NETBEACON INSTITUTE

NetBeacon Measurement and Analytics Platform (MAP)

Annual Report 2025

Contents

Executive Summary

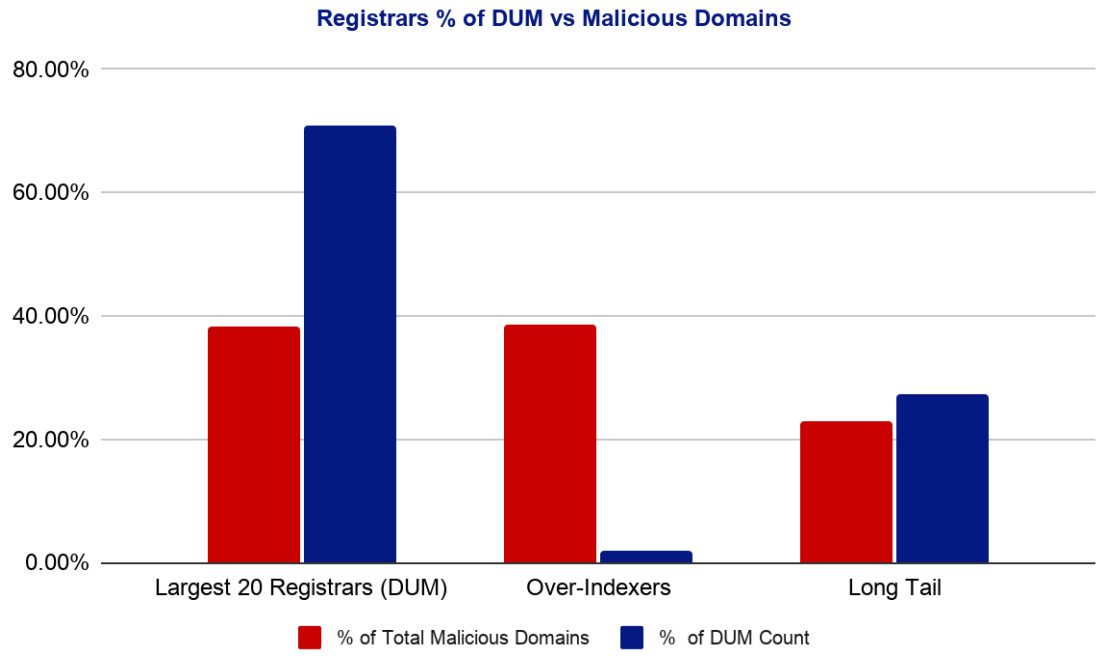
- 393,995 total abusive domains observed in 2025 (98% phishing; 2% malware)
- 84% of unique abusive domains were maliciously registered
- 91% of maliciously registered domains were mitigated – an unattributed metrics which indicates the harm has stopped during our measurement window (30 days)
- 53% of mitigation took place in the first 24 hours and 92% within 72 hours (monthly median)
- Small group of registrars containing 2% of DUM in 2025 is responsible for 39% of total malicious domains

Trends and Campaigns

In March 2025, NetBeacon Measurement and Analytics Platform (MAP) observed a record spike in malicious phishing activity**. A single registrar (Dominet HK Limited, IANA 3775) registered 55% of the unique domains associated with phishing (20,133), while managing just 0.3% (640,480) of all gTLD DUM.** The second-highest concentration was Gname.com Pte. Ltd. (IANA 1923) which registered 9% of unique phishing domains (3,087) while managing only 2% (4,672,094) of total gTLD domains.

We refer to this imbalance as 'over-indexing': when a registrar credential accounts for a higher market share of malicious phishing than what they hold as a market share of domains. Most registrar credentials do not over-index on malicious phishing compared to their market share of domains

We calculated the registrar's percentage of total malicious domains compared to the percentage of DUM count over 2025. **With over 3,000 ICANN-accredited registrars, many of which have no, or low malicious domains identified per month, we can identify a small group of gTLD registrars which have over-indexed on malicious domains.** While this group (over-indexers) maintained less than 2% of total DUM, they carried 39% of total malicious domains in 2025. In contrast, the largest gTLD registrars by DUM with 71% of total DUM and 38% of total malicious domains.

