DNSAI Compass

January 2024

Table of Contents

Contents **2**

Executive Summary **3**

About **4**
Understanding this report 5

General DNS Abuse Trends **6**
Chart 1: Aggregate Trends 6
About this chart 6
Commentary 7
Chart 2: Mitigation 8
About this chart 8
Commentary 9
Chart 3: Registrar Median Mitigation Time 10
About this chart 10
Commentary 11
Chart 4: Malicious vs. Compromised 12
About this chart 12
Commentary 13

Specific Reporting 14
Registrars 19
Registries 22
Appendices 29

Executive Summary

This report is the seventeenth publication from the DNS Abuse Institute's measurement initiative DNSAI Compass.

The 'General DNS Abuse Trends' section of this report sees a decrease in observed levels of malware distribution in November 2023, compared to October 2023. Observed phishing remained similar.

This is the eight month we have included ‘Specific Reporting’, this is intended to show the spectrum of how malicious phishing and malware is concentrated across the DNS registration ecosystem. It identifies registrars and TLDs with higher and lower relative volumes of malicious domain registration in their Domains Under Management (DUM), or new registrations. The Specific Reporting section of this report contains data for September 2023.

Our outreach work continues across the DNS Community. 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. These meetings typically yield insights for both the registry or registrar and the DNSAI.

The methodology for this report is the same as all prior reports (v1.0) and we encourage readers to consider this detailed methodology and contact us with questions, ideas, or suggestions to help us improve this initiative. After all, we are here to support the DNS Community and make it better equipped to tackle DNS Abuse.

The DNS Abuse Institute publishes interactive charts and reports periodically.

About

The DNS Abuse Institute[1] (DNSAI or the "Institute") was created in 2021 by Public Interest Registry[2] ("PIR") in pursuit of its non-profit mission. The Institute aims to reduce DNS Abuse and empower the DNS Community.

The Institute created DNSAI Compass ("Compass") as a reliable, independent, transparent, and sufficiently granular way of measuring DNS Abuse in order to ultimately reduce it at the DNS level.

Compass is a collaboration with KOR Labs[3], led by Maciej Korczynski[4] from Grenoble INP-UGA. This data is then provided to the DNSAI. DNSAI then works with PIR's Data Analytics team to create the interactive charts and for the purposes of writing this report.

Our priorities for Compass 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.

Our first report from September 2022[5] provides the methodology and further context on the background and development of this initiative.

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 us[6].

For clarity, Compass operates completely independently of NetBeacon[7], the centralized abuse reporting service we created for the benefit of the DNS. Reports from NetBeacon do not go into our measurement work with Compass. This is a conscious choice to optimize and encourage usage of NetBeacon and prevent any abuse of NetBeacon as an attempt to influence Compass data. See the methodology[8] for more information on how domains are included in Compass.

[1] https://dnsabuseinstitute.org/
[2] https://thenew.org/org-people/
[3] https://korlabs.io/
[4] https://mkorczynski.com/
[5] https://dnsabuseinstitute.org/wp-content/uploads/2022/09/DNSAI-Intelligence-Report-September-2022-FINAL.pdf
[6] https://dnsabuseinstitute.org/contact/
[7] https://netbeacon.org/
[8] DNSAI-Compass-Methodology.pdf (dnsabuseinstitute.org)

Understanding this Report

This report shows high level aggregate data from **December 2022 to November 2023.**

It focuses on the use of the DNS for phishing and malware:

- **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.

It includes the following charts:

- **Chart 1: Aggregate Trends**
- **Chart 2: Mitigation**
- **Chart 3: Registrar Median Mitigation Time**
- **Chart 4: Malicious vs. Compromised**

Our methodology provides important context and we recommend it is read in full.

Each chart is accompanied by:

- **‘About this Chart’** to help the reader understand the data being displayed, and;
- **‘Commentary’** where we have added any observations on the data.

Where we are showing data over time, the intent is to try and demonstrate trends, year over year, and we are therefore hoping to be able to display about two years of data depending on functionality and viewability.

General DNS Abuse Trends

These charts are available in an interactive format on our website: https://dnsabuseinstitute.org/dnsai-compass

They provide a broad overview of our findings on DNS Abuse trends.

Chart 1: Aggregate Trends

About this chart

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 are engaged in phishing and malware, broken out by category.

