NETBEACON INSTITUTE

NETBEACON MAP

Monthly Analysis

March 2025

Contents

Executive Summary

This publication of NetBeacon MAP: Monthly Analysis contains data from **January 2025**. Refer to the Background section for more information about this initiative and the NetBeacon Institute.

Key highlights from our overall data include:

- **A noticeable month-to-month decrease in the number of unique domains used for phishing was observed.** Our methodology identified a 30% decrease in unique domains engaged in phishing attacks in January 2025 compared to December 2024 (45,699 to 31,761). December 2024 was the highest month on record. This drop returns our numbers closer to the average for 2024.
- **A month-to-month slight decrease in unique domains used for malware distribution.** January 2025 recorded 574 unique domains compared to 583 in December 2024. Our observed data shows that malware numbers tend to fluctuate more than phishing. The highest month on record is 13,941 in December 2022, and the lowest was 163 in August 2023.
- **We observed high mitigation rates in January 2025.** Our methodology observed that 83% of the unique domains associated with phishing were mitigated and 89% of those associated with malware were mitigated. Readers should be aware that these rates include compromised websites and maliciously registered domain names. To understand the impact of the gTLD contract amendments, we released a specific blog which looks at registrar mitigation rates for maliciously registered domains.
- **The number of registrar credentials with an observed median mitigation speed 48 hours or less increased.** In January, 62% of

registrar credentials had a median mitigation time of 48 hours or less, a higher percentage compared to our reports in December (51%). These median mitigation times include compromised websites and maliciously registered domain names.

- **In January, 86% of unique domains used for phishing were classified as maliciously registered by our methodology (a nominal month-on-month decrease from 89%). There were 81% of unique domains used for malware distribution classified as maliciously registered by our methodology (a month-on-month increase from 62%).** This is an exceptionally important distinction when it comes to mitigation; 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 or registrant. In terms of the type of registration, we typically see more compromised websites associated with malware distribution and more maliciously registered domains associated with phishing attacks.

Registrars and Top Level Domains (TLDs):

To understand how phishing and malware is distributed across the ecosystem, we continue to publish our Specific Reporting tables which identify registrars and TLDs with relatively high or low rates of abuse per 100,000 Domains Under Management (DUM), or new registrations.

As we look towards the future, we're contemplating how best to measure the impact of the gTLD contractual amendments and look forward to sharing more information on this in the near future.

General DNS Abuse Trends

General DNS Abuse Trends are useful for understanding phishing and malware across the DNS ecosystem and high level trends over time. This section shows high-level, aggregate data for all months on record at the time of publication.[1]

Chart 1: Aggregate Trends

This chart provides a high-level view on how much DNS Abuse has been identified by our methodology, and how DNS Abuse is changing over time. It shows the absolute volume of unique domains our methodology has identified that are engaged in phishing or malware, broken out by category. For more information: Chart 1: Aggregate Trends

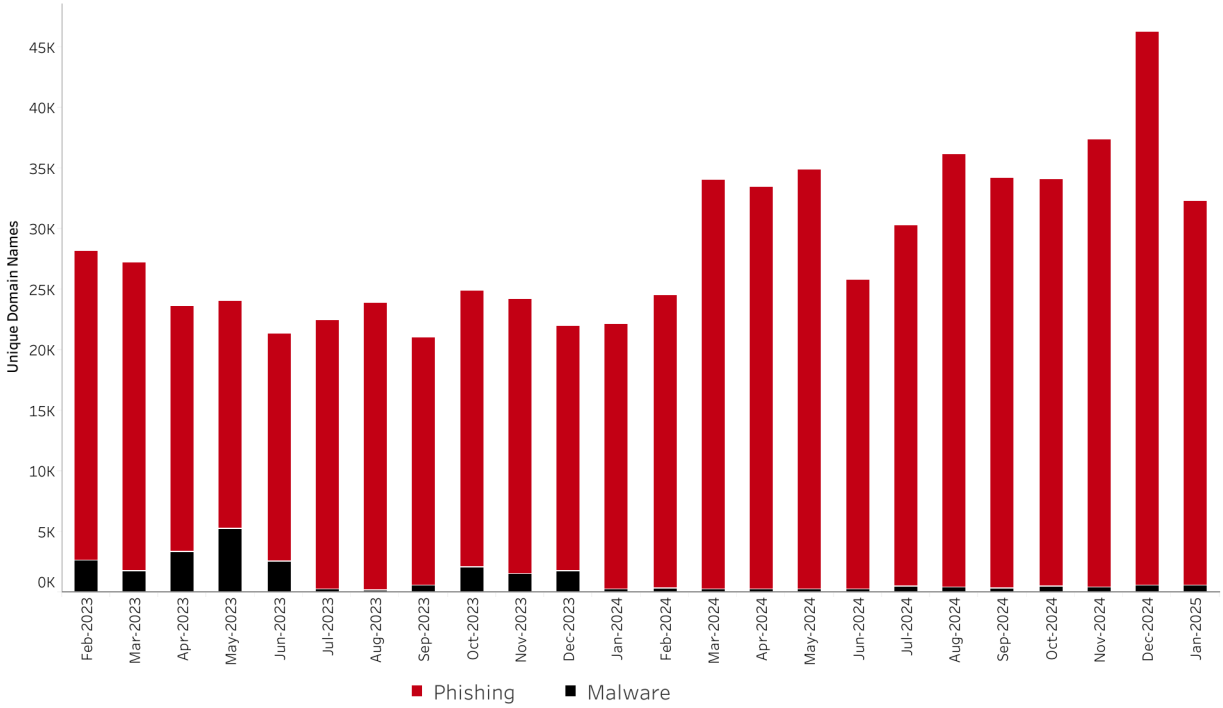

*Figure 1: Aggregate Trends - **Phishing and Malware***

[1] Note: reporting is delayed by two months to allow for the measurement of mitigation.

