DNS RESEARCH FEDERATION

DNS Abuse Mitigation Report

June 2025

DNS Research Team

Contents

Executive Summary

The DNS Research Federation (DNSRF) has launched a data-driven effort to measure the impact of ICANN's 2024 amendments to the Registrar Accreditation Agreement (RAA), which require timely mitigation of DNS Abuse by registrars and registries. Focusing on phishing and malware incidents, we analysed abuse mitigation patterns using our DAP.LIVE platform, tracking how quickly registrars and registries take action to disable malicious domains. Initial findings show that while 24-hour mitigation rates have improved slightly, rising from 13% in September 2024 to 20% in early 2025, most abuse still remains active beyond this critical window, during which users are most vulnerable. Seven-day mitigation rates are more encouraging, increasing to 55% over the same period. Notably, registries currently perform the majority of mitigations within both 1-day and 7-day windows, though registrars begin to take the lead after 90 days.

Introduction

As part of its mission to advance understanding of the DNS's impact on cybersecurity, policy, and technical standards, the DNSRF (Domain Name System Research Federation) is researching the effectiveness of these RAA Abuse Amendments. Using DNSRF tools, we have documented how quickly numerous parties carry out DNS Abuse mitigations. With the RAA amendments in force, our initial focus will be on mitigations that can be actioned and easily associated with both Registries and Registrars. However, in the future, we will add additional parties "downstream" from domain name registration, including hosting providers/web hosters, reverse proxy providers, subdomain providers, domain owners, etc.

In 2013, ICANN (the Internet Corporation for Assigned Names and Numbers) introduced a set of obligations designed to prevent DNS Abuse; the umbrella term defined by ICANN encompassing phishing, pharming, malware, botnets, and any spam acting as a delivery mechanism for these other harms. The obligations, including policies and obligations for monitoring and reporting abuse, are defined in the main contract between ICANN and domain name sellers: the Registrar Accreditation Agreement or "RAA".

In 2024, ICANN updated the Registrar Accreditation Agreement and committed to **enforcing** their original obligations to prevent cyberattacks and clarifying how this should be accomplished. This involves stricter compliance monitoring and penalties for registrars who fail to take action against DNS abuse.

When registrars have "actionable evidence" that a domain is being used for DNS Abuse, they are obliged to "promptly take the appropriate mitigation action(s) that are reasonably necessary to stop, or otherwise disrupt" the abuse. If there are "well-founded reports of Illegal Activity," then the situation "must be reviewed within **24 hours,**" and the registrar "take necessary and appropriate actions."[1]

[1] https://www.icann.org/resources/pages/registrars/registrars-en

Key Takeaways

1. **Significant Progress in Mitigation Tracking**: DNSRF's tracking system offers real-time insights into abuse mitigation actions, adding a critical layer of visibility beyond abuse reporting alone.
2. **Mitigation Rates are Low**: By the end of the reporting period, an average of less than 80% of reports were mitigated by both Registries and Registrars within 24 hours of being reported, indicating the need for more work to achieve better rates.
3. Within the first 24 hours, 64% of mitigations are actioned by registries. With the remaining 36% being mitigated by registrars
4. **Room for Improvement in Response Times**: While the average mitigation time spans a few days, faster responses are crucial, particularly for high-impact abuse like phishing and malware that often are effected on the consumer in the first 24 hours of being activated.

These takeaways reinforce the importance of ongoing monitoring and adaptation as new abuse patterns and mitigation methods emerge, ensuring that all ecosystem players can respond effectively to protect internet users.

Methodology

The DNSRF has been collecting relevant abuse reports associated with phishing and malware in DAP.LIVE. Phishing reports have been sourced from OpenPhish, APWG, Malware Patrol, and URL Abuse. Malware Reports have been sourced from URLHaus, Malware Patrol, and URL Abuse. Spam reports have been excluded from our study.

To ensure a granular level of reporting, we deduplicate reports daily. This means that if we receive multiple reports for the same domain name on different days, we would count them more than once. This is important when measuring the mitigation action taken by contracted parties in the 24-hour timeframe, as it would allow us to capture scenarios where actors may not have taken action until multiple reports have been seen on different days.