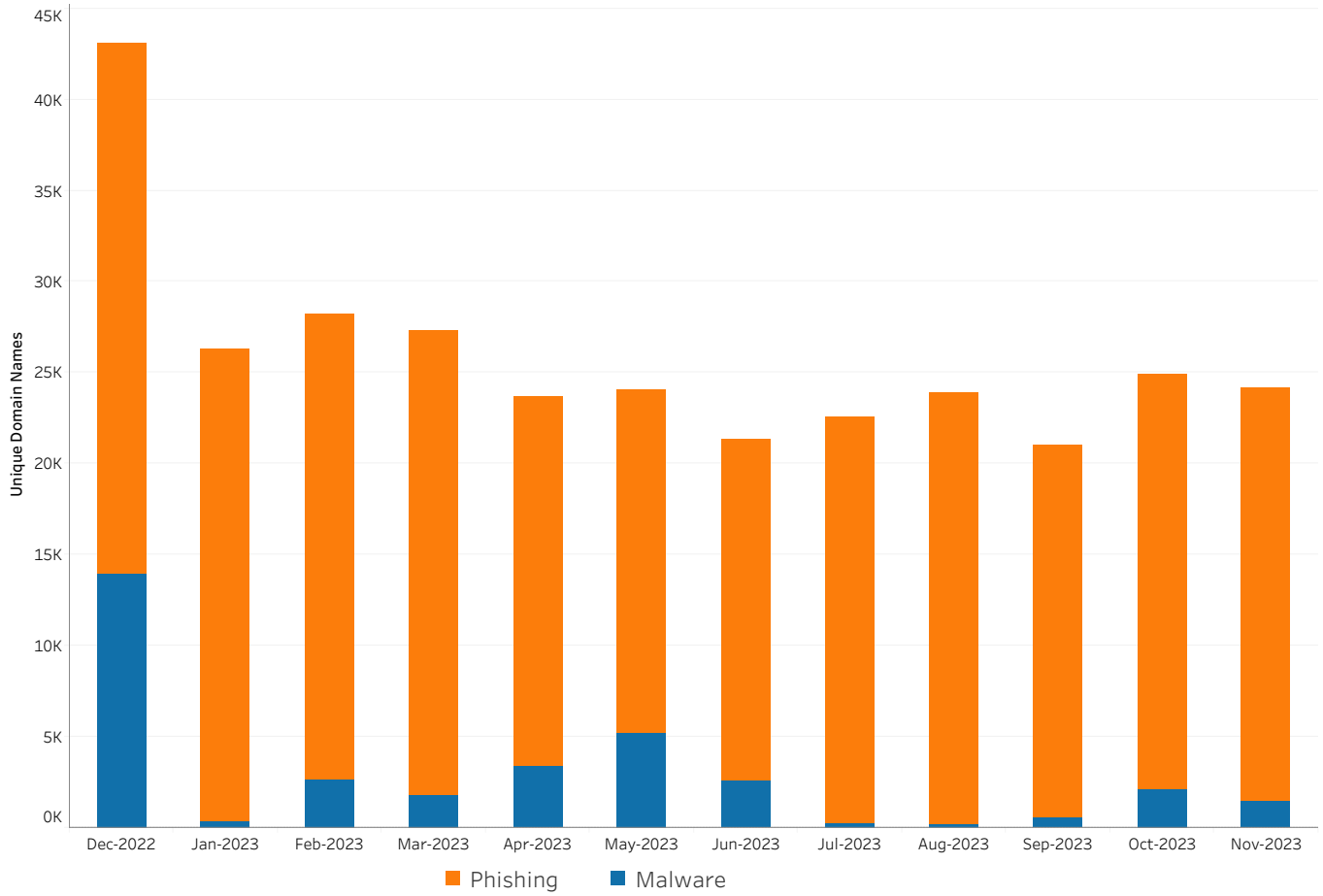

*Figure 1: Aggregate Trends - **Phishing and Malware***

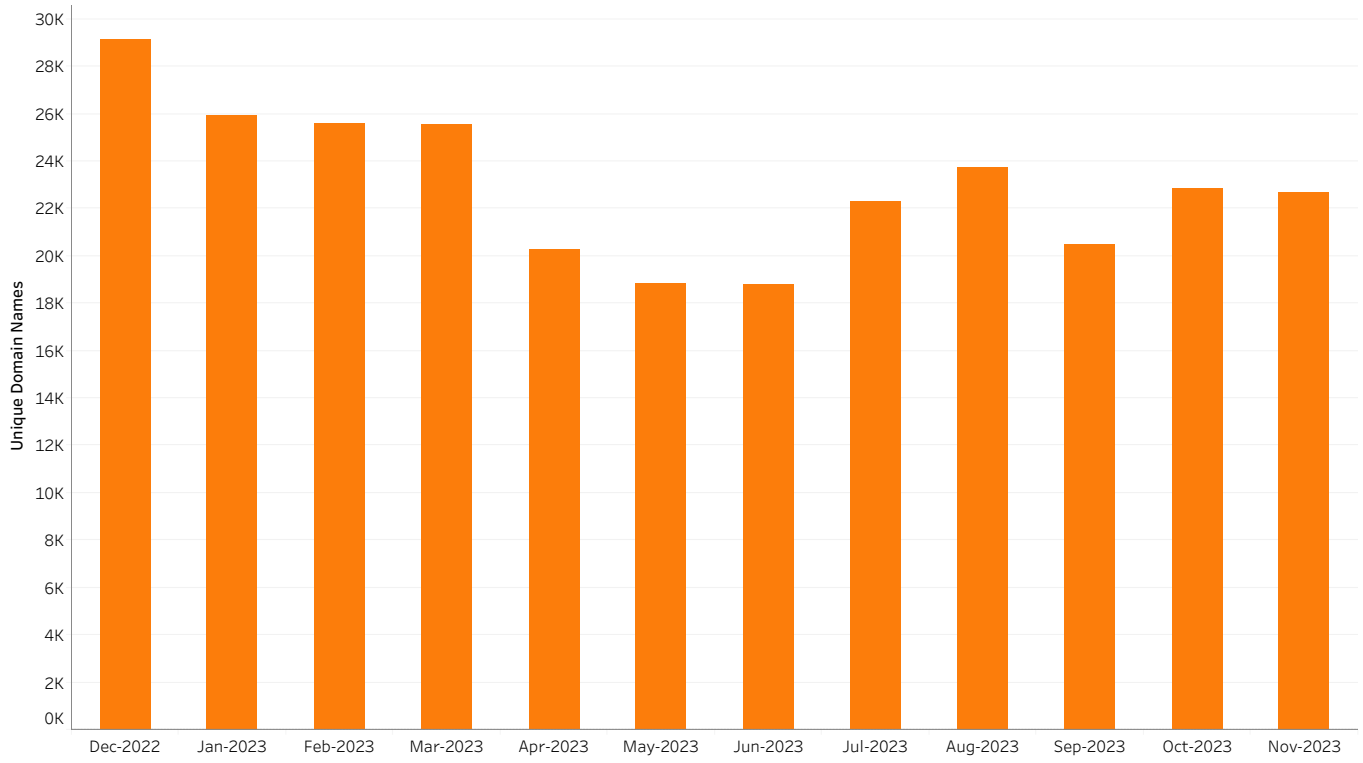

*Figure 2: Aggregate Trends - **Phishing***

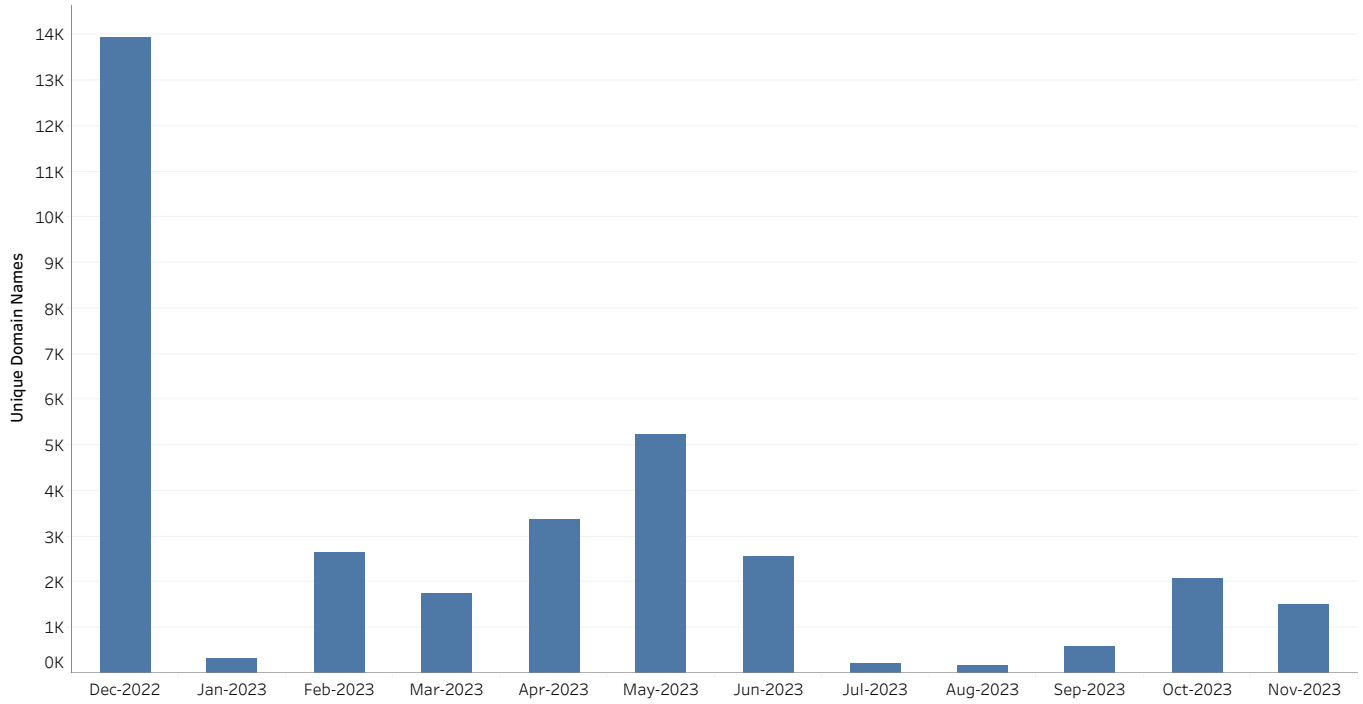

*Figure 3: Aggregate Trends - **Malware***

Commentary

Our methodology observed a decrease in the number of unique domains engaged in malware distribution in November 2023, compared to October 2023. Observed phishing in November 2023 (22,842) remained similar October 2023 (22,703). More detailed information is available in the interactive charts on our website: https://dnsabuseinstitute.org/dnsai-compass/

Chart 2: Mitigation

About this chart

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.

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.