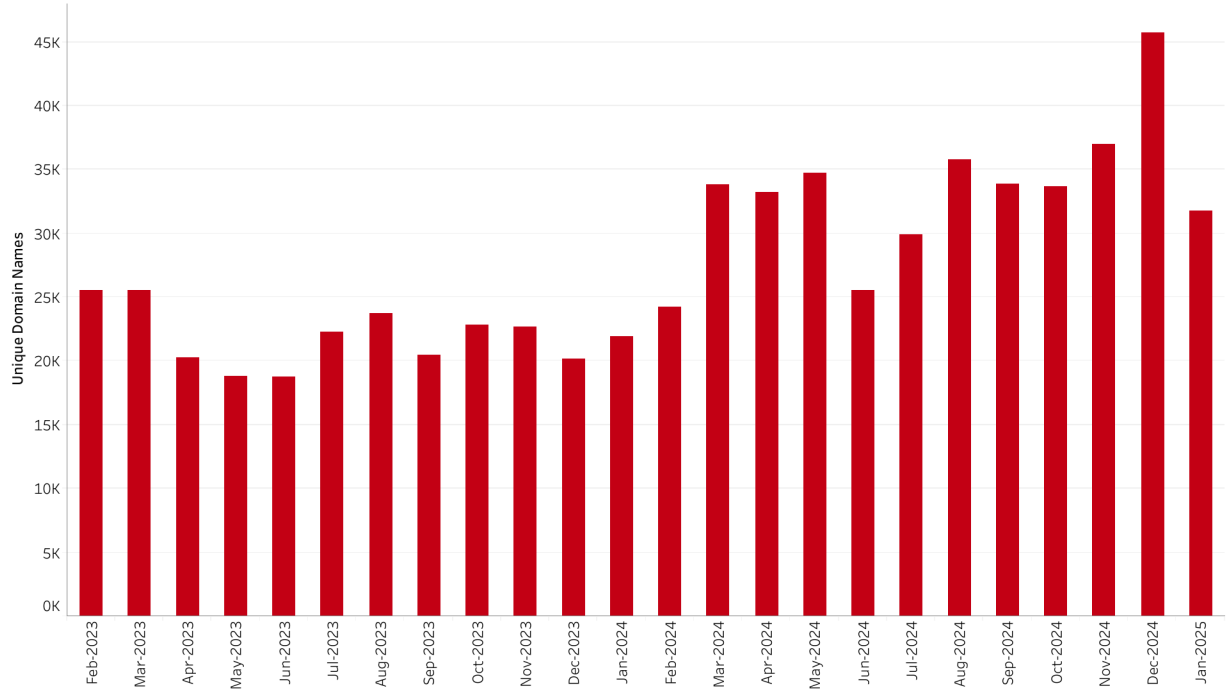

*Figure 2: Aggregate Trends - **Phishing***

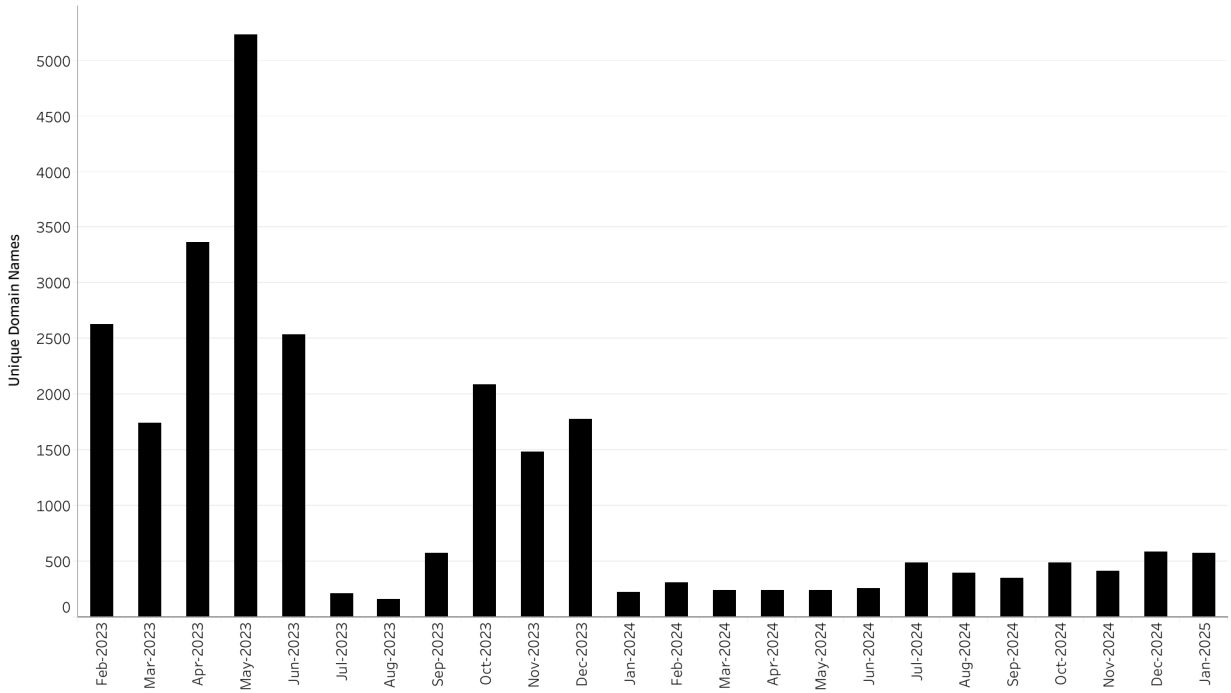

*Figure 3: Aggregate Trends - **Malware***

Chart 2: Mitigation

This chart provides a high-level view on how much DNS Abuse mitigation has been identified by our methodology, and how it's changing over time. More information: [Chart 2: Mitigation]

