Identifier Technology Health Indicators (ITHI)

Alain Durand, Christian Huitema

13 March 2018

ICANN 61
COMMUNITY FORUM
SAN JUAN
10–15 March 2018

ITHI Principles of Operation

- Technical focus
- Problem areas → Metrics → Measurement
- Current value and trend over time
    - Automated process to collect & analyse data
- Measurement, not interpretation
- Extraction of statistics to avoid data privacy issues
- Open source tools & results

7 Metrics and Data Sources

Metric	Name	Data Source
M1:	inaccuracy of Whois Data	ICANN compliance dept.
M2:	Domain Name Abuse	ICANN's DAAR Project https://www.icann.org/octo-ssr/daar
M3:	DNS Root Traffic Analysis	Scans of DNS root traffic
M4:	DNS Recursive Server Analysis	Scan of recursive resolvers traffic
M5:	(TBD)	(TBD)
M6:	IANA registries for DNS parameters	Scan of recursive resolvers traffic
M7:	DNSSEC Deployment	Snapshots of DNS root zone

ITHI Time Line

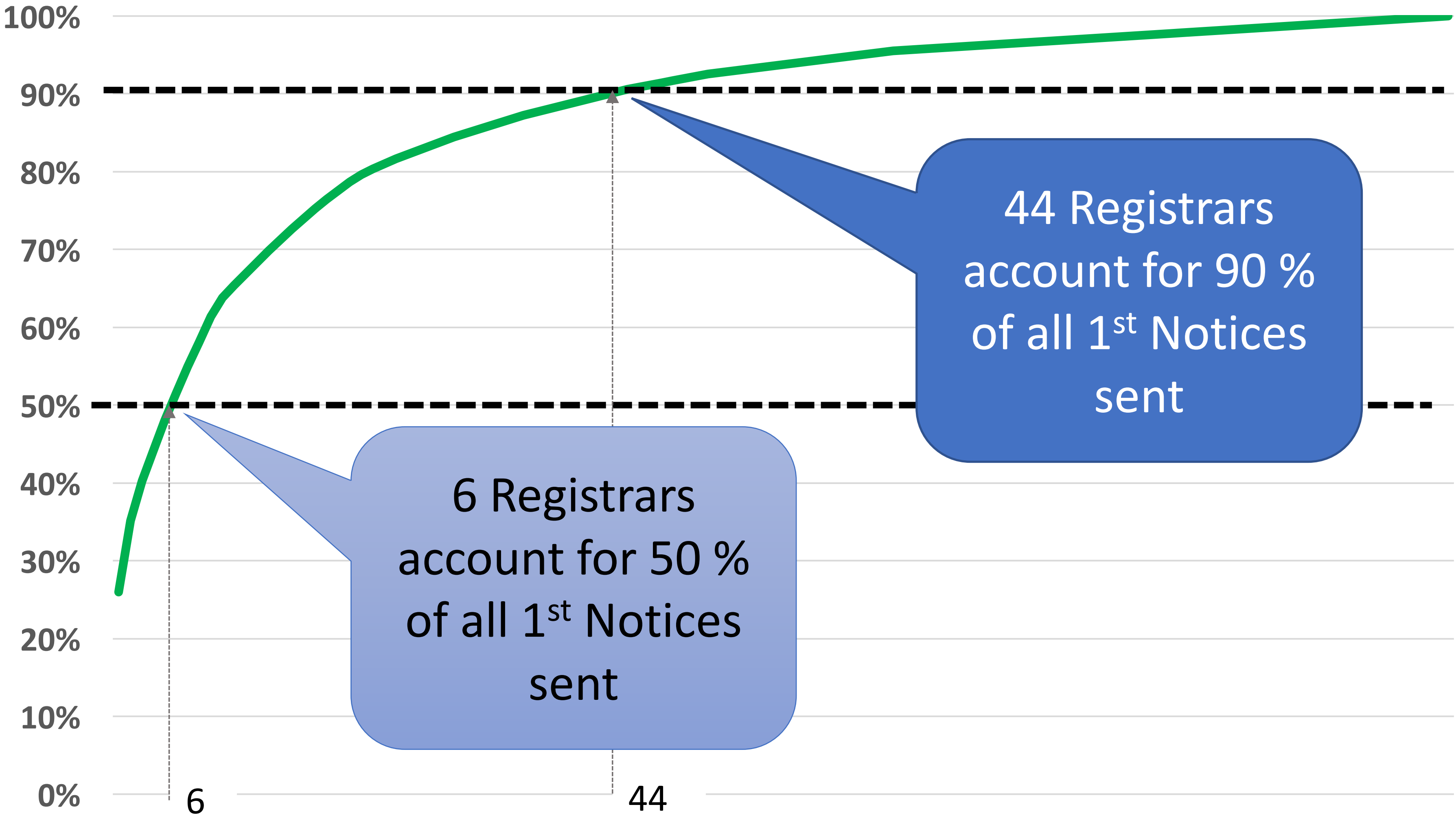
- 2017: definition of metrics, prototype tool chain.
- Jan-Feb 2018: initial captures: M1, M2, M3, and M7
  - Initial result from small set of sources M4 and M6
- Mar 2018: first data presented at ICANN meeting