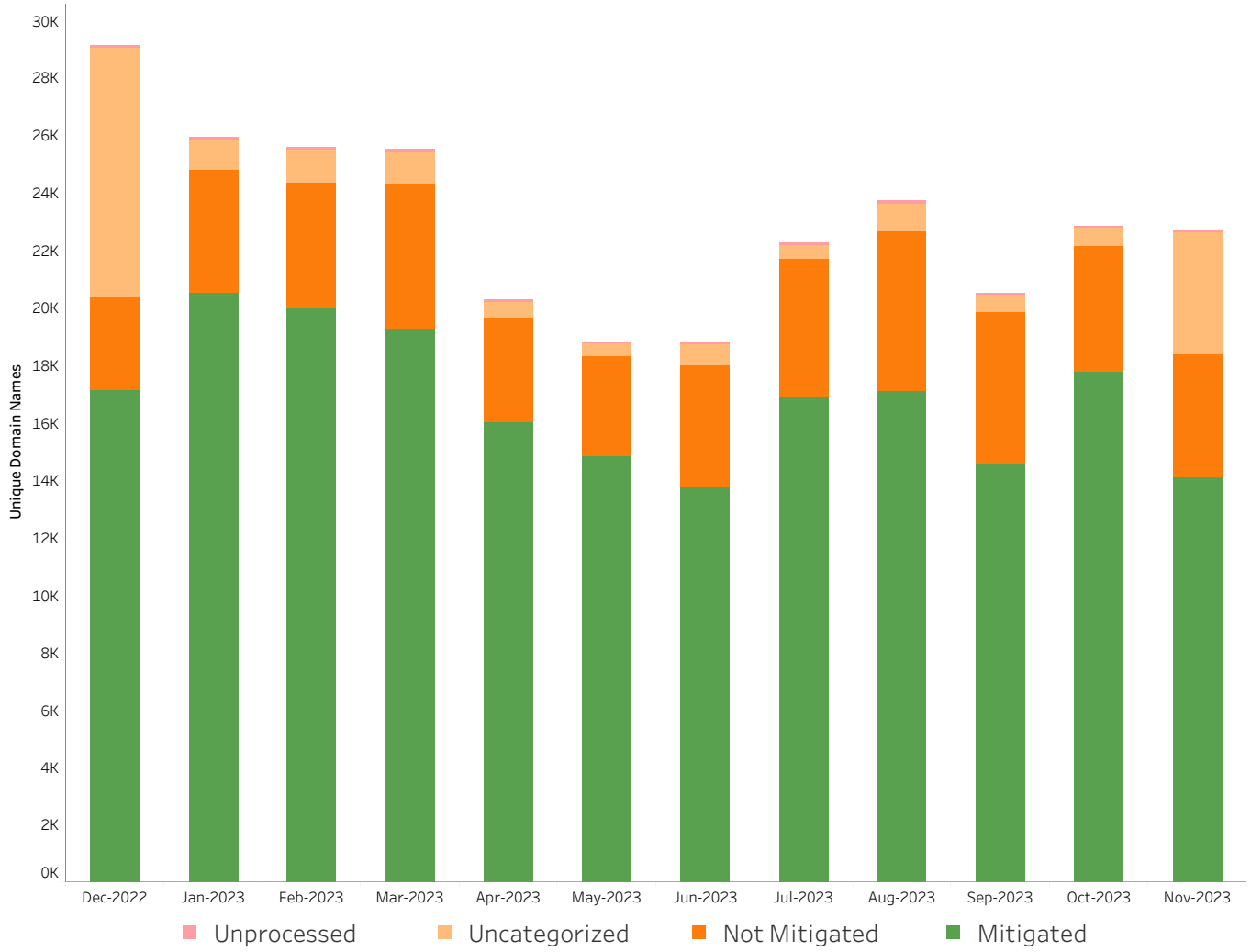

*Figure 4: Mitigation - **Phishing***

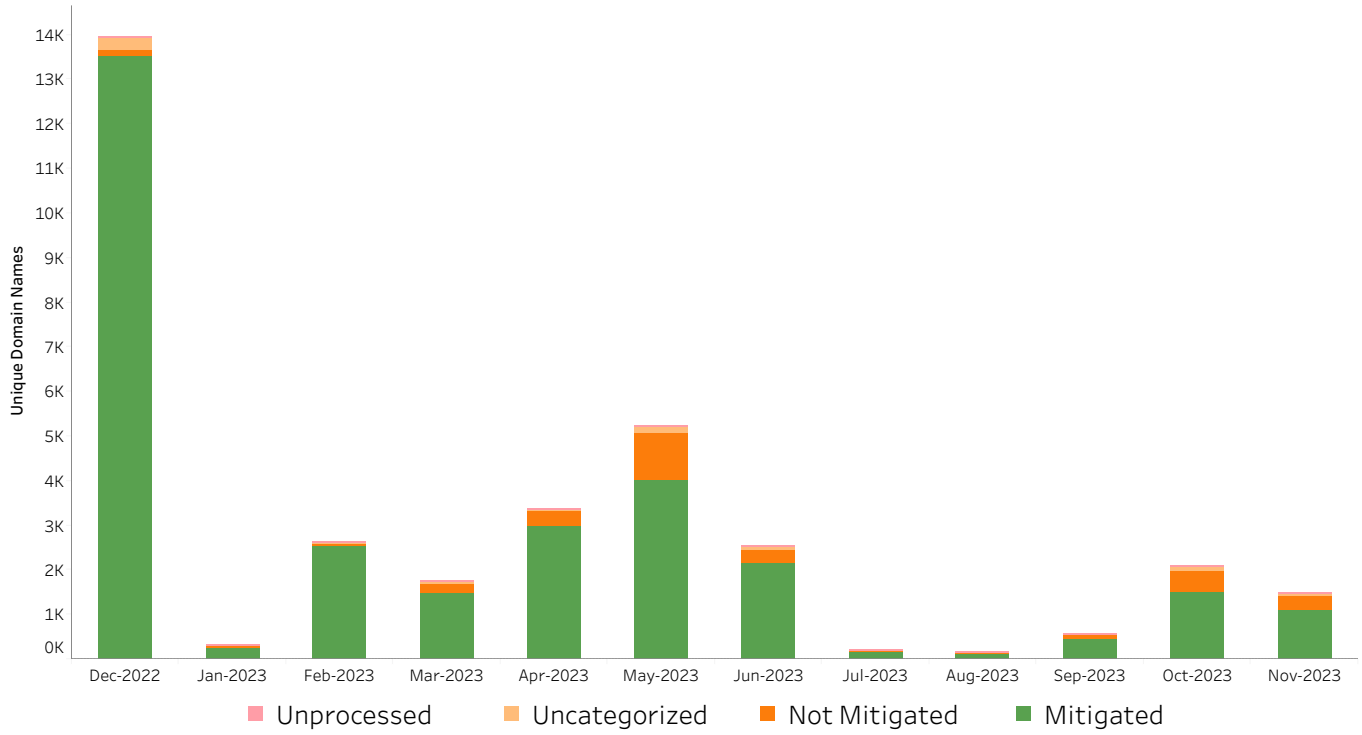

*Figure 5: Mitigation - **Malware***

Commentary

More detailed information is available in the interactive charts on our website: https://dnsabuseinstitute.org/dnsai-compass/

Chart 3: Registrar Median Mitigation Time

About this chart

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.

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, 24hr, 36hr, 48hr, 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.

