs like .gov, .edu, and .mil are vulnerable to some of these new techniques.
- Guarding against bitsquatting need not involve mass registration of domain names. Since DNS is critical for bitsquatting attacks, using a DNS resolver with a RPZ that blocks/redirects likely bitsquat requests can provide the ultimate protection.
- http://blogs.cisco.com/security/

Special thanks to the following individuals. Without their assistance this research would not have been possible:

Adam Katz
Seth Hanford
Gavin Reid
Allyn Romanow
Henry Stern

Thank you.

cisco