Interisle Consulting Group

Exposing Criminal Abuse of Internet Names and Addresses

Colin Strutt, Interisle Consulting Group

Greg Aaron, Illumintel

Presented at Workshop on Internet Economics: Knowledge of Internet Structure: Measurement, Epistemology, and Technology (WIE-KISMET), December 2019

Measuring and Documenting Domain Name Abuse

- Spam, malware, phishing, etc., degrade the online environment
  - Erode user confidence
  - Inflict serious harm on individuals and organizations across the world
- Harms:
  - Financial
  - Election interference
  - Cyber terrorism
  - Physical harms, as criminals target critical infrastructures (e.g., healthcare systems)
- Countering them tops “most important Internet issues” list for most

Interisle Consulting Group

ECAINA Vision

- A measurable and quantifiably safer Internet
- An Internet in which organizations, governments, and individuals have data they can use to
  - Deploy security measures
  - Demonstrate empirically the effectiveness of security and administrative controls
  - Make informed policy and regulatory decisions
  - Conduct research

Interisle Consulting Group

ECAINA Mission

To collect and publish information that identifies, quantifies, and categorizes Internet identifier abuse and the contexts in which it occurs

Interisle Consulting Group

ECAINA Mission (the detailed version)

- We seek the structural, systemic enablers of Internet abuse
- Numerous organizations already compile reputation data or “threat intelligence”
  - Can be used **tactically** to stop crimes in progress, notify victims, pursue legal recourse, and prevent future abuse — in individual instances
- We will collect, process, and warehouse reputation information that identifies, quantifies, and categorizes activities that harm Internet users
  - Can be used **strategically** to identify and fight cybercriminal activity Internet-wide
- Information comprising census & reputation statistics for
  - Domain names
  - IP addresses
  - Autonomous Systems (AS)
  - Associated organizations (e.g., registries, registrars, and hosting, cloud, or ISP operators)

Interisle Consulting Group

ECAINA Project

- ECAINA will provide
  - Scientifically reliable data for researchers to:
    - Observe and report concentrations of criminal activity
    - Measure, quantify, and rank domain name service providers and operators
    - Measure, quantify, and rank addressing service providers and operators
    - Observe criminal flocking and migration behavior over time
    - Discover and codify indicators that allow us to discover additional abuse identifiers
    - Report the above to inform legislators and policy makers
  - Researchers with means to:
    - Study harmful names and addresses

