Measuring & Attributing Disruption

DNSSEC and Security Workshop

8th June 2026, ICANN86, Seville

NetBeacon Institute

Vision: A Safer Internet for Everyone

- Created and operated by Public Interest Registry (.ORG) in service of its public interest mission since 2021.
- Non-commercial, all our products and services are free.
- We do not have customers; we do not sell anything.
- Education, Innovation and Collaboration.

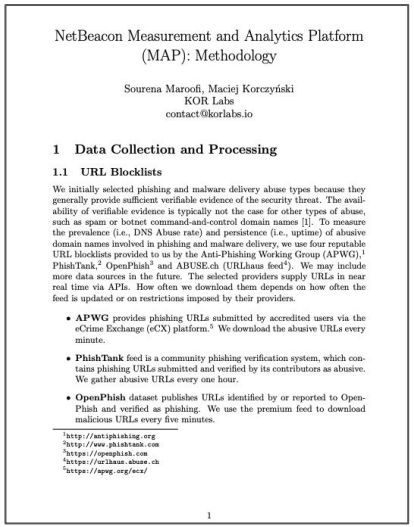
NETBEACON MAP

Measures the prevalence & persistence of phishing and malware in the DNS.

Principles:

- Transparency
- Credibility and independence
- Accuracy and reliability

Delivery partner: KOR Labs, Grenoble Alpes University



NetBeacon Measurement and Analytics Platform (MAP): Methodology

Sourena Maroofi, Maciej Korczyński
KOR Labs
contact@korlabs.io

1 Data Collection and Processing

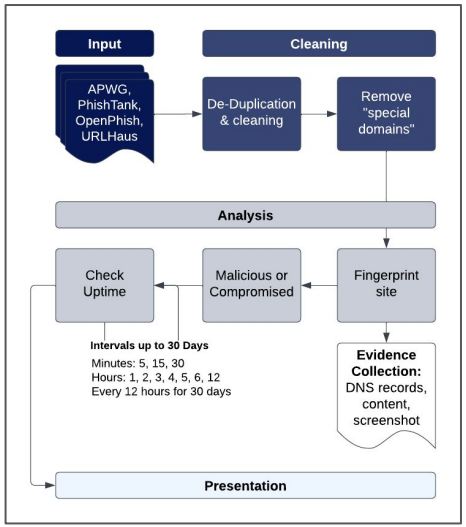
1.1 URL Blocklists

We initially selected phishing and malware delivery abuse types because they generally provide sufficient verifiable evidence of the security threat. The availability of verifiable evidence is typically not the case for other types of abuse, such as spam or botnet command-and-control domain names [1]. To measure the prevalence (i.e., DNS Abuse rate) and persistence (i.e., uptime) of abusive domain names involved in phishing and malware delivery, we use four reputable URL blocklists provided to us by the Anti-Phishing Working Group (APWG),[1] PhishTank,[2] OpenPhish[3] and ABUSE.ch (URLhaus feed[4]). We may include more data sources in the future. The selected providers supply URLs in near real time via APIs. How often we download them depends on how often the feed is updated or on restrictions imposed by their providers.

