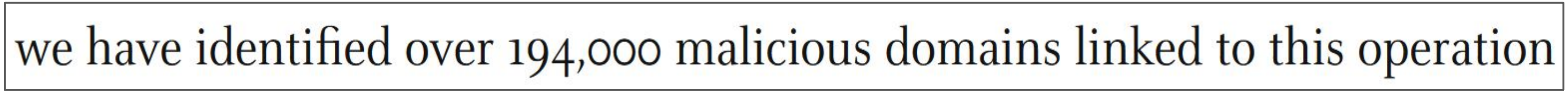
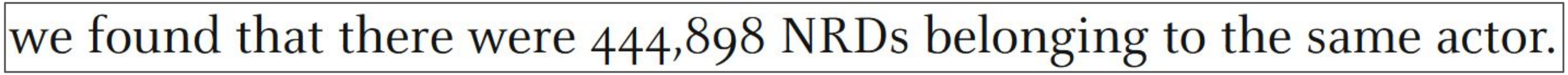
Not What It Used To Be: Generational Analysis of Top-level Domain Reputation

Janos Szurdi, Reethika Ramesh,
Ram Sundara Raman, and Daiping Liu

paloalto NETWORKS

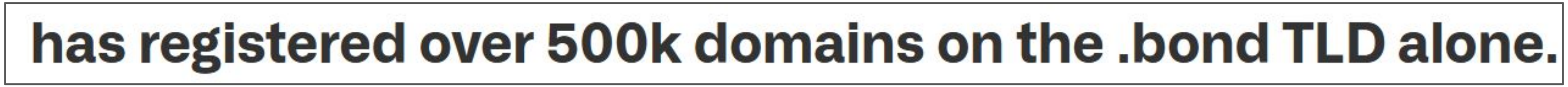


we have identified over 194,000 malicious domains linked to this operation



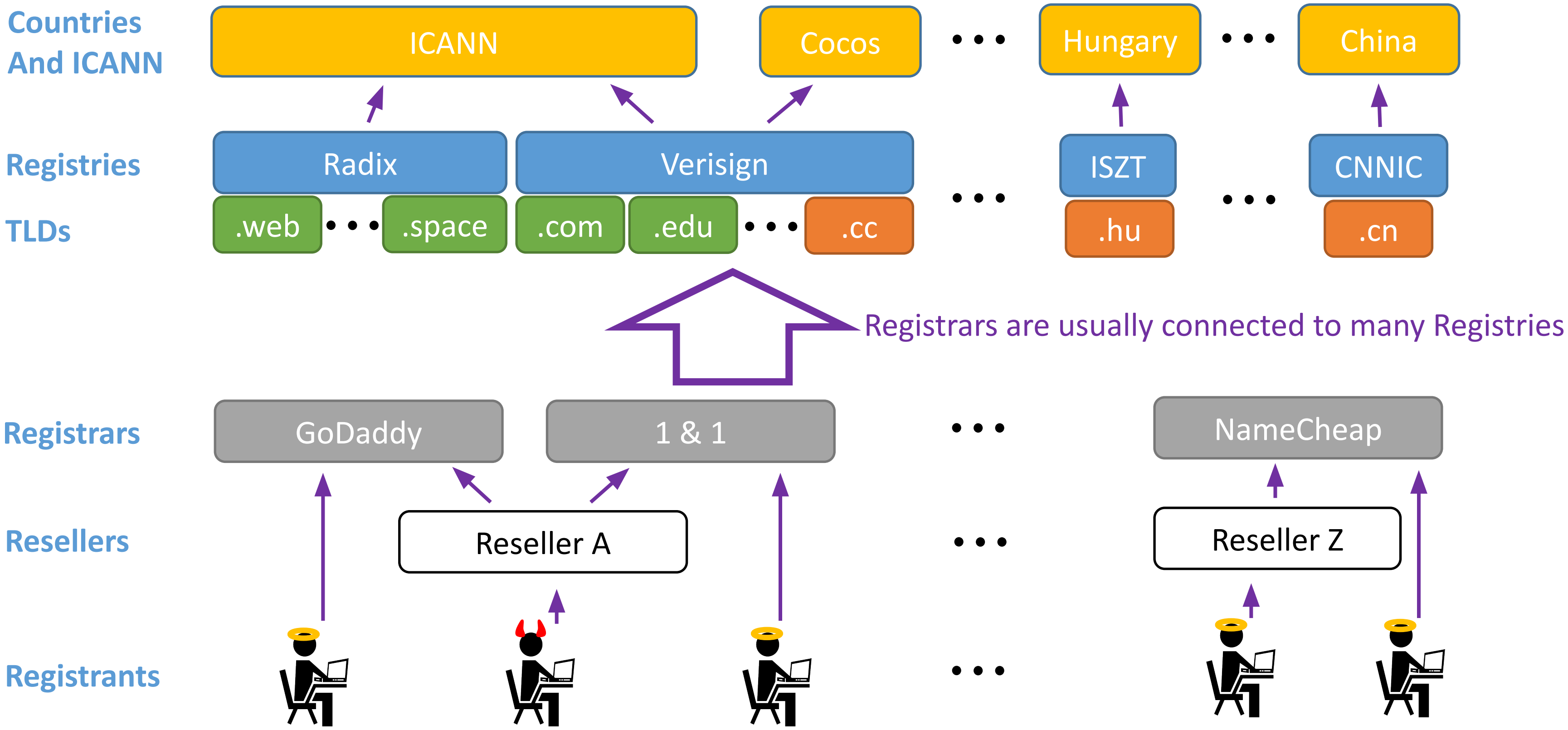
we found that there were 444,898 NRDs belonging to the same actor.

