Interisle Consulting Group

Exposing Criminal Abuse of Internet Names and Addresses – Proof of Concept
3 Sep 2019 to 24 Feb 2020

Colin Strutt

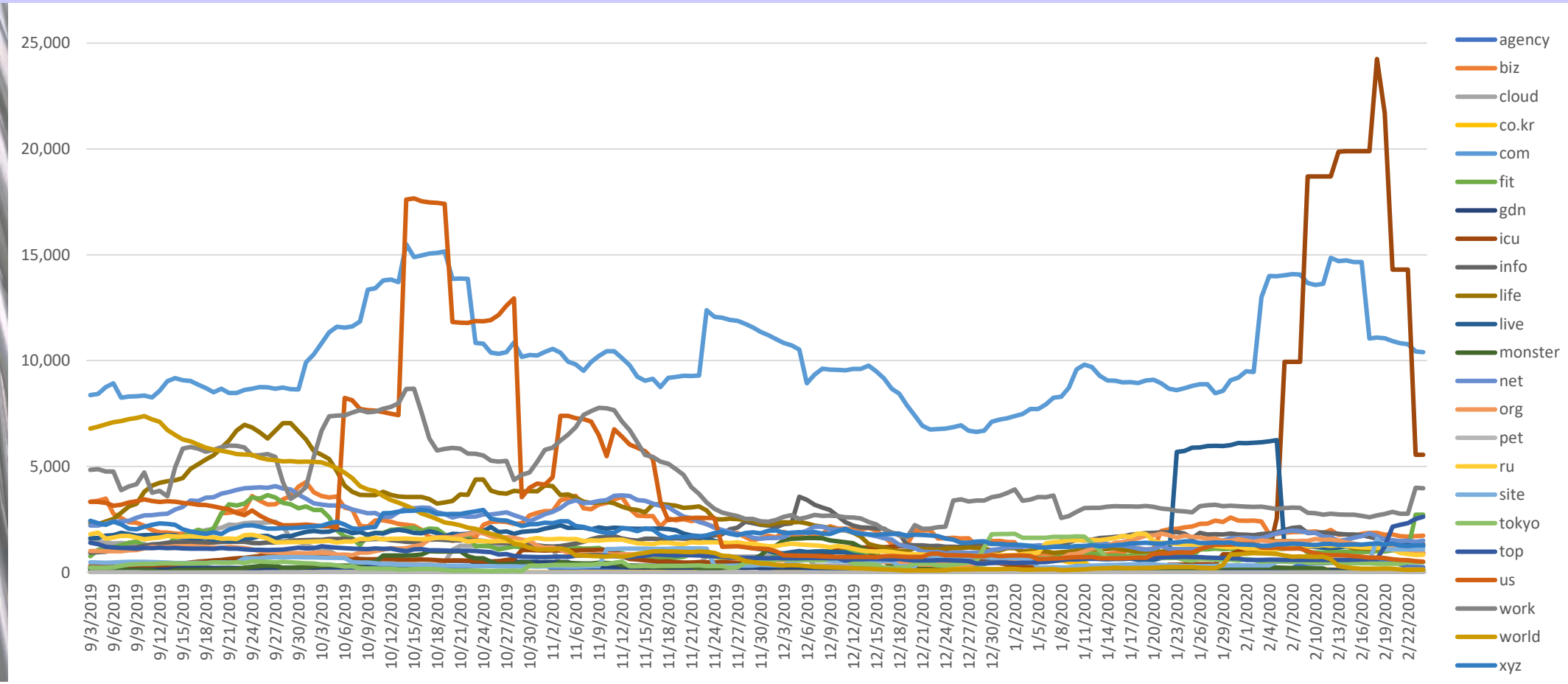
Dave Piscitello

ECAINA Proof of Concept

- Feasibility study begun 3 September 2019
  - Gathering daily blocklist data for 23 TLDs
  - Identifying the associated registrar from available domain name registration data
- Augmenting with data from other sources (where available)
  - Whois, RDAP, Team Cymru, dns.coffee, etc.
- Analysis of blocklist and Whois data for each TLD on each day:
  1. # domain names on blocklist; “sponsoring” registrar
  2. # domain names added to blocklist each day; “sponsoring” registrar
  3. # domain names removed from the blocklist each day
- Demonstrating the value and viability of ECAINA
  - Observed relationships between turnover, bulk registration, and blocklisting “spikes” and well-recognized patterns of criminal behavior