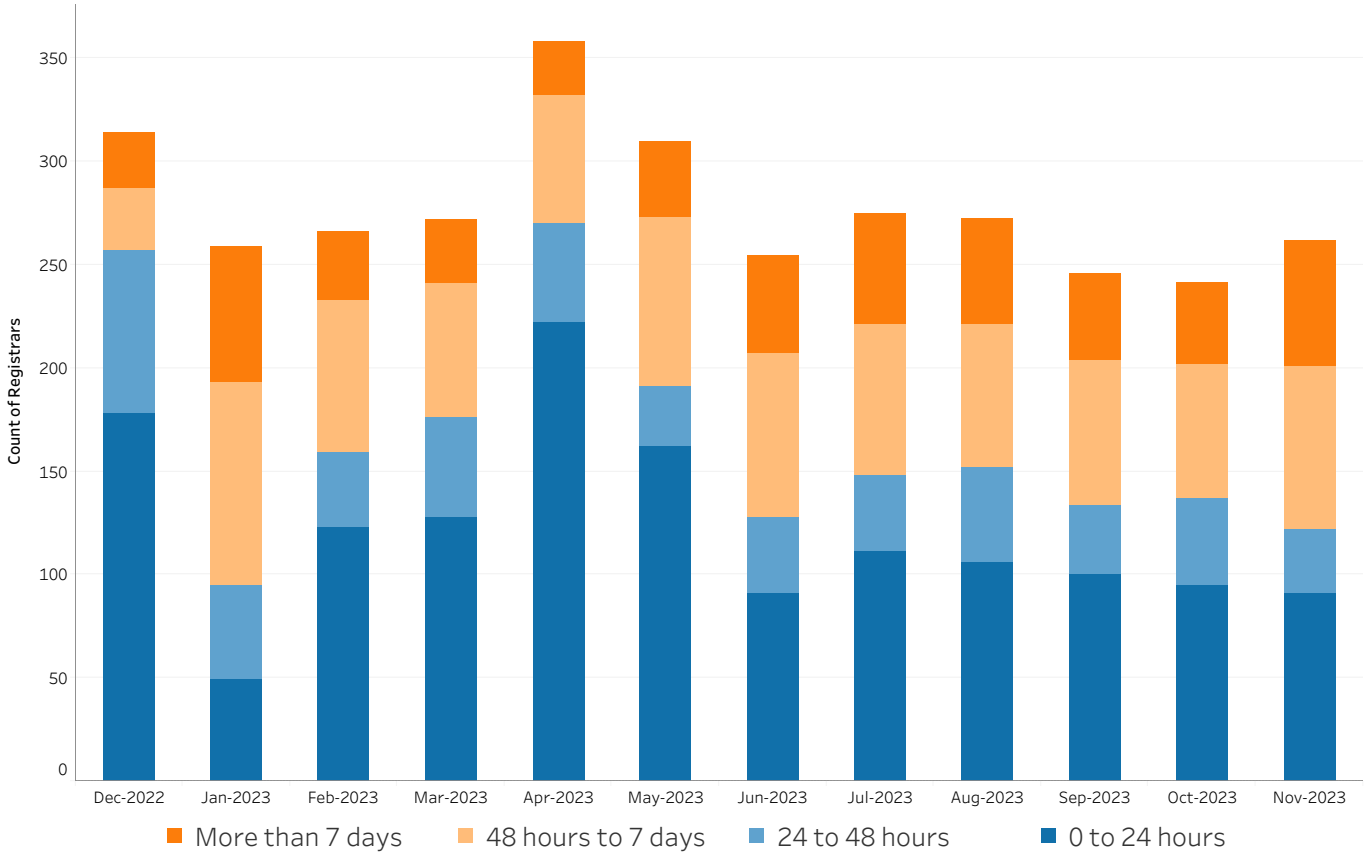

Figure 6: Registrar Median Mitigation Time

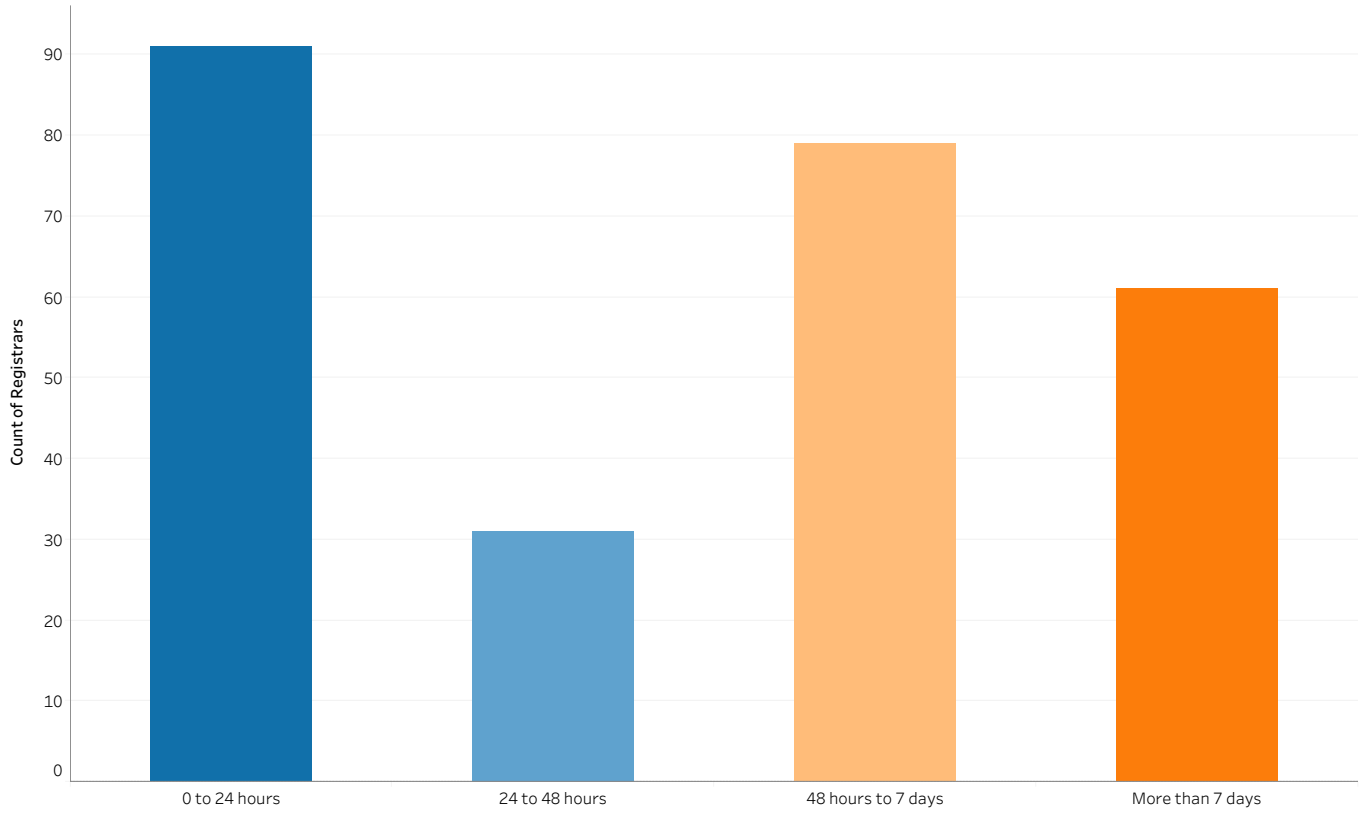

*Figure 7: Registrar Median Mitigation Time **2023-11***

Commentary

There is no agreed upon industry standard for how quickly mitigation should occur. This makes the presentation of mitigation time challenging. We believe there is a general industry view that mitigation within 24 hours is considered a quick response to sufficient evidence of phishing or malware. As phishing and malware are quite time-sensitive issues, with most harm happening at the start of the attack, we believe that mitigation after 7 days is not quick enough to prevent and disrupt harm, which is why we have included “More than 7 days” as a specific category.

More detailed information is available in the interactive charts on our website: www.dnsabuseinstitute.org

Chart 4: Malicious vs. Compromised

About this chart

This chart is intended to show the observed registration type (malicious vs. compromised) and how this is changing over time.

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.