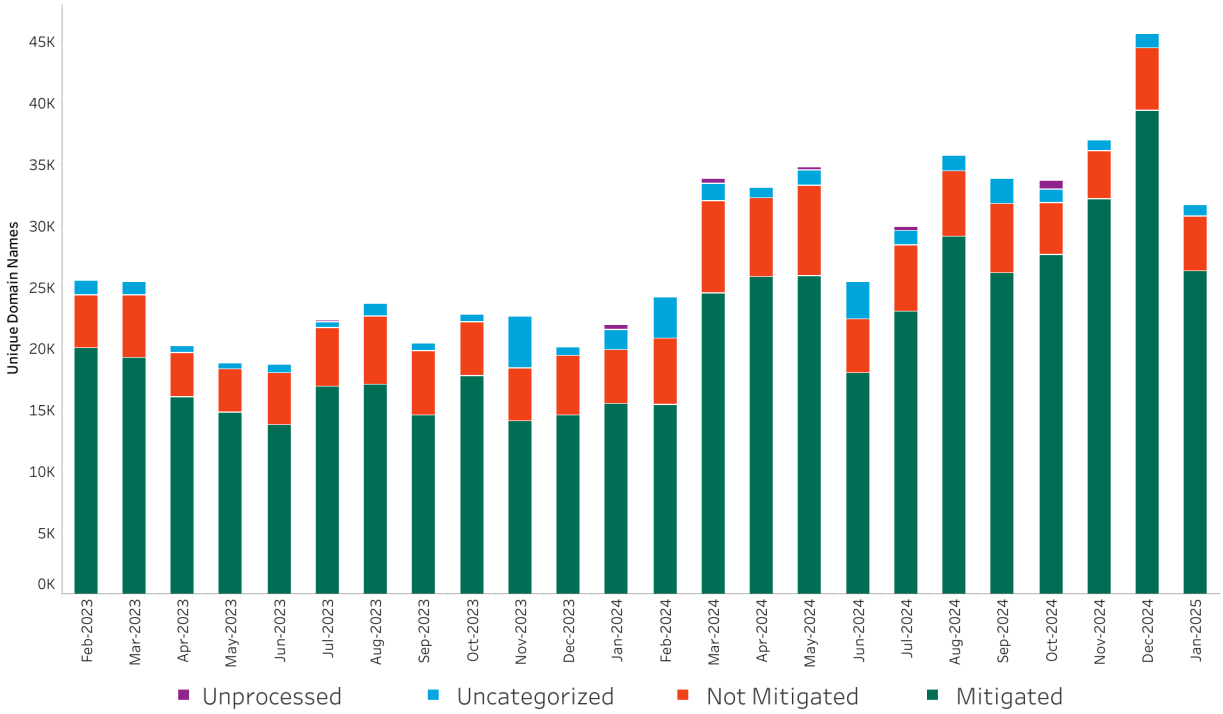

*Figure 4: Mitigation - **Phishing***

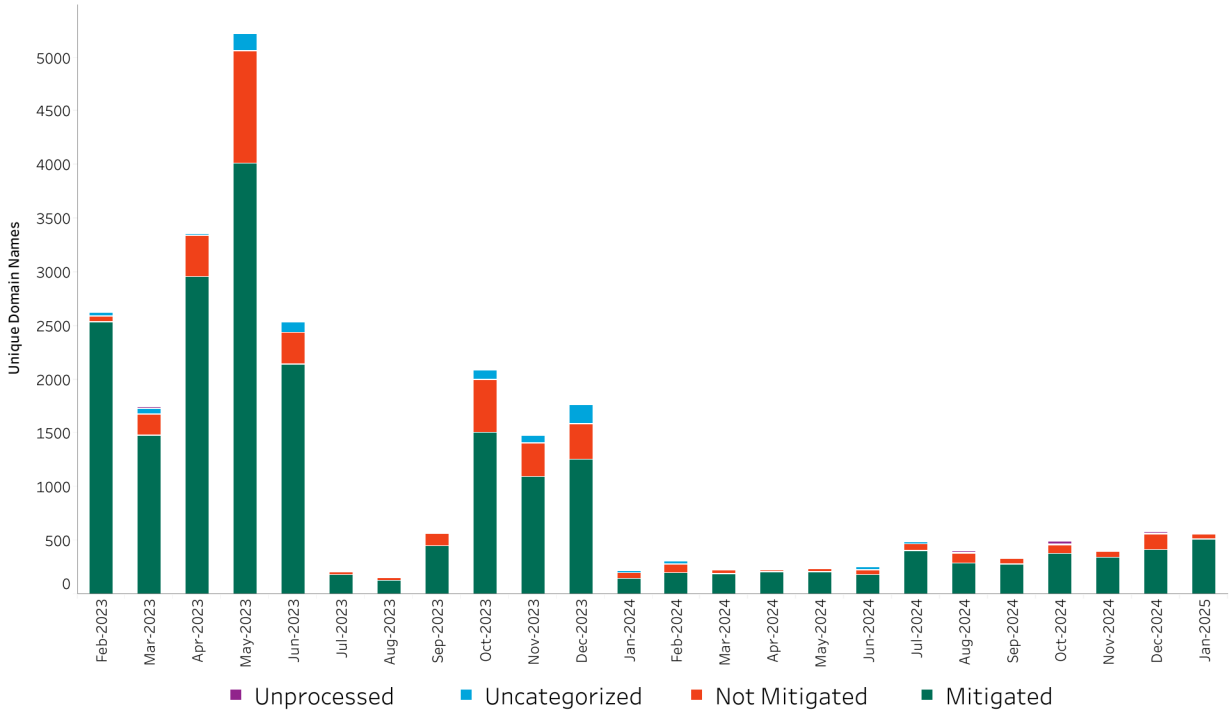

*Figure 5: Mitigation - **Malware***

Chart 3: Registrar Median Mitigation Time

This chart is intended to show the observed time taken to mitigate phishing and malware, and how it is changing over time. For the domains that our methodology determined were mitigated, this chart shows how many registrars had a median time to mitigation in each category. For more information: [Chart 3: Registrar Median Mitigation Time]

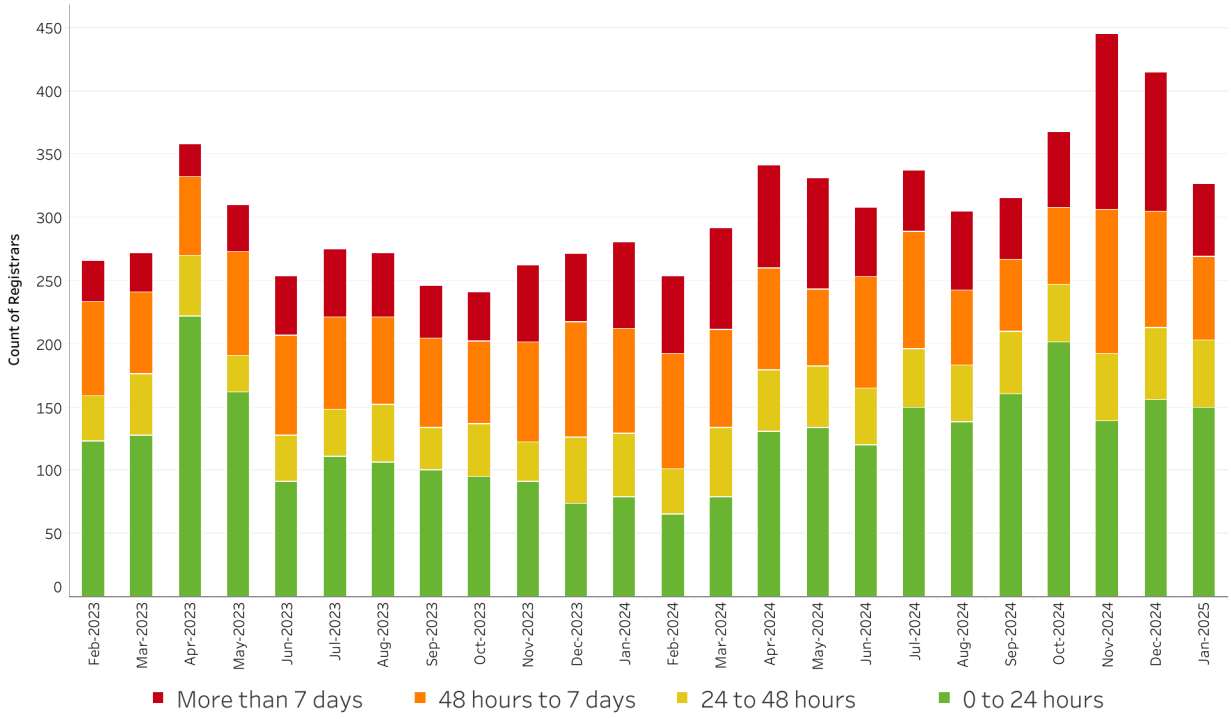

Figure 6: Registrar Median Mitigation Time

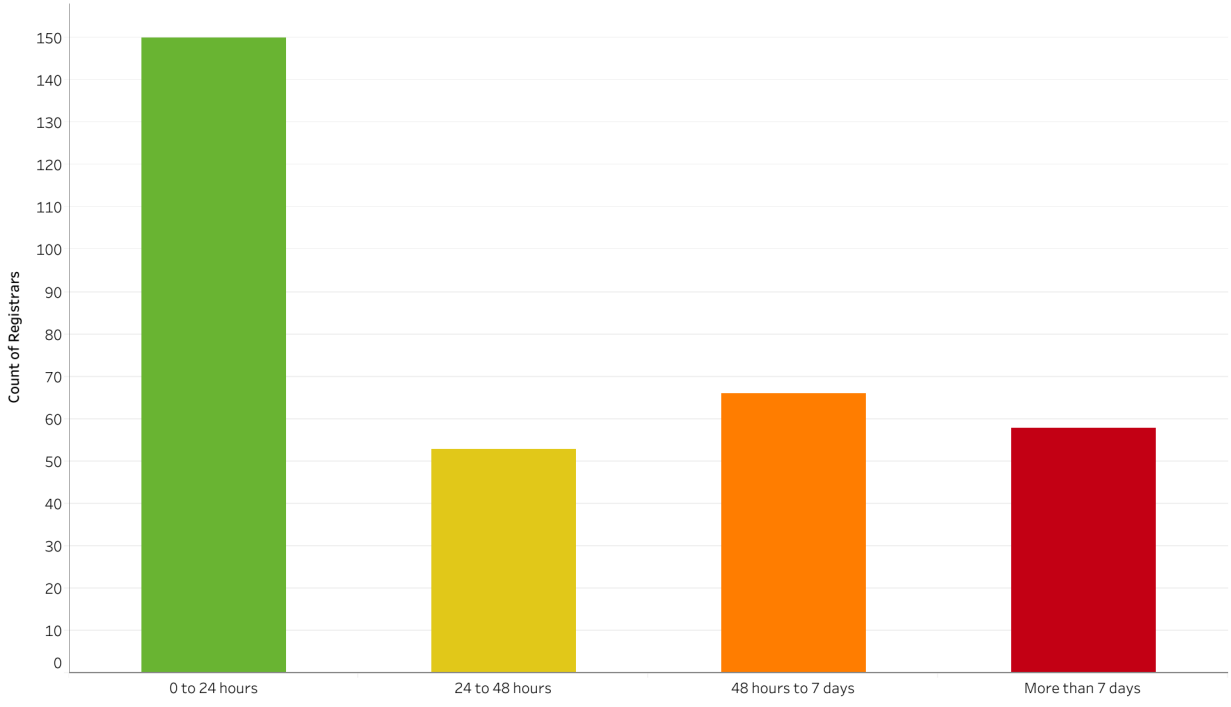

Figure 7: Registrar Median Mitigation Time ***2025-01***

Chart 4: Malicious vs. Compromised

This chart is intended to show the observed registration type (malicious vs. benign but compromised) and how this is changing over time. For more information: Chart 4: Malicious vs. Compromised.