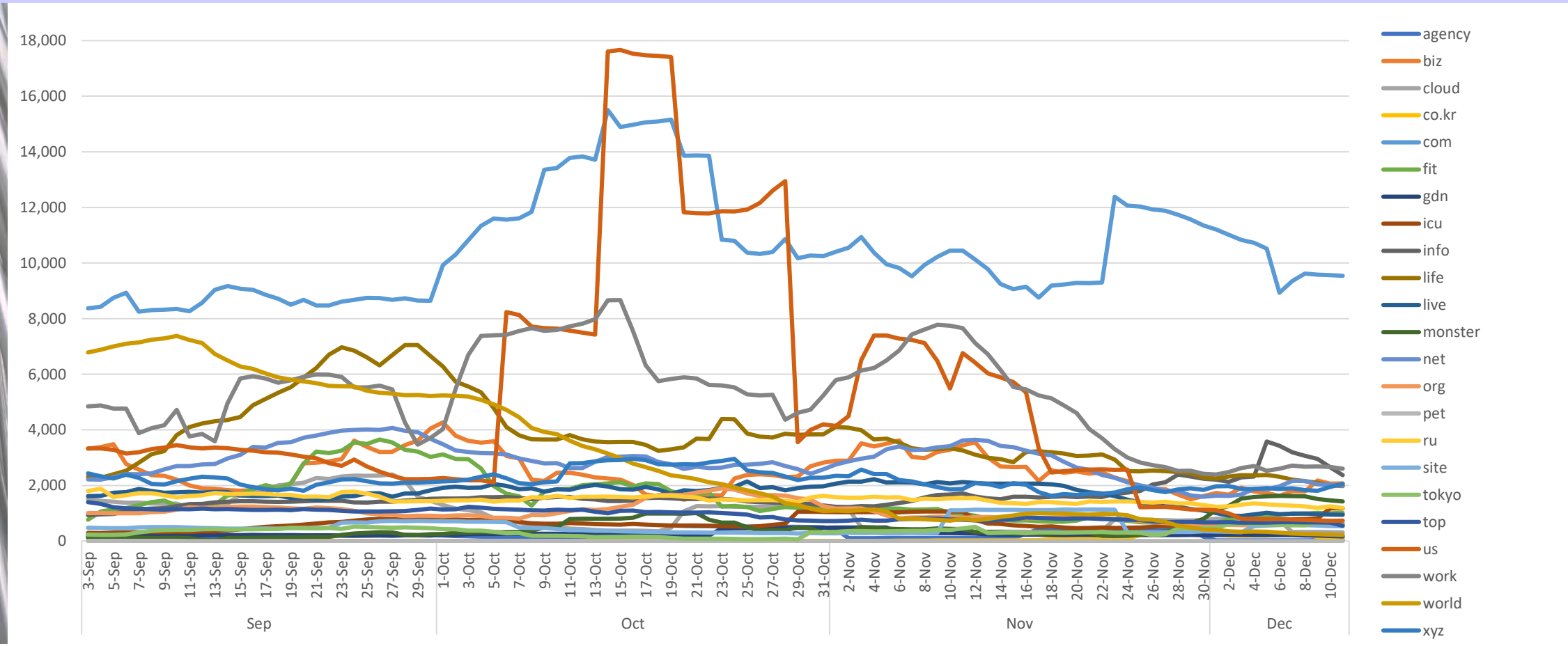
Interisle Consulting Group

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
- 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