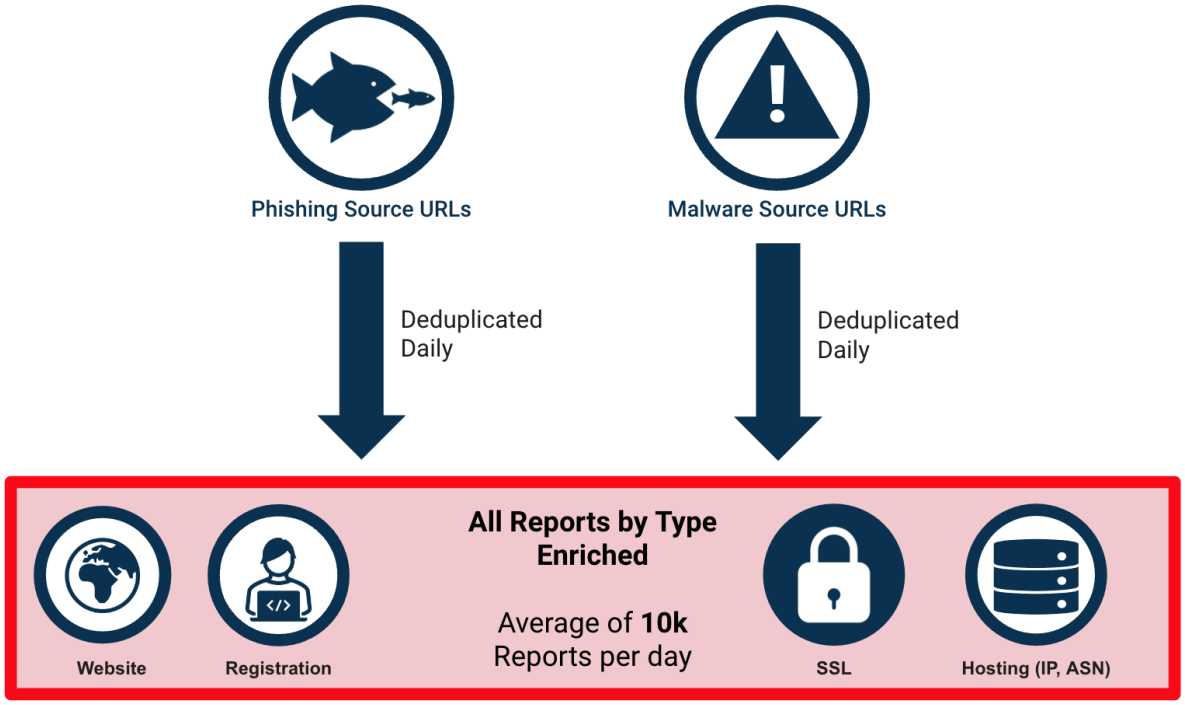

Figure 1 - Data Collection and Deduplication

In addition, as our current focus is on actions taken by only registries and registrars, we have removed reports associated with subdomain providers and URL shorteners. Future versions of this study will add these back in, allowing a more complete picture of who is involved in mitigating abuse and how that has happened.

For each unique abusive domain name, we measure the abuse time-to-live - the time between the malicious URL being blocklisted and the abuse being mitigated. We consider abuse to have been **mitigated** only when specific actions are taken by the registry or registrar, causing the domain name to no longer resolve.

Specifically, the following criteria to indicate that abuse has been **mitigated** by either the registrar or registry:

- Registrar:
    - Addition of “clientHold”, disabling the domain name
    - Removing the name server, disabling the domain name
    - The domain is past its expiry date and so no longer routes
    - The domain is deleted by the registrar and enters a redemption grace period
- Registry:
    - Addition of “serverHold”, as with a clientHold, will prevent the domain from routing.

We calculate the abuse mitigation status for each abuse report at 0 days (upon first report) and then at 1,3,7,14,30,60, 90, and 365 days, respectively. Where no mitigation has been detected after 356 days, we consider the report unmitigated and stop checking. According to ICANN’s RAA Abuse Amendments, we would expect to see more mitigations happening within 1 day to meet compliance criteria. More importantly, given that most DNS abuse occurs in a 24-hour window between activation and when abuse infrastructure is abandoned, we believe the 24-hour abuse rate is a key metric approximating impact on internet users.