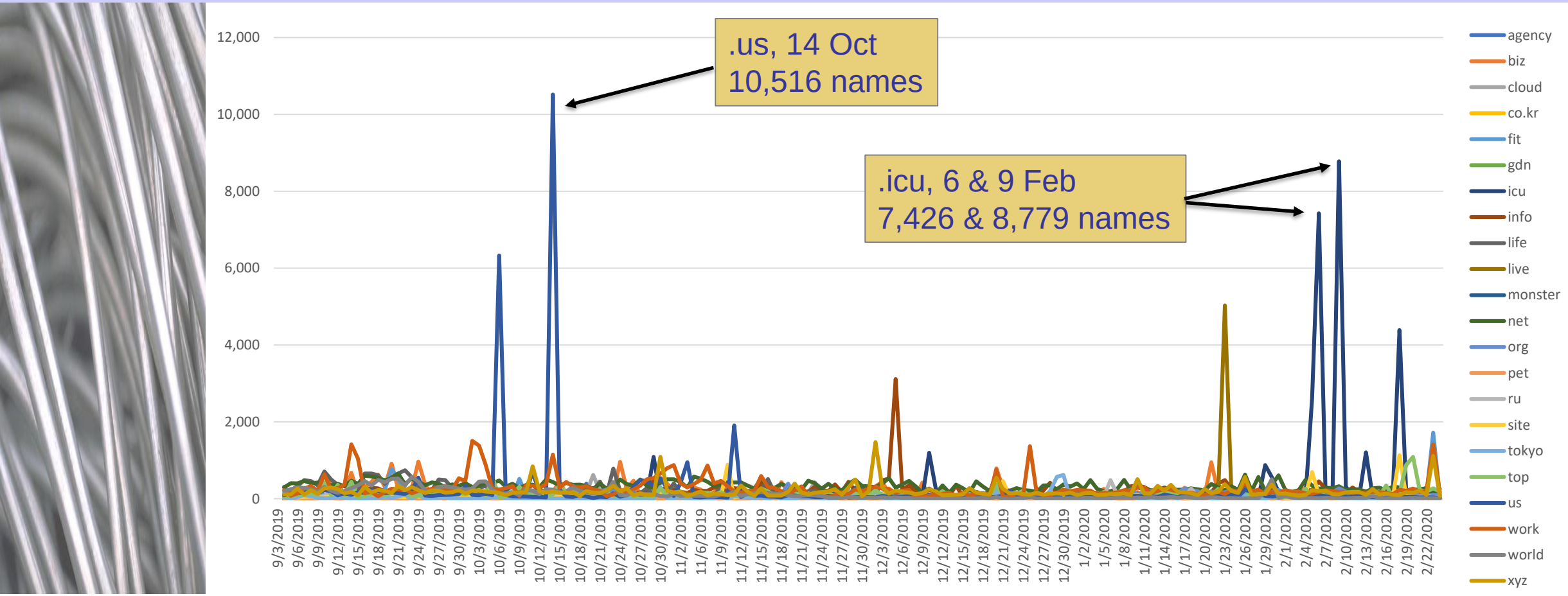
Interisle Consulting Group

Number of Names on Each TLD's Blocklist



Interisle Consulting Group

Number of Names Added to Each TLD's Blocklist



Interisle Consulting Group

Registrars with High Proportion of Blocked Domains

- 18 Feb shows
  - 4,386 names added to .icu
  - 1,132 added to .site
- Many names exhibit a common pattern – 6 random alpha characters
- These registrars account for names added that day for all 23 TLDs:

Registrar	Count
ERANET INTERNATIONAL LIMITED	5,448
GMO Internet, Inc. d/b/a Onamae.com	164
NameCheap, Inc.	48
GoDaddy.com, LLC	25
NameSilo, LLC	12
... and 28 other registrars	53