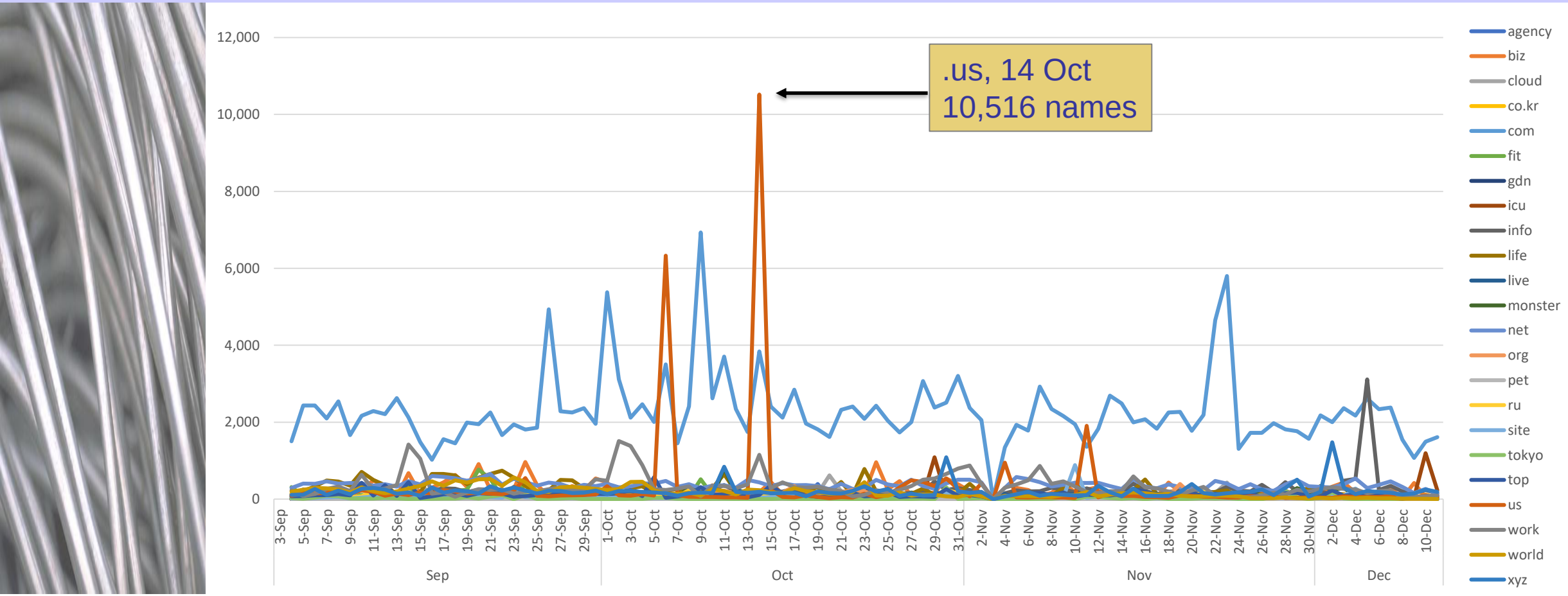
Interisle Consulting Group

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 Blocklisted Domains

TLD	Date	Blocked Domains	Top Registrar for all blocked domains in TLD			Added
			Top Registrar	# domains	% domains	
biz	9/4/2019	4,083	GMO Internet, Inc. d/b/a Onamae.com	3,381	82.8%	132
biz	9/5/2019	4,269	GMO Internet, Inc. d/b/a Onamae.com	3,487	81.7%	245
biz	9/6/2019	3,593	GMO Internet, Inc. d/b/a Onamae.com	2,767	77.0%	163
biz	9/10/2019	3,409	GMO Internet, Inc. d/b/a Onamae.com	2,207	64.7%	244
biz	9/11/2019	3,416	GMO Internet, Inc. d/b/a Onamae.com	2,000	58.5%	484
biz	9/13/2019	3,444	GMO Internet, Inc. d/b/a Onamae.com	1,880	54.6%	76
biz	9/15/2019	4,059	GMO Internet, Inc. d/b/a Onamae.com	1,809	44.6%	131
biz	9/18/2019	4,783	GMO Internet, Inc. d/b/a Onamae.com	1,963	41.0%	629
biz	9/19/2019	4,884	GMO Internet, Inc. d/b/a Onamae.com	2,050	42.0%	317
biz	9/20/2019	5,648	GMO Internet, Inc. d/b/a Onamae.com	2,791	49.4%	911
biz	9/22/2019	5,682	GMO Internet, Inc. d/b/a Onamae.com	2,869	50.5%	164
biz	9/23/2019	5,795	GMO Internet, Inc. d/b/a Onamae.com	2,948	50.9%	253
biz	9/24/2019	6,495	GMO Internet, Inc. d/b/a Onamae.com	3,612	55.6%	966

