Monthly Analysis

August 2024

Contents

Executive Summary

This publication of NetBeacon MAP: Monthly Analysis contains data from **June 2024.** See [Background](#) for more information on this initiative and the NetBeacon Institute.

Key highlights from our overall data include:

- **A significant month to month decrease in the number of unique domains being used for phishing.** Our methodology identified a 27% decrease in unique domains engaged in phishing attacks in June 2024, compared to May 2024 (from 34,728 to 25,537). This is more in line with our data in 2023, the average over 12 months was 22,262 unique domains per month. For context, our highest month on record to date is still 36,862 in September 2022 and the lowest is 18,794 in June 2023.
- **In malware distribution, the number of unique domains associated with this activity remained low.** June 2024 recorded 263 unique domains compared to 245 in May 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 slightly lower mitigation rates in June 2024, compared to May 2024.** Our methodology observed that 70% of the unique domains associated with phishing were mitigated and 68% of those associated with malware were mitigated, compared to 75%, and 82% in May 2024. However, we also observed a higher rate of 'uncategorized' mitigation in June. Our highest month on record for phishing is January 2023, 79% mitigation. Readers should be aware that these rates include compromised websites and maliciously registered domain names.
- **In terms of mitigation speed:** 54% of registrars had a median mitigation time of less than 48 hours, a slight month to month decrease

from 55%. These median mitigation times include compromised websites and maliciously registered domain names.

- **This month, 81% of unique domains used for phishing and 60% of unique domains used for malware distribution were classified as maliciously registered by our methodology. A slight increase for phishing, and a decrease for malware compared to last month (77% phishing, 62% malware).** 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):

- For understanding how phishing and malware is distributed across the ecosystem, we continue to include 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.
- For the first time since publishing these rates, we've noticed one ccTLD listed in both Table 10 (low observed abuse rates) and Table 12 (high observed abuse rates). This reflects the challenges of reporting on a limited number of TLDs. This month, based on our [inclusion and exclusion criteria](#) which include a requirement for a minimum amount of malicious abuse per month, 20 ccTLDs were eligible for Table 10 and 30 for Table 12. Table 10 ranges from 1.53 - 8.50, Table 12 ranges from 7.79 - 86.89. The ccTLD .vn had a malicious abuse rate of 7.79. We will keep this under review and are considering whether it would be beneficial for the community if we published the full list. We encourage

readers to look at the underlying rates, DUM and number of unique domains in each table when interpreting the data for additional context.

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

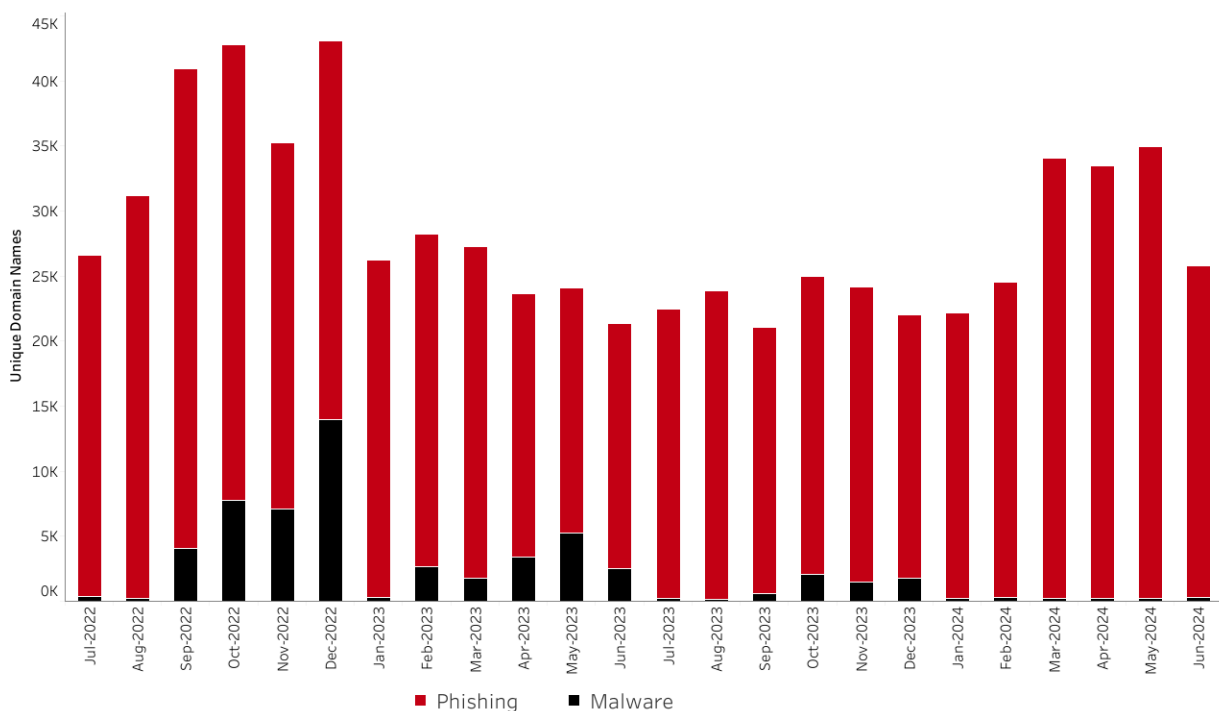*Figure 1: Aggregate Trends - **Phishing and Malware***