Interisle Consulting Group

18 Feb: 6-α Names Added to Blocklists
4,355 to .icu & 1,094 to .site

aaddxs	acjxve	afenbl	ahjmvb	ajztcm	anhepl	apxhcy	arqpsv	auhlwj	awcyxn	aygirf	baxrkc	bdfnxr	bfypmv	bhwlrk		ysiulw
aaeazr	aclopd	affkvc	ahmpzq	akkkjh	anjgbm	apyqvw	artfwb	auirig	awerag	aygmbp	bbaqrb	bdkdqm	bgbent	bhwuhc		ysswen
aagylz	acmmpr	affqvn	ahowhq	akmjpw	annxce	apzjbs	arusmo	aujfxz	awmavn	ayildl	bbawbl	bdpkni	bgcfhv	bhxveb		ytnbdq
aahhad	acqaac	afgzfj	ahyiod	akoayb	anrlsc	aqbcjg	arvgqx	auketk	awmelo	aymfxf	bbgbix	bdtecx	bgcypm	bibwru		yumpyw
aaiqwi	acqieb	afhcwg	aiaeph	aktfrq	anucgh	aqbsvg	arwcmw	aumnok	awmxce	aymski	bbgwph	bdtlvi	bgfbrw	bicefi		yvrmld
aaiyzp	acrsnr	afkmij	aibpow	akttyd	anvbjn	aqciuf	aslhlt	auohsz	awpxjg	ayqjuu	bbjtgm	bdtvuf	bggdrk	bicmih		yxipbq
aakmvx	actdyc	afnley	aicgkm	akvvlj	anwebe	aqdexk	asmwav	aupavf	awsheu	ayrobe	bbjvcr	bdyldw	bgjmbq	bidlzt		yyilti
aaleol	acxouq	afqdmc	aidepv	akztdv	anykhs	aqevbd	asodms	auqfxh	awsmyq	ayyaat	bbmghs	bebedl	bgllaz	bihhga		yzeeqw
aaniox	acyzev	afqorj	aiditm	akzuto	anyysh	aqeytv	asoxxw	aurfyu	awumhn	azbtqh	bbmrqs	bedzuj	bgnjmf	biiipg		yzxcsn
aapbev	adcxhj	afszyl	aidscm	alaoev	anzqke	aqgudh	aspbtg	aussrx	awunxy	azidjm	bbqfqu	befnwy	bgpsen	biobnk		yzxlft
aapvyh	adimin	afxrng	aielok	alekxl	aocmvq	aqhbpw	asphih	ausvgn	awuvmk	aziwmc	bbtekl	begqrp	bgqusr	bisemi		yzzrko
aasxxy	adkvim	afxxag	aiidbe	algsge	aocucv	aqhcgz	assoja	autfkn	awuyjt	azlsrx	bbutcv	bekzot	bgqzbq	biuegl		zaevyr
aavzgg	adltcj	afyabs	aijftc	alhglk	aodiwx	aqhhfe	asvmih	autupx	awwkot	azmewz	bbwzad	bemcwh	bgreym	biuitb		zbsman
aazosu	admrrl	afyauc	aikkbu	alnaou	aofpiw	aqjmwz	asxqds	auuavb	awycmi	azsyml	bbxemq	bemzfm	bgrrcl	bizrww		zbtqbj
abehgh	adntvf	afyvwn	aikzdb	alntim	aogyuq	aqklbl	asyndx	auwzri	axcxww	azthqg	bbxjsm	bencps	bgruax	bjattw		zcvszl
abewbu	adoocl	agengu	ailxqy	alpmxm	aojznw	aqpqht	atbasu	auxksf	axfbnt	azttxy	bbyfpx	benwpb	bgsmqk	bjdwnz		zgpqpu
abezzk	adrcwt	aggdvb	ainmwx	alpqsy	aoosqk	aqqpcs	atblcz	avdfth	axihki	azyikh	bcajyy	berypo	bgsvsq	bjecgi		zhcxfo