Interisle Consulting Group

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

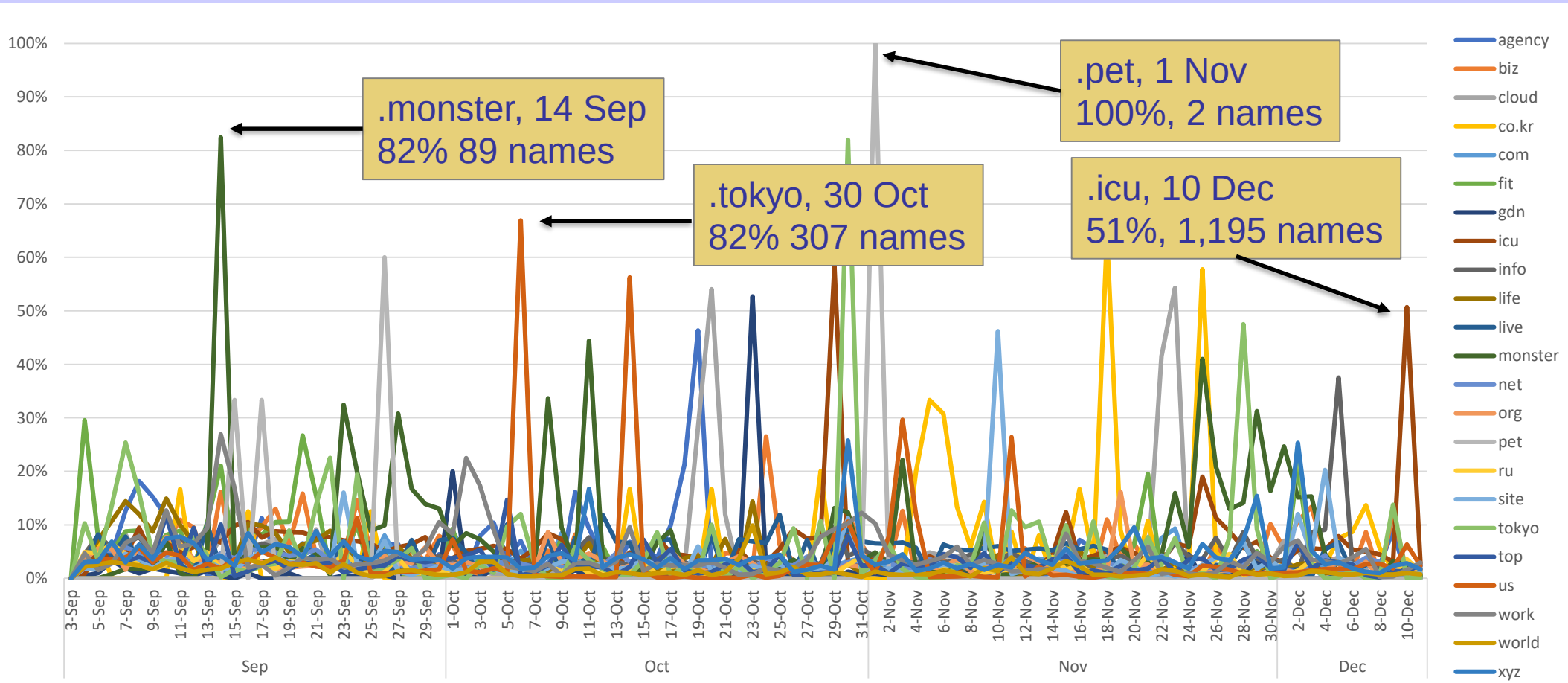
01fl9z	0bgisc	0guvdk	0olerp	0unbec	12dggb	1cbxpw	1hpbxt	1omb8j	1w0ied	27brhe	2fnrye	2o1mfa	2tefgz	2zjp9s	zwscho
01py42	0bhqex	0h4blq	0on1yf	0uradt	13mp4u	1ciuwl	1i7ryf	1ozlxj	1wfsks	29jvhi	2fsvyg	2o9fkd	2tj5vf	2zpqh4	zwuhqg
02gtn1	0bkpju	0h4ofm	0oqq1x	0urq3q	14fjnq	1cjqrg	1iaqnp	1ozmz6	1whdgb	2adoqi	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