---

[1] Note: reporting is delayed by two months to allow for the measurement of mitigation.
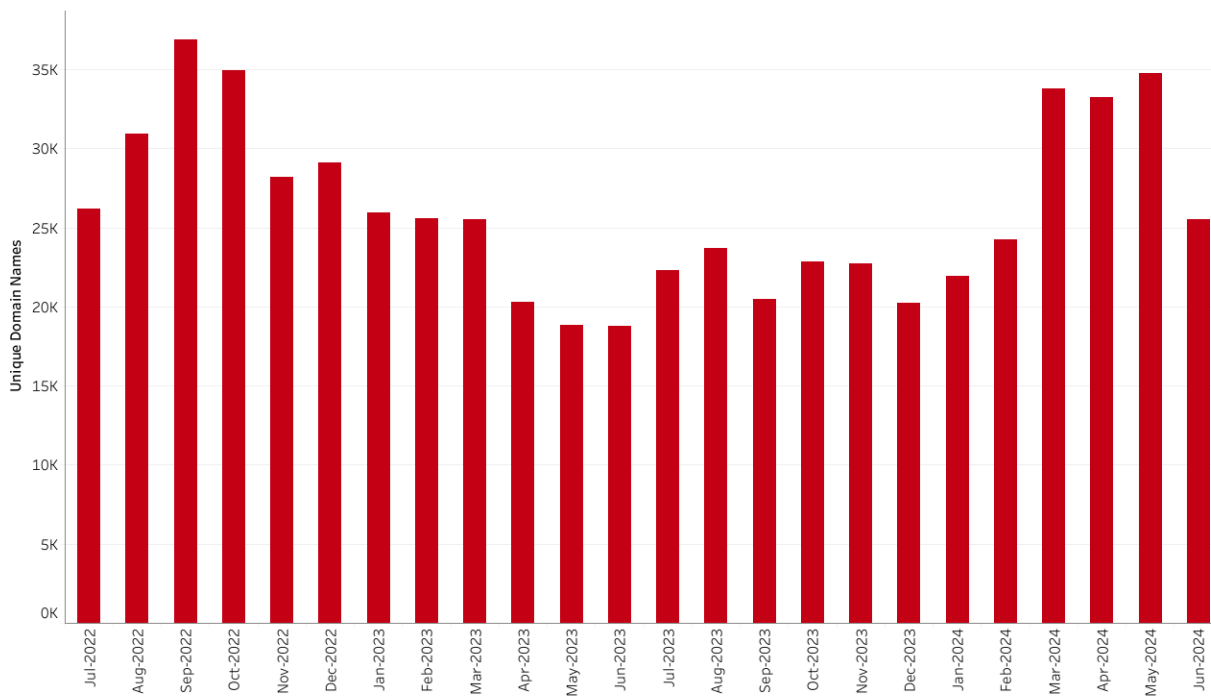
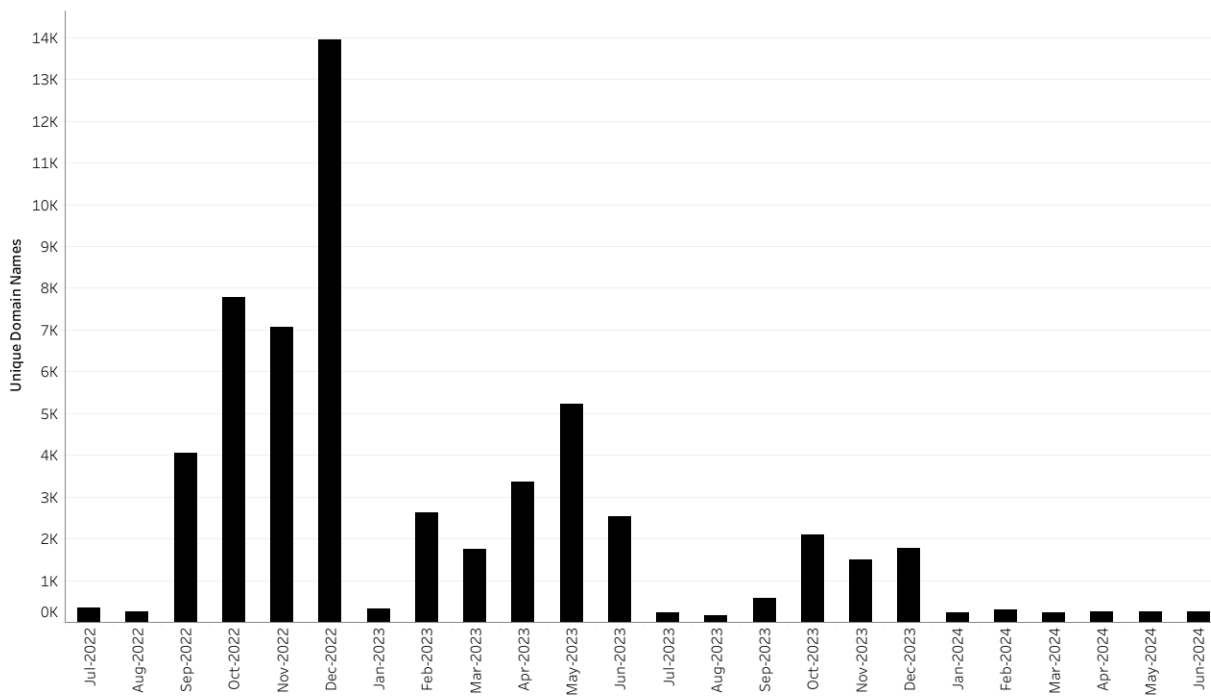*Figure 2: Aggregate Trends - **Phishing***

