Habits of excellence: why are European ccTLD abuse rates so low?

Roadmap

- Who we are

- Background to the project

- Sources and methods

- Results

- Conclusions

- Q&A

What is the DNS Research Federation?

- A UK non profit

- Mission: to advance the understanding of the Domain Name System's impact on cybersecurity, policy and technical standards.

- Achieving our mission through:

    - Education and research

    - Improving access to data

    - Engagement in technical standards

DNS
RESEARCH
FEDERATION

Background

- NIS2 - WHOIS and data verification procedures; reflecting best practices used within the industry

- The study considers:

  - Comparative abuse rates

  - Abuse rates and market share

  - Impact of demonstrated effective practices

  - Other factors?

DNS
RESEARCH
FEDERATION

Sources and methods

- DAP.LIVE data:
    - gTLD zones and DomainTools for ccTLD numbers
    - OpenPhish, APWG, Abuse.ch URLhaus Project, Spamhaus
- Desk based research: ccTLD numbers, pricing, population size
- CENTR study on EU ccTLD data habits; European Commission study on DNS Abuse
- What did we measure, and how did we define abuse?
    - Phishing, malware and spam only
    - Counted distinct/unique domain names found on each abuse list
    - January 1 through December 31, 2022

The unique context for European ccTLDs

- Europe
  - Advanced economies, mature digital development
  - Four G7 members, 26 OECD members
  - Mature cybersecurity institutions and data protection regulations
- European ccTLDs
  - 50 million registrations; 15% of global market share;
  - 84% are non-profits
  - Thick WHOIS; 70% differentiate between legal and natural persons
  - Quality markers: high renewal rates, domestic market share, high 'developed web content'
  - Providing WHOIS within data protection environment since 1995
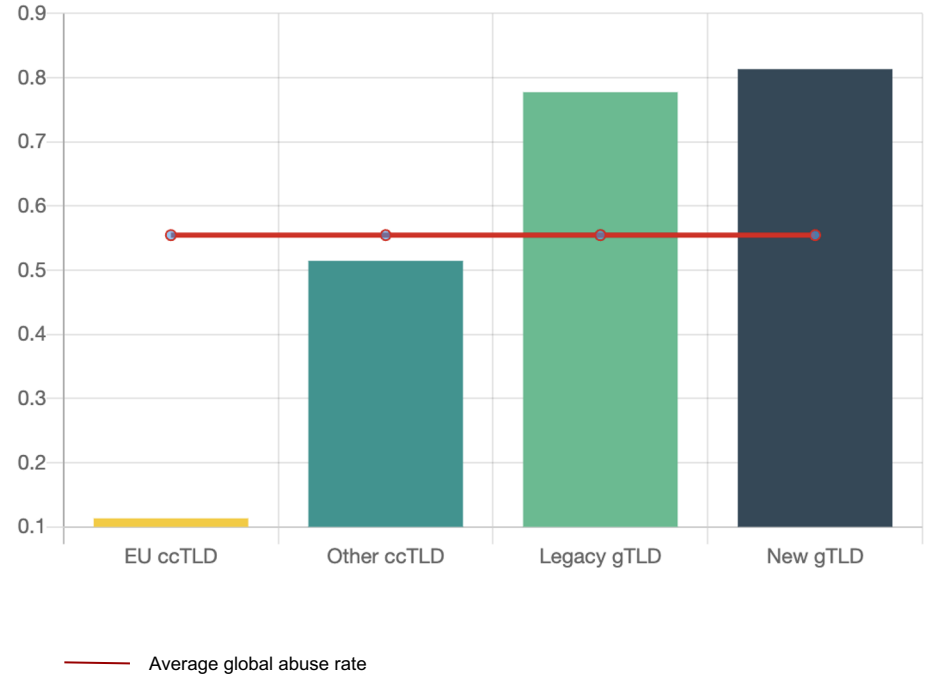
Results

And a note about the data

Abuse Total = All reports across Phishing, Malware, and Spam

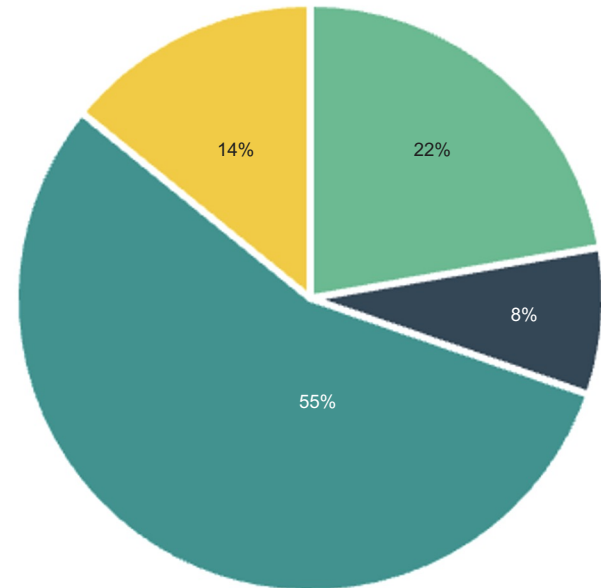**Abuse Rate** = Abuse total / Total registrations