Percent of Each TLD's Blocklist Added



Interisle Consulting Group

10 December – 1,195 Names Added to .icu Blocklist – ERANET names

aaykz	bdqot	bqxya	cevg	cvsn	dkxql	dxggq	epam	fbejj	fohxe	gfadc	gvxdo	hmew	idrbx	ivvgs		xbvqj
aazoj	bdww	brfc	cfhwo	cwcs	dljsv	dzsk	epdt	fcdwk	foqry	gfdzx	gwca	hmlk	ienlu	ivvn		xcolh
adlbq	beei	brgmn	cfoz	cwpg	dluih	eacgz	eqkx	fchjd	fqbar	gfqz	gwfa	hmma	ievs	iwba		xdbbr
afexe	berpm	briak	cgdxe	cwput	dlyc	eahl	eqvm	fcsxp	fqgd	ggyij	gwjib	hnycl	ifbbn	iwjp		xekbp
ajqhg	besm	brtx	cguyl	cwtz	dmgk	ebrou	eraz	fcurz	fqtf	ghavr	gwkea	hnzo	ifqh	iwqaz		xffbu
allcq	bfaei	bscu	chavm	cxbci	dmgu	ebsnf	erbrs	fdgss	frzt	ghfz	gwtnr	hpjo	ihqhy	iwyye		xfocf
arwza	bfbve	bsfly	chfzg	cxnfq	dnhdq	ebvha	eriq	fduck	fsbbk	ghlov	gyev	hpnel	ihyra	ixwmp		xgtjn
atdbf	bfmj	bslev	chpt	cxvwz	dnok	ebzzg	erzo	fdwf	fsdx	gibac	gzjen	hptup	ihzic	ixywm		xhsid
athia	bfwtw	bslml	chsb	cyogl	dnon	echnh	esdv	fejhn	fstqd	gidla	gztq	hpwi	ijdfi	iywvg		xnicj
atpzw	bfzb	bsnk	chuwp	cypz	dnqu	ecnai	esrae	fejzg	ftaf	gipz	gzxi	hrvga	ijfc	izgar		xqjbh
attsl	bfzh	bssr	civzq	czuwx	dnsr	ecspf	estbp	felkl	ftgla	gisxf	habcy	hsit	ijqj	jado		xqonj
atudd	bgfz	bsth	cixe	czyyl	dnxyx	edfmk	etau	fffyy	ftgqy	gjfjy	hamv	hsye	ijtmu	jahra		xxzmz
atyze	bgjl	bthp	cjcdd	daozs	domc	edweg	etdhj	ffpm	ftvyt	gknat	haxge	htgqd	ikkvk	jarxv		xypzk
avqlw	bgury	bung	ckng	daxr	dosia	eehz	etuwm	fgawg	fuaqk	gktfo	hayeu	htqbm	ikssg	jbhg		xysjm
avqxr	bhju	bupvi	ckwa	dcaqz	doudw	eeifo	euwtd	fhdi	fuejj	gmro	hbxqe	htudi	ikwnc	jblik		xzhvb
avrwr	bhsau	buscb	clapi	dcchx	dpsmu	eeri	euxaf	fhrni	fuxsy	gmup	hcdcl	htwxp	ilcwu	jbrr		yaaxq
awpwu	bhuah	bvdb	clbmq	dcyw	dpue	efxo	euzeo	finl	fuxvm	gmxmy	hcemu	hulyx	illld	jchz		yaiyr
awsib	biehw	bvlhv	cmeqg	ddmfp	dpuf	egbwq	evdli	fjko	fvcxs	gntft	hchg	hunx	ilxr	jcih	...	ybldw
aybx	bihne	bvwfv	cnizl	ddneb	dpvpk	ehfvg	evztw	fjlde	fwbs	goqzn	hcjpu	huypa	ilygi	jcjsr		yblrm
ayen	bikqj	byaat	cnqxg	deam	dqjyt	ehga	ewgou	fjqkp	fwou	gosdb	hcovl	hvked	imlwl	jdfww		yddvx
ayma	bipbs	bybe	cnvf	deiat	dsbim	ehkda	ewocs	fjyfe	fxsvo	gqclb	hcslq	hvuui	immc	jdjot		ydura
azbbt	bjaf	bykur	cnzgr	deqkq	dsbm	ehtt	ewpvb	fjzer	fyqe	gqcpt	hdusg	hwvml	injsv	jdugv		ygsd
azje	bjufp	bzffm	cokri	dewkc	dshdl	eifos	ewpzt	fklzi	fzdez	grbe	hedz	hxgob	intdn	jesn		yjka
azrhq	bkas	bzjgx	cpml	dffju	dstua	ejftk	ewvcq	fkozo	fzpn	grccw	hfcm	hycdt	invtk	jeta		ynfvh
azyk	bkdh	bzkqy	cqrhk	dgfgq	dsxf	ejsz	ewxe	flcfy	gaajn	gskd	hftsu	hzgfj	inxlr	jiasn		yruii
balz	bkdoe	bzwcl	cqus	dgln	dtadu	ekcel	exani	flfdq	gawp	gsoyo	hgcgj	hzixt	iocjj	jidb		ytodh
bamt	blaiv	cbas	crajj	dguys	dthro	ekqp	exaxe	flgez	gawzm	gtlxn	hgnmh	hzvjd	ipkfl	jizzl		yudrb
barmy	bluuk	cbcuk	cruud	dhcac	dtlzh	ekwbl	exly	fliud	gaypu	gtrad	hgwqw	iaprn	iprag	jjdio		yvlob
basb	blwg	cbynt	csawg	dixiy	dtnwc	ekxb	exxkw	flqk	gbxf	gugoc	hhap	icacm	iqise	jjiw		ywxhk
bbnz	bmgk	cccpi	csfqm	diyss	dtqrf	elqgi	eysm	fmkte	gcftp	gurq	hhmn	icaeo	isjbp	jjybg		zksop
bbqo	bmjdw	cclfz	ctbxh	djex	dtyf	eltz	eythm	fmmwb	gcgao	gvmca	hifkn	icfjm	ispt	jkee		zmxpq
bckz	bmjxj	cddwb	ctmob	djsj	duvz	emiq	eyxtf	fmtlv	gcte	gvmvt	hiqd	icssm	isvge	jkqaa		zsqik
bcnig	bodoy	cdkjw	ctnay	dkijr	dvogs	emlr	eyzwn	fmtz	gctlf	gvni	hivoq	idbr	ithy	jkxd		ztcmk
bcpxm	bolyh	cdzbj	curn	dkqut	dvot	emtt	ezcfe	fnjkw	gcxuc	gvsmc	hjecy	idjot	itjf	jldy		zyhxe
bcpyl	bqkub	ceqn	cvfq	dksz	dvvxu	enzl	ezeys	foev	genb	gvtt	hkydg	idof	ituy	jmlq		zzzpc

