.CLUB
www.DotClub.com

1640 West Oakland Park Blvd. #30
Oakland Park, FL, 33311
www.dotclub.com
P: 1-877-833-0000
F: 1-888-886-0462

September 16, 2013

Mr. Cherine Chalaby, Chair
New gTLD Program Committee
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-25360
USA

RE: .CLUB DOMAINS' STRATEGY TO REDUCE NAME COLLISION IN DNS TO A LOW RISK LEVEL

Dear Mr. Chairman and Members of the New gTLD Program Committee:

Thank you for giving us the opportunity to address you once again on the collision issue. .CLUB DOMAINS, LLC would like to reiterate that we appreciate and share ICANN's commitment to serving the public interest and preserving the stability of the Domain Name System.

In response to the original Interisle Report, ICANN stated that "**applicant[s] for [uncalculated risk] strings can work towards resolving the issues that prevented their proposed string from being categorized as low risk.**"[1]

The following outlines the process that .CLUB DOMAINS has taken to calculate and mitigate the potential risk of name collision:

- .CLUB DOMAINS has commissioned a report from Interisle that analyzes the "2013 Day in the Life of the Internet" (DITL) root query stream, hosted at DNS Operations, Analysis, and Research Center (OARC), relating to queries where "CLUB" was in the TLD position.[2]
- The .CLUB-Interisle Report highlights the top 50 Second Level Domain (SLD) strings ranked by occurrence, which account for 58.88% of all queries in the 2013 DITL query stream with "CLUB" in the TLD position.
- .CLUB DOMAINS is committed to restricting the top 50 most queried SLD strings from being registered thereby eliminating the possibility of name collision for 58.88% of the queries represented in the DITL root query data stream.
- Blocking the top 50 most queried Second Level Domain strings reduces .CLUB's queries to fewer than that of 62 strings that were classified as *low risk*.[3, 4, 5]

[1] ICANN. *New gTLD Collision Risk Mitigation: Proposals to mitigate the collision risks between new gTLDs and existing private uses of the same strings*, see pg. 3. <http://www.icann.org/en/about/staff/security/ssr/new-gtld-collision-mitigation-05aug13-en.pdf>. (Emphasis added).

[2] Interisle. *Analysis of the ICANN "Name Collision in the DNS" Study Data Specific to Proposed TLD "club"* (September 11, 2013). Attached as Appendix A.

[3] Ibid, see pg. 3.

[4] Interisle. *Name Collision in the DNS*, see pgs. 139-141. <http://www.icann.org/en/about/staff/security/ssr/name-collision-02aug13-en.pdf>.

[5] ICANN. *New gTLD Proposed Classifications*, see pg. 2. <http://www.icann.org/en/about/staff/security/ssr/new-gtlds-proposed-class-08aug13-en.xlsx>.

Based on the above considerations, .CLUB's potential risk for collision in the DNS has been calculated and mitigated; therefore, .CLUB should be classified as a *low risk* gTLD string.