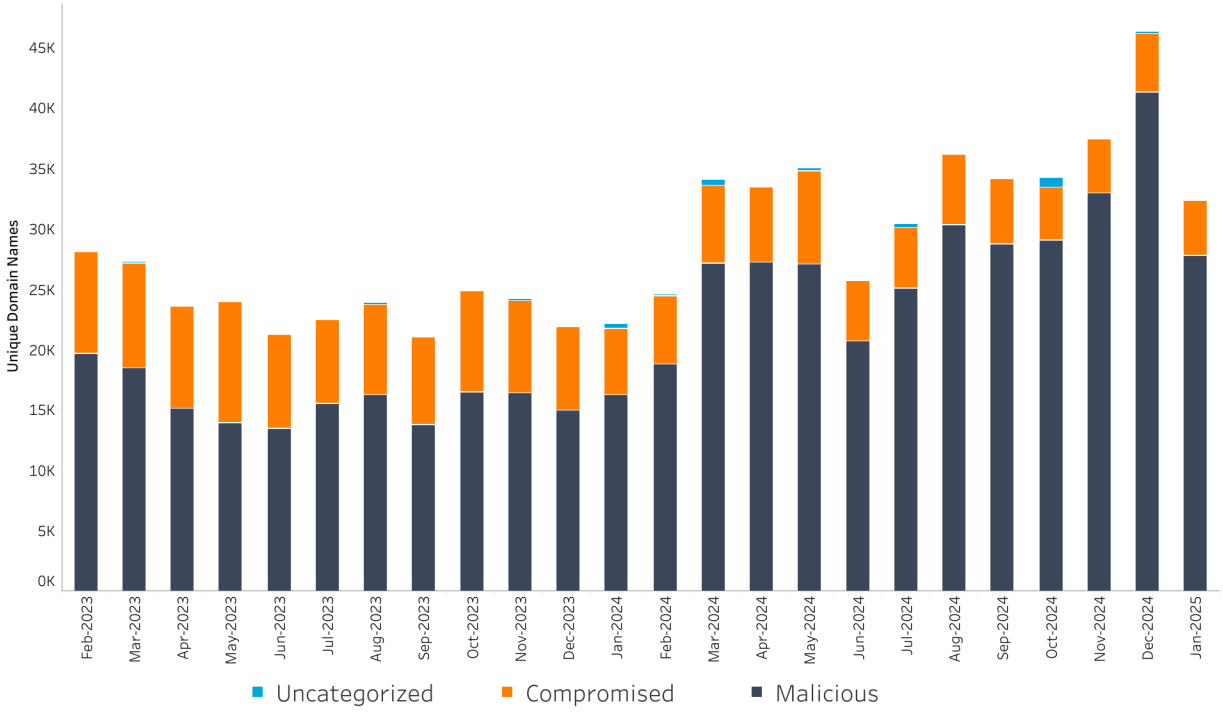

*Figure 8: Compromised vs Malicious - **Phishing and Malware***

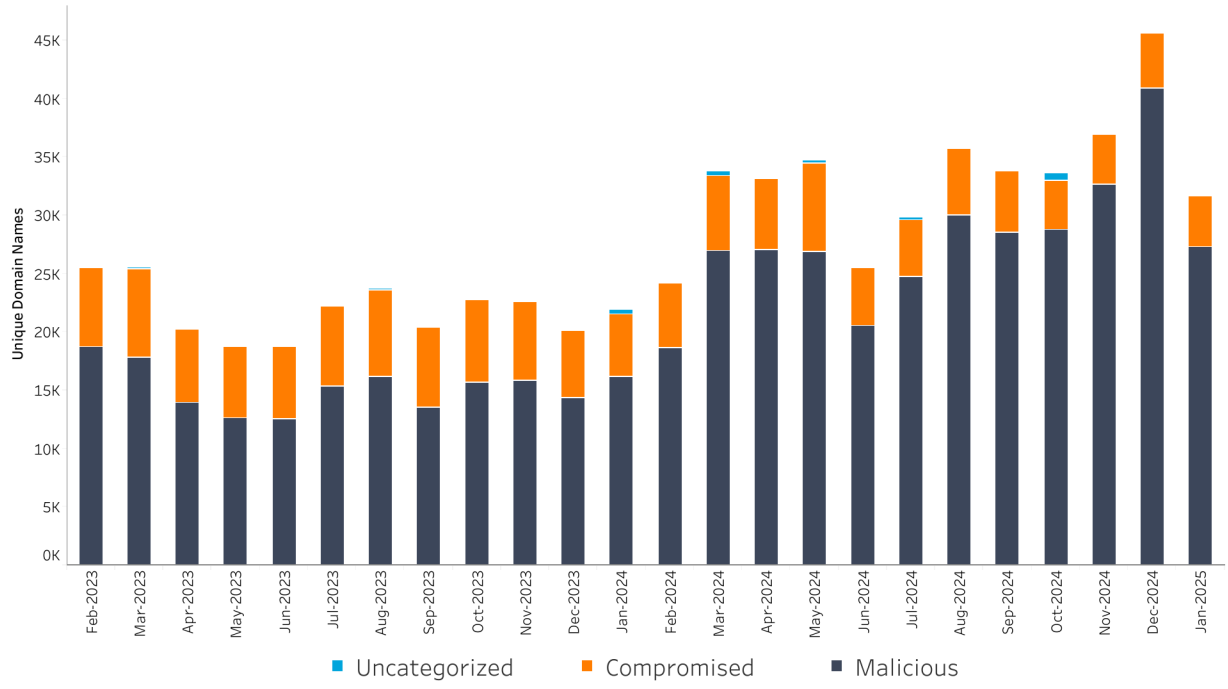

*Figure 9: Compromised vs Malicious - **Phishing***

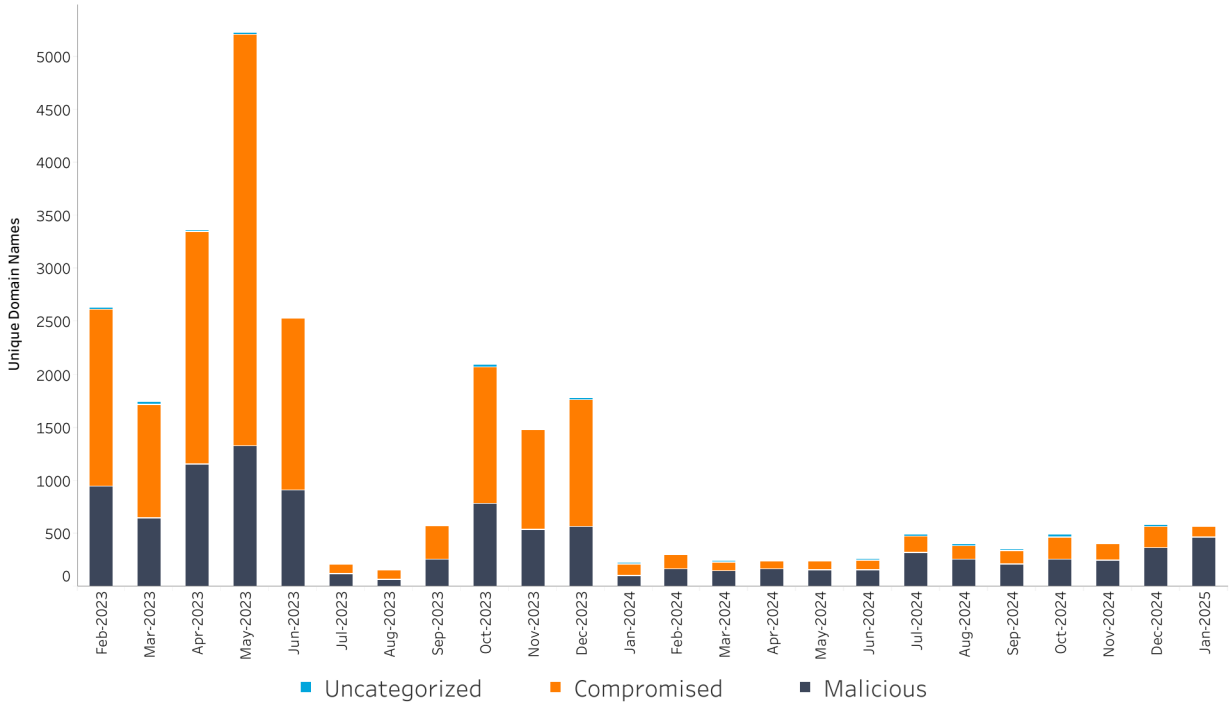

*Figure 10: Compromised vs Malicious - **Malware***

Specific Reporting

We provide registrar and TLD level data on the relative concentration of observed malicious phishing and malware. This section shows data for the most recent month on record.[2]

There are four metrics: two relating to registrars and two relating to Top Level Domains (TLDs). Each metric includes three tables. The first two tables per metric identify the lowest rates of abuse: one table for larger registrars/TLDs, and one table for smaller registrars/TLDs. The final table in each metric identifies the highest rates of abuse.

