SECURE DOMAIN
FOUNDATION

Community Metrics For DNS Abuse

Drew Bagley
drew@securedomain.org
June 2020

CCT Review Team Analysis

- The Competition, Consumer Choice, and Consumer Trust Review Team published its final report in October 2018

https://www.icann.org/en/system/files/files/cct-final-08sep18-en.pdf

- The Report included findings from the ICANN-commissioned Statistical Analysis of DNS Abuse in gTLDs (SADAG)

https://www.icann.org/public-comments/sadag-final-2017-08-09-en

SECURE DOMAIN FOUNDATION

CCT Review Team Findings

CCT Review Team studied DNS Security Abuse

CCT operating definition of DNS Security Abuse:
DNS abuse related to cybersecurity, such as malware distribution, phishing, pharming, botnet command-and- control, and high-volume spam.

Selected Findings

- High levels of DNS abuse are not random nor universal
- Among other identifiable trends, there are systemic, unabated high levels of abuse associated with particular registrars and registries
- These registries and registrars can continue operating for years with high abuse rates without losing accreditation

CCT Review Team Recommendation 15

CCT Review Team issued recommendations related to DNS abuse

Recommendation

"ICANN Org should, in its discussions with registrars and registries, negotiate amendments to the Registrar Accreditation Agreement and Registry Agreements to include provisions aimed at preventing systemic use of specific registrars or registries for DNS Security Abuse…"

Details

"…ICANN should make use of well-regarded abuse/blacklists and establish an initial threshold at which compliance inquiries are automatically generated. We suggest that this initial threshold should be 3% of registrations or 30 total registrations, whichever is higher. Further, ICANN should establish a subsequent threshold at which a contracted party is presumed to be in breach of its agreement. We suggest this subsequent threshold should be 10% of registrations or 100 total registrations, whichever is higher.

https://www.icann.org/en/system/files/files/cct-final-08sep18-en.pdf

SADAG Findings

Extremely high abuse rates can go unabated for years without consequence

- Two registrars highlighted by the Study had overwhelming rates of abuse.
- More than 93% of the new gTLD registrations sold by Nanjing Imperiosus Technology, based in China, appeared on SURBL's blacklists.
- ICANN eventually suspended Nanjing in January 2017, citing its failure to comply with the RAA, provide abuse records, and failure to pay ICANN fees.
- Alpnames Ltd., based in Gibraltar, was associated with a high volume of abuse from .SCIENCE and .TOP domain names.
- Despite extremely high levels of abuse, Alpnames wasn't suspended until 2019, when ICANN cited that Alpnames was no longer providing basic services to its registrants like renewals
- However, for both, the sustained, unabated, high abuse rates alone did not constitute grounds for suspension.

SADAG https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

https://www.icann.org/uploads/compliance_notice/attachment/895/serad-to-hansmann-4jan17.pdf

Registrars with levels of abuse

Some registrars have a significant portion of their domain name portfolio associated with abuse

Table XVI
SURBL TOP10 PERCENTAGE BETWEEN BLACKLISTED NEW AND LEGACY GTLD DOMAINS (#INCIDENTS) AND TOTAL NUMBER OF REGISTRAR GTLD DOMAINS (#DOMAINS).