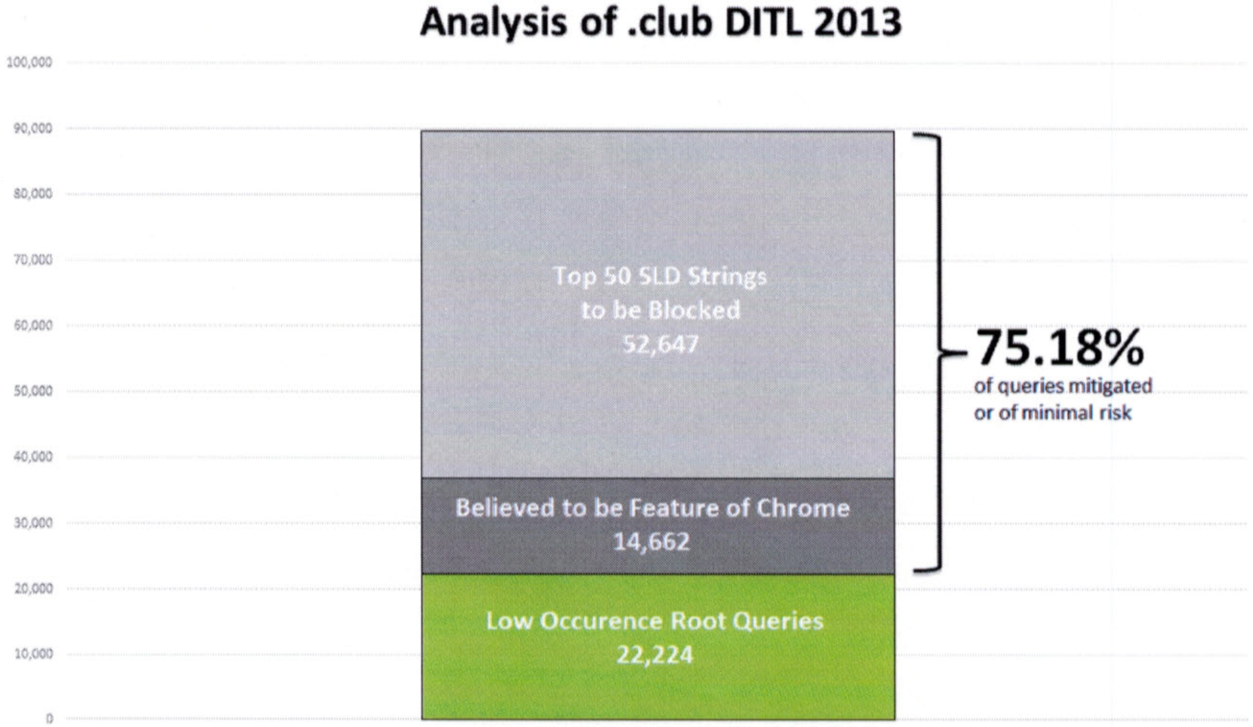

Figure A.

1. **.CLUB DOMAINS has commissioned a report from Interisle for the specific DITL data with "CLUB" in the TLD position. The data in the report supports the solution of restricting the top 50 most queried SLD strings, which will reduce the potential number of name collisions by 58.88%. This greatly reduces any threat .CLUB would pose to the stability and security of the Domain Name System and places .CLUB well within the range of the *low risk* category.**

.CLUB DOMAINS has commissioned a report from Interisle that analyzes the queries for the TLD .CLUB to determine which .CLUB SLD strings receive the highest number of invalid queries at the root (herein referred to as the .CLUB-Interisle Report).[6] The .CLUB-Interisle Report states that "Interisle believes that, within the limits of the data sources, the data presented here is a reasonable representation of the traffic relating to the proposed TLD string 'club' at the root servers."[7] The .CLUB-Interisle Report follows ICANN's lead in taking as axiomatic that the number of invalid queries directed at the root is directly related to the risk of collision for those TLD strings.[8]

[6] Ibid.

[7] Ibid.

[8] Interisle. *Name Collision in the DNS*, see pgs. 41-44.

2. **The .CLUB-Interisle Report highlights the most frequently queried SLD strings based on the DITL 2013 query stream.**[9]

The .CLUB-Interisle Report lists the top 50 strings queried at the Second Level for the TLD .CLUB.[10] The table below indicates the data:[11]

	2nd Level Names (Blocking 50 Strings)	**Occurrences** (Blocking 52,647 out of the 89,533)
1	_udp	7,770
2	kennel	5,974
3	net	2,697
4	wpad	2,627
5	www	2,540
6	cs	2,487
7	_msdcs	2,442
8	com	2,369
9	flagman	1,615
10	org	1,334
11	fedex	1,135
12	local	1,114
13	xvision	1,080
14	hsbcc	1,062
15	info	1,001
16	suwan	960
17	nfl	861
18	isatap	790
19	_tcp	765
20	bankers	704
21	breakfast	686
22	share	647
23	abi	641
24	elite	585
25	saad	545
26	_sites	535
27	forrestmix	524
28	cc	489
29	jenavi	458
30	woldsgliding	417
31	cariari	371

[9] Ibid.

[10] Ibid, see pg. 44.

[11] Ibid, see pg. 3.

32	mail	370
33	youtube	356
34	club-control	334
35	game	319
36	yono	316
37	post	308
38	boyandgirls	307
39	internet	303
40	enterprise	298
41	magnolia	297
42	server	290
43	boysandgirls	281
44	ace	250
45	mby	245
46	club	243
47	lakewood	239
48	dc	236
49	clubnt	216
50	mccoy	214

According to the .CLUB-Interisle data, blocking the 50 SLD strings from registration would prevent 52,647 out of the 89,533 queries from a potential collision (58.88%). After blocking the top 50 strings as SLD strings, only 36,886 (41.12%) queries remain, which is 12,114 fewer invalid queries at the root than .engineering[12] received, which ICANN classified as a *low risk* gTLD.[13, 14] In fact, after blocking the top 50 strings from being registered, .CLUB will receive fewer queries that could result in collisions than 62 gTLD strings which ICANN has already classified as *low risk.*[15]

One could take a hyper-conservative approach to mitigation and decline to take into account the SLD strings being blocked by the registry agreement. If the reduction in queries created by blocking .WWW, .CS, .CC, and .DS were not applied against the total queries at the root, .CLUB's reduction in queries would still have a reduction in queries of 46,895, resulting in a total query count of 42,638. Thus, even this more conservative analysis would result in 6,362 fewer queries than the highest queried *low risk* string. We believe this approach is too conservative; but even if ICANN chooses to implement this approach, .CLUB is clearly placed within the category of *low risk*.

3. **16.4% of the SLD strings queried for .CLUB are for 10 character randomly generated strings that were queried only once or twice.**

[12] .Engineering was chosen as the benchmark because it is the most frequently queried gTLD that ICANN classified as *low risk*.

[13] Interisle. *Name Collision in the DNS*, see pg. 142.

[14] ICANN. *New gTLD Proposed Classifications*, see pg. 2.