*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
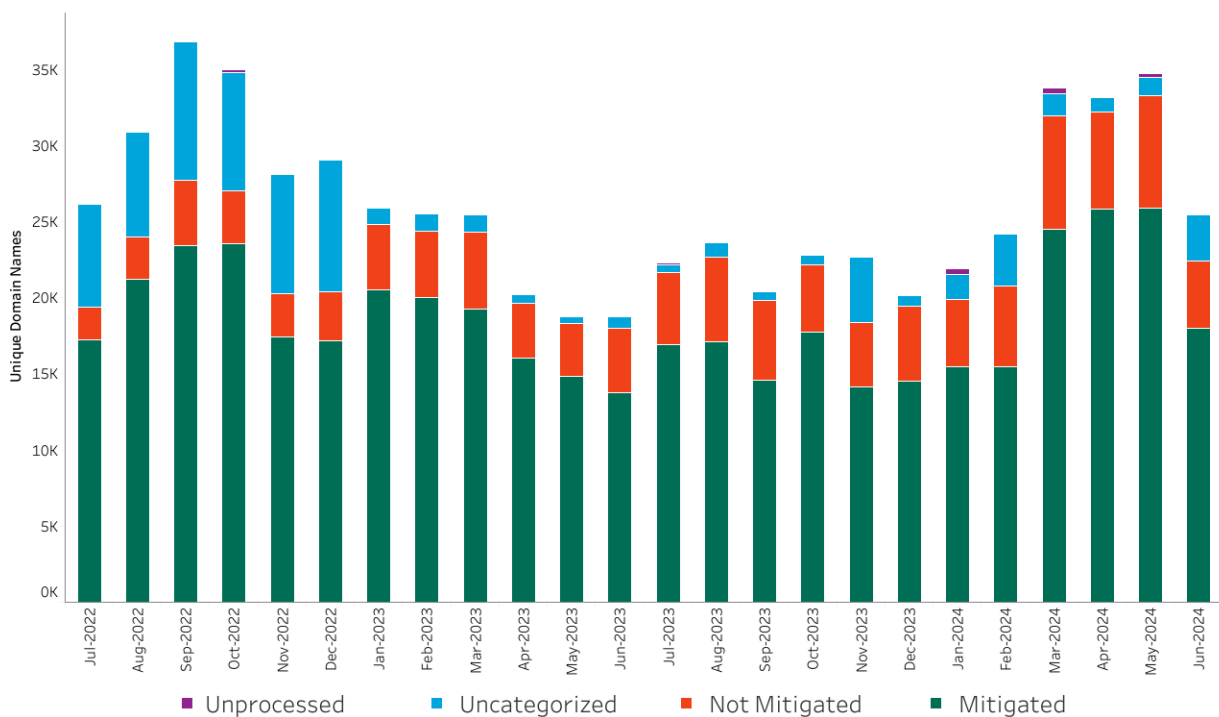
Figure 4: Mitigation - **Phishing**
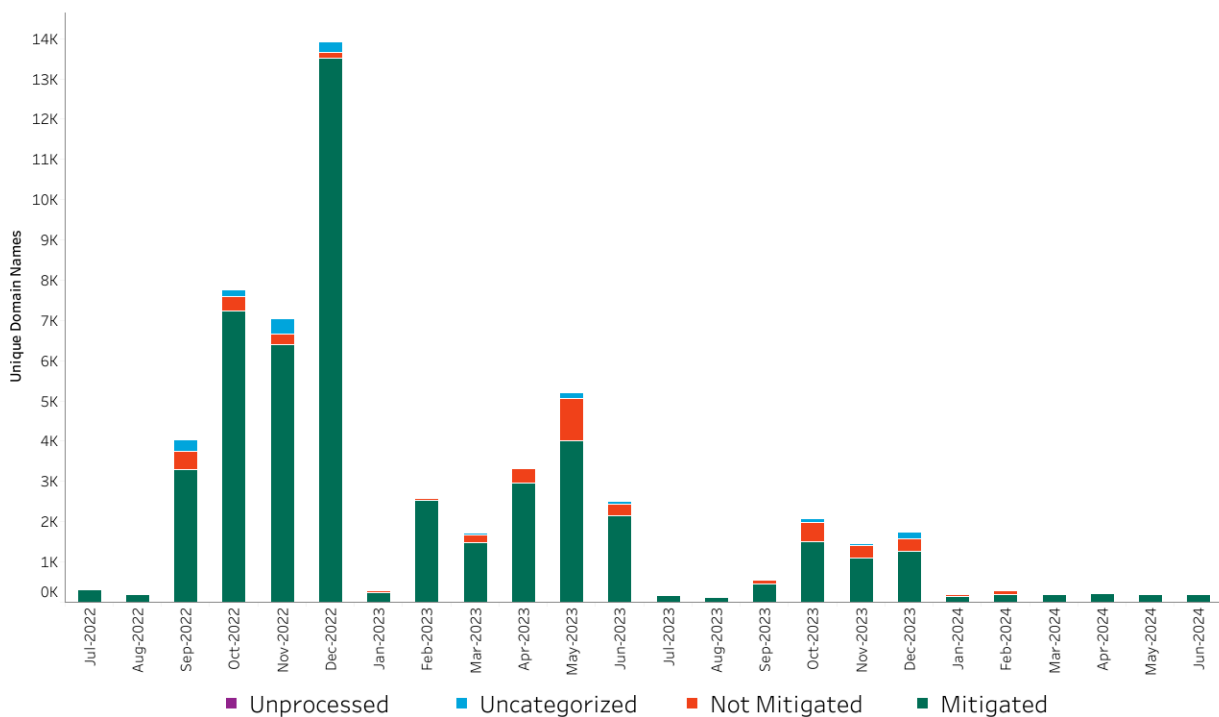
Figure 5: Mitigation - **Malware**