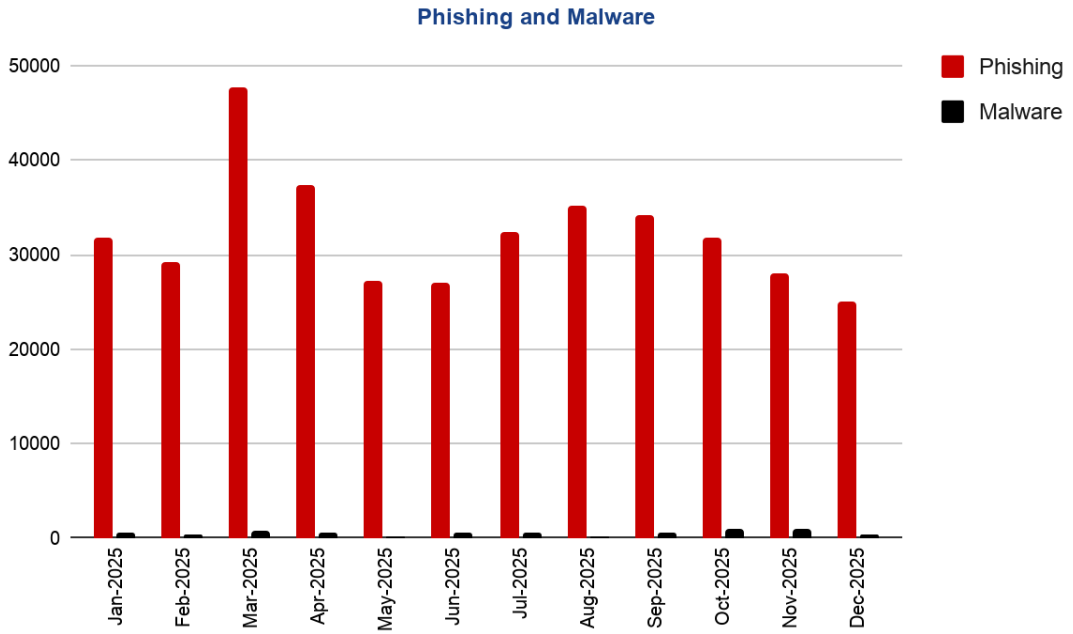


In August, NetBeacon MAP identified 2,227 unique domain names that appear to be part of a coordinated phishing campaign targeting vulnerable UK citizens by impersonating the UK Government. The registrations were primarily concentrated in two registrar credentials: 90% (1994) in Aceville Pte. Ltd. (IANA ID 3858) and 10% (230) Dominet (HK) Limited (IANA ID 3775). The subdomain cloaking technique uses 'TLD-' combinations in a subdomain in an attempt to hide the abuse, manipulating how

the domain appears. Industry should look out for TLD-combinations, for example: com-, uk-, gov-, de-, ca-, org-, pl- etc. or -uk, -com, -gov etc. Read more in our joint blog with Nominet UK.

DNS Abuse at a Glance

In 2025, NetBeacon MAP methodology identified 386,905 unique domains used for phishing attacks, a 0.7% **increase from 2024**. We observed 7,090 unique domains engaged in malware attacks, a 4.6% **increase from 2024**.



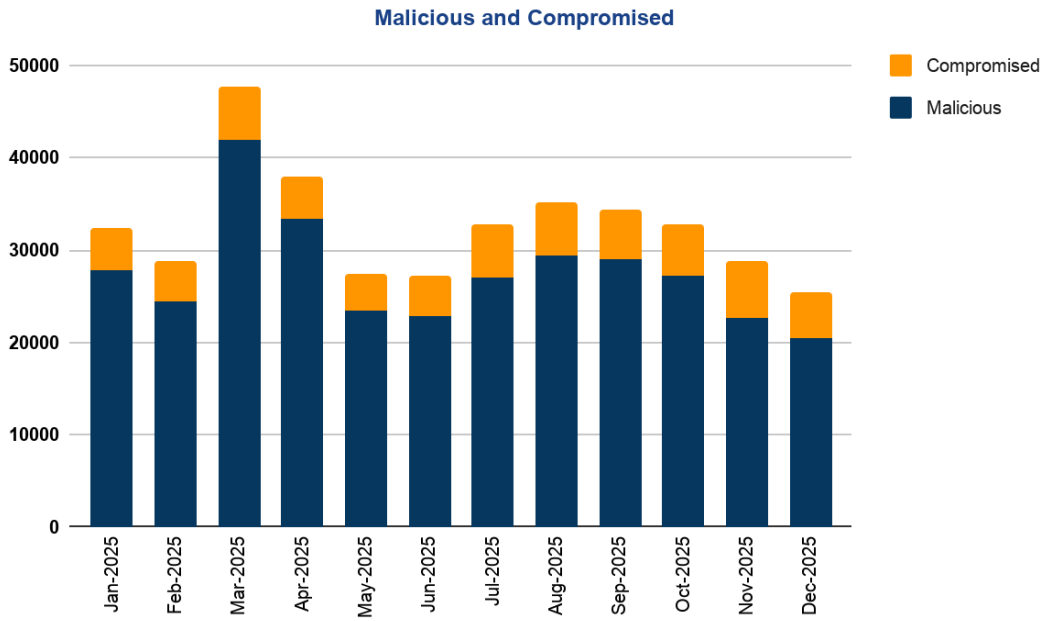
In our methodology, DNS Abuse comes in two 'flavours'—**maliciously registered or compromised**. Typically, the registry and registrar are not well placed to appropriately mitigate harm related to a compromised website. This usually requires action from the web hosting provider[1] or registrant.