[15] Interisle. *Name Collision in the DNS,* see pgs. 142-144.

Additionally, 19% of queries were for 10 character randomly generated strings that pose minimal risk of potential collision. The .CLUB-Interisle Report explains:

> "16,972 (19.0%) of the 89,533 queries had an SLD comprising 10 alphabetic characters, which could be a result of a feature of the Chrome browser, choosing "random" 10-character alphabetic strings to defend against domain name hijacking. 1,930 (2.2%) of these strings occurred only once; 14,662 (16.4%) of these strings occurred only once or twice."[16]

Long strings of randomly generated characters do not pose any potential risk of collision, because the probability of the queried string being resolvable is extremely low. Indeed, the very reason that Chrome generates a query with these characters is to create a Second Level Domain string that will not resolve. Because 52,647 (58.88%) of queries will not resolve due to blocking the top 50, only 36,886 (41.12% of the total) will remain. Of these 36,886, 14,662 (16.4%) appear to randomly generated and are likely the product of the Chrome browser, with no measurable risk of collision; thus, only 22,224 (24.82% of the total) of the original 89,533 remain as queries that can potentially cause collisions. This point is illustrated above in Figure A.

4. .CLUB DOMAINS is committed to blocking these names using whichever process ICANN suggests.

.CLUB is committed to blocking the above mentioned SLD strings, pursuant to Section 2.6 of the Registry Agreement, which states that "Registry Operator may at any time establish or modify policies concerning Registry Operator's ability to [...] block additional character strings within the TLD at its discretion."[17] .CLUB DOMAINS awaits guidance from ICANN regarding the method that it would prefer we use to bind ourselves to the blocking of the aforementioned SLD strings for the time necessary to allay the risk of collision in the DNS. We propose blocking the aforementioned SLD strings for at least three years, subject to future release per the RSEP or other ICANN review mechanism.[18]

5. In accordance with ICANN's proposal for the *low risk* category, .CLUB DOMAINS will implement the two suggested mitigation measures for all remaining SLD strings.

.CLUB DOMAINS will wait 120 days, or whatever standard period ICANN implements, from the execution of the Registry Agreement to activate any unblocked names, in accordance with ICANN's mandate for *low risk* strings:

> "First, registry operators will implement a period of no less than 120 days from the date that a registry agreement is signed before it may activate any names under the TLD in the DNS. This measure will help mitigate the risks related to the internal name certificates issue as described in the Study report and SSAC Advisory on Internal Name Certificates. Registry operators, if they wish, may allocate names during this period, i.e., accept registrations, but they will not activate them in DNS."[19]

[16] Interisle. *Analysis of the ICANN "Name Collision in the DNS" Study Data Specific to Proposed TLD "club"*, see pg. 11.

[17] ICANN. *Approved Registry Agreement - July 2, 2013*, see Section 2.6.

[18] Ibid, see Section 2.1.

[19] ICANN. *New gTLD Collision Risk Mitigation: Proposals to mitigate the collision risks between new gTLDs and existing private uses of the same strings*, see pgs. 2, 3.

.CLUB DOMAINS will wait 30 days, or whatever standard period ICANN implements, after delegation to activate any names in the DNS:

> "Second, once a TLD is first delegated within the public DNS root to name servers designated by the registry operator, the registry operator will not activate any names under the TLD in the DNS for a period of no less than 30 days. During this 30-day period, the registry operator will notify the point of contacts of the IP addresses that issue DNS requests for an un-delegated TLD or names under it."[20]

Applying these two mitigation measures to all .CLUB SLD strings, combined with the blocking of the 50 most queried SLD strings, will be overwhelmingly sufficient to allay any potential risk that .CLUB might pose to the DNS, such that .CLUB will pose an even lower risk than a significant portion of the *low risk* gTLDs that ICANN has permitted to execute Registry Agreements.

6. .CLUB does not carry any of the risks related to issuance of X.509 certificates.

The X.509 issue addressed in the Interisle Report does not apply to .CLUB.[21] The Interisle Report suggests that an important indicator of risk is how many private X.509 certificates have been issued for potential gTLDs.[22] Appendix C of the Interisle Report lists each domain that was assigned three or more private X.509 certificates, and .CLUB does not appear on the list.[23]

7. .CLUB should be categorized as *low risk* because, with these mitigation measures taken into account, it receives fewer resolvable queries than a significant portion of the gTLD strings that ICANN has classified as *low risk.*

"Equitable Treatment. ICANN shall not apply standards, policies, procedures or practices arbitrarily, unjustifiably, or inequitably and shall not single out Registry Operator for disparate treatment unless justified by substantial and reasonable cause."[24]

.CLUB has resolved the issue that prevented it from being categorized as *low risk*. Given that .CLUB DOMAINS is committed to blocking the top 50 most queried Second Level Domain strings, .CLUB presents an even lower risk of collision than 62 domains which have been classified as *low risk*. Therefore, in accordance with ICANN's commitment to equitable treatment, the delegation of .CLUB should not suffer further delays.