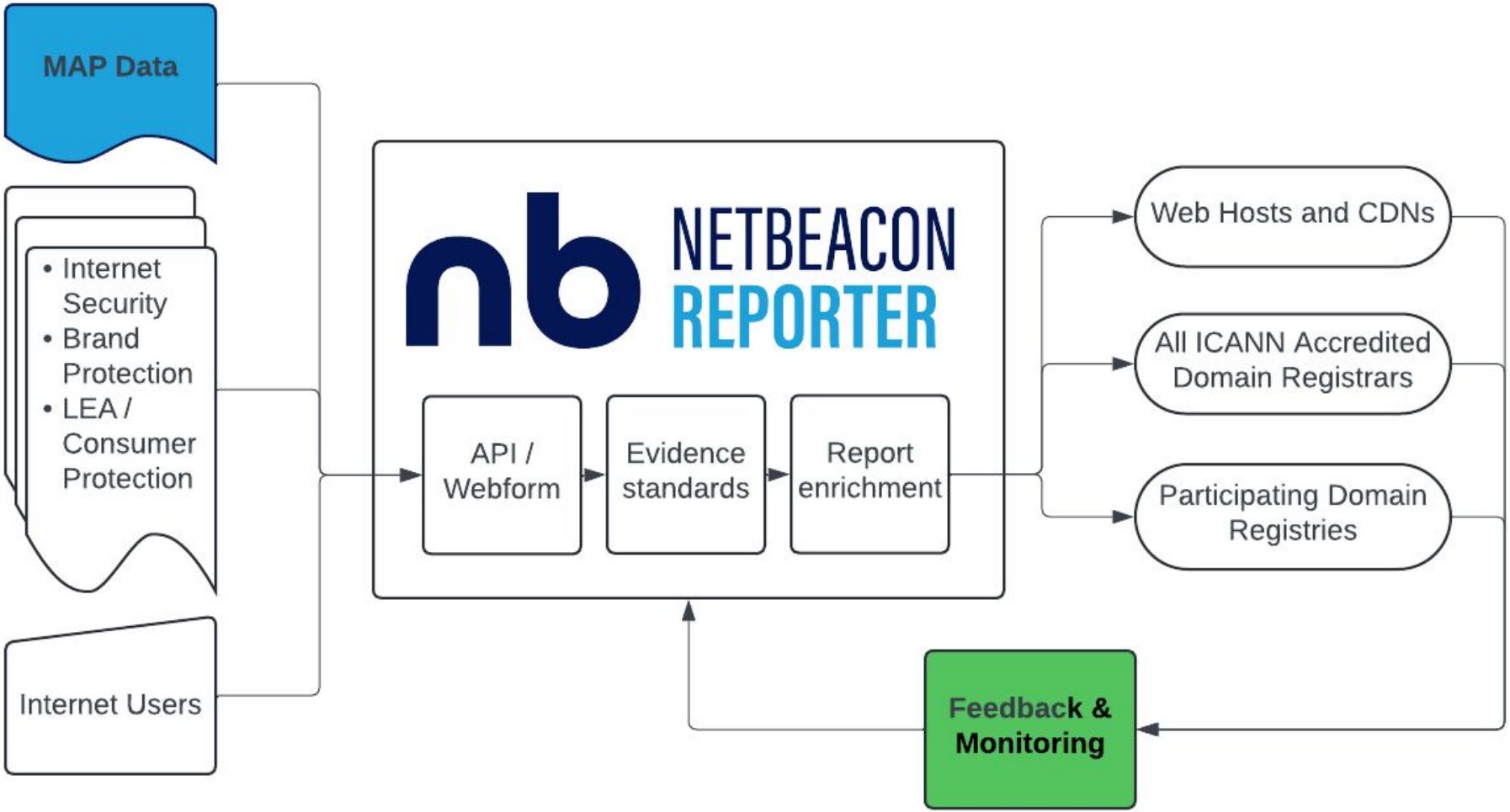
- **APWG** provides phishing URLs submitted by accredited users via the eCrime Exchange (eCX) platform.[5] We download the abusive URLs every minute.
- **PhishTank** feed is a community phishing verification system, which contains phishing URLs submitted and verified by its contributors as abusive. We gather abusive URLs every one hour.
- **OpenPhish** dataset publishes URLs identified by or reported to OpenPhish and verified as phishing. We use the premium feed to download malicious URLs every five minutes.