abfzvj	aducad	aggxet	aipdgm	alqywg	aoumuh	aqrzxv	atizrx	avitoo	axiyzt	azzeze	bcarug	bewkyy	bgvwfn	bjelth	...	zhimqb
abhpnd	adxibm	agilsk	aiqpla	alrcox	aounto	aqtbra	atjatn	avkdop	axjsyi	baabzz	bcbpmb	bezdsf	bgzfcv	bjgxsx		zifxpn
abiuya	adzeia	agjzbq	airzbh	alsqcc	aouwts	aqubae	atjrif	avkwlo	axkozd	babjsw	bccmbf	bfahxs	bhalpb	bjhqur		zkpuwk
abiuzm	adzzos	agkqsq	aisbsq	alusju	aovcws	aqvaof	atjygy	avmbdj	axlpji	babwli	bcdglj	bfbhmx	bhdgfg	bjjxfi		zmmbtm
abnupx	aeadab	agpjqn	aitxww	alwqyf	aowpnt	ararwj	atnvan	avrdra	axmnof	baeobz	bckqwy	bfcbqk	bhdtbd	bjooct		zmyjlg
abpbwg	aeaqow	agrhbk	aiuzrs	alzamo	apajtd	arclkg	atqnnl	avribs	axnxkw	bafvpb	bckscs	bfcpiy	bhegrf	bjpotv		zphdph
abqgug	aecivq	agsdgl	aivvhr	amgqss	apiavv	arejzp	atquau	avrnvo	axpboa	baianr	bclmll	bfgcap	bheueq	bjpynl		zqxllw
aburmd	aeerue	agsqcw	aixfou	amhakd	apimyw	arfjwa	atrrhy	avrtrx	axqreb	baithl	bcsqon	bfibzw	bhgone	bjrwtg		zrhnck
abuwbb	aehzxs	agwzau	aizrni	amhdaz	apjioo	arfqgt	atrsps	avsbqn	axqruc	bajnun	bctjtc	bfkaoi	bhjgrs	bjumaz		zrwvbe
abvbpc	aekcyw	agypig	ajgtzv	amjopa	apjotn	arfspu	atsjxf	avskdw	axsmim	bajumm	bcuajz	bfolhp	bhjsvk	bjvual		zsqsms
abwbmz	aeogvx	agyuko	ajhsos	amjzbx	apkmlj	arhdbn	atvrii	avuggm	axtpkv	bakfez	bculmt	bfpldp	bhmbhk	bkaybs		ztpgre
abwvhz	aeovcf	ahbtdu	ajhukr	amnlca	aplagx	arhwfh	atvsai	avuqnw	axtxvy	balddt	bcvdli	bfuiyh	bhphpk	bkbnwv		zuodtj
abyriu	aerhzk	ahcmoe	ajkgep	amqqqy	apnzjn	arihga	atvvvw	avwmrq	axurvr	banaxp	bcxvve	bfuwfd	bhqwpr	bkdovs		zvfwsn
acbhsz	aesors	ahcvhq	ajkjau	amrbkz	apokor	arivkj	atywzv	avwvgp	axzhuo	batkpr	bdanan	bfvqde	bhrbik	bkdpim		zwbcux
acctdq	aetqfo	ahetga	ajqsix	amwcxz	apsgxn	arjhmz	atyziy	avxmmd	ayahun	batvkf	bdbgzf	bfvzbp	bhsmsi	bkjghe		zwyoyq
acejkm	aevbir	ahewyq	ajrudr	amzwsm	aptglv	arlexz	atzbub	avxtll	aybrux	batyfk	bddfnh	bfwjew	bhtqhq	bkkvsc		zyrrys
acfdza	afakbv	ahhhbc	ajtkva	anajaw	apufvc	armidr	auezwq	awbypc	ayczsy	bavbrv	bddtgi	bfyebl	bhuaqp	bklhwk		zyxiff
acgbsh	afaofy	ahiaky	ajwaqx	anesyt	apxbwm	arnxoz	aufbhe	awcpmq	ayddla	bawubh	bdfbom	bfygva	bhwcgp	bkpjuc		zzbavz

