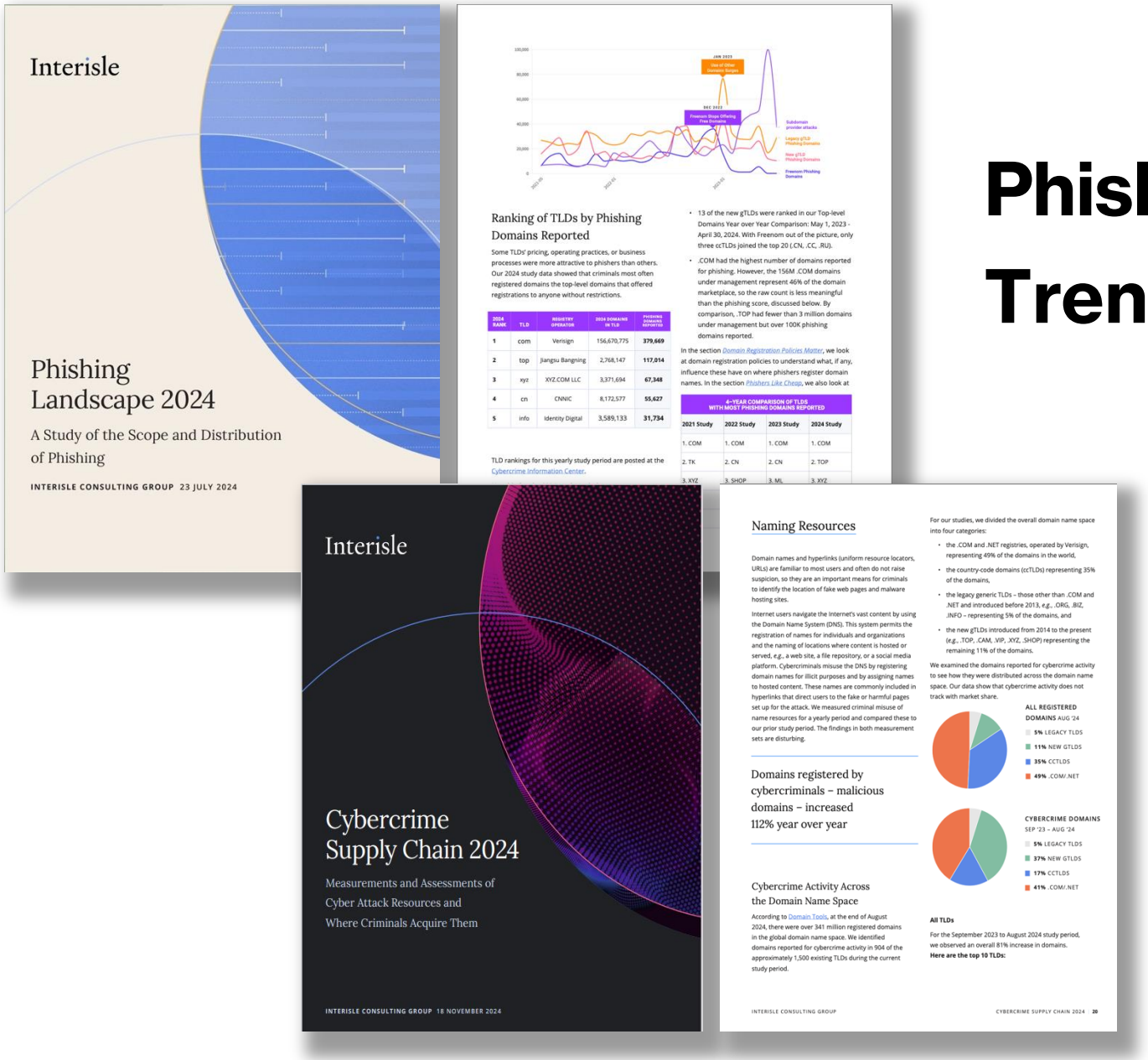


Phishing and Domain Abuse: Trends and Insights

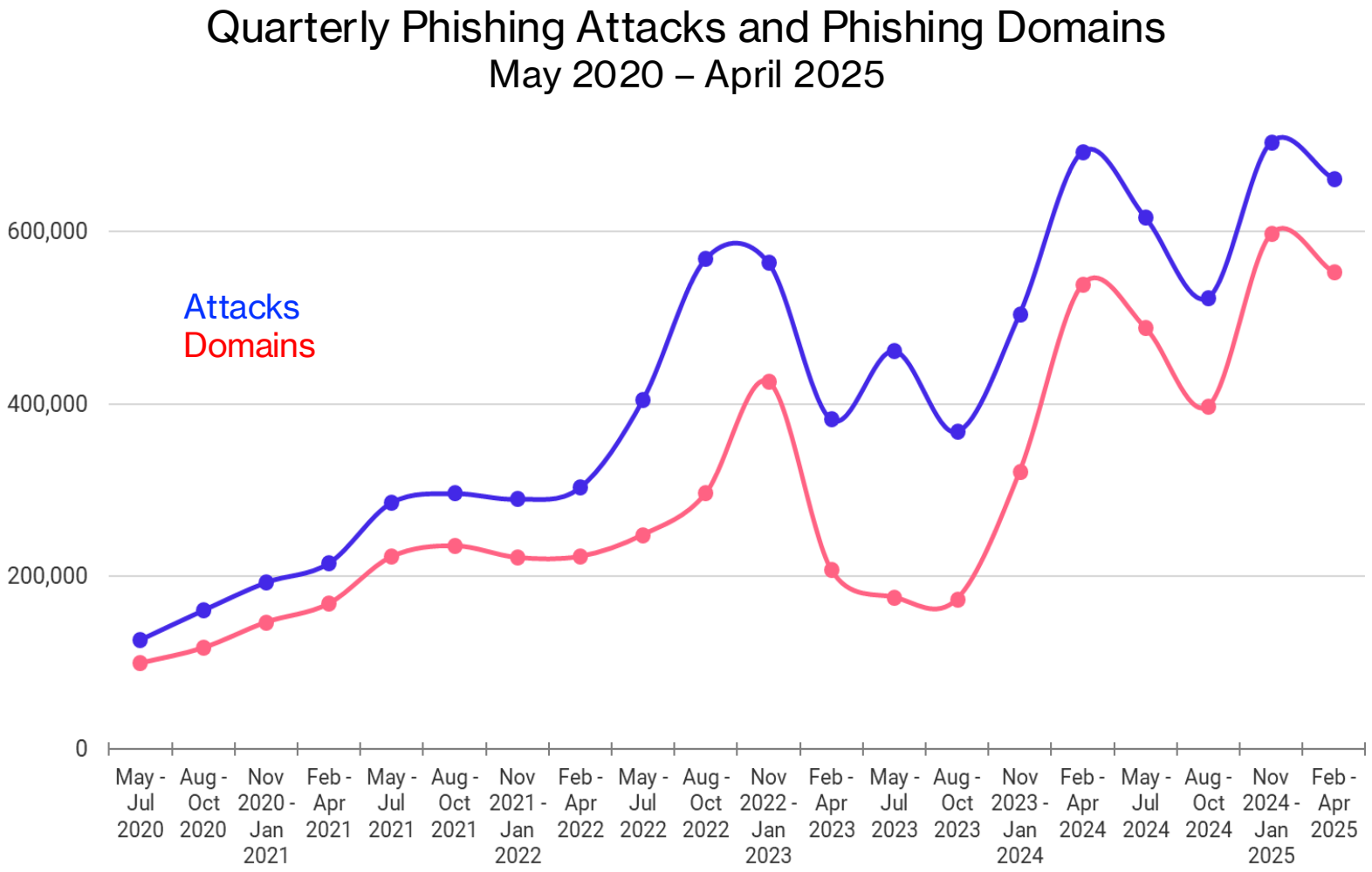
Interisle Consulting Group
Karen Rose & Greg Aaron

June 2025
https://interisle.net

Interisle

DNS Abuse is Growing at an Alarming Rate

- **1,542,900 domain names** reported for phishing **in the last 12 months.**
  - ⇧**425%+** Jul ‘20 to Apr ’25
  - Under-reports the problem
- **77%** of phishing domains **maliciously registered**
- High costs imposed on society
  - **US$18,000** in direct financial loss from phishing *every minute*
- Anti-abuse efforts to date have been ineffective