infoblox



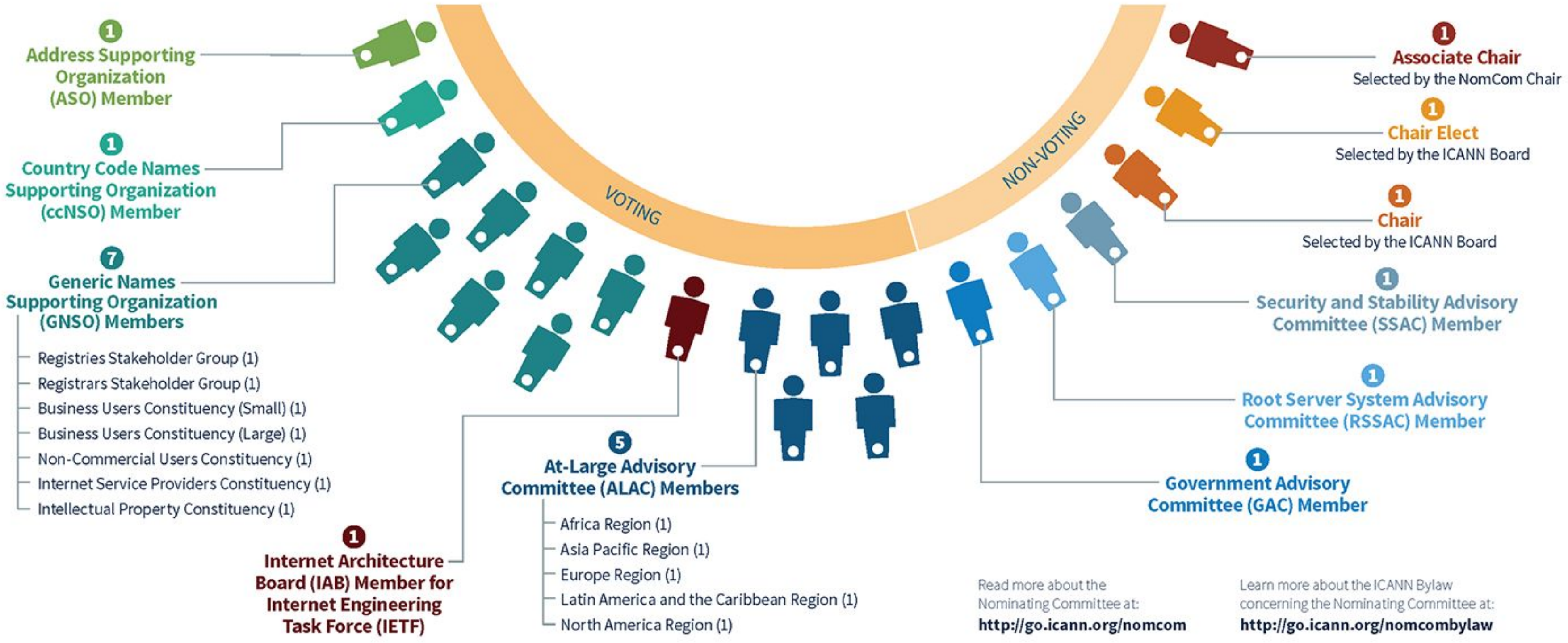
has registered over 500k domains on the .bond TLD alone.