Interisle Consulting Group

14 October – 10,516 Names Added to .us Blocklist

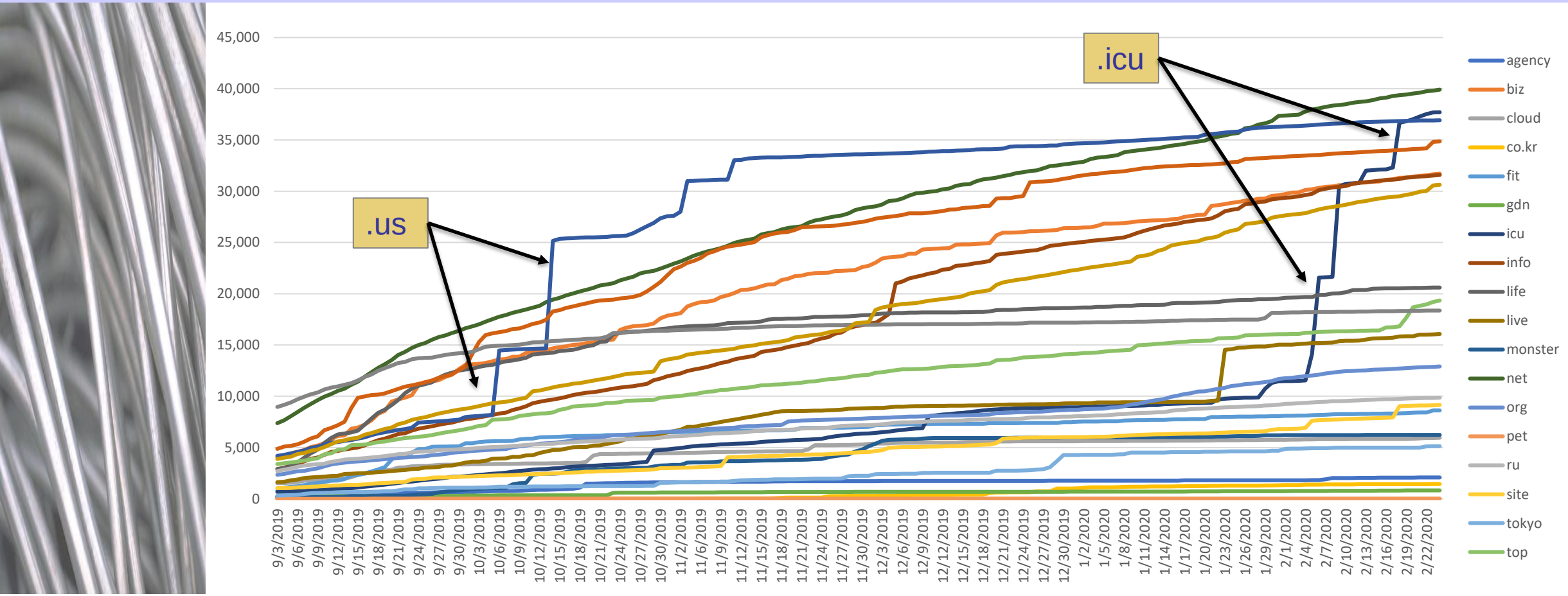
01fl9z	0bgisc	0guvdk	0olerp	0unbec	12dggb	1cbxpw	1hpbxt	1omb8j	1w0ied	27brhe	2fnrye	2o1mfa	2tefgz	2zjp9s	zwscho
01py42	0bhqex	0h4blq	0on1yf	0uradt	13mp4u	1ciuwl	1i7ryf	1ozlxj	1wfsks	29jvhi	2fsvyg	2o9fkd	2tj5vf	2zpqh4	zwuhqg
02gtn1	0bkpju	0h4ofm	0oqq1x	0urq3q	14fjnq	1cjqrg	1iaqnp	1ozmz6	1whdgb	2adoqi	2g4eus	2oaobn	2tjnam	2zsbs5	zwuqvh
02joer	0brnlo	0hfbkg	0oxcwz	0uta83	14fkid	1ckggh	1igeop	1pridj	1wpkre	2akoul	2ga3oe	2ocuye	2tnify	30dtrs	zwxoy6
0317gm	0c2wmp	0hiep1	0oyjgo	0uzprk	14quhf	1cnkef	1igqmr	1pseyq	1wr5rg	2anwem	2gdehd	2odsd0	2tuev3	30kil9	zx2hwj
034wo8	0cb1o3	0hl5vh	0p6zxx	0v5dfu	14zvhy	1coswo	1ipdax	1pxrsn	1wsvrp	2arqez	2gi6jq	2ofeyj	2tzfqn	30pm2n	zxd2gj
047pip	0cbik6	0hlc3x	0pun6d	0vqc2r	15bj8p	1coznb	1j2v0p	1q3ptz	1wzlxn	2azznj	2glrum	2omalh	2tzmd7	31oizc	zxe1ds
048bfu	0cenf4	0hmdi2	0q5ger	0vxhat	15soim	1devil	1jgsyq	1q3thg	1xgow5	2b8n3q	2guqot	2osplf	2tzuhm	326mbg	zxhixb
049eql	0chmtp	0hmdiu	0q6frx	0vxnkw	15topm	1dey2n	1jikfz	1qllzn	1xjjes	2befys	2gwvif	2pizlu	2ubxm6	329rxj	zxhpwa
04bqda	0chyql	0iilt4	0q9ity	0w6jyz	16bhoj	1dgr4p	1jm4cp	1qra03	1y8mr7	2bggcd	2ihrhe	2pntiq	2ud431	32znio	zxjaib