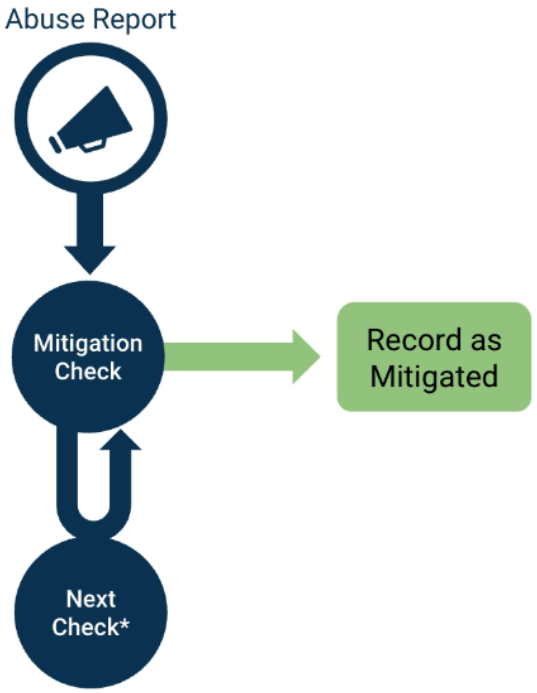

Figure 2 - Detecting and Categorizing Mitigation

Findings

The findings in this report are limited to abuse report data known to the DNSRF's DAP.LIVE platform based on processing an average of 10,000 phishing and malware reports received daily. All visualizations and analyses cover the period starting in early September 2024 and ending in May 2025.

Mitigation Rates Over Time

While we calculate mitigation rates for each of the mentioned intervals, in this report, we will focus on both the 24-hour mitigation rate (e.g., the rate of mitigations within 24 hours of a report) and the mitigation rate after 7 days.

24-Hour Mitigation Rates

The 24-hour mitigation rate trend, Figure 3, from the beginning of September to the present indicates that mitigation of reports of abuse is trending slightly upward, starting at an average of 13% and increasing to 20%. This is an encouraging sign.

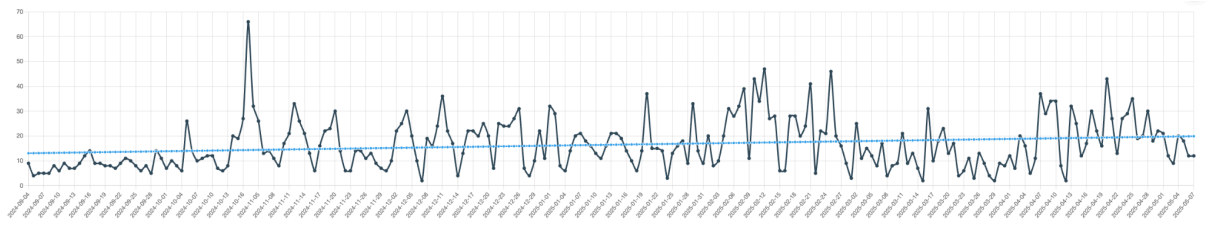

Figure 3 - 24-Hour Mitigation Rates

7-Day Mitigation Rates

The 7-Day mitigation rate trend for the same period, Figure 4, shows improved rates across the board.

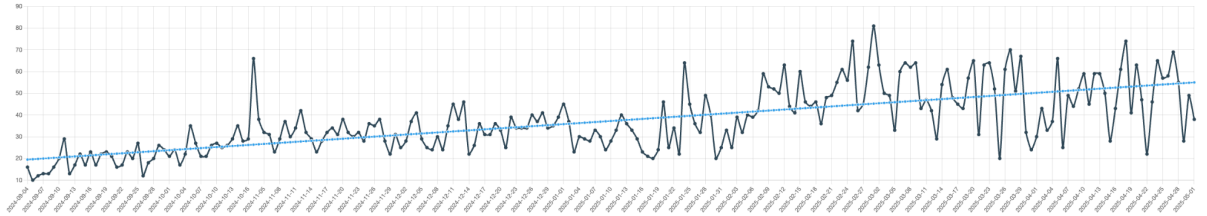

Figure 4 - 7-Day Mitigation Rates

Given the additional time to receive, process, investigate, and ultimately mitigate reports of abuse, we see higher rates after 7 days, starting at an average of 20% and rising to about 55%.