Domain Registration Ecosystem



https://janos.szurdi.com/content/academicpapers/weis2018domainPolicy.pdf

ICANN Multistakeholder Model



1 Address Supporting Organization (ASO) Member

1 Country Code Names Supporting Organization (ccNSO) Member

7 Generic Names Supporting Organization (GNSO) Members

- Registries Stakeholder Group (1)
- Registrars Stakeholder Group (1)
- Business Users Constituency (Small) (1)
- Business Users Constituency (Large) (1)
- Non-Commercial Users Constituency (1)
- Internet Service Providers Constituency (1)
- Intellectual Property Constituency (1)

1 Internet Architecture Board (IAB) Member for Internet Engineering Task Force (IETF)

5 At-Large Advisory Committee (ALAC) Members

- Africa Region (1)
- Asia Pacific Region (1)
- Europe Region (1)
- Latin America and the Caribbean Region (1)
- North America Region (1)

1 Associate Chair
Selected by the NomCom Chair

1 Chair Elect
Selected by the ICANN Board

1 Chair
Selected by the ICANN Board

1 Security and Stability Advisory Committee (SSAC) Member

1 Root Server System Advisory Committee (RSSAC) Member

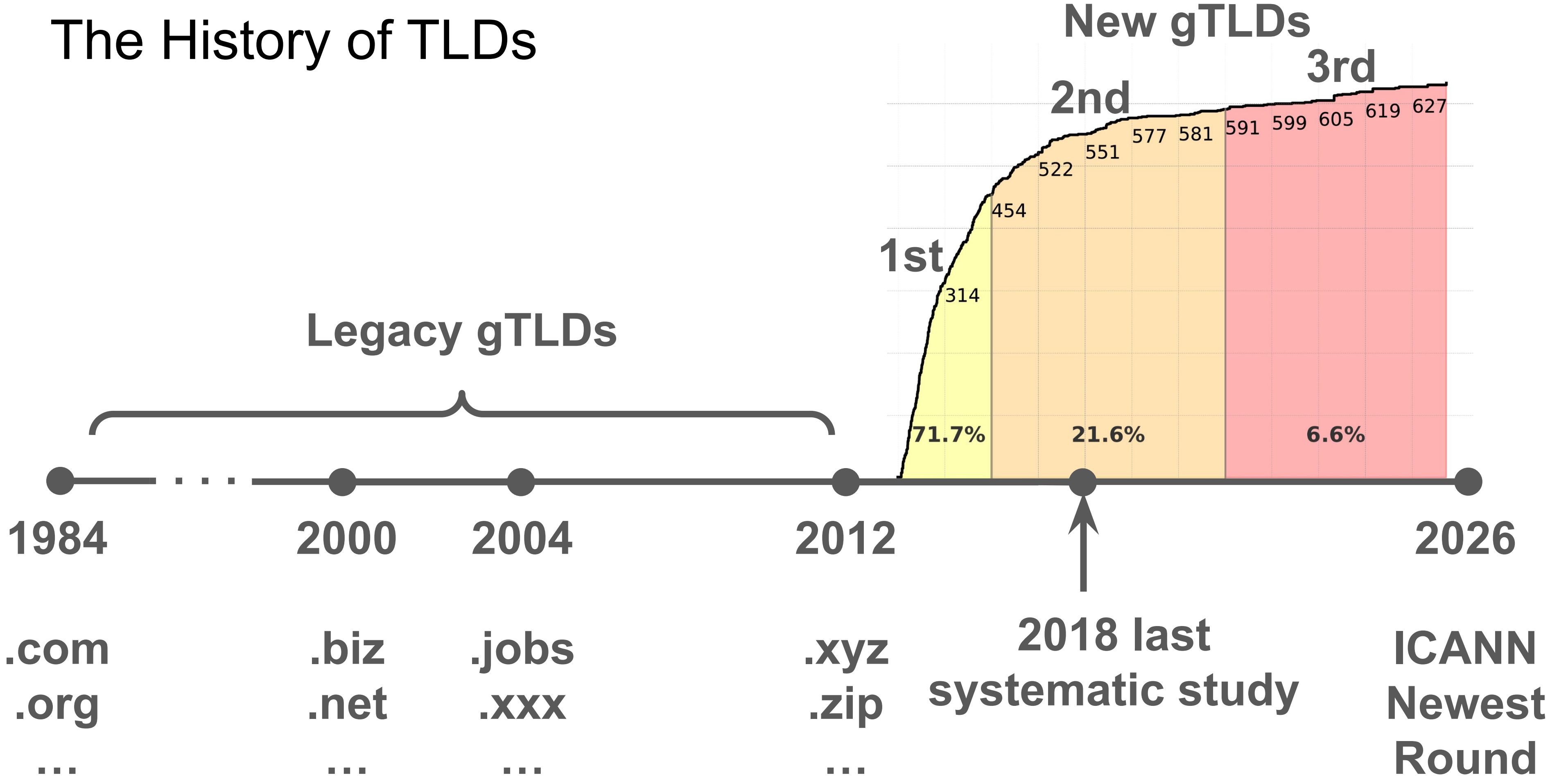
1 Government Advisory Committee (GAC) Member

Read more about the Nominating Committee at:
http://go.icann.org/nomcom

Learn more about the ICANN Bylaw concerning the Nominating Committee at:
http://go.icann.org/nomcombylaw

https://www.icann.org/resources/pages/nomcom2018-guidelines-2017-12-15-en

The History of TLDs



Legacy gTLDs

1984

.com
.org
...

2000

.biz
.net
...

2004

.jobs
.xxx
...

2012

.xyz
.zip
...

2018 last systematic study

2026

ICANN Newest Round

Domain Categorization

Malicious: Malware, Phishing, Command-and-control, and Grayware

Benign: Computer and Internet Info, Business and Economy, Games, Dating, …

Low-Content: Insufficient content, Parked, and Unknown.