1

Compromise usually happens at the Content Management System (CMS) of the website. The CMS allows administrators to make edits on the website, but sometimes there are vulnerabilities in this software which can be compromised by malicious

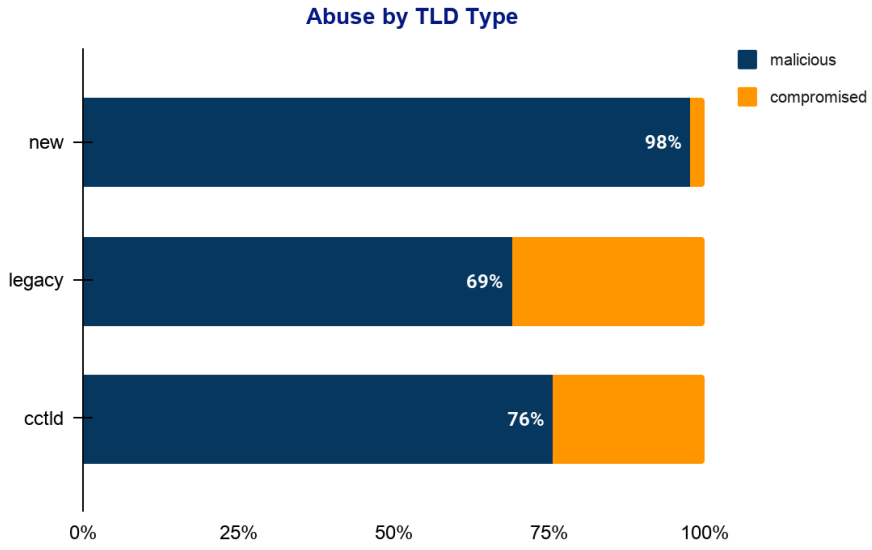
actors. Updates get issued by the CMS maintainer but typically require the website operator or registrant to make the change. Prior to updates, the vulnerability leaves an open window for attackers to wreak havoc across the Internet.

During 2025, most domains (84%) were maliciously registered—i.e., registered for the purpose of phishing or malware. This classification is a result analysis by MalCom, a sophisticated and proprietary classifier created by KOR Labs and used for NetBeacon MAP. Our methodology found that 84% of phishing domains and 80% of malware domains were maliciously registered in 2025.



New gTLDs had the highest rate of malicious registration at 98%, compared to 76% for ccTLDs and 69% for legacy gTLDs. It's possible this is related to the rate of growth in new gTLDs and increased likelihood of ccTLDs and gTLDs to have long standing