Mitigation Actor Analysis: Registrars and Registries

Looking deeper into the mitigations made during this period, we wanted to understand better who was doing the mitigation and when.

Who Is Mitigating?

Looking first at who is responsible for effecting mitigations within 1 day, we see that registries mitigate 64%. With the remaining 36% being mitigated by registrars. (Figure 5).

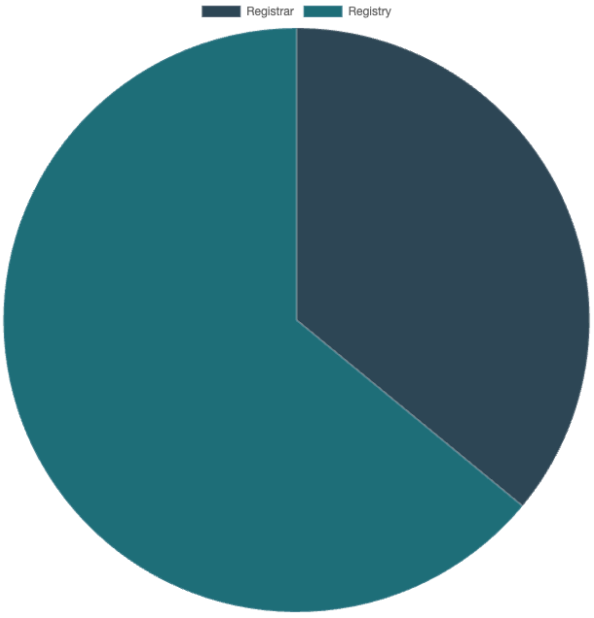

Figure 5 - Percentage of Mitigations Effected within 1 Day

When we perform a similar analysis using a 7-day mitigation period, we see that registries still perform most mitigations, 54%, with registrars catching up, representing 46% of mitigations. (Figure 6)

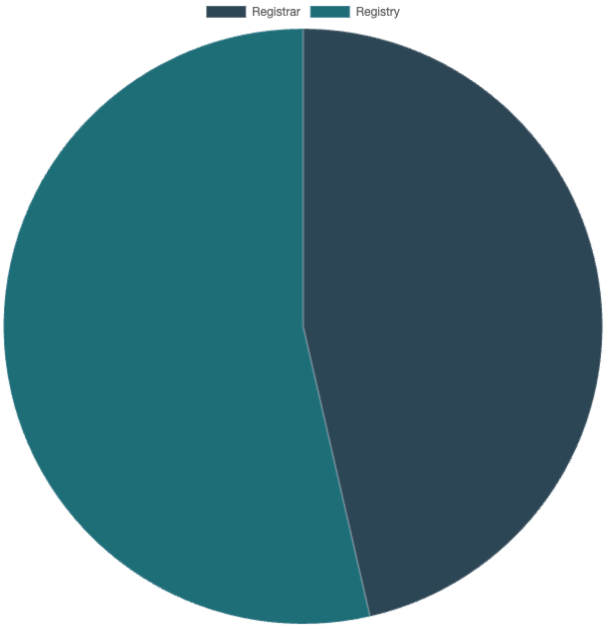

Figure 6 - Percentage of Mitigations Effected within 7 Days

Interestingly, we don't see the number of mitigations performed by registrars pass those done by registries until 90 days, with registrars accounting for 56% of mitigations and registries accounting for 44%.

Most Improved Registrar

Taking a closer look at the performance of all registrars, we calculated which ones are "most improved", meaning which ones have the highest 1-day mitigation rate change since we started analysing the data in September 2024. (Figure 7)