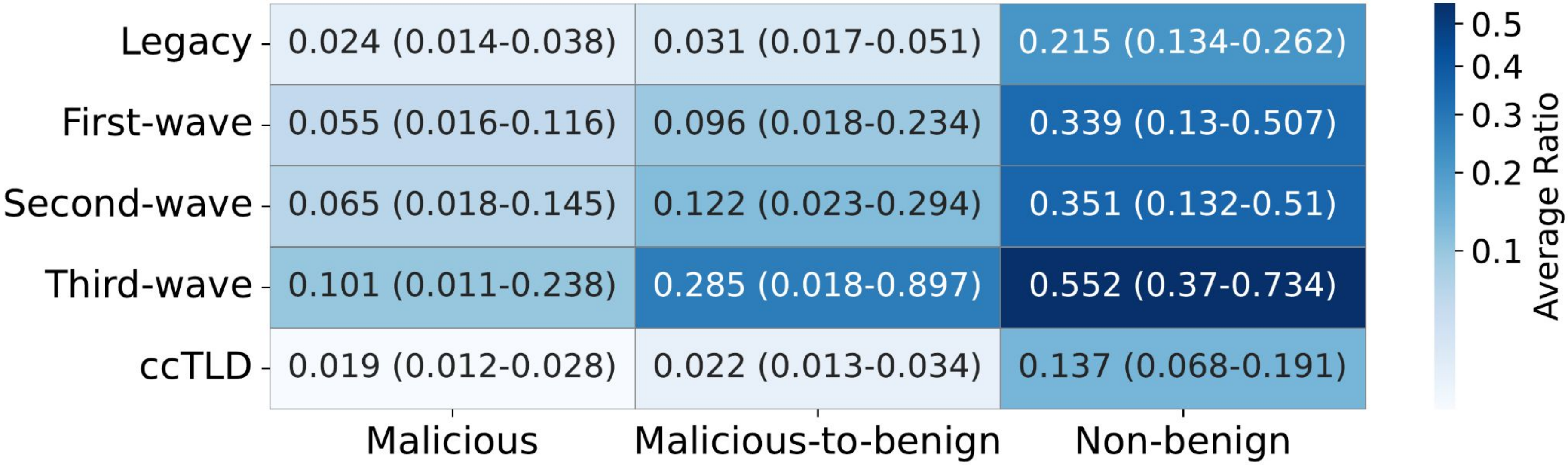
TLD Reputation Metrics

$$\text{Malicious Ratio} = \frac{Malicious\ count}{Total\ count}$$

$$\text{Malicious-to-Benign Ratio} = \frac{Malicious\ count}{Benign\ count}$$

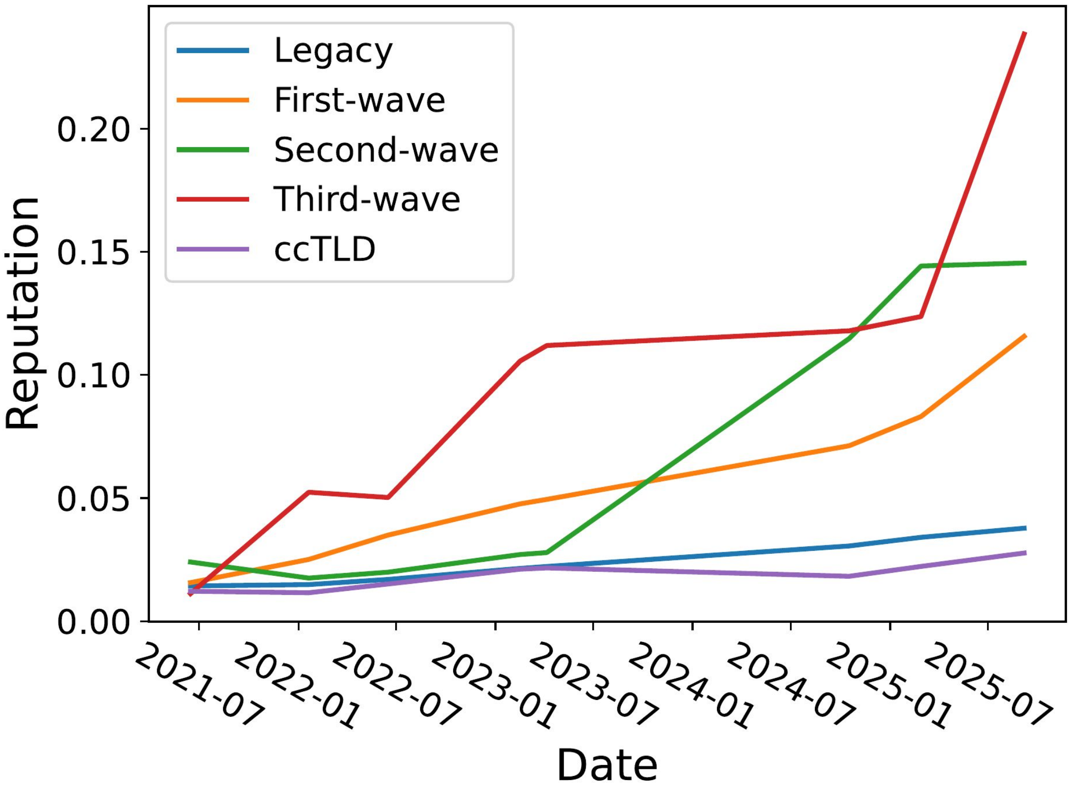
$$\text{Non-Benign Ratio} = \frac{Malicious + Low\text{-}content}{Total\ count}$$