Conclusion

- ICANN has stated that the reason .CLUB was classified as uncalculated risk is that "[t]he Study did not find enough information to properly classify these strings given the short timeline."[25] .CLUB

[20] Ibid.

[21] Interisle. *Name Collision in the DNS*, see pgs. 58-67.

[22] Ibid.

[23] Ibid, see pgs. 175-179.

[24] ICANN. *Approved Registry Agreement - July 2, 2013*, see Section 3.2.

[25] ICANN. *New gTLD Proposed Classifications*, see pg. 2.

DOMAINS commissioned a new study that provides enough information to properly calculate the potential risks associated with the delegation of .CLUB.[26] In addition, the new Interisle study highlights a substantial number of random 10 character queries that likely pose no potential threat of collision.[27]

- In response to ICANN's statement that, "applicant[s] for [uncalculated risk] strings can work towards resolving the issues that prevented their proposed string from being categorized as low risk," .CLUB DOMAINS has committed to blocking the top 50 most queried Second Level Domain strings for .CLUB.[28, 29]

- Blocking the 50 most queried Second Level Domain strings would prevent 52,647 out of 89,533 total queries from being resolvable, leaving only 36,886 resolvable queries.[30] Therefore, after blocking the top 50 most queried Second Level Domain strings, **.CLUB will receive fewer invalid queries at the root than 62 of the gTLD strings that ICANN has classified as *low risk*.**

- .CLUB DOMAINS is taking all necessary steps to protect the Domain Name System from the potential risks associated with collision; therefore, ICANN should classify .CLUB as a *low risk* gTLD string and allow .CLUB DOMAINS to execute a Registry Agreement for .CLUB without unnecessary delays.

Thank you again for your kind attention to this paper and to the attached report.

Very truly yours,

Dirk Bhagat
Chief Technology Officer
.CLUB DOMAINS, LLC

Enclosures: 1

[26] Interisle. *Analysis of the ICANN "Name Collision in the DNS" Study Data Specific to Proposed TLD "club"*.

[27] Ibid, see pg. 11.

[28] ICANN. *New gTLD Collision Risk Mitigation: Proposals to mitigate the collision risks between new gTLDs and existing private uses of the same strings*, see pg. 3.

[29] *Supra*, see pg. 1.

[30] Interisle. *Analysis of the ICANN "Name Collision in the DNS" Study Data Specific to Proposed TLD "club"*, see pgs. 3, 4.

APPENDIX A

Analysis of the ICANN "Name Collision in the DNS" Study Data Specific to Proposed TLD "`club`"

Prepared by Interisle Consulting Group, LLC

Interisle
Consulting Group

Version 1.1
11 September 2013

Approach

Interisle performed a detailed analysis of the data gathered during the "Name Collision in the DNS" study in order to extract specific information concerning the proposed TLD "club".

Interisle analyzed one of the two sets of data on which the "Name Collision" study was based—the root query stream captured during the 2013 "Day in the Life of the Internet" exercise hosted by the DNS Operations, Analysis, and Research Center (OARC)—looking specifically at occurrences of the proposed TLD string "club", and this report presents the results of that analysis for 2013.

This report is a factual presentation of the data analysis results. It does not interpret the results, make recommendations, or otherwise discuss the potential meaning of the results.

Caveats

Specific note is made of the report to ICANN "Name Collision in the DNS" sections 4.3 ("Data limitations and systematic errors"), 4.3.1 ("Incomplete coverage of root servers"), 4.3.4 ("Systematic errors"), 4.3.5 ("Temporal limitation"), and 4.3.6 ("Geographical limitation"). These same considerations apply to the data presented in this report.

Interisle believes that, within the limits of the data sources, the data presented here is a reasonable representation of the traffic relating to the proposed TLD string "club" at the root servers. However, the reader is cautioned not to confuse precision with accuracy - that is, numbers that are cited always have a margin of error.

ICANN Report Summary

In the ICANN report of the "Name Collision in the DNS" Appendix B, the proposed TLD string "club" shows:

- From the DITL 2013 data, "club" ranks 184, with 90k requests at the root.

Full Data

Because of the size of the data involved for some of this report's tables, the report contains limited amounts of the data - the full tables are contained in a companion Excel workbook.

2013 Data

2nd Level Names

The following is a list of the first 50 and last 50 distinct 2nd level names that appears in a queried domain name in which "club" is the TLD, with an occurrence count for each. An asterisk shows which of these names is a 10-alphabetic-character string; this could be due to the Chrome browser "feature". The cumulative percentage is indicated in the third column.

There were a total of 89,533 occurrences comprising 12,164 separate strings.