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](#)
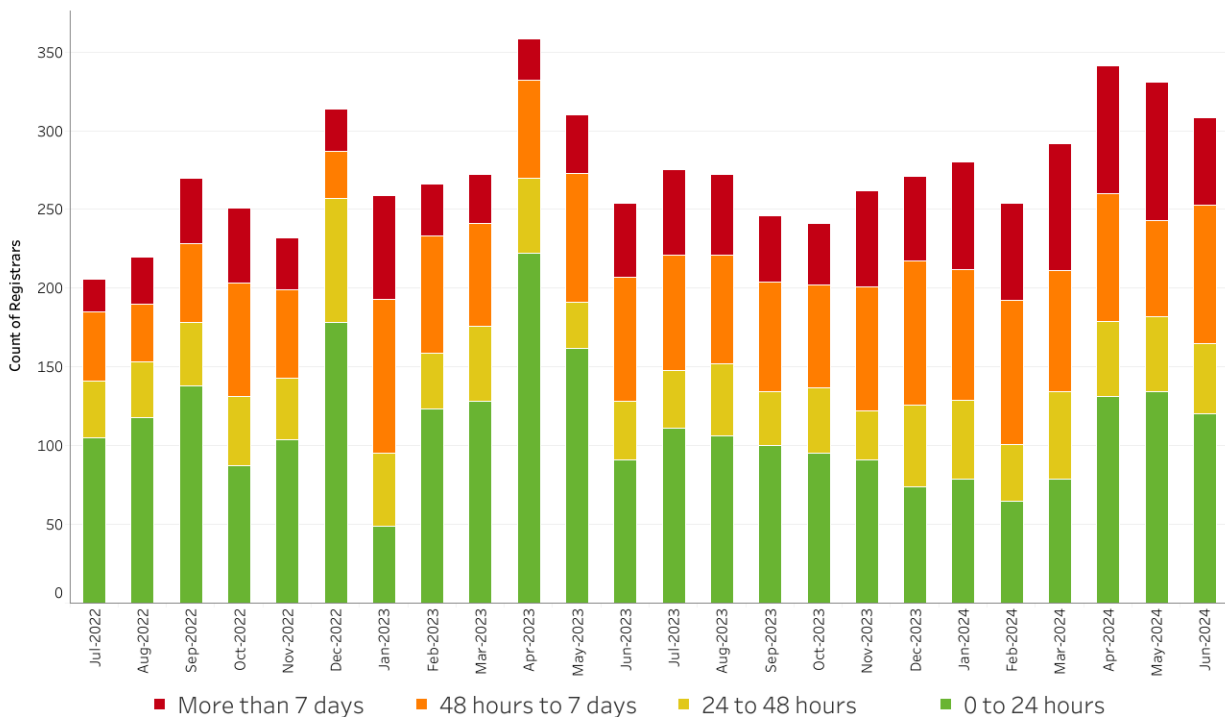
Figure 6: Registrar Median Mitigation Time
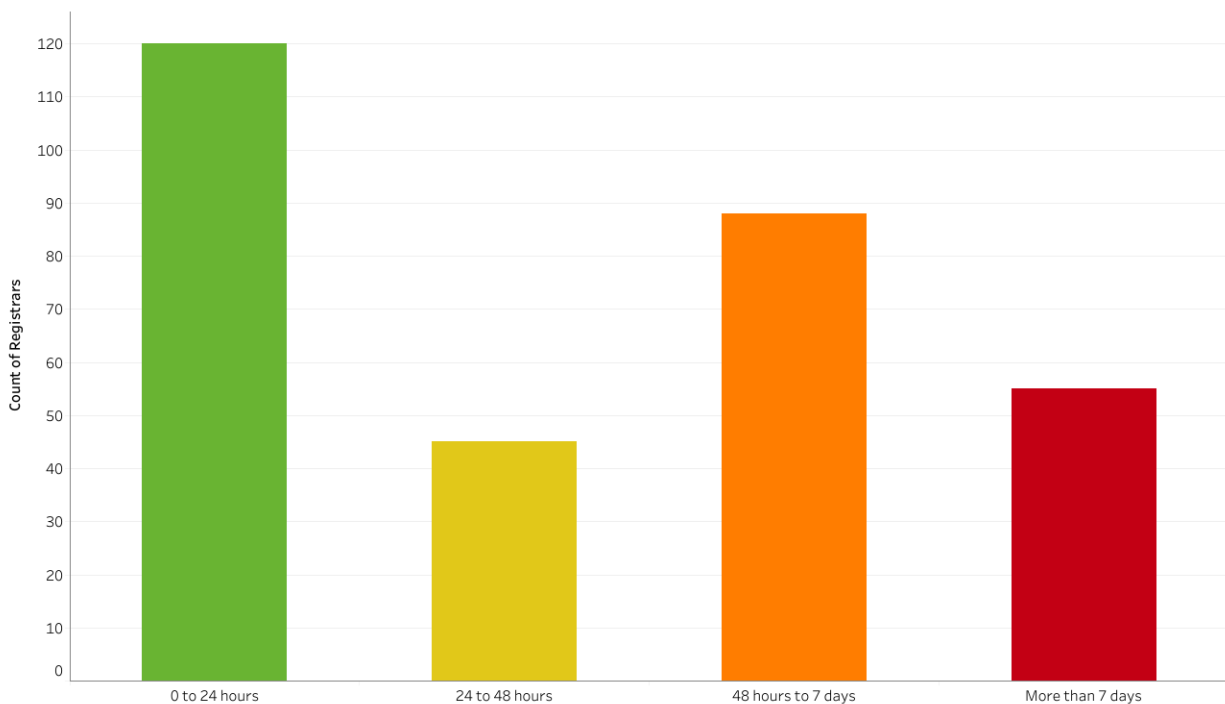
*Figure 7: Registrar Median Mitigation Time **2024-06***