Average TLD Reputation: 2021.06.15 - 2025.09.06

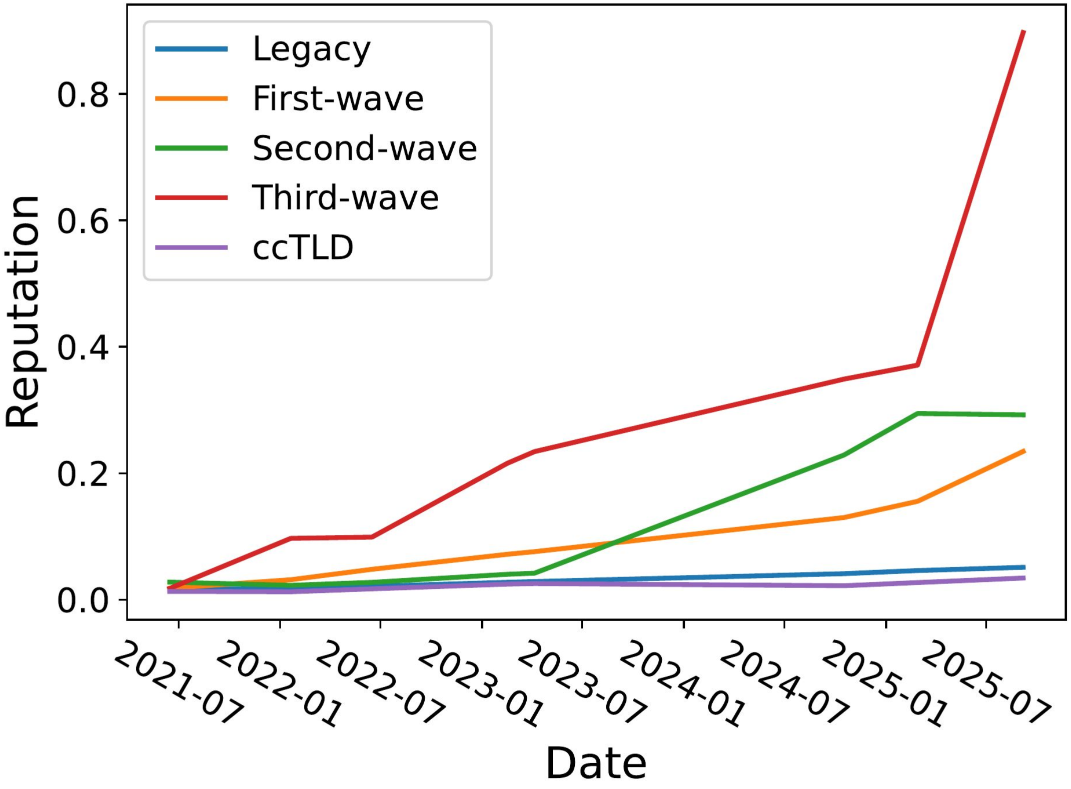


	Malicious	Malicious-to-benign	Non-benign
Legacy	0.024 (0.014-0.038)	0.031 (0.017-0.051)	0.215 (0.134-0.262)
First-wave	0.055 (0.016-0.116)	0.096 (0.018-0.234)	0.339 (0.13-0.507)
Second-wave	0.065 (0.018-0.145)	0.122 (0.023-0.294)	0.351 (0.132-0.51)