- Next steps:
  - Jun 2018: M5
  - pipeline automation, publish metrics on ICANN web site

M1: Inaccuracy of Whois Data

M1 metric name	Current value
M1.1 = Number of “validated complaints” per million registrations.	5.9

Concentration of 1st Notices



44 Registrars account for 90 % of all 1st Notices sent

6 Registrars account for 50 % of all 1st Notices sent

Total number of registrars: 1954

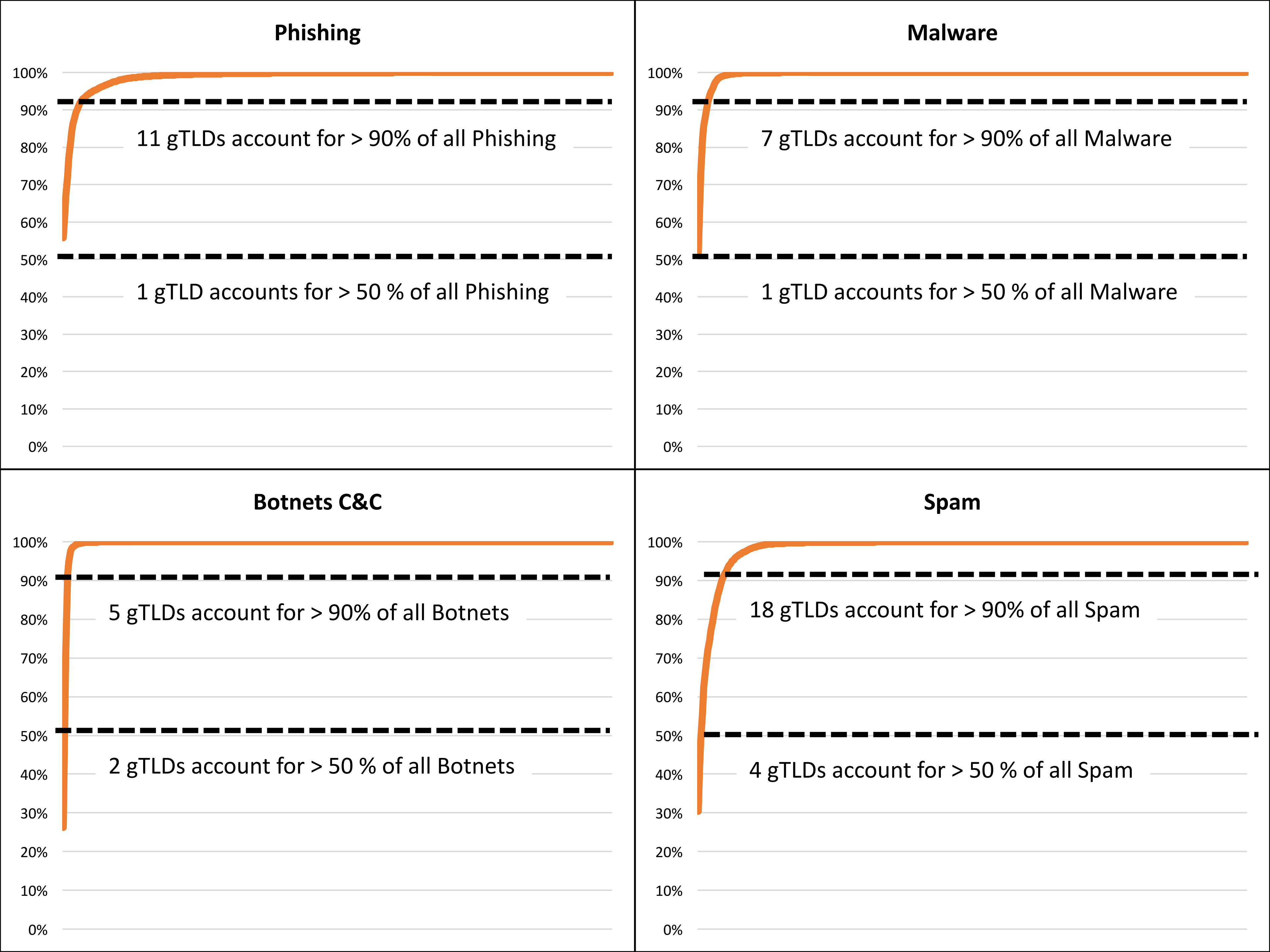
X Axis: Registrars, ranked by number of 1st notices they received