_udp	7,770		9%
kennel	5,974		15%
net	2,697		18%
wpad	2,627		21%
www	2,540		24%
cs	2,487		27%
_msdcs	2,442		30%
com	2,369		32%
flagman	1,615		34%
org	1,334		36%
fedex	1,135		37%
lokal	1,114		38%
xvision	1,080		39%
hsbcc	1,062		41%
info	1,001		42%
suwan	960		43%
nfl	861		44%
isatap	790		45%
_tcp	765		45%
bankers	704		46%
breakfast	686		47%
share	647		48%
abi	641		48%
elite	585		49%
saad	545		50%

_sites	535		50%
forrestmix	524	*	51%
cc	489		51%
jenavi	458		52%
woldsgliding	417		52%
cariari	371		53%
mail	370		53%
youtube	356		54%
club-control	334		54%
game	319		54%
yono	316		55%
post	308		55%
boyandgirls	307		55%
internet	303		56%
enterprise	298	*	56%
magnolia	297		56%
server	290		57%
boysandgirls	281		57%
ace	250		57%
mby	245		58%
club	243		58%
lakewood	239		58%
dc	236		58%
clubnt	216		59%
mccoy	214		59%

taobao	1		100%
t19n-yi95ns6r	1		100%
sexc	1		100%
wos	1		100%

single	1		100%
b3yngk20f73pc	1		100%
watt	1		100%
744fca93f6148be0e4e0c2cb8fd1a774	1		100%

gmk6-4iz-1c1f	1		100%
anvyeipmlf	1	*	100%
3def78894dcc3b4d81bdec15088a4b7335	1		100%
hsc	1		100%
ef78894dcc3b4d81bdec15088a4b7335	1		100%
2520pauls	1		100%
you	1		100%
gilbertsportsman	1		100%
coolpad	1		100%
c4584k4t327ol	1		100%
ba4img9211x8k	1		100%
ga2kf7rvqc9go	1		100%
icsabembvrr4g	1		100%
k5z1i-rv8epip	1		100%
g5igmm3cqk77g	1		100%
zaboe0zf0zt2p	1		100%
w2-ge6vkqgo-c	1		100%
lb3t6t3gc8n3n	1		100%
trmxg0zpmni4f	1		100%
bqta70cogzctj	1		100%
vi6v3r7cf810o	1		100%
a0avg9r9kp-zk	1		100%
x44q5ecap3aoo	1		100%
s55too1qn-sjm	1		100%
ffkibzbjet8zr	1		100%
gi4igp6i4p2vk	1		100%
h391rxm-k--nn	1		100%
uvb2r8j1roc1n	1		100%
d840avm8s8ish	1		100%
cz4qv08ri91yf	1		100%
d5a19j8e2mopq	1		100%
qero1a7nei3-l	1		100%
k405c1jsnjt4l	1		100%
b89rv21rscy9i	1		100%
y840pbj2r3e7f	1		100%
rfot33a8-x50r	1		100%
jknmfgy0csm8l	1		100%
ex0is5zf3rjth	1		100%
ha-7z09egagbk	1		100%
jfjin5vy5668m	1		100%
hnj3i-q908-0d	1		100%
belta	1		100%

3rd Level Names

The following is a list of is a list of the first 50 and last 50 distinct 3rd level names that appear in a queried domain name in which "club" is the TLD, with an occurrence count for each. The cumulative percentage is indicated.

There were a total of 89,533 occurrences comprising 14,011 separate strings.

	31,072	35%
_dns-sd	7,433	43%
_msdcs	5,673	49%
www	1,637	51%
wplatform	1,611	53%
wpad	1,302	54%
dc	1,150	56%
ad	1,055	57%
_tcp	989	58%
showprint2	967	59%
com	797	60%
isatap	719	61%
_sites	652	62%
gc	567	62%
_udp	547	63%
default-first-site-name	534	63%
domaindnszones	520	64%
forestdnszones	504	65%
domains	434	65%
main	376	65%

_kerberos	346	66%
_kpasswd	344	66%
w2kserver	309	67%
server	280	67%
net	236	67%
lap-kc01396	202	67%
shahed	190	68%
toroyan-pc	188	68%
269006b0-d7fa-40a9-92d1-df63dacf7f74	184	68%
_ldap	183	68%
_gc	162	68%
hsb-sbs	156	69%
2k3jonas	148	69%
centos	145	69%
serveur-abi	141	69%

pdc	130	69%
google	129	69%
coffee	129	69%
clargesprint	127	70%
club-control	126	70%
apple	126	70%
85	124	70%
altfile1	115	70%
media	113	70%
fido7	113	70%
reception	109	71%
clargesman2	109	71%
clargesmail1	108	71%
info	107	71%
fedserver	96	71%
org	91	71%

boj553s4f488q	1	100%
p1np2qotbxeqo	1	100%
simeitg-1ft3h	1	100%
b4bca5vm48ceg	1	100%
t0o5krocojfkh	1	100%
cep4x7-qq58og	1	100%
q-kijczyem86p	1	100%
a35pxa1cxf62q	1	100%
wc3m2g5zvntv	1	100%
lx6z4af2gxcbm	1	100%
j-7yx2x3b0r3d	1	100%
ks50gxkax4epl	1	100%
vmxpezka5cqei	1	100%
j6xqt28m9vm7i	1	100%
f1z1v79c78efm	1	100%
w1sjt5grexvbn	1	100%
nt34pnzqnfp-h	1	100%
wmym13c58o4id	1	100%
wc6bf5pb54scf	1	100%
bnq428a0ecnko	1	100%
k40oqgv72efzn	1	100%
ennmixgay3k6	1	100%
xcm0zp932p2m	1	100%