Third-wave	0.101 (0.011-0.238)	0.285 (0.018-0.897)	0.552 (0.37-0.734)
ccTLD	0.019 (0.012-0.028)	0.022 (0.013-0.034)	0.137 (0.068-0.191)

Longitudinal TLD Reputation: Malicious Ratio



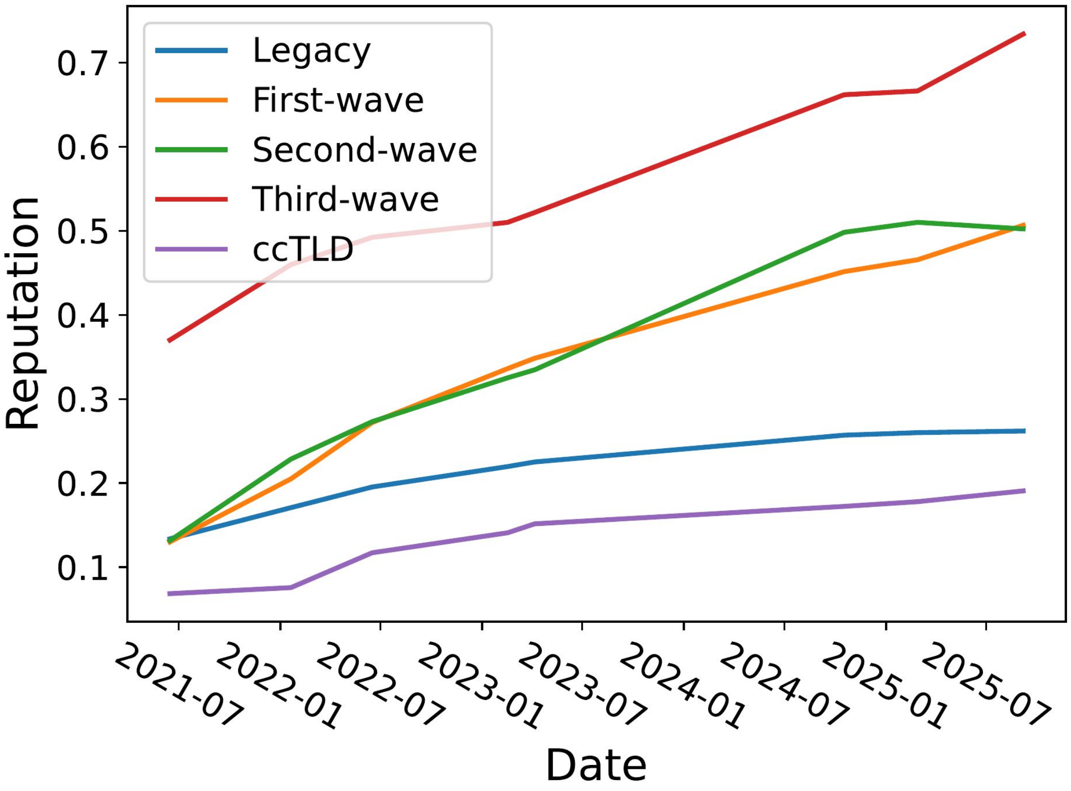
Longitudinal TLD Reputation: Malicious to Benign Ratio