[1] http://antiphishing.org
[2] http://www.phishtank.com
[3] https://openphish.com
[4] https://urlhaus.abuse.ch
[5] https://apwg.org/ecx/

1



https://netbeacon.org/map-analytics/


MAP Data
• Internet Security
• Brand Protection
• LEA / Consumer Protection
Internet Users
NETBEACON REPORTER
API / Webform
Evidence standards
Report enrichment
Web Hosts and CDNs
All ICANN Accredited Domain Registrars
Participating Domain Registries
Feedback & Monitoring

Measuring Mitigation

Two Processes:

- KorLabs/MAP
  - looks for changes in the DNS, at the domain, and at the content level
  - Increasing intervals to 12 hours, then every 12hrs for 30 days
  - Does not halt upon first mitigation

- NetBeacon Reporter
  - looks for changes at the domain
    - ServerHold, ClientHold, Deletion, Known Sinkhole
  - Increasing intervals to 12 hours, then every 12hrs for 7 days
  - Halts at first mitigation

Challenges

- Content/Hosting level changes are hard to attribute, or even verify
  - Is the 403 because my IP is geoblocked, or the host suspended the account?
- Timing:
  - Different checks get results at different speeds, who gets credit?
  - Are threat actors cycling domains super fast?
- Rate limits
  - Registrars don't always love it when you blast their RDAP server
- Ambiguity
  - Who changed nameservers? deleted the domain?
- Edge cases for everything

Mitigation Across the DNS

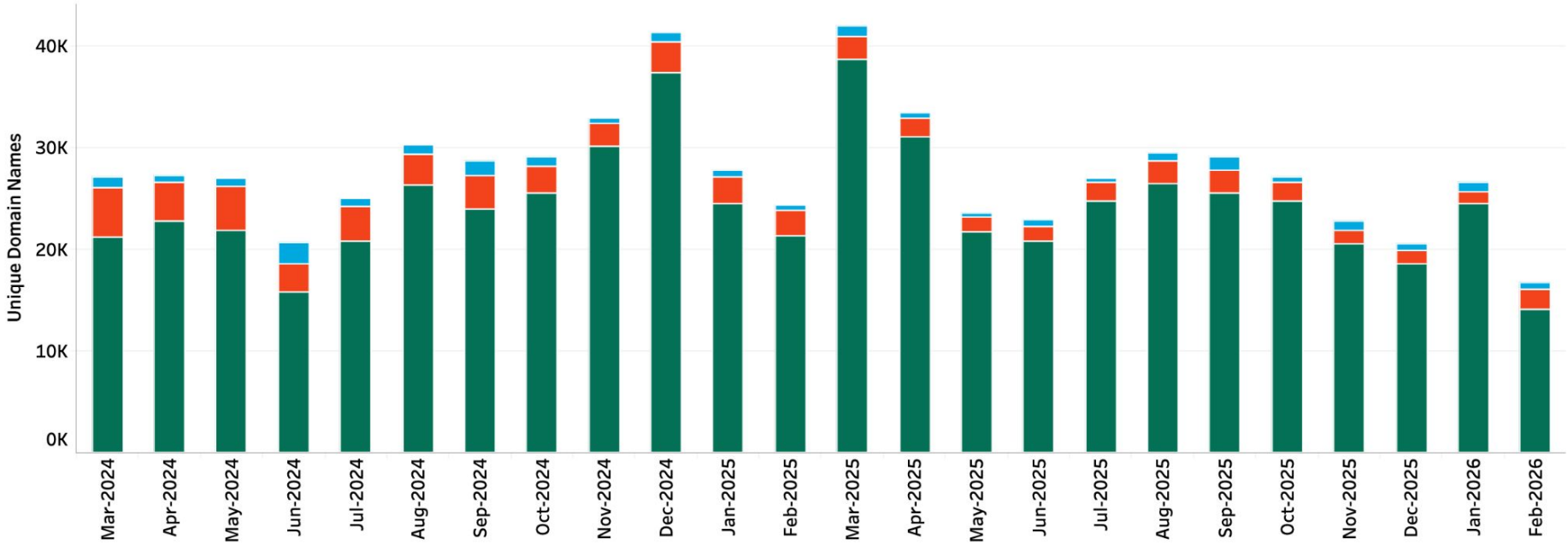
Reporting Periods in View: Last 24 Reporting Periods