k-ygxz6ixf9vi	1	100%
ty9r6iizoa5mk	1	100%
tkzyfigxgc6fo	1	100%
jg26cef9zvnyi	1	100%
gbp2im9q9obvd	1	100%
oe4gtyin61-3g	1	100%
d4k-j4nept8pm	1	100%
jmifjgq5ji7i	1	100%
v-q7t9ayabacq	1	100%
ozr118x2f8fbi	1	100%
cp83nn3j-j3xg	1	100%
cxb69bp2jzqid	1	100%
mma6z0mqgbrel	1	100%
g-b05j9-ot51d	1	100%
hpr2omsfci7kf	1	100%
u7iynyrtt9e0h	1	100%
xrycyy1ns10nk	1	100%
qavakzo65zcjq	1	100%
m-rtak2c07i1r	1	100%
y2yvrk-t2csoo	1	100%
svioz13x02k2m	1	100%
hc4-bq0foz9ar	1	100%
r4m9c10rz0f2h	1	100%

deavo47sep86f	1	100%
kfjtjtif5a54o	1	100%

nzm3yyc9jp7vn	1	100%
tq747vxebmnmj	1	100%

Leaf Names

The following is a list of is a list of the first 50 and last 50 distinct leaf names (i.e., the left most string in a QNAME) that appear in a queried domain name in which "club" is the TLD, with an occurrence count for each. The cumulative percentage is indicated.

There were a total of 89,533 occurrences comprising 28,932 separate strings.

_ldap	8,226	9%
www	4,702	14%
wpad	3,714	19%
_kerberos	1,907	21%
isatap	1,387	22%
dr	1,340	24%
lb	1,330	25%
r	1,304	27%
db	1,292	28%
b	1,291	30%
showprint2	967	31%
nfl	885	32%
_kpasswd	666	32%
satcontrol	632	33%
share	625	34%
_gc	622	35%
ad	622	35%
cf	563	36%
gc	429	36%
mail	379	37%
server	377	37%
youtube	360	38%
post	287	38%
game	262	38%
club-control	261	39%

yono	245	39%
domaindnszones	241	39%
dc	233	39%
forestdnszones	210	40%
lap-kc01396	202	40%
mccoy	200	40%
club	197	40%
epidem	193	40%
shahed	190	41%
toroyan-pc	188	41%
kennel	177	41%
michbuze	176	41%
college	158	41%
alisher	155	42%
flagman	154	42%
269006b0-d7fa-40a9-92d1-df63dacf7f74	153	42%
say	153	42%
time	145	42%
serveur-abi	141	42%
torrent	137	43%
microservice	134	43%
winter	134	43%
grendizer	134	43%
marine	132	43%
abi	129	43%

scsfidevee	1	100%
sbegoueahu	1	100%
wjb9m3y6afcfl	1	100%
gikeszi7bznsl	1	100%

dwspltoanh	1	100%
ryr5j0g-szcad	1	100%
mdopaxqmpv	1	100%
mnmmrakeqj	1	100%

l5n-rj2zo0mpf	1	100%
dqkkreufwc	1	100%
yuyreoarjz	1	100%
ugb4niyeenp-p	1	100%
kisac1sx6c09j	1	100%
ndjedfisng	1	100%
h0xtfvr2qs08d	1	100%
zpfdvkwdtf	1	100%
kn5bf1zvs17vd	1	100%
ub1bvq-0iv29l	1	100%
ctb0-v8bybk1	1	100%
vhphvasqbe	1	100%
lakkavxptsarr	1	100%
oemrsfmedz	1	100%
bxbdnwfotg	1	100%
abjikfwdpw	1	100%
q4mxm7ngjjc1p	1	100%
vciftrf96bc9p	1	100%
tn2p662zvv55n	1	100%
qsvrfjgcit	1	100%
mes56v0yebizf	1	100%

qolwssjjcm	1	100%
ejn093bm5xgiq	1	100%
hywlcotmfv	1	100%
h1i6kban17pel	1	100%
ua31mi6rp03nk	1	100%
yj1iy2mgssbqh	1	100%
ktjmuhxhqe	1	100%
zxmopstf0msbg	1	100%
xz45z10tt7vjh	1	100%
pjfc8xfnggbxm	1	100%
acaozhdews	1	100%
h99vz1s3i2pyd	1	100%
b7pjtyn4ffexq	1	100%
tslpcnpjjr	1	100%
anwwjnzmfv	1	100%
uflsuscqys	1	100%
ylpdonfnpb	1	100%
vz44enjeqaf	1	100%
kpfpys4ai15aj	1	100%
oer38pit77z6i	1	100%
needs	1	100%

IP Address Prefixes

Based on the IP addresses reported in the DITL data (some of which have been obfuscated), the following is a count of the number of distinct IP address prefixes (/24 for IPv4 and /32 for IPv6) from which at least one query appears that refers to a domain name with "`club`" as the TLD.