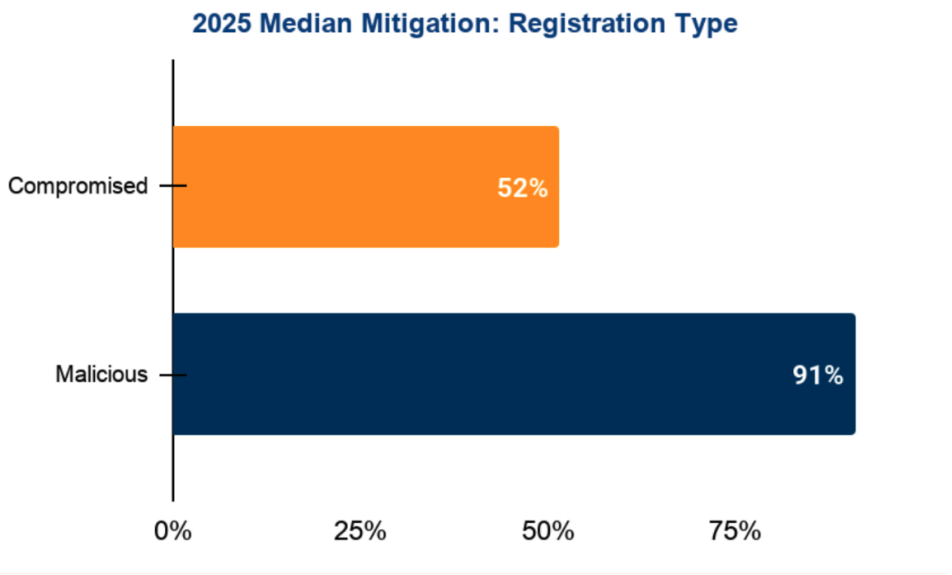
registrations with websites that have existed for a longer period of time and accumulated unpatched software that could be compromised.



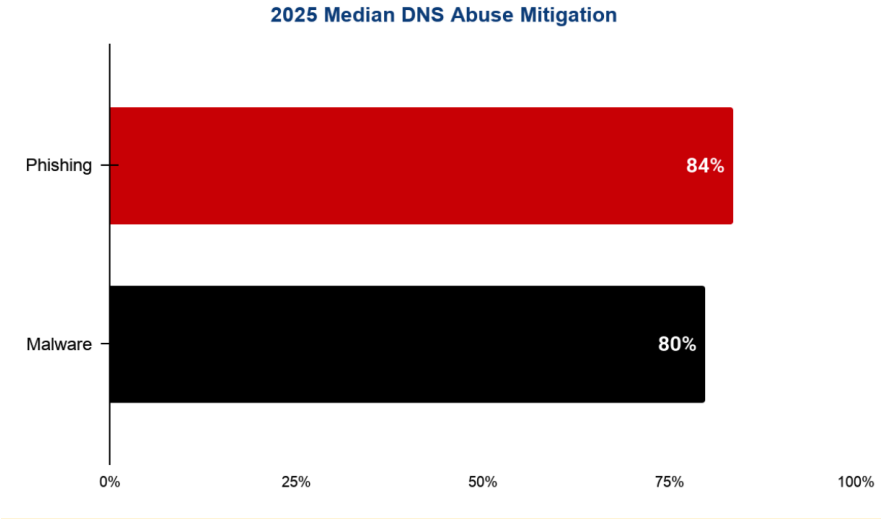
DNS Abuse mitigation rates remained high in 2025, **improving for malicious registrations, with a median of 91% in 2025 compared with 83% in 2024**.

Mitigation is measured holistically—focusing on whether the harm has stopped—without assigning credit to specific actors, since action can be taken at registry, registrar or hosting level, and referrals between them are common.