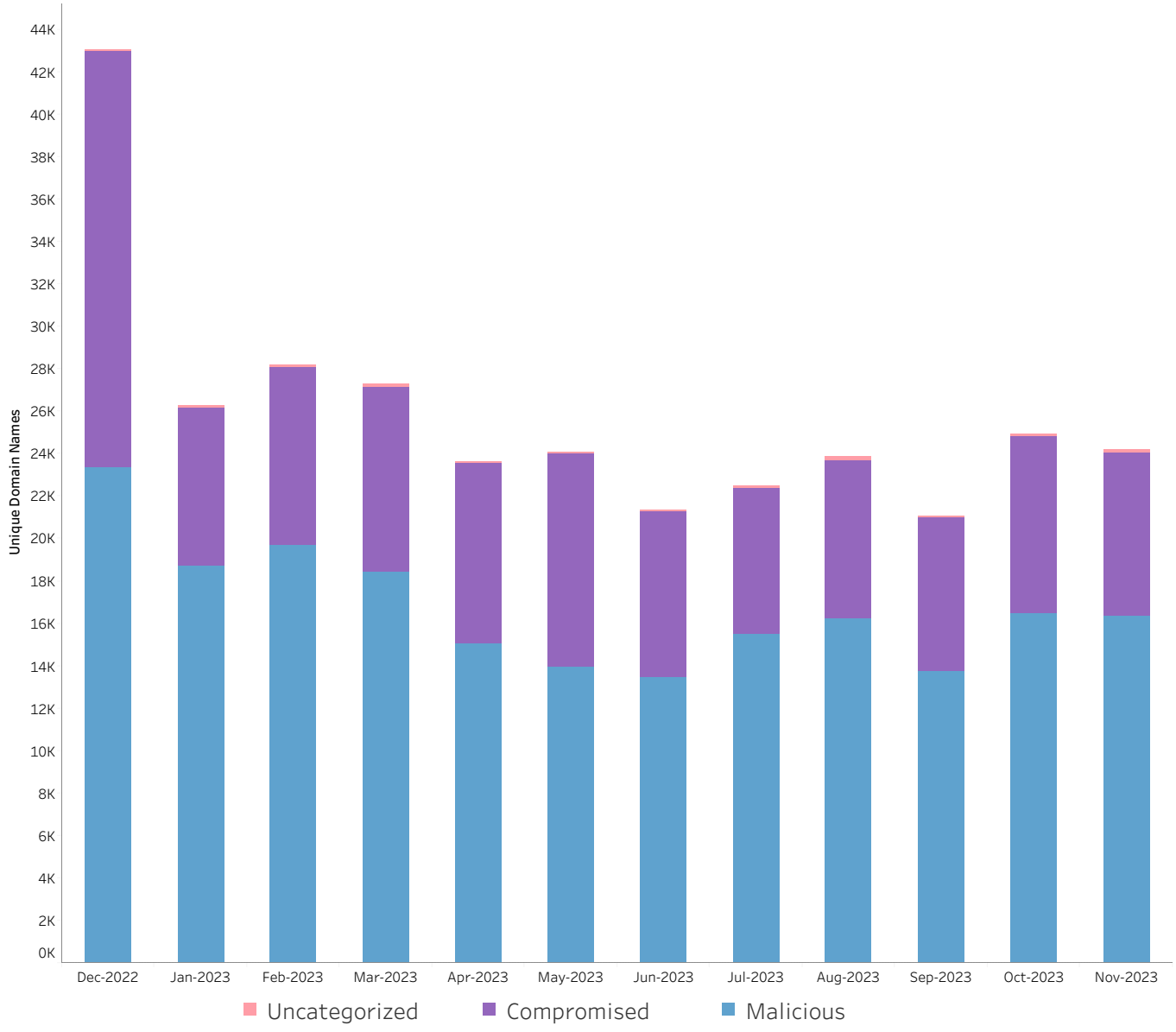

*Figure 8: Compromised vs Malicious - **Phishing and Malware***

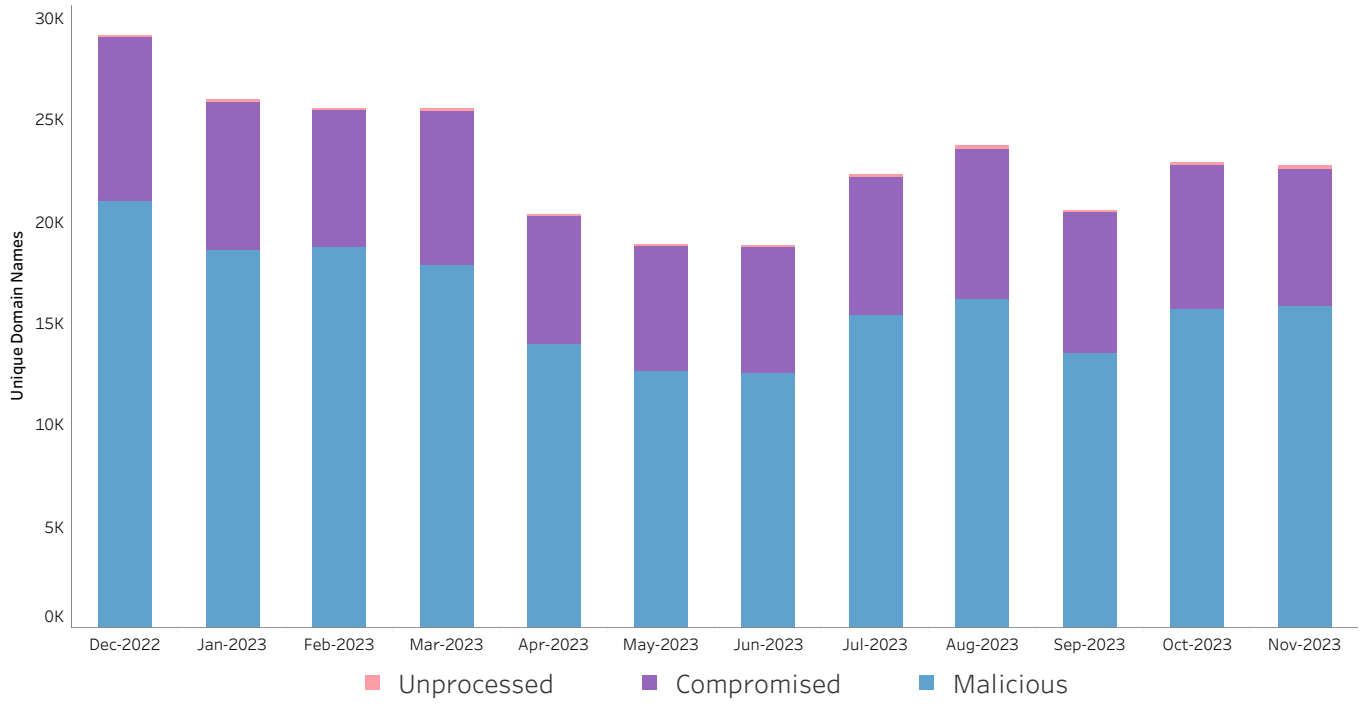

*Figure 9: Compromised vs Malicious - **Phishing***

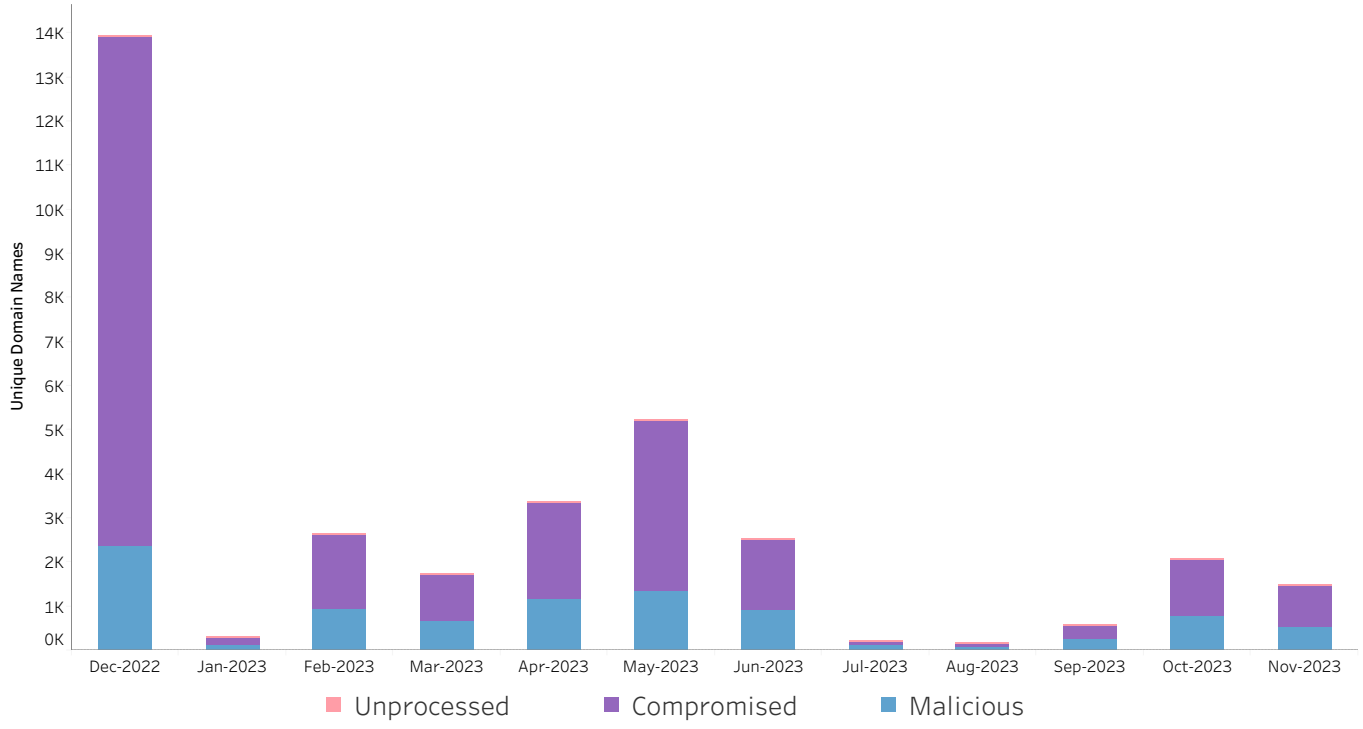

*Figure 10: Compromised vs Malicious - **Malware***

Commentary

More detailed information is available in the interactive charts on our website: www.dnsabuseinstitute.org

Specific Reporting

About

This reporting is intended to show the spectrum of how malicious phishing and malware is concentrated across the DNS registration ecosystem. To demonstrate this, we are[1] 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 future reports, we may add additional metrics or combine various data points.