Out of the 9,011 distinct IP addresses seen, there were 4,467 different IP address prefixes.

One IP address prefix accounted for 17% of the queries; 30 prefixes accounted for 50% of the queries.

IP Address Country Codes

Using the IP addresses reported in the DITL data, and determining the country code to which the IP addresses belong, the following table shows the breakdown by country code.

Note that some entries are shown as country code "local" – we believe these represent either IP addresses that have been obfuscated in the DITL data or they represent private or link local IP addresses that have leaked out to the Internet. We cannot distinguish these situations. In one case an entry shows the country code "none" where an address was used whose country code could not be determined.

Country Code	Occurrences
US	38,831
local	14,751
GB	5,350
EG	3,840
RU	3,734
TW	2,226
DE	2,058
TH	1,679
CN	1,522
MD	1,335
KR	1,296
FR	1,096
KZ	945
EC	881
ES	868
AM	741
CZ	703
AU	681
UA	538
PH	424
JP	423
QA	397
HK	371
MX	357
NL	320
CA	303
BR	296
BY	264
CL	237
AR	234
GI	226
CO	189
UZ	138
SE	130
PR	129
RO	128
CH	121
IN	120
GR	114
IT	109
ID	105
AT	94
IE	77
IR	77
PL	67
BE	57
RS	55
MA	49
NO	45
VE	44
IL	43
SG	41
PT	40
VN	39
PE	34
ZA	31
TR	30
CV	27
KH	27
HU	23
SA	22
EU	22
CR	21
SI	18
CU	16
DK	16
LT	15
AZ	15
MY	14
GT	13

Country Code	Occurrences
SV	12
MN	11
NZ	11
TN	11
SK	10
DO	10
EE	10
BO	10
UY	10
NG	10
FI	8
BG	8
LV	7
AO	7
CI	7
KG	7
UG	6
AE	6
BD	5
JO	5
GH	5
PY	4
CY	4
ME	4
BA	4
MU	4
HR	4
PK	3
GE	3
MK	3
ET	3
TT	3
LU	3
KE	2
IQ	2
ZM	2
ZW	2
SN	2
TZ	2
CM	2
HT	1
SD	1
MV	1
HN	1
NI	1
NP	1
JM	1
TJ	1
MT	1
LY	1
LK	1
BH	1
AL	1
IS	1
MO	1
PA	1
none	1
KW	1
LB	1
Grand Total	**89,533**

QNAME Patterns

The following is a count of the number of queried domain names in which "`club`" is the TLD for which patterns emerged with significant occurrences.

SLD is an Existing TLD

9,039 (10.1%) of the 89,533 queries had an existing TLD at the second level.

The following table shows the full list of 96 existing TLDs along with the cumulative percentage of existing TLDs and of all queries that refers to a domain name with "club" as the TLD.

net	2,697	30%	3%
com	2,369	56%	6%
org	1,334	71%	7%
info	1,001	82%	8%
cc	489	87%	9%
post	308	91%	9%
ru	73	92%	9%
cz	65	92%	9%
cn	59	93%	9%
uk	57	94%	9%
gm	40	94%	10%
cf	38	94%	10%
ua	33	95%	10%
edu	23	95%	10%
de	22	95%	10%
pk	21	96%	10%
gov	20	96%	10%
fi	18	96%	10%
arpa	17	96%	10%
jp	16	96%	10%
fr	16	96%	10%
cat	15	97%	10%
rs	15	97%	10%
se	15	97%	10%
tw	13	97%	10%
hm	11	97%	10%
kz	11	97%	10%
es	10	97%	10%
hr	10	98%	10%
cl	10	98%	10%
ph	9	98%	10%
travel	9	98%	10%
me	9	98%	10%
pl	8	98%	10%
gl	8	98%	10%
ro	7	98%	10%
lt	7	98%	10%
tr	7	98%	10%
pr	6	98%	10%
ch	6	99%	10%
mobi	6	99%	10%
my	6	99%	10%
gs	5	99%	10%
at	5	99%	10%
bg	5	99%	10%
to	5	99%	10%
az	5	99%	10%
bb	4	99%	10%
al	4	99%	10%
gr	4	99%	10%
biz	4	99%	10%
pt	4	99%	10%
ca	4	99%	10%
dk	4	99%	10%
eu	4	99%	10%
au	3	99%	10%
mx	3	99%	10%
tj	3	99%	10%
sj	3	99%	10%
no	3	99%	10%
pw	3	99%	10%
co	3	100%	10%
dj	3	100%	10%
fm	2	100%	10%
im	2	100%	10%
sb	2	100%	10%
is	2	100%	10%
xxx	2	100%	10%
ma	2	100%	10%
bs	2	100%	10%
nl	2	100%	10%
uz	2	100%	10%

yt	2	100%	10%
na	2	100%	10%
ec	1	100%	10%
th	1	100%	10%
vn	1	100%	10%
mp	1	100%	10%
xn--p1ai	1	100%	10%
sk	1	100%	10%
sg	1	100%	10%
ac	1	100%	10%
br	1	100%	10%
ly	1	100%	10%

gb	1	100%	10%
tt	1	100%	10%
hu	1	100%	10%
am	1	100%	10%
om	1	100%	10%
do	1	100%	10%
ir	1	100%	10%
cm	1	100%	10%
sv	1	100%	10%
nz	1	100%	10%
md	1	100%	10%
us	1	100%	10%