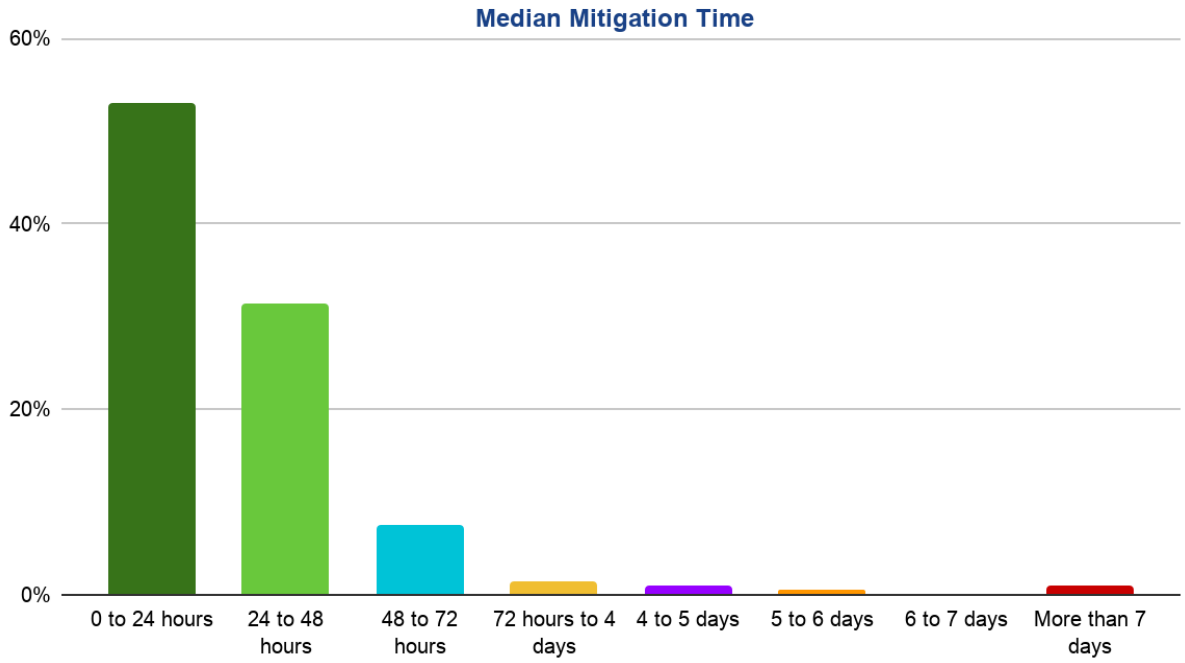
Mitigation improved for malicious registrations, with a median of 91% in 2025 compared with 83% in 2024. Mitigation is more complex for compromised domains, where an innocent registrant is typically involved and DNS-level takedown is not always appropriate. Lower rates reflect this complexity but remained consistent at a median of 52% across 2024 and 2025.



Our methodology observed that 84% of the unique domains associated with phishing were mitigated (up from 79% in 2024) while the mitigation rate in malware was slightly lower, at 80%. These rates include compromised websites and maliciously registered domain names.



Most (92%) of abusive unique domains had a median mitigation time of 72 hours or less, with 53% taking place within 24 hours of the domain being added to a blocklist. We proportion the number of unique domains per registrar into a time bucket based on the median mitigation time of the registrar credential. Observed mitigation activity includes DNS level and content level actions, and the data includes both compromised and malicious registrations.



Specific Reporting

We provide registrar and TLD level data on the relative concentration of observed malicious phishing and malware. There are four metrics: two relating to registrars and two relating to Top Level Domains (TLDs).

In 2025, there were a handful of registrars and TLDs that appeared in our specific reporting tables for 8 or more months. We highlight the registrar credentials, gTLDs and ccTLDs with the lowest (green) and highest (red) abuse in the tables below. **Large registrar credentials and TLDs with low abuse highlight the impact of strong anti-abuse practices.**

Rates of abuse	Lowest	Lowest	Highest
Size	Smaller	Larger	All
Registrars: DUM	Table 1	Table 2	Table 3
Registrars: new registrations	Table 4	Table 5	Table 6
gTLDs	Table 7	Table 8	Table 9
ccTLDs	Table 10	Table 11	Table 12

Registrars: Low Abuse *(Tables 1-3)*

Observed Maliciously Registered Domains Per 100,000 DUM: **Median .29 (Wix.com, Ltd) to 1029.45 (Aceville Pte. Ltd.)**

IANA ID	Registrar Credential	Number of Months	Median Maliciously Registered Domains/100K gTLD DUM
2	Network Solutions, LLC	12	0.685
146	GoDaddy.com, LLC	12	0.99
433	OVH sas	12	0.64
895	Squarespace Domains II..	12	0.53
1291	Dreamscape Networks In..	10	1.44
48	eNom, LLC	10	0.985
113	CSL Computer Service La..	9	1.53
168	Register SPA	9	1.25
1387	1API GmbH	9	1.31
440	Wild West Domains, LLC	9	1.14
431	DreamHost, LLC	8	2.17
1390	Mesh Digital Limited	8	0.965
83	IONOS SE	8	0.99
3817	Wix.com Ltd.	8	0.29

IANA ID	Registrar Credential	Number of Months	Median Maliciously Registered Domains/100K gTLD DUM
3858	Aceville Pte. Ltd.,	12	1029.45
3765	NiceNIC International Group Co., Limited,	12	336.19
460	Web Commerce Communications Limited dba WebNic.cc	12	152.08
3775	Dominet (HK) Limited, Ultahost, Inc.	10	865.26
4331	Ultahost, Inc.	10	793.19