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

[2] Note: reporting is delayed by two months to allow for the measurement of mitigation.

Registrars: DUM

For a detailed description of this metric see: Registrars: DUM (Tables 1-3).

Table 1: Smaller registrars: lowest observed rates of abuse 2025-01

IANA ID	Registrar Credential	Observed Maliciously Registered Domains Per 100,000 gTLD DUM	Observed Malicious gTLD Domains	Observed gTLD DUM
106	Ascio Technologies, Inc. Danmark - ..	0.81	7	868,197
151	InterNetX GmbH	1.02	10	984,602
1390	Mesh Digital Limited	1.08	8	742,494
1387	1API GmbH	1.51	13	860,981
113	CSL Computer Service Langenbach ..	1.53	8	523,383
168	Register SPA	1.67	11	658,631
1331	eName Technology Co., Ltd.	1.73	7	405,105
1291	Dreamscape Networks Internation..	2.36	11	466,536
1449	URL Solutions, Inc.	2.91	6	206,498
418	CommuniGal Communication Ltd.	2.95	9	304,768

Table 2: Larger registrars: lowest observed rates of abuse 2025-01

IANA ID	Registrar Credential	Observed Maliciously Registered Domains Per 100,000 gTLD DUM	Observed Malicious gTLD Domains	Observed gTLD DUM
3817	Wix.com Ltd.	0.27	8	2,963,145
433	OVH sas	0.64	14	2,195,395
895	Squarespace Domains II LLC	0.69	49	7,136,941
1345	Key-Systems, LLC	0.92	10	1,089,082
48	eNom, LLC	1.00	35	3,516,558
146	GoDaddy.com, LLC	1.09	689	63,495,720
269	Key-Systems GmbH	1.10	19	1,734,589
81	Gandi SAS	1.14	12	1,056,940
440	Wild West Domains, LLC	1.21	28	2,309,437
2	Network Solutions, LLC	1.30	64	4,924,613

Table 3: Highest observed rates of abuse 2025-01

IANA ID	Registrar Credential	Observed Maliciously Registered Domains Per 100,000 gTLD DUM	Observed Malicious gTLD Domains	Observed gTLD DUM	Number of Months
Redacted	*Redacted*	3,429.65	*	*	3
3775	Dominet (HK) Limited	1,487.31	7,981	536,607	6
3858	Aceville Pte. Ltd.	806.48	249	30,875	5
3765	NICENIC INTERNATIONAL GR..	696.19	522	74,979	6
Redacted	*Redacted*	148.48	*	*	2
Redacted	*Redacted*	122.20	*	*	3
3956	Global Domain Group LLC	117.34	69	58,801	4
Redacted	*Redacted*	103.49	*	*	1
1250	OwnRegistrar, Inc.	84.24	248	294,390	4
460	Web Commerce Communicati..	81.37	558	685,790	6

Registrars: New registrations

For a detailed description of this metric, see: Registrars: New registrations (Tables 4-5)

Table 4: Smaller volume: lowest observed rates of abuse 2025-01

IANA ID	Registrar Credential	Observed Maliciously Registered Domains Per New gTLD Domain Registration	Observed Malicious gTLD Domains	Observed Newly Registered gTLD Domains	Observed gTLD DUM
418	CommuniGal Communicat..	0.05%	9	16,584	304,768
106	Ascio Technologies, Inc. D..	0.09%	7	7,820	868,197
1469	Jiangsu Bangning Science..	0.09%	7	7,545	180,850
113	CSL Computer Service La..	0.09%	8	8,479	523,383
1449	URL Solutions, Inc.	0.10%	6	5,829	206,498
168	Register SPA	0.11%	11	10,049	658,631
1387	1API GmbH	0.12%	13	10,721	860,981
81	Gandi SAS	0.14%	12	8,511	1,056,940
819	Turkticaret.net Yazılım Hi..	0.15%	12	7,849	169,238
269	Key-Systems GmbH	0.16%	19	12,226	1,734,589

Table 5: Higher volume: lowest observed rates of abuse 2025-01

IANA ID	Registrar Credential	Observed Maliciously Registered Domains Per New gTLD Domain Registration	Observed Malicious gTLD Domains	Observed Newly Registered gTLD Domains	Observed gTLD DUM
1345	Key-Systems, LLC	0.01%	10	111,546	1,089,082
3817	Wix.com Ltd.	0.01%	8	65,595	2,963,145
1331	eName Technology Co., Ltd.	0.03%	7	24,708	405,105
895	Squarespace Domains II LLC	0.06%	49	78,642	7,136,941
433	OVH sas	0.07%	14	20,320	2,195,395
3827	Squarespace Domains LLC	0.08%	72	91,437	2,646,231
1599	Alibaba Cloud Computing Lt..	0.08%	69	86,994	3,401,241
1861	Porkbun LLC	0.08%	47	58,673	1,920,749
146	GoDaddy.com, LLC	0.09%	689	750,453	63,495,720
48	eNom, LLC	0.09%	35	37,833	3,516,558

Table 6: Highest observed rates of abuse 2025-01

IANA ID	Registrar Credential	Observed Maliciously Registered Domains Per New gTLD Domain Registration	Observed Malicious gTLD Domains	Observed Newly Registered gTLD Domains	Observed gTLD DUM	Number of Months
3858	Aceville Pte. Ltd.	28.23%	249	882	30,875	6
Redacted	*Redacted*	13.31%	*	*	*	3
3775	Dominet (HK) Limited	10.47%	7,981	76,239	536,607	6
Redacted	*Redacted*	8.20%	*	*	*	3
3765	NICENIC INTERNATION..	7.17%	522	7,283	74,979	6
1556	Chengdu West Dimensi..	7.06%	1,186	16,801	970,528	4
Redacted	*Redacted*	4.05%	*	*	*	1
Redacted	*Redacted*	3.21%	*	*	*	1
Redacted	*Redacted*	3.06%	*	*	*	1
Redacted	*Redacted*	2.69%	*	*	*	1

Generic Top Level Domains

For a detailed description of this metric, see Generic Top Level Domains (Tables 7-9)

Table 7: Smaller gTLDs: lowest observed rates of abuse 2025-01

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
tokyo	3.88	7	180,455
studio	4.84	6	123,889
loan	8.41	6	71,365
services	9.29	8	86,159
autos	9.40	7	74,451
bet	10.24	9	87,848
network	12.86	10	77,779
ltd	13.41	17	126,750
email	14.00	16	114,322
win	14.21	11	77,435

Table 8: Larger gTLDs: lowest observed rates of abuse 2025-01

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
dev	1.99	9	452,763
biz	2.01	25	1,240,867
net	2.18	275	12,619,580
today	2.32	13	559,384
mobi	2.47	6	242,765
store	2.74	48	1,748,689
tech	2.89	14	483,853
org	3.63	406	11,179,342
com	3.88	6,058	156,161,752
blog	4.26	13	305,281

Table 9: gTLDs: highest observed rates of abuse 2025-01

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM	Number of Months
Redacted	7,585.57	*	*	2
help	255.63	92	35,990	6
top	253.35	7,883	3,111,537	6
Redacted	249.20	*	*	3
Redacted	243.23	*	*	3
Redacted	184.00	*	*	1
ink	175.71	145	82,522	5
Redacted	153.19	*	*	1
Redacted	134.73	*	*	1
Redacted	133.55	*	*	1

Country Code Top Level Domains

For a detailed description of this metric, see: Country Code Top Level Domains (Table 10-12)

Table 10: Smaller ccTLDs: lowest observed rates of abuse 2025-01

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
ai	1.71	10	583,148
ar	1.77	9	508,359
pt	1.93	8	413,900
tv	1.94	8	412,316
cl	2.00	11	549,511
ua	2.13	10	469,322
ae	2.16	6	277,488
vn	4.23	22	520,403
uz	4.56	6	131,446
kz	4.86	9	185,288