Interisle Consulting Group

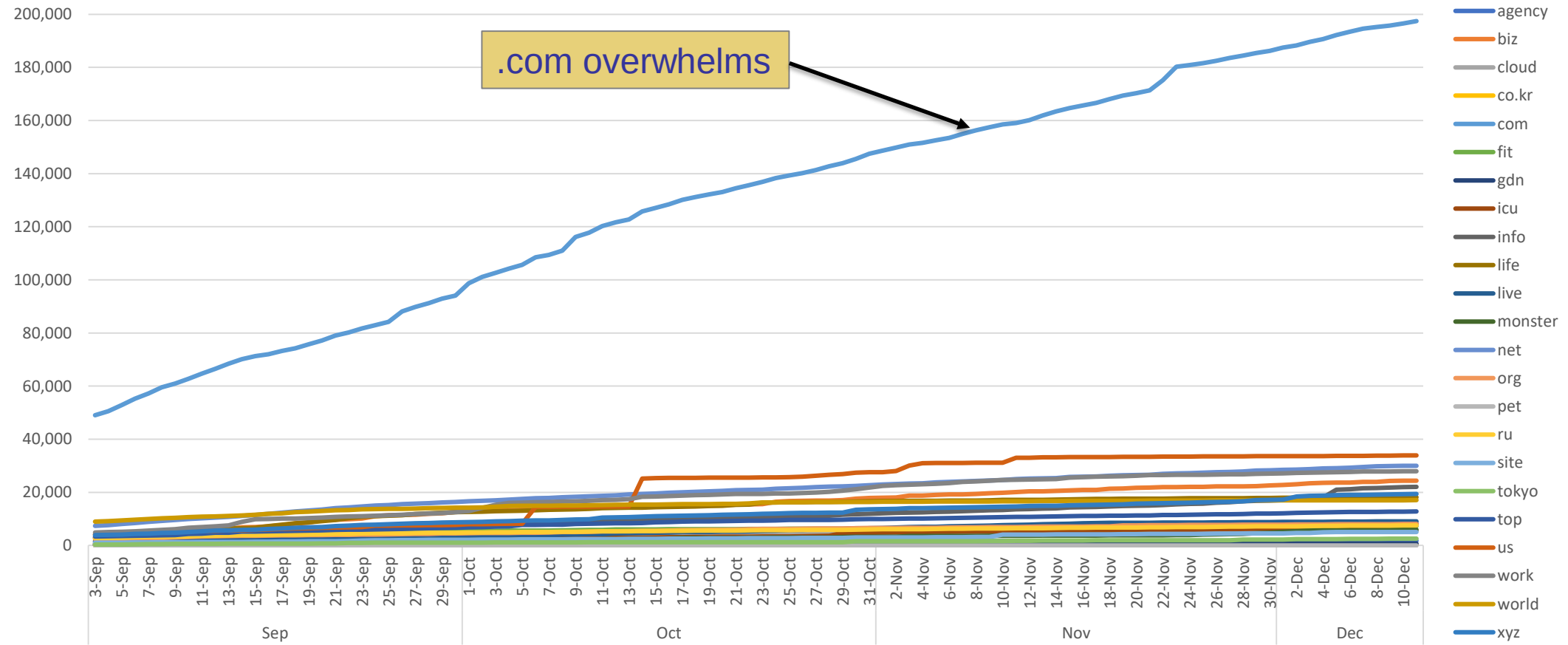
Turnover Rate

Date	TLD	Blocklist Size	Names Added
14 Sep	.monster	108	89
6 Oct	.us	9,401	6,329
14 Oct	.us	18,636	10,516
20 Oct	.cloud	1,072	620
23 Nov	.cloud	779	429
25 Nov	.co.kr	213	123
2 Dec	.xyz	4,653	1,052
5 Dec	.info	7,952	3,115