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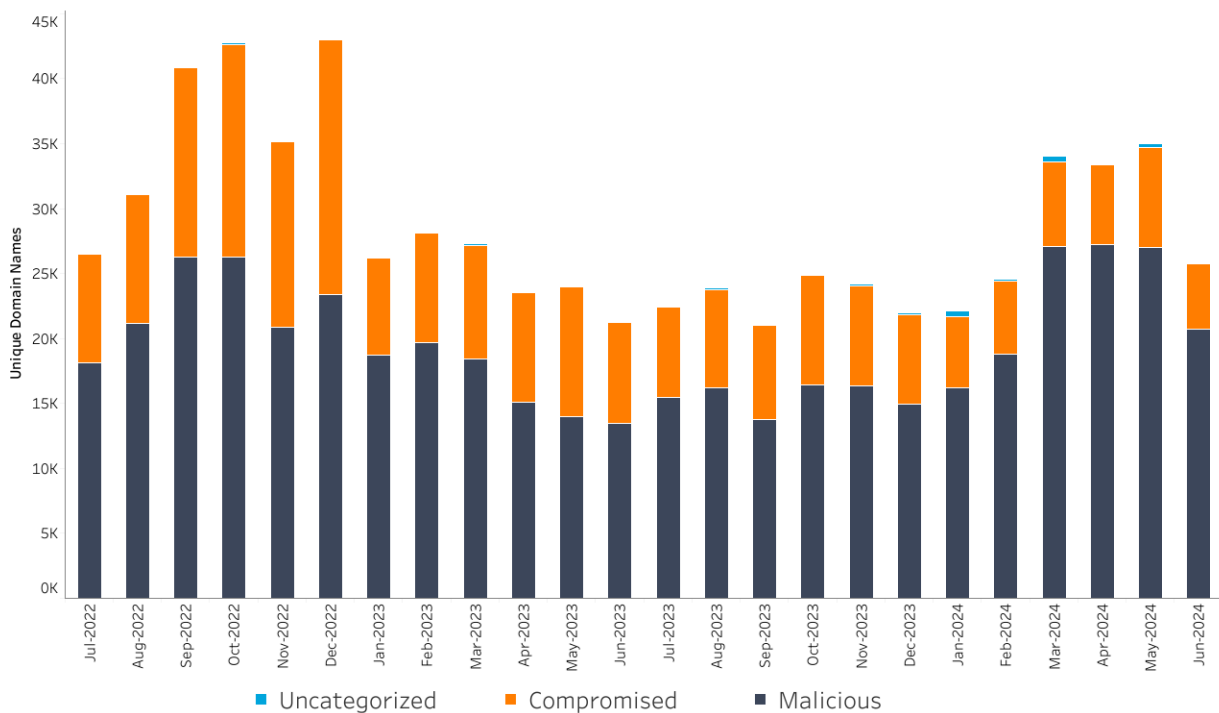
*Figure 8: Compromised vs Malicious - **Phishing and Malware***