04dtr9	0ck65z	0j5mer	0qaf4b	0w7knj	16jsrg	1dioyr	1jyawi	1raqpw	1yanr7	2bir8b	2irkap	2pvxdo	2ufozp	34hagr	zxmion
04otrs	0cmddq	0jef9e	0qfuof	0wu4kl	16oldc	1dph6j	1k2kvp	1rb2gu	1yhunx		2izmeu	2px0et	2up8cg	34opqr	zxnmer
058dax	0cornp	0jh2vh	0qrqeu	0wz5tr	16onzh	1dv5vq	1kbpgd	1rbtu4			2jdj9v	2pxnr0	2uuvfz	34rhps	zxpnva
05cfis	0cyxbl	0jhtex	0qtl67	0x1qiw	17hed6	1e9jbj	1kdu98				jgzqt	2pxogx	2uvn1g	34sgyb	zxppcl
05h3tx	0d3q2g	0jjzqc	0qyrcj	0x63s4	17mkzd	1eabcv					kozr	2qjalh	2uxdh3	34v6fo	zxrgfh
05kbpy	0d4ayv	0joebq	0r6tbq	0x6a7o	17usze						qv3h	2qkvtc	2uz7dm	358hx2	zxtoh5
05ourk	0d6gml	0juxgq	0rmgbe	0xaaub							sukg	2qpthe	2vdwcg	35j01w	zxvamd
05vbdo	0dm5hn	0jvtes	0rpimy	0xeil1							tbh	2r8ttl	2vfcjy	35jly4	zxy3kl
05vmdi	0duz8q	0kjboo	0rpmyl	0xo5yn							zhj	2rcmci	2vrno7	35qcmb	zy4nw0
06mwpx	0dzwfo	0kngxi	0rv1f8	0xrpvu							u8	2rfbhp	2wpdwh	36hvuq	zy5wco
07ebdo	0e2lrg	0kwngu	0rxnru	0xx3hk								2r7dky	2rjxvu	2wrvwi	36mgrp	zy61nk
07ktun	0eganq	0kxtzj	0sbtxd	0y8n4q							2dm1hd	2lgawo	2rknin	2x4ct9	36naqh	zyabti
081uq5	0enwfg	0lcosd	0senfy	0ycepx						21ndte	2dqfjn	2lgayw	2rkwug	2x8jlc	36zdwc	zyapks
082asy	0es5oz	0lezti	0sgonf	0yeapq					1cpb1j	21oyjn	2dwyn7	2lh1gv	2rspug	2xj59t	37ieeb	zyfota