Date	TLD	Names Removed	Blocklist Size
29 Oct	.us	9,821	3,928
2 Nov	.agency	1,615	247
12 Sep	.monster	160	41

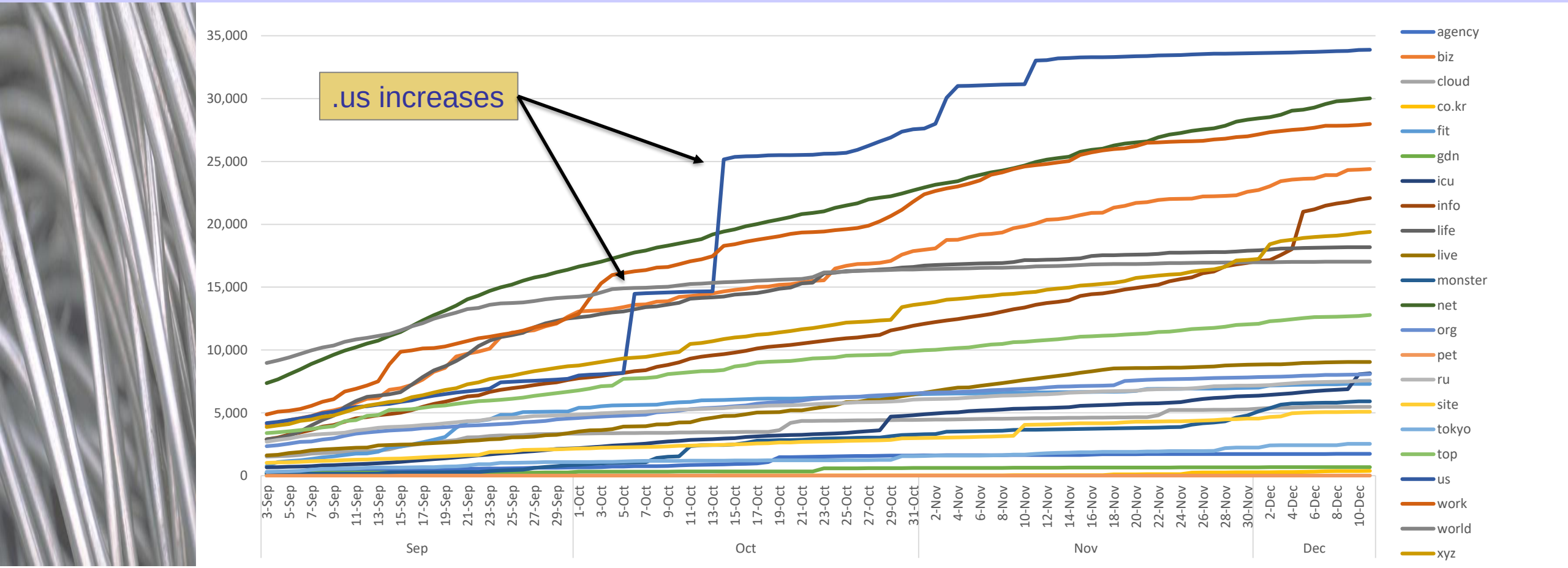
Interisle Consulting Group

Cumulative Unique Blocked Domains



Interisle Consulting Group

Cumulative Blocked Domains (excluding .com)