#	new gTLD registrar	#Domains	#Incidents	Percent	Legacy gTLD registrar	#Domains	#Incidents	Percent
1	Nanjing Imperiosus Technology	38,025	35,502	93.36	HOAPDI INC.	141	126	89.36
2	Intracom Middle East FZE	20,640	11,255	54.53	asia registry r2-asia (700000)	1,379	598	43.36
3	Dot Holding Inc.	153	76	49.67	Nanjing Imperiosus Technology	35,309	10,834	30.68
4	Alpnames Limited	3,028,011	751,748	24.83	Paknic (Private) Limited	10,525	3,083	29.29
5	Todaynic.com, Inc.	329,399	69,404	21.07	OwnRegistrar, Inc.	22,188	5,238	23.61
6	Web Werks India Pvt. Ltd	785	146	18.6	Eranet International Limited	6,109	1,339	21.92
7	GMO Internet, Inc. d/b/a Onamae.com	1,734,775	295,641	17.04	BR domain Inc. dba namegear.co	847	158	18.65
8	TLD Registrar Solutions Ltd.	163,988	24,700	15.06	Netlynx Inc.	17,612	3,030	17.2
9	Xiamen Nawang Technology Co., Ltd	282,925	42,089	14.88	AFRIREGISTER S.A.	1,551	266	17.15
10	Instra Corporation Pty Ltd.	77,642	6,200	7.99	GMO Internet, Inc. d/b/a Onamae.com	7,306,312	1,177,886	16.12

Table XVII
SPAMHAUS TOP10 RATE BETWEEN BLACKLISTED NEW AND LEGACY GTLD DOMAINS (#INCIDENTS) AND TOTAL NUMBER OF REGISTRAR GTLD DOMAINS (#DOMAINS).

#	new gTLD registrar	#Domains	#Incidents	Percent	Legacy gTLD registrar	#Domains	#Incidents	Percent
1	Nanjing Imperiosus Technology	38,025	29,682	78.06	ABSYSTEMS INC	688	632	91.86
2	Alpnames Limited	3,028,011	1,208,509	39.91	Eranet International Limited	6,109	4,074	66.69
3	Shanghai Best Oray Information S&T	3,600	1,324	36.78	Ednit Software Private Limited	524	285	54.39
4	Dot Holding Inc.	153	50	32.68	Dynamic Dolphin, Inc.	12,515	5,870	46.9
5	MAT BAO CORPORATION	3,116	746	23.94	Webair Internet Development, Inc.	19,607	7,484	38.17
6	NameSilo, LLC	31,084	6,718	21.61	asia registry r2-asia (700000)	1,379	460	33.36
7	Zhengzhou Century Connect Elec. Tech. Dev.	16,057	3,235	20.15	Nanjing Imperiosus Technology	35,309	11,475	32.5
8	TLD Registrar Solutions Ltd.	163,988	32,043	19.54	Alpnames Limited	27,558	7,604	27.59
9	Netowl, Inc.	1,190	206	17.31	GoName-TN.com, Inc.	7,088	1,815	25.61
10	GMO Internet, Inc. d/b/a Onamae.com	1,734,775	263,681	15.2	Paknic (Private) Limited	10,525	2,553	24.26

SADAG https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

SADAG Findings

Some registries had a significant portion of their zones tied to abuse

- The SADAG identified several TLDs with more than 10% of their domain names associated with abuse:
- .science (51%)
- .stream (47%)
- .study (33%)
- .download (20%)
- .click (18%)
- .top (17%)
- .gdn (16%)
- .trade (15%)
- .review (13%)
- .accountant (12%)

https://www.icann.org/news/announcement-2-2019-03-15-en

Registries with high levels of abuse

SADAG chart on new gTLDs

Table XXIV
TOP 10 NEW GTLDS WITH THE HIGHEST RELATIVE CONCENTRATION OF BLACKLISTED DOMAINS FOR STOPBADWARE SDP, APWG, SPAMHAUS, SECURE DOMAIN FOUNDATION, SURBL, AND CLEANMX DATASETS (FOURTH QUARTER OF 2016). SCORES ARE CALCULATED AS FOLLOWS: $S = 10,000 * \#blacklisted\ domains/\#all\ domains$.