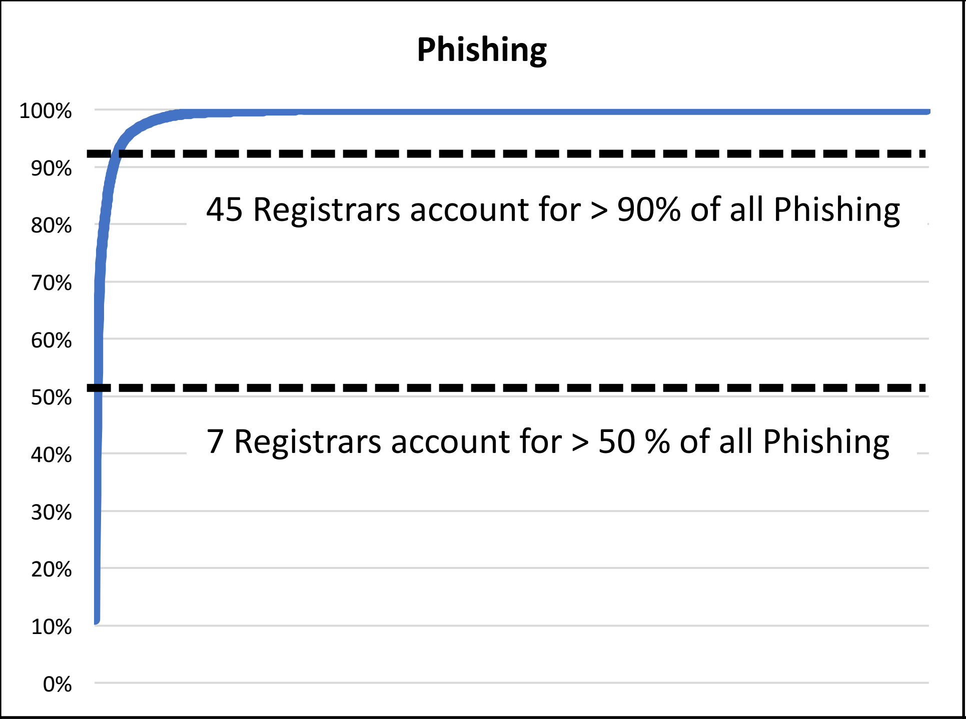
M2.*: Number of Abused Domain per 10,000 Registrations