*Figure 9: Compromised vs Malicious - **Phishing***
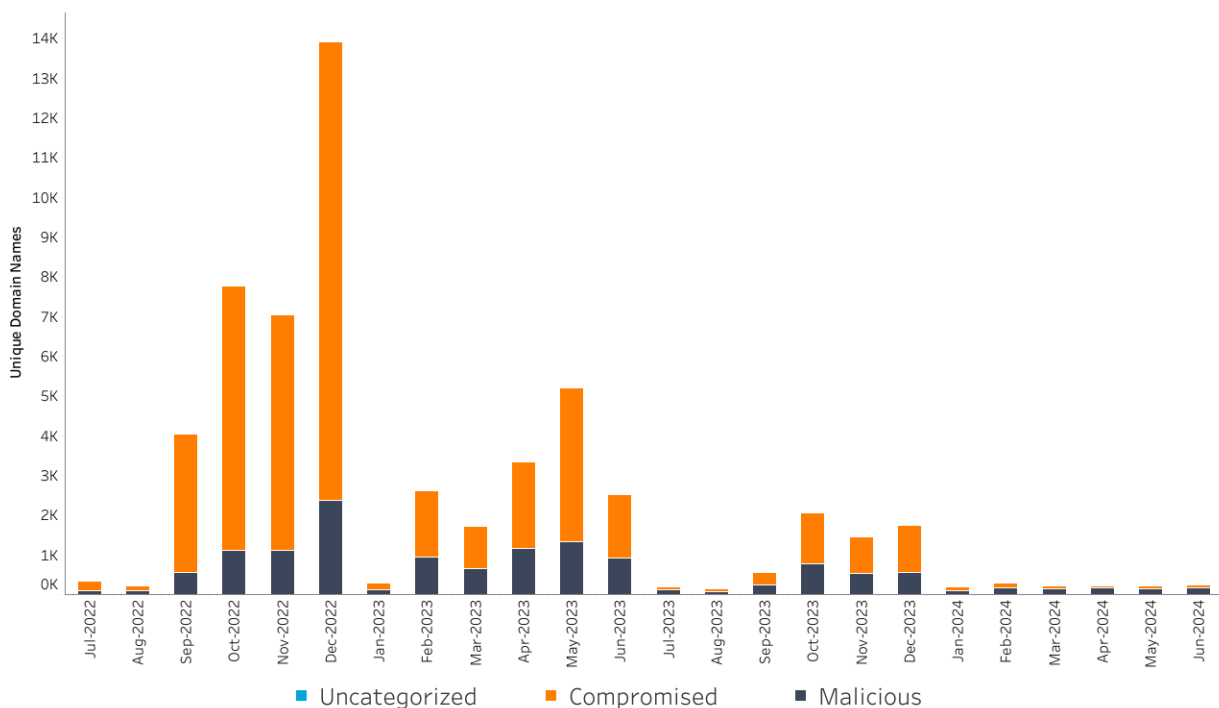
*Figure 10: Compromised vs Malicious - **Malware***