StopBadware			APWG			Spamhaus			SDF		
TLD	# Domains	Score	TLD	# Domains	Score	TLD	# Domains	Score	TLD	# Domains	Score
TOYS	32	78	LIMITED	31	66	SCIENCE	117,782	5,154	SUPPORT	510	294
TRADE	221	15	SUPPORT	43	24	STREAM	18,543	4,756	TECH	4,409	158
TATAR	1	11	CENTER	72	22	STUDY	1,118	3,343	ONLINE	4,179	83
WANG	1,086	11	CREDITCARD	1	13	DOWNLOAD	16,399	2,016	LIMITED	15	32
JUEGOS	1	9	SERVICES	24	10	CLICK	20,713	1,814	REVIEW	161	24
TOP	3,830	8	ONLINE	417	8	TOP	736,339	1,705	CLAIMS	3	19
MOE	5	8	MOE	5	8	GDN	45,547	1,602	PRESS	91	19
CAB	3	7	HOST	32	7	TRADE	23,581	1,521	FURNITURE	4	18
PICS	10	7	LEASE	1	6	REVIEW	9415	1,318	WEBSITE	298	15
TATTOO	2	7	REPORT	3	6	ACCOUNTANT	6,722	1,279	CREDITCARD	1	13

SURBL ph			SURBL mw			SURBL ws			SURBL jp		
TLD	# Domains	Score	TLD	# Domains	Score	TLD	# Domains	Score	TLD	# Domains	Score
LIMITED	51	109	FOOTBALL	7	16	RACING	51,443	3,812	SCIENCE	152,719	6,683
SUPPORT	82	46	TOP	5,066	11	DOWNLOAD	21,515	2,645	CLICK	27,871	2,441
CENTER	93	29	RIP	1	5	ACCOUNTANT	10,543	2,007	GDN	50,940	1,792
SERVICES	61	25	BID	200	3	REVIEW	12,615	1,766	STREAM	6,033	1,547
CRICKET	57	22	DENTIST	1	3	GDN	49,427	1,739	LINK	39,764	1,238
ONLINE	903	16	LGBT	1	3	FAITH	5,540	1,301	REVIEW	8,705	1,219
WEBSITE	318	14	ACCOUNTANT	11	2	TRADE	19,330	1,247	CRICKET	2,468	993
REPORT	7	14	CAB	1	2	CLICK	13,270	1,162	TRADE	14,535	937
HOST	65	13	SUPPORT	5	2	STREAM	4,406	1,130	FAITH	3,130	735
CREDITCARD	1	13	POKER	1	2	DATE	1,3851	999	TOP	285,488	661

CleanMX ph			CleanMX mw			CleanMX pt		
TLD	# Domains	Score	TLD	# Domains	Score	TLD	# Domains	Score
SARL	4	46	RODEO	1	12	QPON	1	20
LIMITED	9	19	TATAR	1	11	GRATIS	5	13
SUPPORT	19	10	MOE	6	10	CRICKET	32	12
ONLINE	493	9	HOW	1	4	TATAR	1	11
REPORT	4	8	ONLINE	183	3	DURBAN	2	8
MOE	4	6	CASINO	1	3	CLICK	72	6
CENTER	21	6	CHEAP	1	3	WEBCAM	18	4
REST	1	5	TAX	1	2	TAXI	2	4
SERVICES	13	5	CAB	1	2	WEBSITE	105	4
LAT	1	4	COMPUTER	1	2	LIMITED	2	4

SADAG https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

Findings to build from

Why should the Community permit systemic, unabated DNS abuse?

- Some registrars, registries and resellers are used or targeted by cybercriminals (malicious registrations and compromised)
- Absent effective incentives or disincentives for permitting high levels of abuse, these parties benefit from registrations regardless of whether they are being used for malware distribution, phishing, pharming, botnet command-and-control, and high-volume spam
- Unabated, systemic abuse is incompatible with the security and stability of the Domain Name System
- The CCT Review Team proposed to the Board a recommendation to create 3% and 10% abuse thresholds to provide a means to remedy abuse and suspend parties that will not mitigate abuse

SECUREDOMAIN
FOUNDATION

www.securedomain.org

Drew Bagley
drew@securedomain.org