Data from
01/31/2018

M2 metric name	Global Average
M2.1 = number of Phishing Domains per 10000 registered domain names	4.28
M2.2 = number of Malware Domains per 10,000 registered domain names	3.28
M2.3 = number of Botnet C&C Domains per 10,000 registered domain names	2.89
M2.4 = number of Spam Domains per 10,000 registered domain names	86.73

Total number of gTLDs: 1143, Total number of registrars: 1952

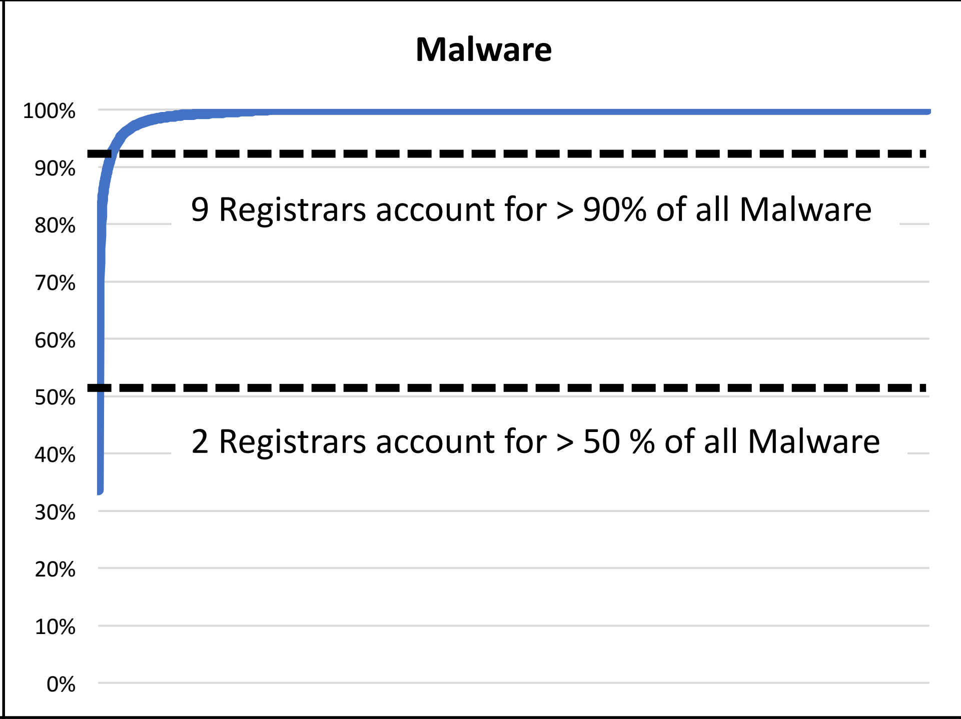

Phishing
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
11 gTLDs account for > 90% of all Phishing
1 gTLD accounts for > 50 % of all Phishing
Malware
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
7 gTLDs account for > 90% of all Malware
1 gTLD accounts for > 50 % of all Malware
Botnets C&C
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
5 gTLDs account for > 90% of all Botnets
2 gTLDs account for > 50 % of all Botnets
Spam
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
18 gTLDs account for > 90% of all Spam
4 gTLDs account for > 50 % of all Spam