View As: Count of Unique Domain Names

Date Range: 2024-03 to 2026-02

Abuse Type: Malware and Phishing

Registration Type: Malicious



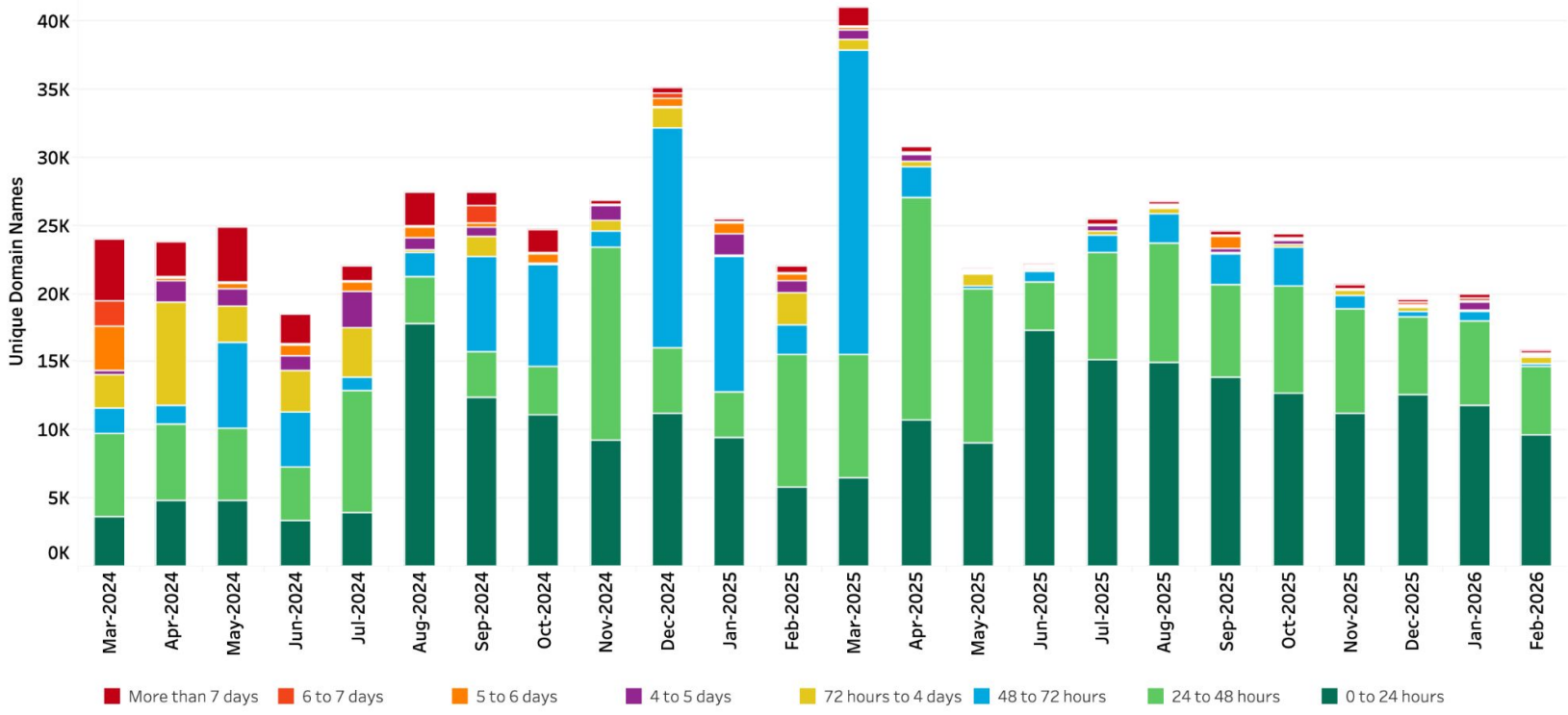
Mitigation Speeds

Reporting Periods in View: Last 24 Reporting Periods

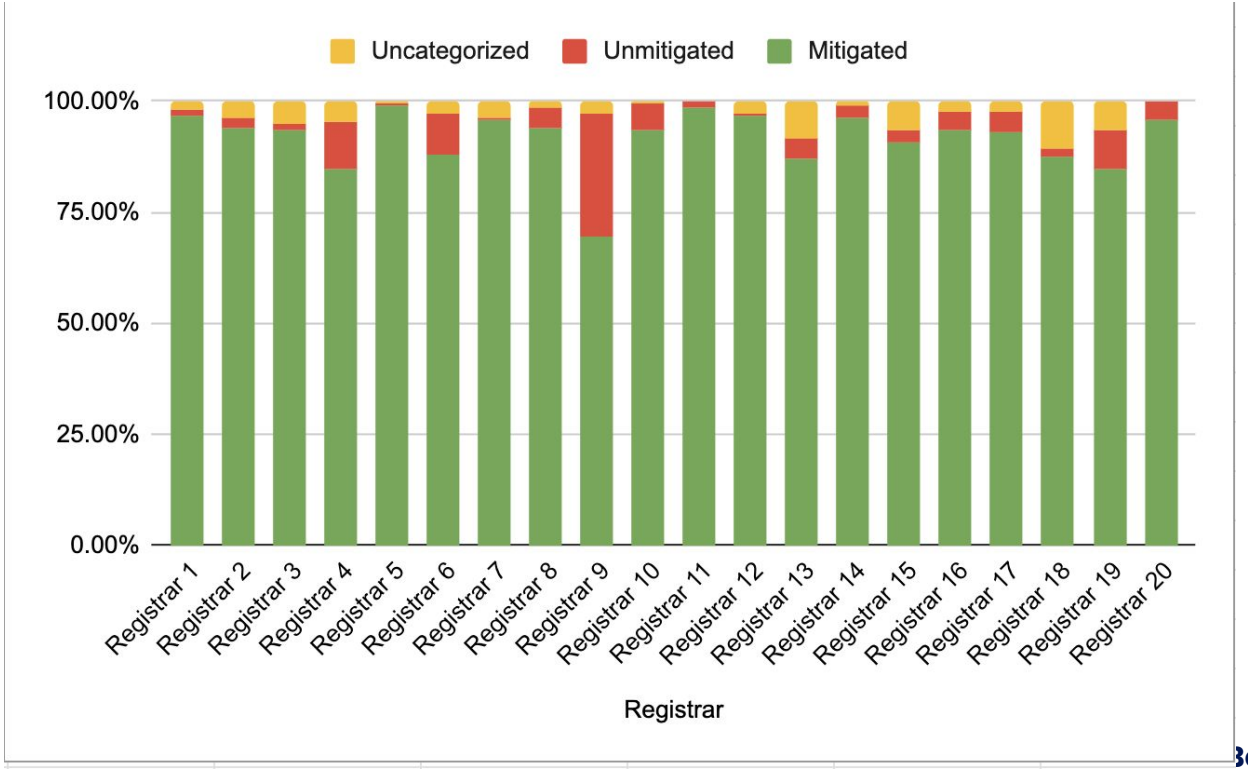
Date Range: 2024-03 to 2026-02

Abuse Type: Malware and Phishing

View As: Count of Unique Domain Names

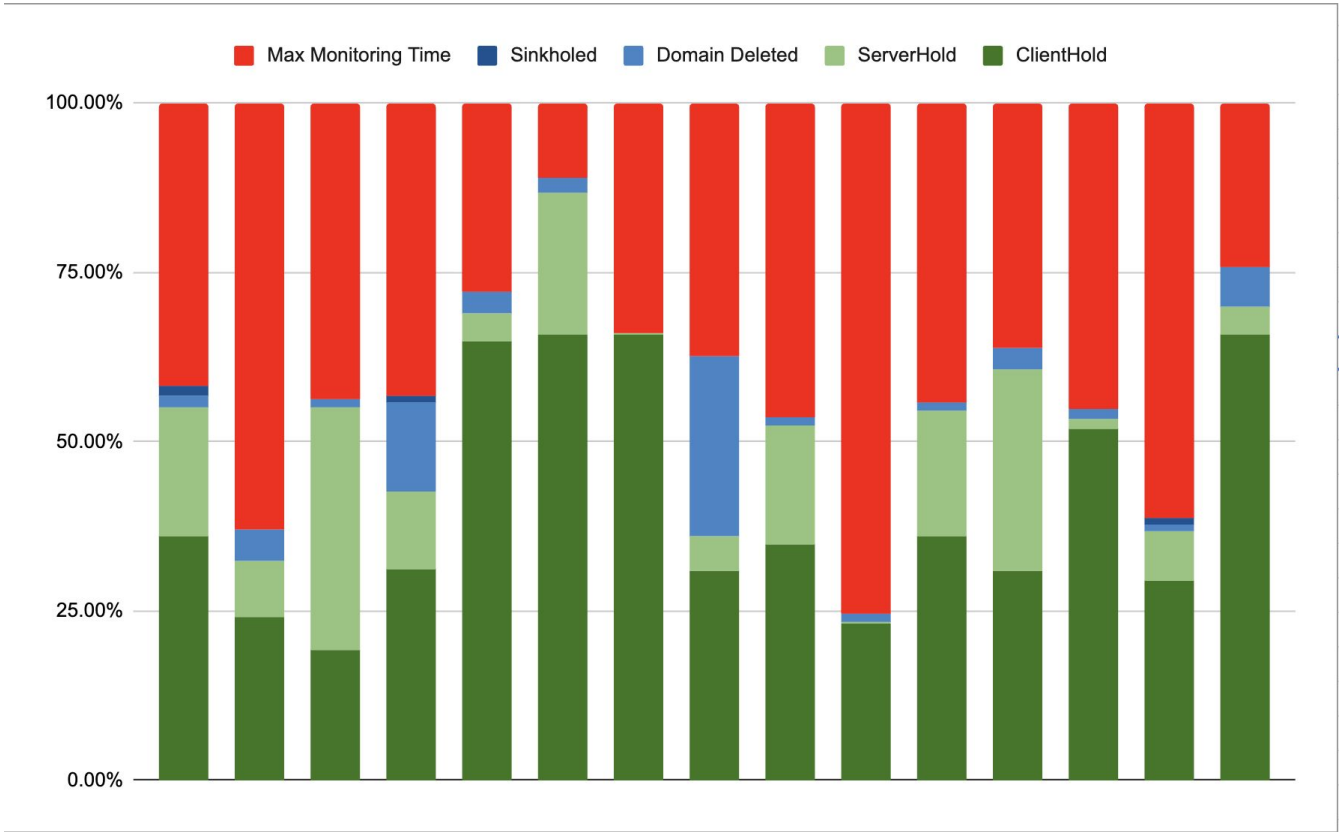


Jan' 26 Mitigation Rates by Registrar



Mitigation Rates by Reporter

- Measured from NB Reporter