Table 11: Larger ccTLDs: lowest observed rates of abuse 2025-01

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
uk	0.34	33	9,771,333
be	0.37	6	1,632,415
nl	0.37	22	5,967,487
ch	0.39	10	2,560,463
jp	0.41	7	1,721,908
it	0.46	15	3,230,124
de	0.49	85	17,217,514
za	0.68	9	1,325,966
eu	0.80	29	3,627,045
au	0.83	34	4,119,004

Table 12: ccTLDs: highest observed rates of abuse 2025-01

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM	Number of Months
cc	67.29	1,141	1,695,610	6
im	40.65	18	44,280	4
id	35.12	339	965,260	6
Redacted	16.54	*	*	2
Redacted	10.21	*	*	2
me	8.39	89	1,060,525	6
my	8.11	26	320,533	4
ng	6.00	11	183,220	6
cn	4.70	508	10,808,506	6
vn	4.23	22	520,403	5

About General DNS Abuse Trends

These charts are available in an interactive format on our website:

Chart 1: Aggregate Trends

- **Phishing:** is an attempt to trick people into sharing important or sensitive information – for example logins, passwords, credit card numbers or banking information – in either a personal or business context.
- **Malware:** is malicious software designed to compromise a device on which it is installed.

Chart 2: Mitigation

The methodology includes a process to determine whether any mitigation has been observed. This involves taking an initial measurement of various factors related to the URL and repeating these measurements for one month. Further details are set out in the methodology.

Our methodology includes four labels:

- **Mitigated**: We detected that a mitigating action has occurred. This action could have been taken by a registrar, registry, a hosting provider, or another relevant actor, including the registrant.
- **Not Mitigated**: We did not detect any indication of mitigation.
- **Uncategorized**: We were unable to determine whether or not mitigation occurred.
- **Unprocessed**: The domains were not processed due to network connectivity, server problems, or other similar issues.

Chart 3: Registrar Median Mitigation Time

After an initial measurement, KOR Labs repeats measurements for one month to determine if mitigation has occurred. The intervals used are (starting at the time of acquiring the URL from the blocklist): 5m, 15m, 30m, 1hr, 2hr, 3hr, 4hr, 5hr, 6hr, 12hr, and then once every 12 hours for one month.

While we are describing this information as a "median registrar mitigation time," it should be noted that we do not know definitively that it was the registrar that took action. This data could include mitigation taken by the registry, the host, or any other relevant party. The reference to a registrar is indicative that the domain is under their management.

Chart 4: Malicious vs. Compromised

Our methodology includes three labels:

- **Malicious**: a domain registered for malicious purposes (i.e., to carry out DNS Abuse).
- **Compromised**: A benign domain name that has been compromised at the website, hosting, or DNS level.
- **Uncategorized**: A domain that our methodology was unable to categorize for a number of reasons, including problems in collecting the metadata necessary to categorize domain names accurately.

About Specific Reporting

Specific Reporting is intended to show the spectrum of how malicious phishing and malware is concentrated across the DNS registration ecosystem.[3] To demonstrate this, we are identifying registrars and TLDs with higher and lower relative volumes of malicious domain registrations in their Domains Under Management (DUM), or new registrations.

The metrics we have chosen in this section of reporting were selected to provide a straightforward mechanism to understand DNS Abuse using the data points observed by our methodology. In the future, we may add additional metrics or combine various data points.

To the best of our ability in accordance with our methodology, all metrics are compiled using only observed maliciously registered domains, and exclude observed as compromised.[4] We also provide registrars and registries with data relating to compromised domain names within their DUM on a one-to-one basis.

It is important to recognise the limitations of this work. We are faced with the universal challenge of understanding malicious activity in society; we can only measure the harms that are identified. In our case, we identify phishing and malware through the source lists we use for NetBeacon MAP. Identified phishing and malware will always be a subset of all existing phishing and malware. There will also be "false positives," that is, domain names categorized as phishing and malware that actually aren't due to both

[3] NetBeacon MAP reporting currently focuses on the DNS registrars and DNS registry operators. The DNS ecosystem also includes additional parties such as hosting providers which are typically a more appropriate point of contact for compromised domain names, where a benign domain has been compromised at the website or hosting level.

[4] NetBeacon MAP uses the following definition of compromised: "A benign domain name that has been compromised at the website, hosting, or DNS level.

classification errors and differences in standards. There is also the potential that identified DNS Abuse is biased to particular geographic regions or activities that are more likely to be subject to reporting.

Another challenge we encounter is accurately enumerating the number of DUM for each registrar and TLD (which can impact "per 100K DUM" density metrics). Generally, our observed DUM is lower than officially reported DUM for all TLDs and registrars. For additional information on the limitations of this work, please refer to our methodology.

With these metrics, we want to provide the industry with evidence and information on how phishing and malware is distributed across the ecosystem. We have made several exclusions from each table to reduce the risk of including false positives and to increase the focus on credentials that account for the bulk of domain registrations exhibiting generalizable practices and policies.

Registrars: DUM (Tables 1-3)

This metric is intended to show the prevalence of observed maliciously registered domains in each registrar. We use observed maliciously registered domains per 100,000 DUM to allow comparison across registrars. Focusing only on absolute numbers of observed maliciously registered domains would typically result in the largest registrars having the largest number of malicious domain registrations. The observed maliciously registered domains is a count of the number of unique domain names, not URLs.[5]

[5] Typically reputation block lists—the starting point of our methodology—are created for the purposes of network blocking, not measuring DNS Abuse. As described in our methodology, we have observed incidences of malicious websites generating a unique URL for each individual visit of a website (human or crawler). One incident resulted in the same domain name being reported over 70,000 times with different URLs. While this is typically valuable information for the purposes of network blocking, counting unique URLs is less appropriate for measuring DNS abuse at the registration level. Registries and registrars have limited blunt tools for mitigation, all of which operate at the domain level. As a result, we

Our reporting is indifferent to registrar corporate families as we report on the registrar IANA ID (i.e., at the credential level).[6] This means that some corporate entities will have more than one IANA ID, and they may choose to operate these credentials differently; for example, by using one credential for all new registrations. We chose not to manually combine credentials to minimize the risk that we could unintentionally attribute data to the incorrect registrar family as a result of missing a credential sale or corporate acquisition.

Our methodology identified a substantial number of registrar credentials that have zero observed maliciously registered domains in the current month of reporting. There are several reasons for why a registrar credential may have zero observed malicious domain names. For example, the credential may be:

- used for corporate purposes,
- operate a business model of brand protection (offering defensive registrations for existing brands),
- register low numbers or no new domain names, or
- used predominantly for registering expiring domain names for the purposes of resale ("drop catching").

A specific business model or operational practice (rather than a generalizable policy or practice that other registrars could adopt) may cause registrar credentials to be identified as having zero observed maliciously registered domains. Zero observed maliciously registered domains is likely not feasible for typical credentials held by most registrars, particularly large retail registrars who sponsor the overwhelming majority of domains.

measure and calculate the occurrence metrics for unique observed abusively registered domain names.

[6] See https://www.iana.org/assignments/registrar-ids/registrar-ids.xhtml for the authoritative list of ICANN-acccredited registrars, which links the assigned IANA ID to the registrar name. The corporate entity controlling the registrar accreditation may not have (or do business under) the same name.

Nevertheless, zero observed maliciously registered domains is still a laudable achievement. Accordingly, we have listed these registrar credentials in Appendix A: Registrar Credentials With Zero Observed Maliciously Registered Domains.

While every effort has been made to reduce the chance of false positives, it is impossible to eliminate this risk. To minimize the impact of false positives, we have required a minimum number of observed maliciously registered domains per registrar ID. With this requirement we are aiming to avoid where tables are largely composed of registrar credentials that would—other than for the existence of a few false positives—be listed in Appendix A. However, as very low numbers of observed malicious domain names is also a laudable result, we have included a list of these registrars in Appendix B: Registrar Credentials With One to Five Observed Maliciously Registered. We also exclude Brand Protection registrars in Appendix H. We determined this list based on a research paper focusing on exclusions to improve accuracy.[7] Finally, the registrar data excludes ccTLD domains due to challenges in mapping domains to registrars in ccTLD ecosystems.