Phishing

45 Registrars account for > 90% of all Phishing

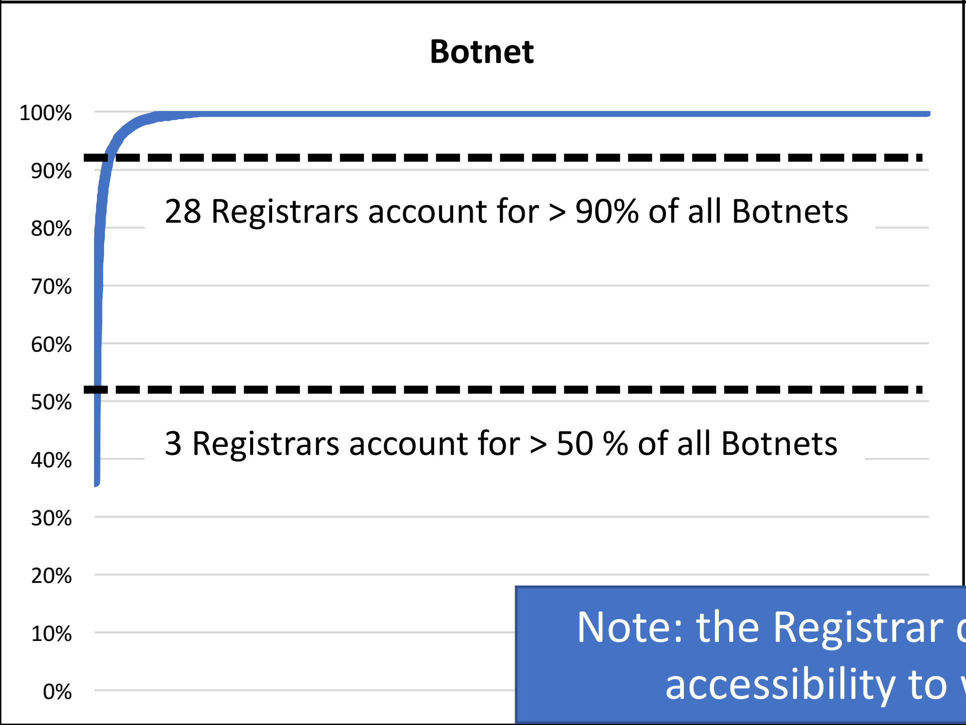
7 Registrars account for > 50 % of all Phishing



Malware

9 Registrars account for > 90% of all Malware

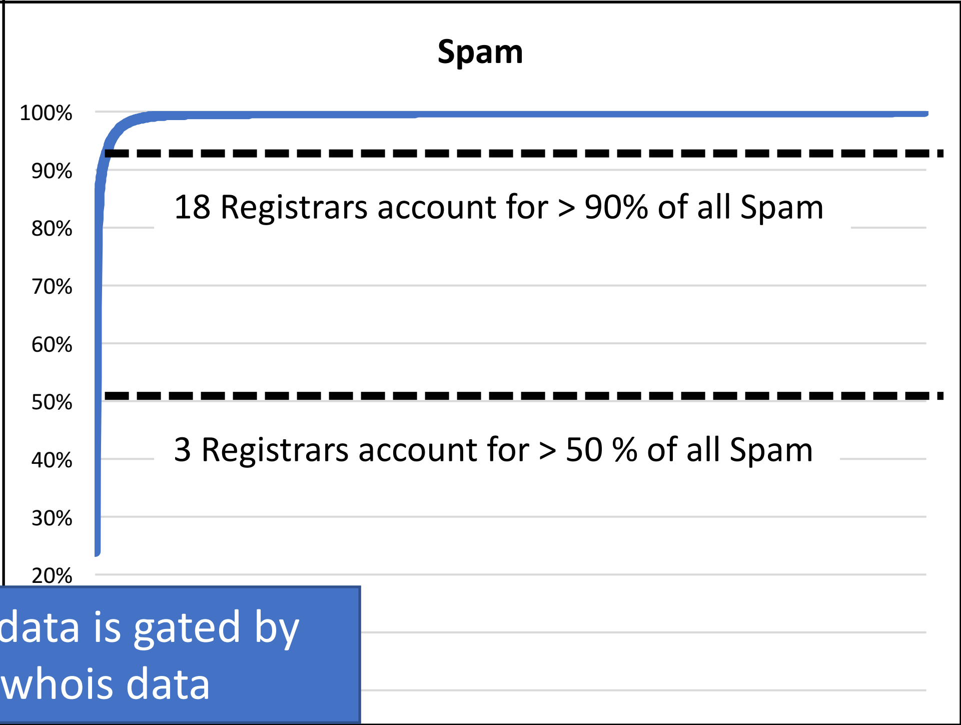
2 Registrars account for > 50 % of all Malware