Registrars: New Registrations *(Tables 4-6)*

Observed Maliciously Registered Domains Per New gTLD Registered Domains: **Median .02% (Wix.com, Ltd) to 22.5% (Aceville Pte Ltd)**

IANA ID	Registrar Credential	Number of Months	Median Malicious Domains per New Registrations
895	Squarespace Domains II..	12	0.04%
168	Register SPA	9	0.08%
1291	Dreamscape Networks In..	9	0.10%
2	Network Solutions, L..	9	0.08%
83	IONOS SE	9	0.06%
3827	Squarespace Domains LLC	9	0.09%
113	CSL Computer Service L..	8	0.09%
433	OVH sas	8	0.07%

3817	Wix.com Ltd.	8	0.02%

IANA ID	Registrar Credential	Number of Months	Median Malicious Domains per New Registrations
3858	Aceville Pte. Ltd.,	12	22.50%
3765	NiceNIC International Group Co., Limited,	12	3.00%
460	Web Commerce Communications Limited dba WebNic.cc	12	6.50%
3775	Dominet (HK) Limited, Ultahost, Inc.	10	12.00%
4331	Ultahost, Inc.	10	6.00%
3956	Global Domain Group LLC	8	2.00%

A handful of TLDs (.com, .net, .org, .dev, .de) were in the low abuse tables all 12 months, with a median observed maliciously registered domains per 100,000 DUM of 1.9 (dev) to 3.9 (com). The following table highlights the TLDs which were most consistently listed in our low abuse (green) and high (red) tables.

Many TLDs were excluded from the abuse tables as they had less than five malicious registrations per month. These are listed in our appendix.

gTLDs *(Tables 7-9)*

Observed Maliciously Registered Domains Per 100,000 DUM: **Median 1.92 (.dev)-235.99 (icu)**

gTLD	Number of Months	Median Maliciously Registered Domains/100K DUM
com	12	3.95
dev	12	1.93
net	12	2.52
org	12	2.10
biz	11	2.79
bet	10	9.84
tech	10	3.28
blog	8	3.12
today	8	2.35

gTLD	Number of Months	Median Maliciously Registered Domains/100K DUM
cfd	12	188.82
icu	11	235.99
help	11	162.79
qpon	8	185.35

ccTLDs *(Tables 10-12 ccTLDs)*

Large ccTLDs showed a median of .51 maliciously registered domains per 100,000 DUM. Small ccTLDs showed a median of 2.1 maliciously registered domains per 100,000 DUM.

Observed Maliciously Registered Domains Per 100,000 DUM: **Median 0.27 (.nl) to 48.73 (.im)**

ccTLD	Number of Months	Median Maliciously Registered domains/100K DUM
de	12	0.475
uk	11	0.53
ua	11	2.09
ch	11	0.43
nl	11	0.27
it	11	0.34
cl	11	2.37
ca	11	0.41
ai	11	1.77
be	10	0.49
vn	9	4.49
ae	9	2.49
ar	9	1.33
tv	8	1.985
ro	8	1.255

ccTLD	Number of Months	Median Maliciously Registered domains/100K DUM
cc	12	46.09
id	12	22.36
im	12	48.73
my	12	11.14
cn	11	9.49
me	10	5.97

Background

Our methodology, available on the NetBeacon Institute website, provides important context and we recommend it is read in full. We offer a number of options for consuming NetBeacon MAP data: see our website for more information.

Our approach is one of collaboration and engagement, and we endeavor to speak to interested parties and provide them with early access to data that concerns their organization. We are committed to refining this project as work continues and welcome insights from across the industry to help us iterate and improve. We encourage registrars and TLD operators to contact us to review their data and access their free Individual Dashboards.

NetBeacon MAP operates independently of NetBeacon Reporter, the centralized abuse reporting service we created for the benefit of the DNS. Reports from NetBeacon Reporter do not go into our measurement work with NetBeacon MAP. This is a conscious choice to optimize and encourage usage of NetBeacon Reporter and prevent any abuse of NetBeacon Reporter as an attempt to influence NetBeacon MAP data. Our research partner, KOR Labs, submit reports into NetBeacon Reporter for domains that are still live, well evidenced and maliciously registered. See the methodology for more information on how domains are included in NetBeacon MAP.