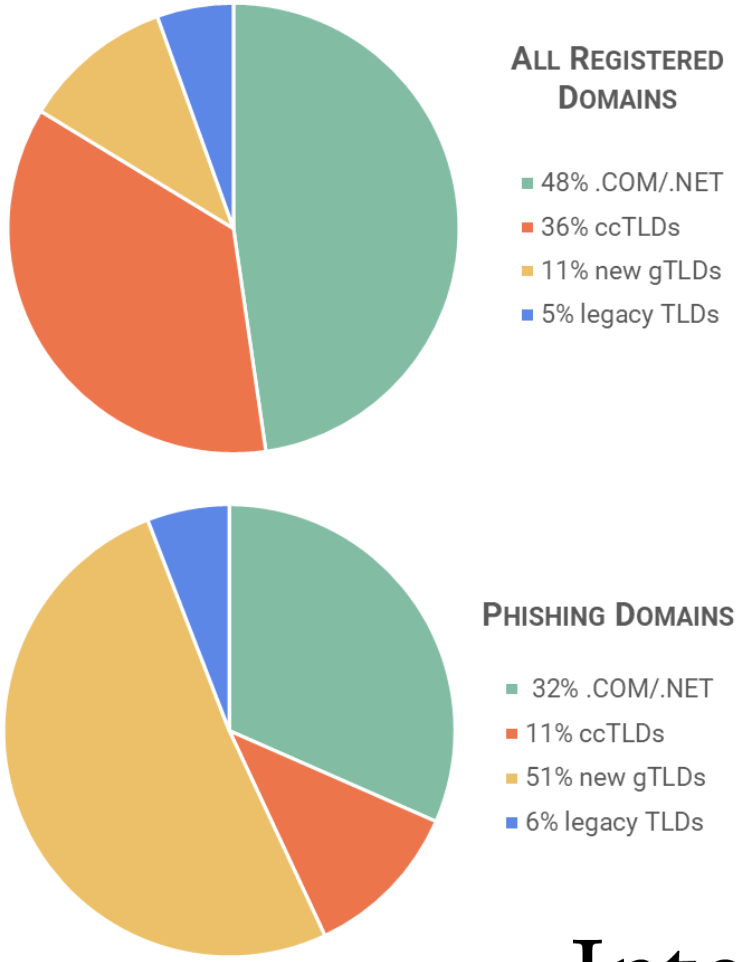


Interisle

Phishers Exploit Cheap Prices and Easy Registration

- **Phishers exploit cheap**
  - Top 27 TLDs with highest proportions of abuse priced at US**$2 or less**
  - **51%** of abusive registrations in the new gTLDs, **32%** .com/.net
  - Free promotions and bundle deals
- **Phishers exploit easy**
  - Target registrars and TLDs with few requirements and no identity verification / data validation
- **Phishers have known, preferred suppliers**
  - Most-abused registries and registries by volume and proportion appear in the top 10 year after year.

Market Share and Phishing Domains by TLD Type



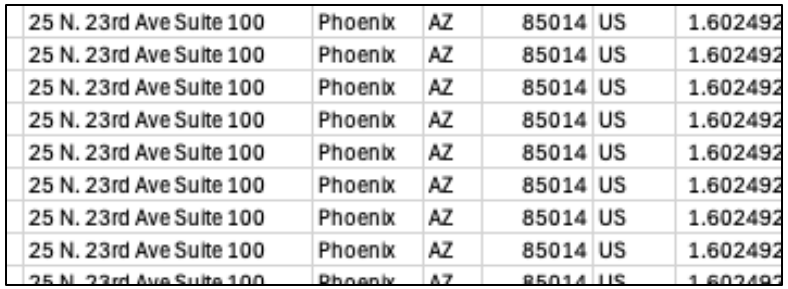
Interisle

Abusive Registrations are Often Conspicuous

Algorithmically generated names

Names containing / closely matching brands

Repetitive use of same / similar registrant information



Clearly false registration information

Automated tools can screen for these and other suspicious patterns

- Anti-abuse systems already deploy by some ccTLDs
- Commercial data validation tools available

Interisle

Bulk Registration: Arsenals of Domains

- **37%** of phishing domains registered in bulk over the last 12 mo.
- Over **17,000** malicious domains were registered in **under 8 hours**. (CSC 2024)
- Phishers weaponize domains and launch attacks quickly.
- By the time an attack is detected and mitigation started **the damage is already done** & multiples more in progress.