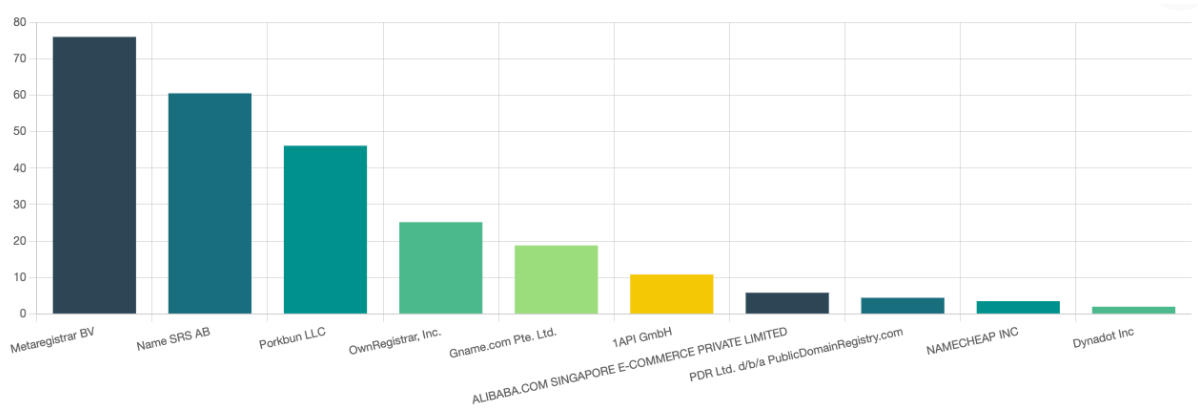

Figure 7 - Most Improved Registrars

We see Metaregistrar, in front, improving their mitigation rate by approximately 75% since September 2024.

Most Improved Registry

Here is the graph for the most improved registries, calculated like the most improved registrars above.

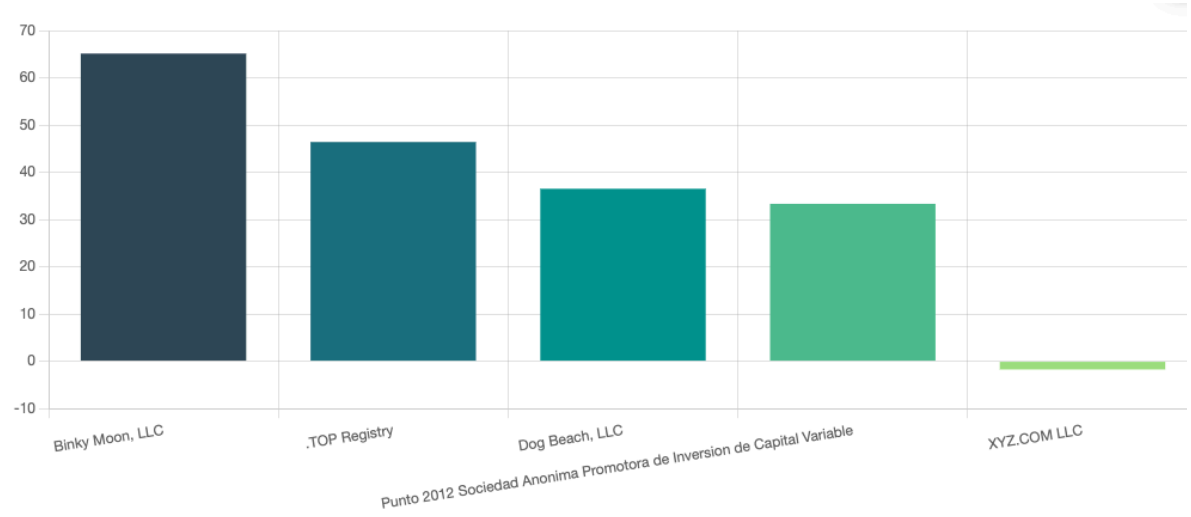

Figure 8 - Most Improved Registries

It's interesting to see both .TOP and .XYZ listed here, as they have a reputation of being two of the top registries for abusive domain registrations. Seeing .TOP improve by 45% indicates they have made an effort to mitigate the abuse in their TLD, but there is room for improvement.

How Fast is Mitigation Happening?

Finally, when we look at the time between a report and a detected mitigation, we find that average takedown times happen in a matter of days. (To calculate these figures, we only considered reports that had been checked for at least 14 days)

Abuse Type	Average Mitigation Time (Days) All Actors	Average Mitigation Time (Days) Registrars	Average Mitigation Time (Days) Registries
Phishing and Malware	8.99	9.13	8.87
Phishing Only	9.06	9.6	8.61
Malware Only	7.87	4.3	16.32

Figure 9 - Mitigation Times

While these times might seem reasonable, we know from previous research that most internet abuse, including Phishing and Malware attacks, lasts no more than 24 hours and sometimes only 2 hours before the attacker tears down the abusive infrastructure to cover their tracks. So, there is room for improvement to ensure verifiable instances of abuse are mitigated as quickly as possible to minimize the impact on internet users. It is also interesting to note that when registries are involved in mitigating abuse, their response time is quicker than that of registrars.