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.

---

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

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: DUM

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

Table 1: Smaller registrars: lowest observed rates of abuse 2024-06

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 - ..	0.87	7	808,125
1328	RegistryGate GmbH	1.26	7	554,182
1454	Nics Telekomunikasyon A.S.	1.43	6	419,817
431	DreamHost, LLC	2.62	19	725,486
168	Register SPA	2.66	17	640,089
1462	One.com A/S	2.77	11	397,436
65	DomainPeople, Inc.	3.01	6	199,210
3758	Hefei Juming Network Technology ..	3.10	6	193,658
13	Netregistry Wholesale Pty Ltd	3.80	6	157,992
2288	Metaregistrar BV	4.11	10	243,016

Table 2: Larger registrars: lowest observed rates of abuse 2024-06

IANA ID	Registrar Credential	Observed Maliciously Registered Domains Per 100,000 gTLD DUM	Observed Malicious gTLD Domains	Observed gTLD DUM
420	Alibaba Cloud Computing (Beijing) Co..	0.36	8	2,249,148
433	OVH sas	0.48	10	2,069,730
886	Domain.com, LLC	0.49	8	1,618,556
141	Cronon GmbH	0.62	7	1,128,605
9	Register.com, Inc.	0.63	9	1,428,428
81	Gandi SAS	0.80	8	1,005,498
83	IONOS SE	0.93	41	4,426,796
895	Squarespace Domains II LLC	0.94	70	7,475,686
1154	FastDomain Inc.	0.95	17	1,791,589
440	Wild West Domains, LLC	1.04	24	2,298,662

Table 3: Highest observed rates of abuse 2024-06

IANA ID	Registrar Credential	Observed Maliciously Registered Domains Per 100,000 gTLD DUM	Observed Malicious gTLD Domains	Observed gTLD DUM	Number of Months
3765	NICENIC INTERNATIONAL GR...	664.39	339	51,024	6
3775	ALIBABA.COM SINGAPORE E-...	397.54	1,066	268,151	6
3862	Spaceship, Inc.	138.39	888	641,650	5
3858	Aceville Pte. Ltd.	108.52	116	106,889	6
1250	OwnRegistrar, Inc.	103.60	334	322,380	6
1556	Chengdu West Dimension Di...	88.72	731	823,916	5
Redacted	*Redacted*	49.69	*	*	1
Redacted	*Redacted*	47.48	*	*	1
Redacted	*Redacted*	46.62	*	*	1
Redacted	*Redacted*	42.26	*	*	2

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 2024-06

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
433	OVH sas	0.05%	10	18,235	2,069,730
1454	Nics Telekomunikasyon A..	0.06%	6	10,124	419,817
141	Cronon GmbH	0.06%	7	10,789	1,128,605
1462	One.com A/S	0.07%	11	16,893	397,436
1621	Shanghai Meicheng Tech..	0.08%	9	11,443	129,842
81	Gandi SAS	0.09%	8	9,035	1,005,498
65	DomainPeople, Inc.	0.09%	6	6,743	199,210
9	Register.com, Inc.	0.09%	9	9,749	1,428,428
638	Name SRS AB	0.09%	12	12,782	193,988
1420	INWX GmbH	0.10%	18	17,834	156,463