To account for the diversity of registrar credential sizes, we have reported low numbers of observed maliciously registered domains for both smaller (1-999,999 gTLD DUM) registrars (Table 1) and larger (1 million + gTLD DUM) registrars (Table 2). We note that this threshold of 1 million is somewhat arbitrary and slightly different rankings would result from a different threshold.

For higher numbers of observed maliciously registered domains, we have used one table (Table 3) and introduced a concept of consistency: a registrar credential will only be listed if they appear in this table of ten registrars for 4 or more of the last 6 months, otherwise they will be redacted. We attempt to

[7] "Building a Resilient Domain Whitelist to Enhance Phishing Blocklist Accuracy", Jan Bayer, Sourena Maroofi, Olivier Hureau, Andrzej Duda, Maciej Korczynski, Symposium on Electronic Crime Research (eCrime), Spain, 2023.

contact all registrars in advance of publications, regardless of redaction. To further reduce the possibility of false positives, we also require a higher threshold of minimum malicious domain names for inclusion: more than 10 observed malicious domain names per month.

Data for this metric is presented in the following tables:

Table 1: Smaller registrars: lowest observed rates of abuse

Inclusion criteria:

- Observed Maliciously Registered Domains: More than 5 per month
- Observed DUM: 1 - 999,999

Table 2: Larger registrars: lowest observed rates of abuse

Inclusion criteria:

- Observed Maliciously Registered Domains: More than 5 per month
- Observed DUM: Equal to or greater than 1 million

Table 3: Highest observed rates of abuse

Inclusion criteria:

- Observed Maliciously Registered Domains: More than 10 per month
- Consistency: If a registrar does not appear in the list of 10 registrars with the highest observed maliciously registered domains per 100,000 DUM for 4 or more of the last 6 months, its data has been redacted.

For excluded data, see Appendices:

- Appendix A: Registrar Credentials With Zero Observed Maliciously Registered Domains
- Appendix B: Registrar Credentials With One to Five Observed Maliciously Registered Domains

- Appendix H: Brand Protection Registrars

Registrars: New registrations (Tables 4-5)

This metric is intended to show the relationship between new registrations and observed malicious registration abuse. If the number of observed malicious domain names is a significant proportion of newly registered domain names, it may be an indication that a registrar should consider mechanisms to prevent incoming maliciously registered domains such as utilizing improved fraud prevention techniques.[8]

As with our previous registrar metric, we have excluded registrar credentials with zero observed maliciously registered domains, and those with low numbers (1-5) of observed maliciously registered domains to reduce the risk of false positives. Instead we have focused on registrar credentials that account for the bulk of domain registrations that may exhibit generalizable practices and policies.

As our reporting is based on registrar IANA ID (credential), not registrar corporate family, there may be some unexpected results in the data. It should be noted that a registrar may use one ID for new registrations, and another ID for holding registrations. We have minimized the risk of this type of discrepancy by introducing an inclusion requirement for registrar credentials to have a substantial amount of new registrations per month: 300 per month or approximately 10 new gTLD domain registrations per day.

To account for the diversity of registrar credential sizes, we have reported low numbers of observed maliciously registered domains for both smaller (300-20,000 Newly Registered gTLD Domains) registrars (Table 4) and larger (20,000+ Newly Registered gTLD Domains) registrars (Table 5). We note that

[8] https://netbeacon.org/best-practice-anti-fraud-tools-and-registration-flows-for-registrars/

this threshold of 20,000 is somewhat arbitrary and slightly different rankings would result from a different threshold.

Finally, the registrar data excludes ccTLD domains due to challenges in mapping domains to registrars in ccTLD ecosystems.

To account for the diversity of registrar credential sizes, we have reported low numbers of observed maliciously registered domains for both smaller (1-999,999 gTLD DUM) registrars (Table 1) and larger (1 million + gTLD DUM) registrars (Table 2). We note that this threshold of 1 million is somewhat arbitrary and slightly different rankings would result from a different threshold.

For higher numbers of highest observed maliciously registered domains per new domain registration, we have used one table (Table 6) and introduced a concept of consistency: a registrar credential will only be listed if they appear in this table of ten registrars for 4 or more of the last 6 months, otherwise they will be redacted. We attempt to contact all registrars in advance of publications, regardless of redaction. To further reduce the possibility of false positives, we also require a higher threshold of minimum malicious domain names for inclusion: more than 10 observed malicious domain names per month.

Data for this metric is presented in the following tables:

Table 4: Smaller volume: lowest observed rates of abuse

Inclusion criteria:

- Observed Maliciously Registered Domains: More than 5 per month
- Observed Newly Registered Domains: 300 - 20,000

Table 5: Higher volume lowest observed rates of abuse

Inclusion criteria:

- Observed Maliciously Registered Domains: More than 5 per month
- Observed Newly Registered Domains: Equal to or greater than 20,000

Table 6: Highest observed rates of abuse

Inclusion criteria:

- Observed Maliciously Registered Domains: More than 10 per month
- Observed Newly Registered Domains: Equal to or greater than 300
- Consistency: If a registrar does not appear in the list of 10 registrars with the highest percentage of new registrations observed as malicious 4 or more of the last 6 months, its data has been redacted.

For excluded data, see Appendices:

- Appendix A: Registrar Credentials With Zero Observed Maliciously Registered Domains
- Appendix B: Registrar Credentials With One to Five Observed Maliciously Registered
- Appendix C: Registrars With Registrars with Less Than 300 New Registrations per Month
- Appendix H: Brand Protection Registrars

Generic Top Level Domains (Tables 7-9)

This metric is intended to show the prevalence of observed maliciously registered domains in each gTLD.

When reported in raw numbers, the TLDs with the largest DUM will typically have the most observed maliciously registered domains. To create a benchmark which takes into account the different sizes of TLDs, we have reported the number of observed maliciously registered domains per 100,000 DUM. The observed abuse is a count of the number of unique domain names, not URLs.

We report on gTLDs and ccTLDs separately to reflect the fact that gTLDs have a consistent contractual framework,[9] are bound by consensus policies produced through the ICANN multistakeholder process, while ccTLDs are largely unique in their policies, processes, and governance models (e.g., nexus requirements, three-party contracts that include the ccTLD registry, only names for accredited businesses).

However, there is considerable policy, process, and business model diversity within gTLDs, any of which can influence abuse rates. For example, some gTLDs are brand-operated, closed for public registration, and have dozens of registrations, while others are operated by publicly traded companies, open for public registration, and have millions of registrations.

Our methodology observed a substantial number of gTLDs that have zero observed maliciously registered domains in the current month of reporting. There are several reasons for why a gTLD may have zero observed malicious domain names. Some TLD operators have specific and unique business models that may not translate to open gTLDs. For example, operating at very small volumes, maintaining a closed and exclusive number of customers, or applying human verification to every single domain name registration. This can result in very low concentrations of abuse, but is less helpful for generalizable information and not scalable to the wider ecosystem. Zero observed maliciously registered domains is likely not feasible for most gTLDs. Nevertheless, zero observed maliciously registered domains is still a laudable achievement. Accordingly, we have listed these TLDs in Appendix D: gTLDs with Zero Observed Maliciously Registered Domains.

While every effort has been made to reduce the chance of false positives (reports of malware or phishing that prove to be mistaken), it is impossible to

[9] Registry Agreement (RA); https://www.icann.org/en/registry-agreements/base-agreement Registrar Accreditation Agreement (RAA)
https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

entirely eliminate this risk. To minimize the impact of false positives, we have required a minimum number of observed maliciously registered domains per TLD. As very low numbers of observed malicious domain names is also a laudable result, we have included a list of these TLDs in Appendix E: gTLDs with One to Five Observed Maliciously Registered Domains.