- No Content or Hosting attribution
- ~30% lift from late mitigation & content



Up Next

- Publish mitigation rates
- Publish median times to mitigation
- Reduce redactions
- Homogenize exclusions
- Publish full table

Table 3: Highest observed rates of abuse 2026-03

IANA ID	Registrar Credential	Observed Maliciously Registered Domains Per 100,000 gT..	Observed Malicious gTLD Domains	Observed gTLD DUM	Number of Months
3858	Aceville Pte. Ltd.	718.96	857	119,200	6
3956	Global Domain Group LLC	646.73	1,424	220,183	6
3765	NICENIC INTERNATIONAL GR..	359.54	550	152,972	6
3254	CNOBIN INFORMATION TEC..	290.75	173	59,502	5
Redacted	*Redacted*	238.10	*	*	3
Redacted	*Redacted*	189.19	*	*	3
4331	Ultahost, Inc.	182.29	48	26,331	5
Redacted	*Redacted*	150.31	*	*	1
Redacted	*Redacted*	130.62	*	*	3
Redacted	*Redacted*	70.87	*	*	2

Final Thoughts

- Measuring abuse is **Hard**
- Measuring mitigation is even **Harder**
- Accurately attributing that mitigation is **Harder** still
- NetBeacon is working towards increased transparency

Questions?

Graeme@netbeacon.org