Table 5: Higher volume: lowest observed rates of abuse 2024-06

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
3827	Squarespace Domains LLC	0.04%	37	98,518	2,072,004
1861	Porkbun LLC	0.05%	41	83,618	1,319,091
83	IONOS SE	0.09%	41	46,341	4,426,796
146	GoDaddy.com, LLC	0.09%	706	745,138	61,027,333
895	Squarespace Domains II LLC	0.10%	70	66,857	7,475,686
440	Wild West Domains, LLC	0.11%	24	21,320	2,298,662
468	Amazon Registrar, Inc.	0.12%	25	20,669	1,395,752
48	eNom, LLC	0.13%	42	32,332	3,360,958
49	GMO Internet Group, Inc. d/..	0.13%	171	130,441	4,114,421
839	Realtime Register B.V.	0.14%	39	27,979	719,737

Table 6: Highest observed rates of abuse 2024-06

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.	11.57%	116	1,003	106,889	6
Redacted	*Redacted*	8.29%	*	*	*	2
3775	ALIBABA.COM SINGAPO..	7.84%	1,066	13,597	268,151	6
3765	NICENIC INTERNATION..	5.82%	339	5,829	51,024	6
1556	Chengdu West Dimensi..	4.17%	731	17,530	823,916	4
Redacted	*Redacted*	2.46%	*	*	*	1
Redacted	*Redacted*	1.90%	*	*	*	1
1923	Gname.com Pte. Ltd.	1.78%	1,401	78,880	4,340,450	4
Redacted	*Redacted*	1.69%	*	*	*	1
1469	Jiangsu Bangning Scien..	1.66%	15	903	126,353	4

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 2024-06

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
tokyo	6.07	11	181,139
services	7.25	6	82,747
agency	8.02	9	112,261
bio	8.13	6	73,843
fyi	9.52	6	62,994
ltd	10.06	12	119,302
win	10.70	10	93,468
wiki	12.98	8	61,644
network	14.30	11	76,942
digital	15.13	20	132,188

Table 8: Larger gTLDs: lowest observed rates of abuse 2024-06

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
org	2.59	282	10,906,446
net	2.95	382	12,950,843
today	3.00	10	333,801
bond	3.36	11	327,726
blog	3.49	9	258,243
store	3.51	52	1,480,572
tech	3.88	18	463,421
biz	4.16	51	1,227,428
com	4.16	6,606	158,650,260
space	4.22	15	355,161

Table 9: gTLDs: highest observed rates of abuse 2024-06

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM	Number of Months
fit	111.70	39	34,914	6
Redacted	103.62	*	*	1
Redacted	89.74	*	*	3
Redacted	86.36	*	*	1
top	80.97	2,247	2,774,985	6
Redacted	64.25	*	*	3
Redacted	64.03	*	*	3
Redacted	60.55	*	*	3
Redacted	54.79	*	*	1
Redacted	50.54	*	*	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 2024-06

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
ar	1.53	8	524,215
pw	1.71	6	350,736
ai	1.81	8	441,304
tv	1.85	8	433,039
cl	2.02	11	543,469
tr	3.09	30	971,063
ke	7.25	7	96,565
vn	7.79	41	526,111
pe	7.88	10	126,905
ng	8.50	15	176,378

Table 11: Larger ccTLDs: lowest observed rates of abuse 2024-06

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
nl	0.23	14	5,988,471
it	0.34	11	3,211,709
jp	0.35	6	1,708,594
ca	0.36	12	3,307,204
be	0.37	6	1,642,303
de	0.41	70	16,911,169
au	0.42	17	4,083,442
at	0.62	9	1,459,709
ch	0.63	16	2,551,395
za	0.77	10	1,301,798

Table 12: ccTLDs: highest observed rates of abuse 2024-06

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM	Number of Months
id	86.89	639	735,381	6
Redacted	74.89	*	*	2
Redacted	20.21	*	*	1
cc	17.96	229	1,275,369	6
kz	13.29	24	180,634	6
su	10.64	11	103,368	5
cn	9.26	767	8,279,976	6
Redacted	8.73	*	*	2
Redacted	8.50	*	*	1
vn	7.79	41	526,111	6

About General DNS Abuse Trends

These charts are available in an interactive format on <u>our website:</u>

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