Botnet

28 Registrars account for > 90% of all Botnets

3 Registrars account for > 50 % of all Botnets



Spam

18 Registrars account for > 90% of all Spam

3 Registrars account for > 50 % of all Spam

Note: the Registrar data is gated by accessibility to whois data

M2.*: Concentration of Abuse

Abuse	gTLD50	Registrar50	gTLD90	Registrar90
Phishing	1	7	11	45
Malware	1	2	7	9
Botnet	2	3	5	28
Spam	4	3	18	18

Table shows the number of TLDs/Registrars to account for > 50%/90% of all abuse of the specified type.

Total number of gTLDs: 1143, Total number of registrars: 1952*

(*) We removed two parking registrars from those statistics

M3: Root Traffic Analysis

Metric	Current	Average
M3.1 (% No Such Domain queries)	**64.44%**	**64.83%**
M3.2 (% cacheable queries)	**28.94%**	**28.77%**
Core (100% - M3.1 - M3.2)	**6.63%**	**6.40%**

Components of M3.1:		
M3.3.1 (% RFC 6761 names)	**3.44%**	**3.44%**
M3.3.2 (% frequently leaked strings)	**9.37%**	**9.37%**
M3.3.3 (% frequent patterns)	**41.47%**	**40.67%**
M3.3.4 (% other types of names)	**9.80%**	**11.35%**

M3.3.1, M3.3.2, M3.3.3 also provide the list of frequently seen RFC 6761 names, leaked strings, or generated patterns.

M3.3.1 (% RFC 6761 names)

3.44% / 3.44%

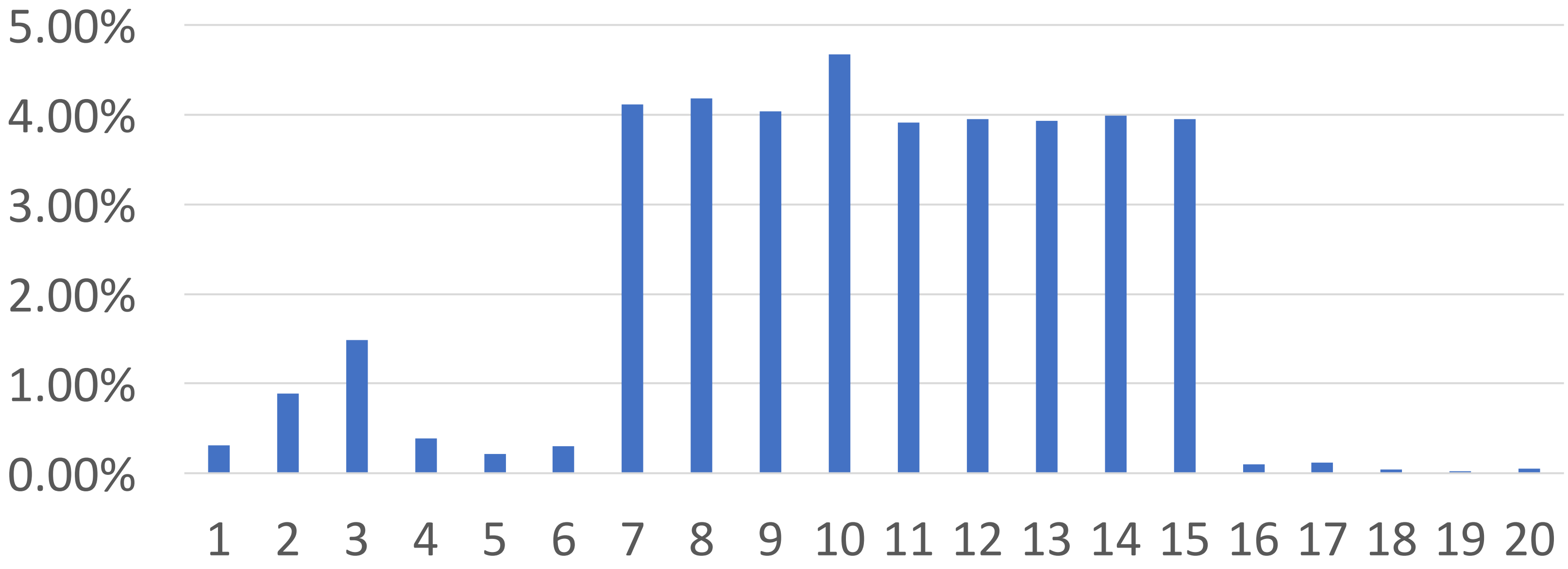
RFC 6761 name	Current value	Average value
LOCAL	2.77%	2.78%
LOCALHOST	0.35%	0.34%
INVALID	0.31%	0.30%
TEST	0.01%	0.01%
EXAMPLE	0.01%	0.01%
ONION	0.00%	0.01%