Global Rate = Average Abuse Rate

TLD TYPE	ABUSE RATE	DIFFERENCE
EU ccTLD	0.1133%	- 0.4414%
Other ccTLD	0.5146%	- 0.0401%
Global Abuse Rate	0.5547%	
Legacy gTLD	0.7775%	+ 0.2228%
New gTLD	0.8133%	+ 0.2587%

DNS
RESEARCH
FEDERATION

Abuse data obtained from OpenPhish, APWG, URLHause, and Spamhaus

The EU ccTLD abuse rates are the lowest of any TLD bloc within the global market.

Average global abuse rate

The EU ccTLD abuse rates are significantly lower than the market share of the EU ccTLDs

Other ccTLD
New gTLD
Legacy gTLD
EU ccTLD

14%
22%
8%
55%

TLD Market Share

DNS RESEARCH FEDERATION

Domain counts provided by https://research.domaintools.com/statistics/tld-counts/
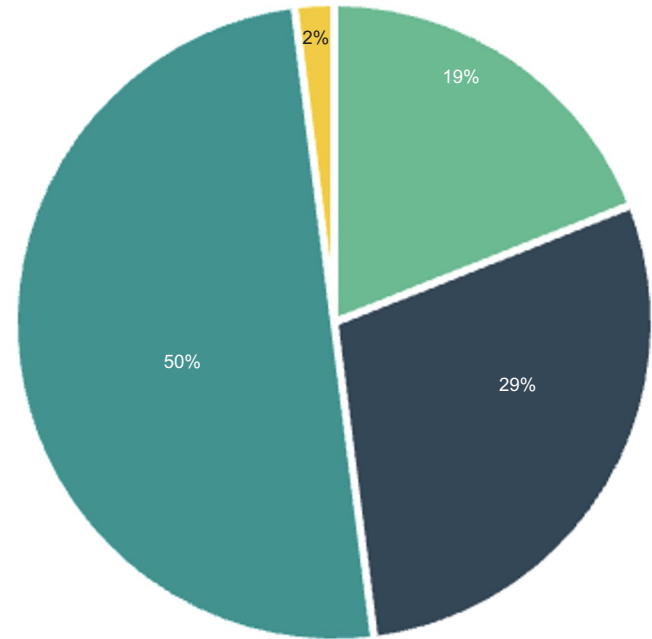
EU ccTLD - combined abuse rates (%) for spam, phishing, malware
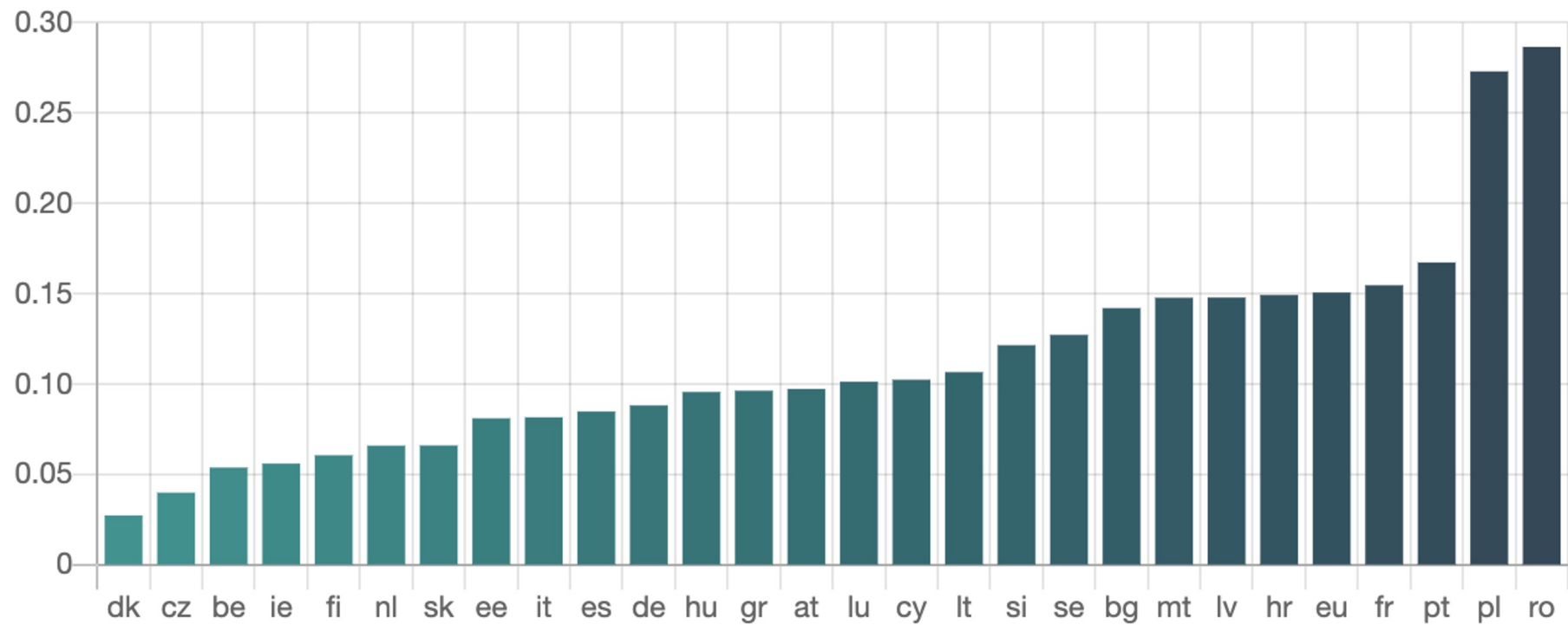
Global Abuse rank (/577)x	TLD	COUNTRY	At registration	Ad hoc	Periodically	Use eID	External verification services / checks	Require address in country / region	Checks on postal / phone details / bank account	Copy of registrant passport
19	dk	Denmark	X	X		X	X		X	
31	cz	Czech Republic		X			X	X	X	
54	ie	Ireland	X		X					
72	nl	Netherlands					X			X
74	sk	Slovak Republic		X						
92	ee	Estonia	X	X	X					
95	it	Italy		X	X					
108	de	Germany		X						
122	hu	Hungary	X	X						
126	at	Austria		X		X	X			
175	lv	Latvia	X	X	X					
197	mt	Malta	X	X						
203	eu	Europe		X		X			X	X
209	fr	France		X						X
220	pt	Portugal	X	X						
323	ro	Romania		X						X