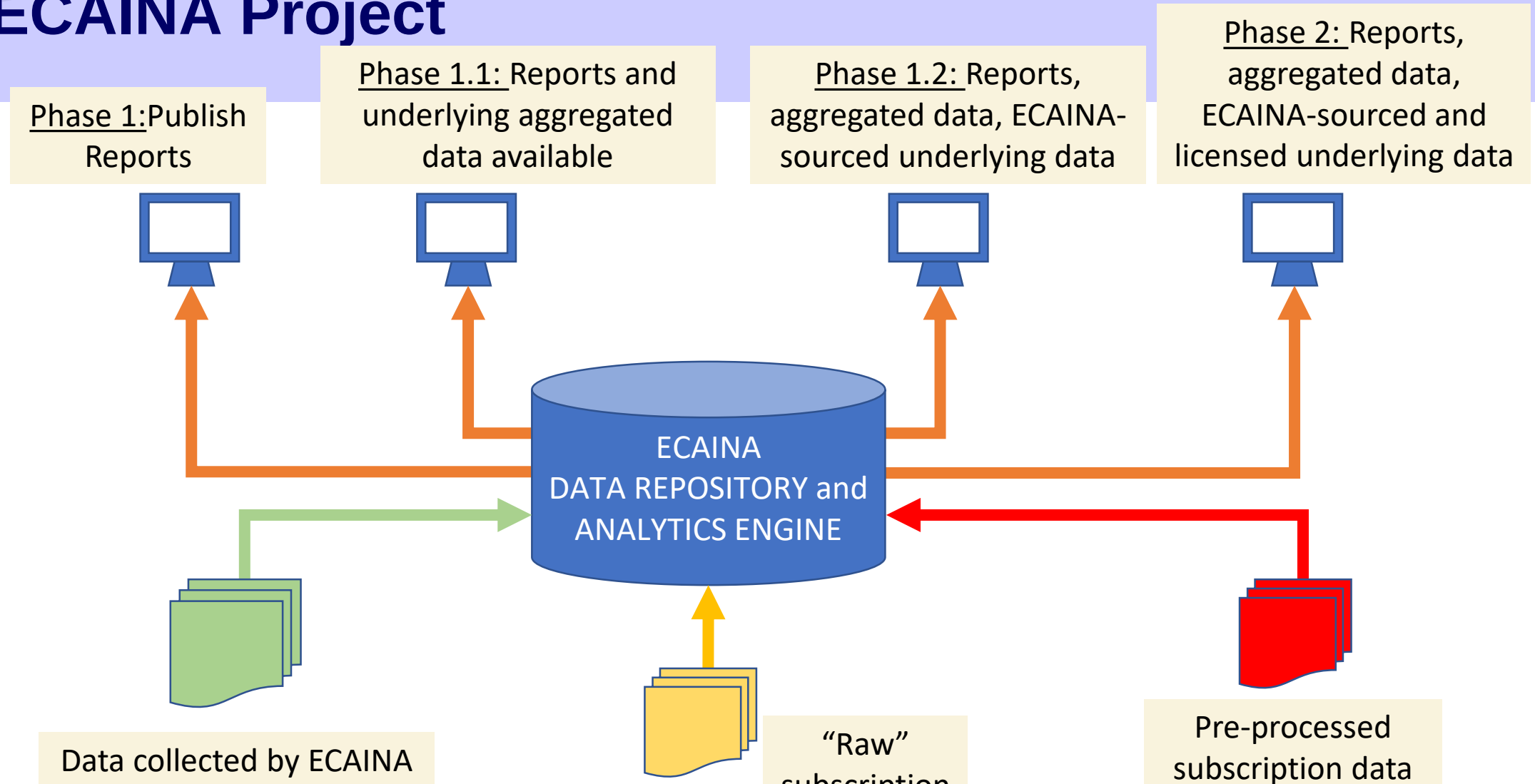
Interisle Consulting Group

ECAINA Plan

- ECAINA will operate a trusted, neutral, public clearinghouse
- ECAINA will use trusted reputation data sources with additional high fidelity “curation”
- ECAINA will expand the reputation data to allow classification and analysis of additional security threats
- ECAINA will operate as a research project at George Mason University
- University and commercial participation will be part of ECAINA’s DNA
- Interisle staff will participate as co-Principal Investigators to provide subject matter expertise, recommend research activities, co-advise University graduate research assistants, and solicit industry or foundation participation and financial support

Interisle Consulting Group

ECAINA Project



Interisle Consulting Group

ECAINA – The Players So Far

- Interisle
  - Dave Piscitello
  - Lyman Chapin
  - Colin Strutt
- Illumintel
  - Greg Aaron
- George Mason University (GMU)
  - Eric Osterweil
- Others welcome!

Interisle Consulting Group