SLD is a 10-alphabetic-character string

16,972 (19.0%) of the 89,533 queries had an SLD comprising 10 alphabetic characters, which could be a result of a feature of the Chrome browser, choosing "random" 10-character alphabetic strings to defend against domain name hijacking.

1,930 (2.2%) of these strings occurred only once; 14,662 (16.4%) of these strings occurred only once or twice.

Service discovery and related names

The following indicate any names with more than a few occurrences of the 89,533 queries that related to service discovery or similar protocols:

- 8,226 (9.2%) included "_ldap" as the first string in the QNAME
- 7,433 (8.3%) included "_dns-sd" as the 3rd level string
- 3,940 (4.4%) included "wpad" as a string in the QNAME
- 1,907 (2.1%) included "_kerberos" as the first string in the QNAME
- 1,387 (1.5%) included "isatap" as the first string in the QNAME
- 8 (0.0%) the QNAME started with "_sip"
- 3 (0.0%) the QNAME started with "_xmpp"

Together, these cases cover 22,944 (25.6%) of the 89,533 queries.

www.club

2,399 (2.7%) of the 89,533 queries were just for `www.club`.

2-alphabetic-character SLD

4,237 (4.7%) of the 89,533 queries had an SLD comprising 2 alphabetic characters. These do not include the ccTLDs which have been counted in the section "SLD is an Existing TLD" above. (However, see the next section below "`.cs.club`".)

.cs.club

The DITL 2013 data shows an interesting SLD "`.cs.club`."

.cs used to be the country code for the former Czechoslovakia; cs is also a commonly used abbreviation for computer science departments.

We observe 2,487 queries for QNAMES ending in `.cs.club` many of which appear to be related to Microsoft's Active Directory.

The 2,487 queries for "cs.club " come from a mere 141 distinct IP addresses (noting that some addresses in the DITL 2013 data have been obfuscated).

The following table shows the breakdown of queries by country code, where known:

Country Code	Occurrences
TW	2,066
local	418
US	2
GB	1
Grand Total	**2,487**

The 418 "local" occurrences represent private IPv4 addresses (10.0.0.0/8) which can be the result of either obfuscation of IP addresses in DITL data or leaking of private (RFC1918) addresses to the Internet.

Service Requests

Generalizing from the results obtained from investigation .cs.club. names, a subset of the .club. data where the QNAMES contained a potential service request was examined. The following leaf names which included an underscore character occurred more than 10 times:

- _ldap
- _kerberos
- _gc
- _vlmcs
- _msdcs
- _minecraft

The request where any of these strings occurred anywhere in the QNAME were examined, yielding a total of 13,839 queries. Of these, 7,323 where for QTYPE SOA, and 6,474 were for QTYPE SRV (the remaining being 39 for CNAME and 3 for A).

Reverse IPv4 address and .club

914 (1.0%) of the 89,533 queries were of the form of an IPv4 address (in reverse) with "club" as the TLD. For example, a name of the form :

- 279.130.70.10.club.

These types of queries are normally associated with reverse IP lookup (in-addr.arpa.) Note that there were an additional 17 queries of the form:

- 51.207.134.10.in-addr.arpa.club.

DNS Request Types

The following is a count of the number of queried domain names in which "club" is the TLD with respect to the DNS request type (distinct values of Opcode, RA flag, RD flag, and QTYPE):

- Every request used Opcode 0 (Query)
- Every request had the RA flag set to 0
- Almost every request had the RD flag set to 0; 24 occurrences had RD set to 1

The following shows the distribution of the QTYPE field in the DNS request:

QTYPE	Occurrences
A	50,160
SOA	12,911
AAAA	7,717
PTR	6,897
SRV	6,494
MX	3,407
NS	783
TXT	744
ANY	297
CNAME	71
DS	40
SPF	12
Total	**89,533**

Low Occurrence Counts

While looking for patterns in the QNAME, the following shows those patterns for domain names where "club" is the TLD and the number of occurrences was low (less than 1% of the 89,522 queries):

- the QNAME include the string mail at any position – 421 occurrences

- the QNAME was only the string `.club.` – 0 occurrences
- the SLD comprised a single non-alphabetic character – 16 occurrences
- the SLD comprised a single alphabetic character – 299 occurrences
- the SLD comprised two characters, at least one non-alphabetic – 356 occurrences