Sampled Malicious Domains

.xin	.sbs	.bond
com-dpuj.xin	xy831.sbs	cybersecuritydegreesonline.bond
com-mcob.xin	ya2twm.sbs	cleaning-gel-82085.bond
com-ticketli.xin	ideaakdi.sbs	portable-power-station-88407.bond
com-ytcr.xin	intesasanpaolo97it.sbs	247-nurse-92799.bond
com-tieuy.xin	eiylfrm.sbs	telegelrs.bond
org-tlj.xin	luis625.sbs	warehouse-inventory-48771.bond
paymentxtt.xin	9880005com10xl01.sbs	prefabricated-homes-67793.bond
txtagwxw.xin	trmhsn.sbs	home-care-17857.bond
telegeltla.xin	qweftjtp.sbs	air-condition-98954.bond
com-web.xin	zuekvnua.sbs	hr-outsourcing-66318.bond

Longitudinal TLD Reputation: Non-Benign Ratio



TLD Reputation and Price

TLD Generation	Weighted Average Price
Legacy	7.76
First-wave	2.91
Second-wave	2.55
Third-wave	1.79
ccTLD	10.42

Sponsoring Organizations

Sponsor	**Malicious Ratio**	**Malicious to Benign**	**Pricing**	**TLDs**
Elegant Leader Limited	0.77	5.14	$2.29	xin
Shortdot SA	0.52	2.75	$0.83-$1.42	bond, cyou, 'icu
SPECIAL BROADCASTING*	0.29	1.24	$0.94	sbs
DOTCFD REGISTRY LTD	0.21	0.75	$0.60	cfd
dot Date Limited	0.27	0.65	$2.99	date
DOTSTRATEGY CO.	0.26	0.54	$1.10	buzz
dot Loan Limited	0.27	0.45	$2.99	loan
First Registry Limited	0.20	0.44	$2.99	win
dotCOOL, Inc.	0.25	0.43	$1.48	qpon
dot Bid Limited	0.26	0.42	$2.99	bid

Sampled Malicious Domains

.xin	.sbs	.bond
com-dpuj.xin	xy831.sbs	cybersecuritydegreesonline.bond
com-mcob.xin	ya2twm.sbs	cleaning-gel-82085.bond
com-ticketli.xin	ideaakdi.sbs	portable-power-station-88407.bond
com-ytcr.xin	intesasanpaolo97it.sbs	247-nurse-92799.bond
com-tieuy.xin	eiylfrm.sbs	telegelrs.bond
org-tlj.xin	luis625.sbs	warehouse-inventory-48771.bond
paymentxtt.xin	9880005com10xl01.sbs	prefabricated-homes-67793.bond
txtagwxw.xin	trmhsn.sbs	home-care-17857.bond
telegeltla.xin	qweftjtp.sbs	air-condition-98954.bond
com-web.xin	zuekvnua.sbs	hr-outsourcing-66318.bond

ICANN’s DNS Abuse Mitigation Program

ICANN Domain Metrica (previously DAAR)

Research and Public Forums: **INFERMAL** and **SIFT**

Enforce Contractual Obligations

- Registrars and Registries
- Mitigation actions against well-evidenced DNS abuse

Alternative Domain Registration Policies

Incentivizing registries and registrars

Bulk registration limitations

Stricter registrant identity verification

Increased registration pricing

Minimum mandatory registration pricing

Summary

Newer gTLD generations

- Worse reputation
- Less benign use
- Reputation deteriorates faster

Low pricing enables mass malicious registrations

Current ICANN policies will not help

We need a new policy intervention

- E.g., minimum mandatory registration price

Q&A

Janos Szurdi - szurdi.janos@gmail.com

Reethika Ramesh - reramesh@paloaltonetworks.com

Ram Sundara Raman - rsundar2@ucsc.edu

Daiping Liu - dpliu@paloaltonetworks.com

Full Paper

TLD Reputation Metrics Data