08phqx	0ess1k	0lhlgs	0slxkr	0yi3nm				1mg3ha	1txwra	21s8os	2dzvpw	2limoc	2rtm13	2xouvk	37ksrr	zyogai
09feqg	0faari	0lnajf	0sogh3	0yiobn				1micki	1tycqx	23mdip	2e1zvh	2m9zho	2rxhfn	2xv1pi	37upab	zytotn
09nb2a	0foksf	0lqpph	0sq6ie	0yxwkl				1mqdsx	1ueqgd	23yd0z	2ecpom	2mcer1	2s1elx	2xwqmf	384vwt	zyvlss
09w8yh	0gd9bf	0lrgre	0sxqqu	0zcues	1bcg2o	1getts	1mupiw	1ukude	24aro5	2ejalk	2mfda6	2sdryw	2ylexc	38ktvt	zyw7k5
09zzc4	0gia1m	0lvdaw	0szzsa	0zelby	1bg94j	1ghxzy	1mvofp	1uo8iy	24cpne	2epwfb	2mktqo	2si9ts	2ysyu5	38qe1m	zz7yld
0aaior	0gim9b	0mbvys	0t8acb	0ziu9u	1blmny	1gyexj	1n2xo5	1urwba	25fhdd	2ercji	2mqbvz	2sndla	2ytahr	38rper	zzf38l
0aec3m	0gjswb	0mi31c	0t9pfs	0zmkya	1bslan	1h6icu	1nfexj	1usqrj	25ikb6	2etrfa	2mwcld	2somkm	2yzkip	3aa8rp	zzgktf
0afxwz	0gjvxp	0mm2de	0tfks6	0zreem	1bukmx	1hbglt	1ngw50	1uvxmd	25lzj3	2etvis	2mxo1l	2sprjd	2z37mp	3afsfu	zzlbeu
0ahncl	0gklqr	0nbd8d	0tgque	0zvms9	1bw9f8	1hfluh	1nr5sy	1uzwhl	260uwp	2eymrl	2mzaxq	2strin	2zamxh	3ao2zr	zzojwa
0amepc	0gnnt9	0nfegu	0tjx8h	0zwgx9	1cahhd	1hhqna	1o4m2i	1vgxt9	26vlcz	2f0wxk	2nhlrn	2t7pvz	2zfivy	3atdol	zzr3fs
0ammbh	0gtkue	0ogm1f	0u5k7v	10g8ki	1cb4ko	1hjat2	1ojyrx	1vwkoc	26x5na	2fersd	2o0lov	2tbspk	2zil5a	3awnhp	zzryek