Comparison with Other Reports

The NetBeacon Institute has also analyzed and reported on the mitigation times of domain names reported to various abuse lists. Their findings indicate that mitigation rates are much higher than we have calculated, with monthly mitigation rate averages between 80 and 90 percent.

Looking at publicly available information from the Net Beacon Institute, several key differences account for the differences.

Deduplication Window and Report Timeframe

As mentioned above, our methodology focuses on mitigations effected within a 24-hour timeframe, with reports being considered as duplicates only if they are reported within 24 hours of each other. This means that if we receive multiple reports for the same domain name on different days, we count the mitigation time for that domain more than once. This is important when measuring the mitigation action taken by contracted parties in the 24-hour timeframe, as it would allow us to capture scenarios where actors may not have taken action on a particular domain name until multiple reports have been seen on different days.

In contrast, the NetBeacon Institute focuses on mitigations effected within a 30-day timeframe, with reports being considered as duplicates if they are reported within the same 30-day period. This results in a single mitigation time recorded on a single domain each month if a mitigation is detected within 30 days. This extended period allows more time to receive, process, investigate, and ultimately mitigate reports of abuse, which would result in a considerably higher mitigation rate.

Mitigation Measurement

Our methodology focuses solely on “high confidence” mitigation indicators that can be actioned directly by either registries or registrars. Currently, we do not include indicators of mitigations that might occur by downstream entities.

While the NetBeacon Institute has not explicitly detailed what indicators they include in their analysis, we believe they include entities beyond registries and registrars, including hosting providers and “other relevant” actors.[2] Including these downstream entities in their calculation would also account for the higher calculated mitigation rates. Future updates to the DNSRF methodology will include mitigations made by entities other than registries and registrars.

[2] https://netbeacon.org/how-have-the-gtld-contractual-amendments-impacted-dns-abuse/ - “‘Mitigated’ means that, according to our methodology, we believe a mitigating action has occurred. This action could be taken by a registrar, registry, a hosting provider, or another relevant actor. ‘Not Mitigated’ means that our methodology did not detect any indication of mitigation.”

Potential Further Study

The full mitigation picture can be improved further by analyzing the full range of mitigations beyond those done by registries and registrars. This includes mitigations done by hosting providers, subdomain providers, law enforcement agencies, registrants, browser vendors, etc. We view these indicators as lower confidence, as the changes below could be done for various reasons, some unrelated to abuse mitigation. Some of the mitigation indicators we are considering include

- Changes of Registrar (Registry/Registrar)
- Nameserver Changes (Registry/Registrar/Hosting Provider/Registrant)
- DNS Record Changes - A, AAAA Records Removed or Changed (Registrar/Hosting Provider/Registrant)
- Website status change - to not found or error statuses (Hosting Provider / Registrant)

Undoubtedly, these indicators will change and evolve as new mitigation methods appear in the ecosystem, and systems will have to evolve along with them. Tracking changes in response to the implementation of NIS2 in 2025 in light of the risk-based processes recommended by the NIS2 Cooperation Guidelines would also highlight trends in abuse over time. Additionally, as some of these mitigation methods are “downstream” to the Registrar (i.e., the mitigation action taken is on only specific subdomains or URLs rather than domain names), an alternative approach may be required to measure and report on these mitigations.

Conclusion

The DNSRF's new system for tracking abuse mitigation rates and takedown times provides a critical lens for evaluating the effectiveness of the Global Signal Exchange partnership and related industry and regulatory frameworks. By continuously monitoring mitigation actions across multiple actors and types of abuse, the system quantifies how abuse reports are being addressed and highlights areas where response times and accountability can be improved. Our initial findings underscore the role of registrars in handling the majority of mitigations while also revealing the need for more rapid intervention to keep up with abuse lifecycles that often end within 24 hours.

DNS
RESEARCH
FEDERATION