M3.3.2 (Frequently Leaked Strings)
9.37% / 9.37%

Frequently used string	Current value	Average value
HOME	**3.54%**	**3.67%**
DHCP HOST	**0.85%**	**0.88%**
DHCP	**0.75%**	**0.68%**
LAN	**0.49%**	**0.64%**
INTERNAL	**0.45%**	**0.46%**
LOCALDOMAIN	**0.43%**	**0.44%**
IP	**0.43%**	**0.64%**
OPENSTACKLOCAL	**0.34%**	**0.40%**
DLINK	**0.34%**	**0.31%**
CORP	**0.23%**	**0.22%**
DAVOLINK	**0.20%**	**0.19%**

M3.3.3 (% Frequent Patterns)

41.47% / 40.67%



"Patterns" defined as "length of TLD string"

Chart shows % of "no such domain" queries for specific TLD lengths

Length 21 to 63 omitted – very small, account for less than 1% of queries

Many strings of length 7..15 look like "Domain Generation Algorithms"

M4: DNS Recursive Server Analysis

	Metric	Current	Average
M4.1	% delegated TLDs.	**98.75%**	**99.03%**
M4.2	% RFC 6761 names	**0.07%**	**0.07%**
M4.3	% frequently used strings.	**0.87%**	**0.58%**
M4.4	All other traffic	**0.32%**	**0.31%**

M4.1, M4.2, M4.3 also provide the list of frequently seen RFC 6761 names, leaked strings, or generated patterns.
M4 presents “what the DNS clients are sending”
M3 presents “what the root is receiving, after filters by DNS resolvers

Results for January and February from single point of measurement!

M4.2: Queries to RFC 6761 Names
0.07%/0.07%

RFC 6761 name	Current value	Average value
LOCALHOST	0.06%	0.07%
LOCAL	0.01%	0.00%
INVALID	0.00%	0.00%

M4.3: Queries to Frequently Used Strings

0.87%/0.58%

Frequently used string	Current value	Average value
(local host names)	0.79%	0.47%
UNIFI	0.04%	0.07%
DNS	0.03%	0.02%
INTERNAL	0.01%	0.01%
HOME	0.00%	0.00%
DOMAIN	0.00%	0.01%
LAN	0.00%	0.00%

M6: IANA Registries for DNS Parameters

M6.<r>.<n>.1: Usage. Nb values seen / values registered

Metric	Registry table name	Current	Average
M6.DNS.01.1	DNS CLASSes	33.33%	33.85%
M6.DNS.02.1	Resource Record (RR) TYPEs	19.77%	19.77%
M6.DNS.08.1	DNS EDNS0 Option Codes (OPT)	40.00%	40.00%
M6.DNSSEC.3.3	DNS Security Algorithm Numbers	70.59%	70.59%
M6.DANE.1.1	**TLSA Certificate Usages**	**0.00%**	**0.00%**

M6.<r>.<n>.2: Squatting. Nb non registered/ total usage

Metric	Registry table name	Current	Average
M6.DNS.01.2	DNS CLASSes	0.00%	0.00%
M6.DNS.02.2	Resource Record (RR) TYPEs	0.00%	0.00%
M6.DNS.08.2	**DNS EDNS0 Option Codes (OPT)**	**0.11%**	**0.60%**
M6.DNSSEC.3.3	DNS Security Algorithm Numbers	0.00%	0.00%
M6.DANE.1.2	TLSA Certificate Usages	0.00%	0.00%

The DNS EDNS0 options code 0 is “reserved” and option code 65001 is “reserved for local/experimental use”.