This specific reporting has an additional month of delay from our aggregate reporting which has allowed us to attempt to contact all named registrars and registries prior to the publication of this data. We believe it is important to speak to registrars and registry operators prior to publication whenever possible. This allows registries and registrars to provide us with context for their data which we may choose to include in commentary, the opportunity to prepare public communications, and us to offer support on improving their management of DNS Abuse where appropriate.

To the best of our ability in accordance with our methodology, all metrics are compiled using only **observed maliciously registered domains**, and exclude observed compromised domain names[2]. This decision was made following significant outreach with the DNS Community and because malicious registrations are typically more directly within the control of a registrar or registry operator. 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 Compass, as detailed in our methodology. 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 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 therefore 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.

We look forward to improving this reporting and working with the DNS Community to better understand, reduce, and prevent abuse. If you would like to provide feedback, please contact us.

[1] Compass 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.
[2] DNSAI Compass uses the following definition of compromised: “A benign domain name that has been compromised at the website, hosting, or DNS level.”

Understanding this report

This report shows specific data for **November 2023**.

There are four detailed metrics: two relating to registrars and two relating to Top Level Domains (TLDs).

- **Registrars**: observed maliciously registered domains per 100,000 DUM
- **Registrars**: observed maliciously registered domains per new domain registration
- **Generic Top Level Domains**: observed maliciously registered domains per 100,000 DUM
- **Country Code Top Level Domains**: observed maliciously registered domains per 100,000 DUM

Each metric is accompanied by:

- **'About this Metric'** to help the reader understand the data being displayed and any exclusionary criteria, and;
- **'Commentary'** where we have added any observations on the data, as appropriate for each month.

Our reporting is indifferent to registrar corporate families; we report on the level of the registrar credential, as identified by the IANA ID.[3] We understand that some corporate entities have more than one IANA ID, and an entity may choose to use its registrar 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 includes two labels for the type of registration at the registrar and TLD level:

- 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.

Our registrar and TLD specific reporting only includes registrations identified as "malicious." It excludes those identified as "compromised".

The end of the report includes Appendices on exclusions:

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

[3] 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.

Registrars: Observed maliciously registered domains per 100,000 DUM

About this metric

This metric is intended to show the prevalence of observed maliciously registered domains in each registrar according to our methodology. 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.[4]

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. 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 (reports of malware or phishing that prove to be mistaken), 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 the situation 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—Appendix H. We determined this list based on a research paper focusing on exclusions to improve accuracy.[5] Finally, the registrar data excludes ccTLD domains due to challenges in mapping domains to registrars in ccTLD ecosystems. See our methodology for more details.

For excluded data, see:

- 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

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

[5] "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.

Commentary: Registrar Credentials

Our reporting is indifferent to registrar corporate families, we report on the registrar IANA ID (i.e., at the credential level). This means that some corporate entities will have more than one IANA ID, and they may choose to operate these credentials differently.

Tables

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.

Table 1: Smaller registrars in ascending order of lowest observed maliciously registered domains per 100,000 DUM for 2023-11

Inclusion criteria:

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

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 - ..	0.80	7	871,289
1515	123-Reg Limited	1.13	8	706,065
431	DreamHost, LLC	1.33	10	753,398
1390	Mesh Digital Limited	1.35	11	812,878
1697	DNSPod, Inc.	2.06	20	970,690
1316	Xiamen 35.Com Technology Co., Ltd.	2.46	7	284,117
168	Register SpA	2.60	17	653,881
3824	Cloud Yuqu LLC	2.75	9	327,534
113	CSL Computer Service Langenbach ..	2.80	14	500,561
1291	Dreamscape Networks Internation..	3.26	17	521,399

Table 2: Larger registrars in ascending order of lowest observed maliciously registered domains per 100,000 DUM for 2023-11

Inclusion criteria:

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

IANA ID	Registrar Credential	Observed Maliciously Registered Domains Per 100,000 gTLD DUM	Observed Malicious gTLD Domains	Observed gTLD DUM
1441	TurnCommerce, Inc. DBA NameBright..	0.31	15	4,869,657
141	Cronon GmbH	0.50	6	1,202,458
420	Alibaba Cloud Computing (Beijing) Co..	0.66	17	2,575,347
433	OVH sas	0.78	17	2,192,162
886	Domain.com, LLC	0.86	15	1,745,970
3817	Wix.com Ltd.	0.89	24	2,697,503
1531	Automattic Inc.	0.90	10	1,106,653
440	Wild West Domains, LLC	1.16	28	2,421,615
48	eNom, LLC	1.51	57	3,769,520
146	GoDaddy.com, LLC	1.66	1,069	64,239,196

Table 3: Registrars in descending order of highest observed maliciously registered domains per 100,000 DUM for 2023-11

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 attempted 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.**

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.

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..	868.78	394	45,351	6
Redacted	*Redacted*	233.37	*	*	1
3858	Aceville Pte. Ltd.	179.93	267	148,391	6
3775	ALIBABA.COM SINGAPORE E-..	174.06	729	418,826	6
3972	Hongkong Kouming Internati..	89.98	47	52,233	4
Redacted	*Redacted*	61.92	*	*	3
1606	Registrar of Domain Names ..	39.01	232	594,768	5
1636	Hostinger, UAB	34.70	668	1,925,050	4
Redacted	*Redacted*	34.14	*	*	3
Redacted	*Redacted*	31.49	*	*	2

Registrars: observed maliciously registered domains per new domain registration

About this metric

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, for example, by utilizing improved fraud prevention techniques.[6]

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 this threshold of 20,000 is somewhat arbitrary and slightly different rankin..

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

Finally, the registrar data excludes ccTLD domains due to challenges in mapping domains to registrars in ccTLD ecosystems. See our methodology for more details.