Interisle CSC 2024
Largest gTLD Malicious Bulk Batch Runs

Registration Time Span (UTC)	Registrar	Bulk Domains	Sample Cybercrime Domains
2/19/2024 03:48 to 11:35	GMO d/b/a Onamae.com	17,687	hqkzmnsi.lol nlaxbwtd.lol xohxkvbi.lol nzsyaxjf.lol wpimhhcl.lol gzrqwxeb.lol hznsttlm.lol ozztavmv.lol wifthlsu.lol owhnubyw.lol gneozzwz.lol ioszozla.lol
8/22/2024 07:36 to 11:48	GMO d/b/a Onamae.com	9,885	college-mwiz.xyz rbmgls-small.xyz fxiucd-direction.xyz drai-discussion.xyz kqrf-attention.xyz weah-news.xyz rielac.com iogmti-force.xyz order-yhkmfo.xyz zxfiy-school.xyz qvlso-six.xyz usuij-rest.xyz
9/18/2023 04:02 to 07:35	July Name Limited	8,827	limls.net lexiom.net llpl.net lmey.net mahko.net matanca.net megye.net mengfei.net mfarltd.net mfhv.net mfyp.net midten.net
4/29/2024 13:36 to 4/30/2024 07:51	Stichting Registrar of Last Resort Foundation	7,451	2723d0.org 274ad4.org 283802.org 289dff.org 28dd2c.org 2a38a4.org 2a79ea.org 2b24d4.org 2b4492.org
9/18/2023 08:40 to 10:01	July Name Limited	7,062	fsjuice.net ants365.net hytgxcl.net zwxtech.net yxhuaer.net jinziqp.net heiqiqp.net mmyoux.net ynzxjy.net

Short Durations

Conspicuous Volumes

Suspicious Name Patterns

Interisle

Business and Economic Choices set the Stage for Abuse

- Competition is good, but "over competition" in markets, **absent reasonable rules, can have negative consequences.**

- **The DNS market is highly competitive**
  - Low barriers to entry & abundant competitors
    - 2,000+ Registrars, 100s of open TLDs
  - Largely commodity goods with near 0 marginal production cost
  - Fierce battles for market share, loss-leader pricing, etc.

- **DNS abuse is like pollution: a negative externality that imposes costs on consumers and society**.

- Reasonable measures are needed **to curb abuse, not just mitigate it.**

- It's ICANN's function to set minimum standards for doing business.

Interisle

Better Policies Curb Abuse: Identity Verification & Validation Case Study

- Both Interisle and the INFERMAL study found that TLDs with greater identity verification requirements have less abuse.
- ICANN's current requirements are minimal.
  - 2024 compliance audit found that 20% of registrars failed to do the minimum required validations.
- The EU's **NIS 2** require registries and registrars to have verification procedures that "**ensure .... accurate and complete information**" and use "**risk-based approaches**" to check accuracy.
- Many European ccTLDs have implemented these checks and have some of the lowest incidence of domain abuse.

COMPARISON OF TLD SETS WITH NO REGISTRATION REQUIREMENTS	COMPOSITE PHISHING DOMAIN SCORE	COMPOSITE MALICIOUS PHISHING DOMAIN SCORE
EU ccTLDs	6.9	5.2
ccTLDs (Asia and EU ccTLDs studied)	14.0	6.8
Legacy gTLDs	25.5	18.8
Asia ccTLDs	33.7	18.8
Legacy and hew gTLDs combined	40.2	33.3
New TLDs	273.7	262.2

Interisle

More Effective Anti-Abuse Measures are Needed

- **Strengthen Verification Requirements**
  - Require better verification of gTLD registrant contact data, similar to NIS2.
- **Implement Bulk Registration Requirements**
  - Require identity verification, limit registration volumes
- **Allow Registries to Better Manage their Business**
  - Registries should not be required to do business with registrars that have high abuse rates / present risk
- **Adopt Automated Systems to Screen for Abusive Registrations**
  - Catch and investigate suspicious names and data before delegation.

See our Phishing Landscape and Cybercrime Supply Chain for additional recommendations.

Interisle

For More Information

New Reports Out Q3 2025!

Reports: interisle.net/insights

Data sources, methodology, additional data: cybercrimeinfocenter.org

Substack: interisle.substack.com

Web: interisle.net

Email: info@interisle.net

Interisle