List of DNS Parameter Registries Tracked in M6

Group	Parameters	Metric Index
DANE	TLSA Certificate Usages	M6.DANE.1
	TLSA Selectors	M6.DANE.2
	TLSA Matching Types	M6.DANE.3
DNS	DNS CLASSes	M6.DNS.1
	Resource Record (RR) TYPEs	M6.DNS.2
	DNS OpCodes	M6.DNS.3
	DNS RCODEs	M6.DNS.4
	AFSDB RR Subtype	M6.DNS.5
	DHCID RR Identifier Type Codes	M6.DNS.6
	DNS Label Types	M6.DNS.7
DNS	DNS EDNS0 Option Codes (OPT)	M6.DNS.8
	DNS Header Flags	M6.DNS.9
	EDNS Header Flags (16 bits)	M6.DNS.10
	EDNS version Number (8 bits)	M6.DNS.11
	Child Synchronization (CSYNC) Flags	M6.DNS.12
DNS SEC	DNS Security Algorithm Numbers	M6.DNSSEC.1
	DNS KEY Record Diffie-Hellman Prime Lengths	M6.DNSSEC.2
	DNS KEY Record Diffie-Hellman Well-Known Prime/Generator Pairs	M6.DNSSEC.3

M7: DNSSEC Deployment

	Metric	Current	Average
M7.1	number of signed TLD / total number of TLD	**90.6%**	**90.6%**
M7.2	% DNS Queries requesting DNSSEC	**TBD**	**TBD**

M7.1 Measured by parsing the root zone, looking for DS records for each TLD.

M7.2 Measured by parsing DNS queries at participating DNS recursive resolvers

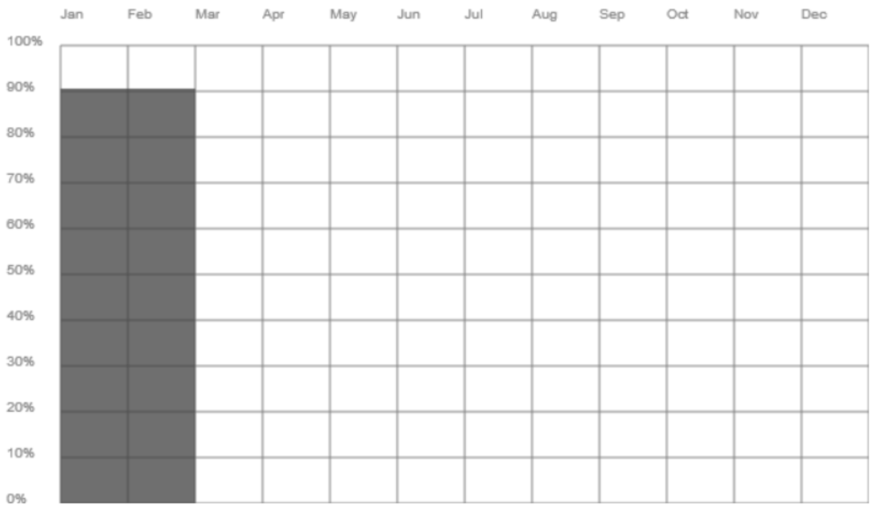
- Clients set DO option flag to request DNS responses

M7.1: Number of Signed TLDs

M7.1: number of signed TLD / total number of TLD

Measured by parsing the root zone, looking for DS records for each TLD.

Current value: **90.6%**



Engage with ICANN

Thank You and Questions

Visit us at **icann.org**

Email: email

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/ icannpresentations

soundcloud/icann