For excluded data, see:

- 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

Table 4: Registrars with a smaller volume of new registrations, in ascending order of lowest observed maliciously registered domains per new domain registration for 2023-11

Inclusion criteria:

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

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
141	Cronon GmbH	0.05%	6	12,931	1,202,458
106	Ascio Technologies, Inc. D..	0.07%	7	9,411	871,289
1449	URL Solutions, Inc.	0.08%	8	10,373	188,056
3824	Cloud Yuqu LLC	0.08%	9	11,537	327,534
1675	CV. Rumahweb Indonesia	0.10%	6	5,841	112,248
1291	Dreamscape Networks In..	0.11%	17	15,411	521,399
431	DreamHost, LLC	0.13%	10	7,743	753,398
113	CSL Computer Service La..	0.13%	14	10,773	500,561
1868	Eranet International Limi..	0.14%	20	14,686	494,945
2374	Hosting Ukraine LLC	0.14%	8	5,809	103,979

Table 5: Registrars with a higher volume of new registrations, in ascending order of lowest observed maliciously registered domains per new domain registration for 2023-11

Inclusion criteria:

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

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
3817	Wix.com Ltd.	0.04%	24	65,254	2,697,503
1531	Automattic Inc.	0.04%	10	24,263	1,106,653
1556	Chengdu West Dimension Di..	0.04%	50	111,435	1,174,394
3862	Spaceship, Inc.	0.05%	17	31,363	234,998
1697	DNSPod, Inc.	0.06%	20	35,952	970,690
886	Domain.com, LLC	0.06%	15	26,798	1,745,970
49	GMO Internet, Inc. d/b/a On..	0.06%	78	121,459	4,391,471
3827	Squarespace Domains LLC	0.06%	61	94,683	1,308,201
433	OVH sas	0.06%	17	26,361	2,192,162
1861	Porkbun LLC	0.09%	58	65,594	1,298,686

Table 6: Registrars in descending order of highest observed maliciously registered domains per new domain registration for 2023-11

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.

IANA ID	Registrar Credential	Observed Maliciously Registered Domains Per New gTLD Domain Registration	Observed Newly Registered gTLD Domains	Observed Malicious gTLD Domains	Observed gTLD DUM	Number of Months
817	MAFF Inc.	9.68%	310	30	87,885	6
3858	Aceville Pte. Ltd.	9.17%	2,911	267	148,391	5
3765	NICENIC INTERNATION..	7.30%	5,397	394	45,351	6
1555	22net, Inc.	5.29%	2,344	124	200,260	6
Redacted	*Redacted*	4.10%	*	*	*	1
Redacted	*Redacted*	3.19%	*	*	*	1
Redacted	*Redacted*	3.09%	*	*	*	3
3775	ALIBABA.COM SINGAPO..	2.59%	28,141	729	418,826	5
Redacted	*Redacted*	1.67%	*	*	*	2
Redacted	*Redacted*	1.64%	*	*	*	1

Generic Top Level Domains: Observed maliciously registered domains per 100,000 DUM

About this metric

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[7], 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, etc.).

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.

[7] 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

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 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.

For excluded data, see:

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

Commentary: Comparing ccTLDs and gTLDs

We have split ccTLD and gTLDs into two separate sections for the reasons described above and used the same methodology for reporting and abuse categorization. However, the absolute numbers of Observed Maliciously Registered Domains and rates of Maliciously Registered Domains Per 100,000 DUM are noticeably lower in the ccTLD table.

Tables

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.

Table 7: Smaller gTLDs in ascending order of lowest observed maliciously registered domains per 100,000 DUM for 2023-11

Inclusion criteria:

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

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
email	5.23	6	114,789
tokyo	5.53	6	108,573
services	8.26	6	72,615
win	8.42	8	94,974
fyi	9.98	6	60,138
bio	13.84	10	72,246
lat	13.98	15	107,281
ltd	14.09	16	113,568
lol	14.29	16	111,975
digital	15.41	19	123,323

Table 8: Larger gTLDs in ascending order of lowest observed maliciously registered domains per 100,000 DUM for 2023-11

Inclusion criteria:

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

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
org	1.88	204	10,855,800
dev	1.98	8	403,535
biz	2.59	33	1,276,437
net	3.14	412	13,131,889
com	3.86	6,224	161,082,896
cfd	4.01	39	972,180
art	4.25	10	235,495
world	5.83	12	205,820
asia	7.01	21	299,686
tech	7.20	33	458,221

Table 9: gTLDs in descending order of highest observed maliciously registered domains per 100,000 DUM for 2023-11

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

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM	Number of Months
Redacted	119.81	*	*	3
Redacted	95.07	*	*	1
Redacted	82.29	*	*	3
help	69.96	18	25,729	5
Redacted	61.20	*	*	2
Redacted	50.21	*	*	3
Redacted	45.74	*	*	1
icu	44.84	161	359,021	6
top	44.29	1,142	2,578,421	4
Redacted	37.31	*	*	1

Country Code Top Level Domains: Observed maliciously registered domains per 100,000 DUM

About this metric

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, etc.).

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 (reports of malware or phishing that prove to be mistaken), 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.

[8] 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

For excluded data, see:

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

Commentary: Comparing ccTLDs and gTLDs

We have split ccTLD and gTLDs into two separate sections for the reasons described above and used the same methodology for reporting and abuse categorization. However, the absolute numbers of Observed Maliciously Registered Domains and rates of Maliciously Registered Domains Per 100,000 DUM are noticeably lower in the ccTLD table.

Tables

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.

Table 10: Smaller ccTLDs in ascending order of lowest observed maliciously registered domains per 100,000 DUM for 2023-11

Inclusion criteria:

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

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
qq	1.03	10	975,517
fi	1.13	6	532,173
hu	1.17	10	856,005
nz	1.40	10	716,537
ua	1.43	7	488,863
ar	1.51	8	528,891
ro	2.48	14	563,633
ie	2.53	8	316,706
hk	3.57	8	224,355
pw	3.95	15	379,893

Table 11: Larger ccTLDs in ascending order of lowest observed maliciously registered domains per 100,000 DUM for 2023-11

Inclusion criteria:

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

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
ch	0.36	9	2,519,136
ca	0.37	12	3,280,319
nl	0.48	29	6,023,743
be	0.49	8	1,647,516
cz	0.50	7	1,406,605
uk	0.62	63	10,211,053
de	0.62	103	16,692,659
at	0.67	10	1,481,707
it	0.82	26	3,178,082
za	1.01	13	1,289,966

Table 12: ccTLDs in descending order of highest observed maliciously registered domains per 100,000 DUM for 2023-11

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

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM	Number of Months
Redacted	60.94	*	*	2
id	57.13	392	686,135	6
pk	30.43	38	124,895	5
cc	29.43	321	1,090,663	6
pl	21.72	534	2,458,130	6
ng	19.25	31	161,036	4
pe	15.25	19	124,619	5
Redacted	13.65	*	*	2
Redacted	12.64	*	*	1
Redacted	8.30	*	*	3

Appendices

Registrars

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

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

All Appendices are available on our website at:
https://dnsabuseinstitute.org/dnsai-compass-appendices