To account for the diversity of gTLD registry sizes, we have reported low numbers of observed maliciously registered domains for both smaller (1 - 199,999 DUM) gTLDs (Table 7) and larger (200,000+ DUM) gTLDs (Table 8). We note that this threshold of 200,000 is somewhat arbitrary and slightly different rankings would result from a different threshold.

For higher numbers of observed maliciously registered domains, we have used one table (Table 9) and introduced a concept of consistency: a TLD will only be listed if they appear in this table of ten TLDs for 4 or more of the last 6 months, otherwise they will be redacted. We attempt to contact all TLDs in advance of publications, regardless of redaction. To further reduce the possibility of false positives, we also require a higher threshold of minimum malicious domain names for inclusion: more than 10 observed malicious domain names per month.

Data for this metric is presented in the following tables:

Table 7: Smaller gTLDs: lowest observed rates of abuse

Inclusion criteria:

- Observed Maliciously Registered Domains: More than 5 per month
- Observed DUM: 1 - 200,000

Table 8: Larger gTLDs: lowest observed rates of abuse

Inclusion criteria:

- Observed Maliciously Registered Domains: More than 5 per month
- Observed DUM: Equal to or more than 200,000

Table 9: gTLDs highest observed rates of abuse

Inclusion criteria:

- Observed Maliciously Registered Domains: More than 10 per month 27
- Consistency: If a TLD does not appear in the list of 10 TLDs with the highest observed maliciously registered domains per 100,000 DUM for 4 or more of the last 6 months, its data has been redacted

For excluded data, see Appendices:

- Appendix D: gTLDs with Zero Observed Maliciously Registered Domains
- Appendix E: gTLDs with One to Five Observed Maliciously Registered Domains

Country Code Top Level Domains (Table 10-12)

This metric is intended to show the prevalence of observed maliciously registered domains in each ccTLD.

When reported in raw numbers, the largest TLDs will typically have the most observed maliciously registered domains. To create a benchmark which takes into account the different sizes of TLDs we have reported the number of observed maliciously registered domains per 100,000 DUM. The observed abuse is a count of the number of unique domain names, not URLs.

We report on gTLDs and ccTLDs separately to reflect the fact that gTLDs have a consistent contractual framework[8], are bound by consensus policies produced through the ICANN multistakeholder process, while ccTLDs are largely unique in their policies, processes, and governance models (e.g.,

nexus requirements, three-party contracts that include the ccTLD registry, only names for accredited businesses).

This allows ccTLDs to create policies that are relevant and appropriate for their distinct local circumstances and population. This can still involve the use of multi-stakeholder processes, but is conducted by each individual country in line with its local regulations, values, languages, and expectations of the communities it serves. There is considerable diversity within the ccTLD community, so caution should be applied in comparing these TLDs.

Our methodology observed a substantial number of ccTLDs that have zero observed maliciously registered domains in the current month of reporting. There are several reasons for why a ccTLD may have zero observed malicious domain names. Some TLD operators have specific, unique, and typically untranslatable business models when applied to other ccTLDs or gTLDs. For example, operating at very small volumes, having a geographical nexus requirement, requiring a government identity number, restricting the number of domains available to each individual or business, or applying human or electronic identity verification to every domain name registration. This can result in very low concentrations of abuse, but is less helpful for generalizable information and not scalable to the wider ecosystem. Zero observed maliciously registered domains is likely not feasible for most TLDs. Nevertheless, zero observed maliciously registered domains is still a laudable achievement. Accordingly, we have listed these TLDs in Appendix F: ccTLDs with Zero Observed Maliciously Registered Domains.

While every effort has been made to reduce the chance of false positives, it is impossible to entirely eliminate this risk. To minimize the impact of false positives we have required a minimum number of observed maliciously registered domains per TLD. As very low numbers of observed malicious domain names is also a laudable result, we have included a list of these TLDs

in Appendix G: ccTLDs with One to Five Observed Maliciously Registered Domains.

To account for the diversity of ccTLD registry sizes, we have reported low numbers of observed maliciously registered domains for both smaller 1 - 999,999 DUM ccTLDs (Table 10) and larger 1,000,000+ DUM ccTLDs (Table 11). We note that this threshold of 1 million is somewhat arbitrary and slightly different rankings would result from a different threshold.

For higher numbers of observed maliciously registered domains, we have used one table (Table 9) and introduced a concept of consistency: a TLD will only be listed if they appear in this table of ten TLDs for 4 or more of the last 6 months, otherwise they will be redacted. We attempt to contact all TLDs in advance of publications, regardless of redaction. To further reduce the possibility of false positives, we also require a higher threshold of minimum malicious domain names for inclusion: more than 10 observed malicious domain names per month.

Data for this metric is presented in the following tables:

Table 10: Smaller ccTLDs: lowest observed rates of abuse

Inclusion criteria:

- Observed Maliciously Registered Domains: More than 5 per month
- Observed DUM: 1 - 999,999

Table 11: Larger ccTLDs: lowest observed rates of abuse

Inclusion criteria:

- Observed Maliciously Registered Domains: More than 5 per month
- Observed DUM: Equal to or more than 1 million

Table 12: ccTLDs: highest observed rates of abuse

Inclusion criteria:

- Observed Maliciously Registered Domains: More than 10 per month
- Consistency: If a TLD does not appear in the list of 10 TLDs with the highest observed maliciously registered domains per 100,000 DUM for 4 or more of the last 6 months, its data has been redacted

For excluded data, see Appendices:

- Appendix F: ccTLDs with Zero Observed Maliciously Registered Domains
- Appendix G: ccTLDs with One to Five Observed Maliciously Registered Domains

Background

The NetBeacon Institute ("Institute") was created in 2021 by Public Interest Registry ("PIR") in pursuit of its non-profit mission. The Institute aims to reduce DNS Abuse and empower the DNS Community.

This report is the Monthly Analysis from NetBeacon Measurement & Analysis Platform (MAP) ("NetBeacon Map"). This initiative is a collaboration with KOR Labs, led by Dr Maciej Korczynski a professor at Grenoble Alpes University in France. It focuses on the use of the Domain Name System (DNS) for phishing[10] and malware.[11]

Our priorities for NetBeacon MAP are:

- **Transparency**: The methodology that collects, cleans, and aggregates the data must be as transparent as possible. To the extent that anyone should wish to, they could replicate the process.
- **Credibility and Independence**: We aim to have an academically robust and independent approach, separate from commercial interests.
- **Accuracy and Reliability:** The goal of these reports is to enable focused conversations, and to identify opportunities for abuse reduction. The data needs to be of high enough quality to serve as the foundation for meaningful changes to the ecosystem.

In this Report, we provide General DNS Abuse Trends which are a snapshot of the interactive charts available on our website.

[10] **Phishing** is an attempt to trick people into sharing important or sensitive information – for example logins, passwords, credit card numbers or banking information – in either a personal or business context.

[11] **Malware** is malicious software designed to compromise a device on which it is installed.

We provide Specific Reporting which identifies registrars and Top Level Domains (TLDs) with high and low relative levels of malicious phishing and malware in their domains under management (DUM). We also identify registrars with higher and lower rates of malicious phishing and malware compared to new registrations.

We encourage all registrars and registries to get in contact with us and take the opportunity to view the data associated with their registrar or registry.

The Executive Summary provides monthly commentary and insight for the current report.

Our methodology is available on our website. It 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. If you would like to review your data, please contact: support@netbeacon.org

For clarity, NetBeacon MAP operates completely 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. See the methodology for more information on how domains are included in NetBeacon MAP.

Appendices

Appendices on exclusions are published on our website, they include:

Registrars

Appendix A: Registrar Credentials With Zero Observed Maliciously Registered Domains

Appendix B: Registrar Credentials With One to Five Observed Maliciously Registered Domains

Appendix C: Registrar Credentials With with Less Than 300 New Registrations per Month

Appendix H: Brand Protection Registrars

gTLDs

Appendix D: gTLDs with Zero Observed Maliciously Registered Domains

Appendix E: gTLDs with One to Five Observed Maliciously Registered Domains

ccTLDs

Appendix F: ccTLDs with Zero Observed Maliciously Registered Domains

Appendix G: ccTLDs with One to Five Observed Maliciously Registered Domains