At least 10,300 of these names were registered via NameCheap, Inc.

...

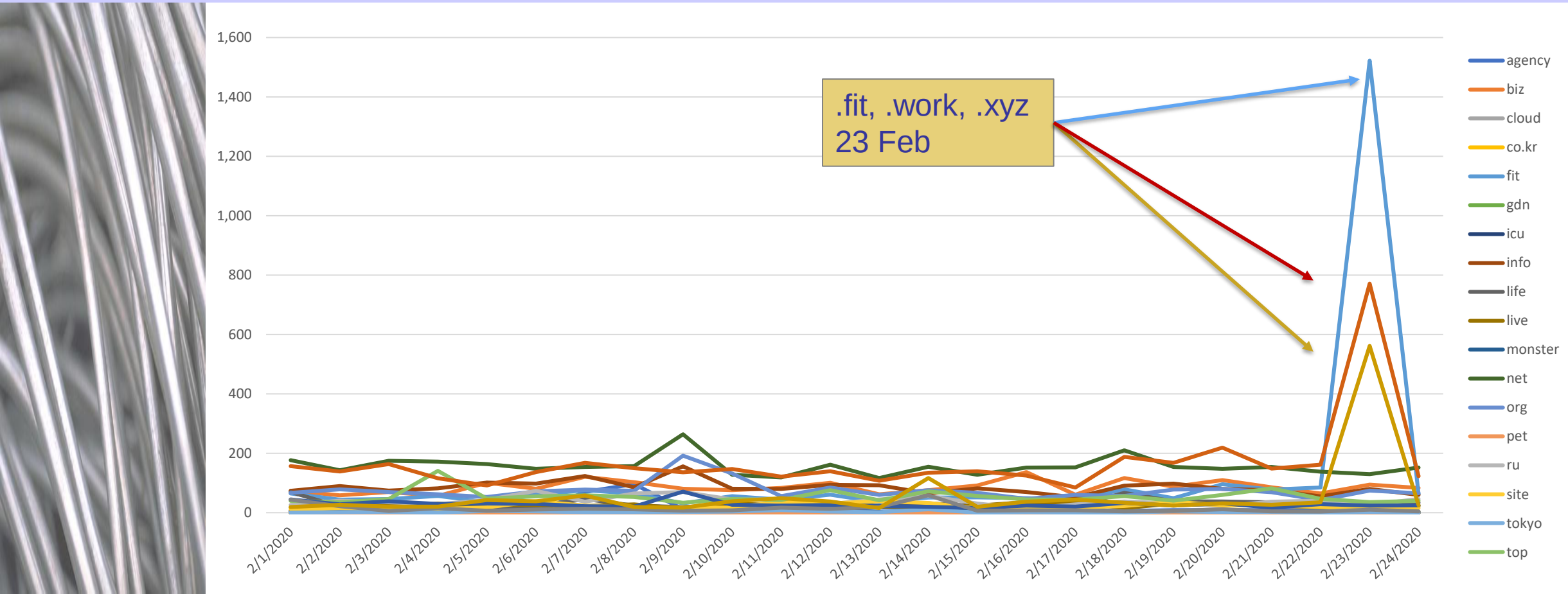
Interisle Consulting Group

Cumulative Blocked Domains (excluding .com)



Interisle Consulting Group

Blocked Names Often Get Blocked Again
(excludes .com; this month)



Interisle Consulting Group

Top 10 Subnets for Blocked Domains (23 Feb)

Subnet	Owner	Occurrences
3.208.0.0/12	Amazon AWS	1,569
3.80.0.0/12	Amazon AWS	549
34.192.0.0/12	Amazon AWS	263
18.232.0.0/14	Amazon AWS	262
3.224.0.0/12	Amazon AWS	155
54.80.0.0/14	Amazon AWS	134
160.181.224.0/19	ZA	115
49.156.160.0/19	Ace, Inc., JP	100
104.238.196.0/24	Infiltrate, LLC, US	99
116.50.32.0/20	TW	93

Interisle Consulting Group

Top 10 AS for A Addresses (23 Feb)

ASN	AS	Occurrences
14618	AMAZON-AES - Amazon.com, Inc.	3,012
16509	AMAZON-02 - Amazon.com, Inc.	232
13335	CLOUDFLARENET - CloudFlare, Inc.	144
26496	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC	143
137443	ANCHGLOBAL-AS-AP Anchnet Asia Limited, HK	117
40034	CONFLUENCE-NETWORK-INC - Confluence Networks Inc	108
56291	ACE-AS-AP Ace, Inc.	107
22612	NAMECHEAP-NET - Namecheap, Inc.	107
396932	HOSTINSANITY, US	99
18046	DONGFONG-TW DongFong Technology Co. Ltd.	93

Interisle Consulting Group

Top 10 AS for NS Addresses (23 Feb)

ASN	AS	Occurrences
14618	AMAZON-AES - Amazon.com, Inc.	6,020
38283	CHINANET-SCIDC-AS-AP CHINANET SiChuan Telecom Internet Data Center	722
4134	CHINANET-BACKBONE No.31,Jin-rong Street	604
16509	AMAZON-02 - Amazon.com, Inc.	582
26496 & 44273	GO-DADDY-COM-LLC, US, GODADDY-DNS, CH	532
13335	CLOUDFLARENET - CloudFlare, Inc.	452
55002	DEFENSE-NET - Defense.Net, Inc	402
2519	VECTANT VECTANT Ltd.	368
4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	284
133119	UNICOM-CN China Unicom IP network, CN	240

Interisle Consulting Group

Challenges

- Unavailability/reliability of Whois data
- Unavailability of RDAP data
- Rate limiting – e.g., Whois, dns.coffee
- Timing of Whois/RDAP data vs. appearance on blocklist
- Registrar names are not canonical

Interisle Consulting Group

Interisle Consulting Group

ECAINA …
Exposing Criminal Abuse of Internet Names and Addresses

Questions?