Proportionate data quality practices in low price ccTLDs seem effective in mitigating abuse

market penetration vs. price

DNS RESEARCH FEDERATION
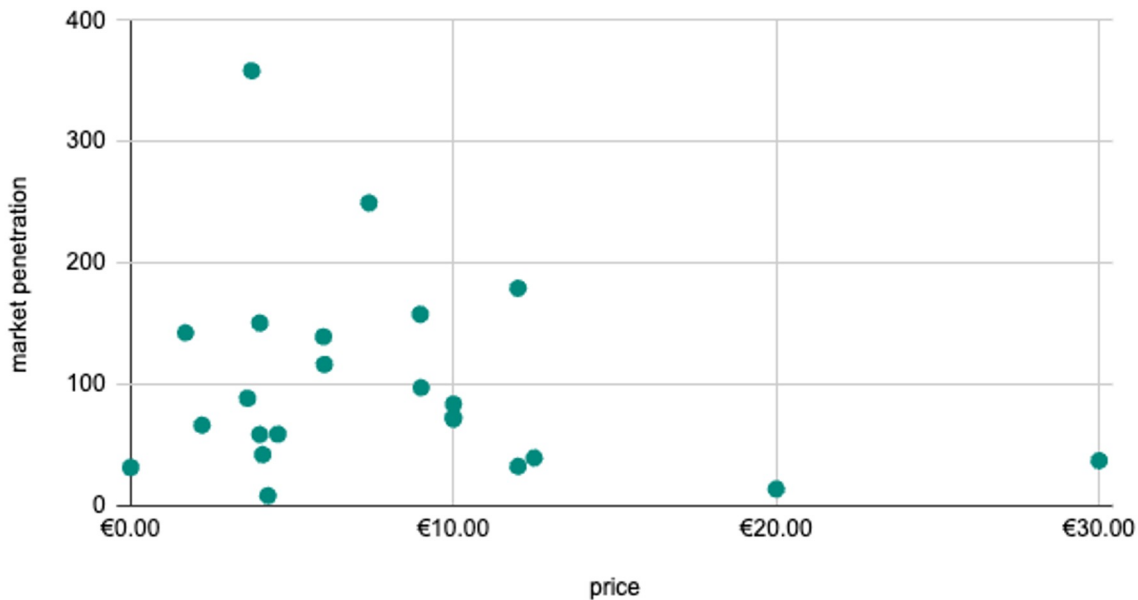
Conclusions

Low rates of abuse

EU ccTLDs
Are both high quality
and low priced

Many take
proactive measures
to improve data quality

Adopt
multiple approaches to
manage data quality

Proactive data checks
do not impede strong
market penetration

Questions?

Find out more at dnsrf.org

DNS
RESEARCH
FEDERATION