



To: Göran Marby, CEO, ICANN; Maarten Botterman, COB, ICANN; Rod Rasmussen, ICANN SSAC

From: Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) and Anti-Phishing Working Group (APWG)

Date: June 8, 2021

Subject: 2021 ICANN, GDPR, and the WHOIS: A Users Survey - Three Years Later.

Dear Sirs:

The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) is an industry association that comes together to work against botnets, malware, spam, viruses, DDoS attacks and other online exploitation. We are the largest global anti-abuse industry association, with more than 250 member companies worldwide, bringing together all the stakeholders in the online community in a confidential, open forum. We develop cooperative approaches for fighting online abuse.

APWG is the international coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors and NGO communities. APWG's membership of more than 2200 institutions worldwide is as global as its outlook, with its directors, managers and research fellows advising: national governments; global governance bodies like the Commonwealth Parliamentary Association, Organisation for Economic Co-operation and Development, International Telecommunications Union and ICANN; hemispheric and global trade groups; and multilateral treaty organizations such as the European Commission, the G8 High Technology Crime Subgroup, Council of Europe's Convention on Cybercrime, United Nations Office of Drugs and Crime, Organization for Security and Cooperation in Europe, Europol EC3 and the Organization of American States. APWG is a member of the steering group of the Commonwealth Cybercrime Initiative at the Commonwealth of Nations.

In 2018 M3AAWG and APWG conducted a survey of cyber investigators and anti-abuse service providers to determine the impact of ICANN's implementation of the EU GDPR, the Temporary Specification for gTLD Registration Data (Temporary Specification, adopted in May 2018) and shared our findings along with recommendations to you for your consideration. M3AAWG and APWG recently conducted a follow up survey to determine the current state of those impacts.

From our analysis of 277 survey responses, we find that respondents report that changes to WHOIS access continue to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyber attacks.

Specifically, the survey responses indicate that the Temporary Specification has reduced the utility of public WHOIS data due to wide-ranging redactions, beyond what is legally required. It also introduces considerable delays, as investigators have to request access to redacted data on a case-by-case basis; often with unactionable results. Furthermore, with limited or no access to the data that had previously been obtained or derived from WHOIS data, some investigators struggle to identify perpetrators and put an end to criminal campaigns. The resulting delays and roadblocks are a boon to attackers and criminals, prolonging their windows of opportunity to cause harm during cybercrime activities such as phishing and ransomware distribution, or the dissemination of fake news and subversive political influence campaigns.

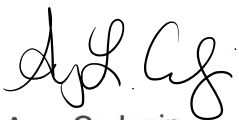
M3AAWG and APWG observe that there are four issues that ICANN needs to address:

- 1. Access to some relevant data like contact data of legal persons needs to be readily available while protecting natural persons' privacy.**
- 2. Both sporadic WHOIS users who make relatively few requests, as well as bulk users who use data-driven approaches for blocklisting should be accommodated by ICANN.**
- 3. ICANN should establish a functional system of registrant data access for accredited parties; such a system needs to be workable for cybersecurity professionals and law enforcement in terms of time delays and administrative burden, and should include strict privacy and security controls.**
- 4. The survey responses indicate that the solutions currently discussed at ICANN would not meet the timeline requirements of law enforcement and cybersecurity actors.**

We respectfully requests that the ICANN organization, community and Board consider the attached survey report. The report is also published on the M3AAWG website under our Public Policy Comments and available directly at <https://www.m3aawg.org/for-the-industry/published-comments>

Thank you in advance for your consideration.

Sincerely,



Amy Cadagin
Executive Director
Messaging, Malware and
Mobile Anti-Abuse Working Group



Foy Shiver
Deputy Secretary-General
Anti-Phishing Working Group



ICANN, GDPR, and the WHOIS: A Users Survey - Three Years Later.

Principal Investigators

Laurin B Weissinger, DPhil, The Fletcher School and Computer Science, Tufts University

Dave Piscitello, Interisle Consulting Group

Bill Wilson, M3AAWG Senior Advisor

www.m3aawg.org

www.apwg.org

Table of Contents

Executive Summary	3
The WHOIS and the Impact of the Temporary Specification	5
Introduction	5
Key Findings in Context	6
Detailed Analysis	8
Introduction	8
Methodology	8
Demographics and Use of WHOIS	9
RDAP Use	12
Effects of the Temporary Specification on WHOIS Use for Abuse Mitigation	14
Disclosure of Redacted Data	20
Disclosure Systems under ICANN consideration	25
Complaints to ICANN	25
Summary	26

Executive Summary

The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) and The Anti-Phishing Working Group (APWG) have again collaborated to conduct a survey of cyber investigators and anti-abuse service providers to understand how ICANN's application of the European Union's General Data Protection Regulation (GDPR) has impacted on the distributed WHOIS service and anti-abuse work. In particular, we are discussing the effect of the Temporary Specification on anti-abuse actors' access and usage of domain name registration information, which is central for various types of investigations.

At its core, the WHOIS is a protocol widely used for accessing data on registered assignees of an Internet resource, in our case domain names. WHOIS services are available via multiple channels, e.g. Web-based tools, Port 43, and more recently RDAP.

From our analysis of over 270 survey responses, we find that respondents report that changes to WHOIS access following ICANN's implementation of the EU GDPR, the Temporary Specification for gTLD Registration Data¹ (Temporary Specification, adopted in May 2018), continue² to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyber attacks.

Specifically, the survey responses indicate that the Temporary Specification has reduced the utility of public WHOIS data due to wide-ranging redactions,³ beyond what is legally required. It also introduces considerable delays, as investigators have to request access to redacted data on a case-by-case basis; often with unactionable results. Furthermore, with limited or no access to the data that had previously been obtained or derived from WHOIS data, some investigators struggle to identify perpetrators and put an end to criminal campaigns. The resulting delays and roadblocks are a boon to attackers and criminals, prolonging their windows of opportunity to cause harm during cybercrime activities such as phishing and ransomware distribution, or the dissemination of fake news and subversive political influence campaigns.

M3AAWG and APWG observe that there are four issues that ICANN needs to address:

- 1. Access to some relevant data like contact data of legal persons needs to be readily available while protecting natural persons' privacy.**
- 2. Both sporadic WHOIS users who make relatively few requests, as well as bulk users who use data-driven approaches for blocklisting should be accommodated by ICANN.**

¹ Temporary Specification for gTLD Registration Data, <https://www.icann.org/resources/pages/gtld-registration-data-specs-en>

² See report 1 from 2018 for further information. See: <https://www.m3aawg.org/WhoisSurvey2018-10>

³ The Temporary Specification allows for far reaching redactions, beyond what the GDPR requires. An Interisle study concludes that contact data for 57% of all generic TLDs are now redacted, many times more than necessary. The Interisle study further notes that registrants of 86.5% of all names cannot be ascertained due to redactions and the use of privacy and proxy services. See: <http://interisle.net/ContactStudy2021.html>

- 3. ICANN should establish a functional system of registrant data access for accredited parties; such a system needs to be workable for cybersecurity professionals and law enforcement in terms of time delays and administrative burden, and should include strict privacy and security controls.**
- 4. The survey responses indicate that the solutions currently discussed at ICANN would not meet the needs of law enforcement and cybersecurity actors in terms of timelines**

The WHOIS and the Impact of the Temporary Specification

Introduction

WHOIS records are a key resource used by cybersecurity experts, law enforcement agents, blocklist providers and others to attribute criminal activity, understand malware campaigns, flag malicious domains, and more. Users of the WHOIS tend to use the system for different reasons but two use cases seem worth highlighting.

Investigators might use the WHOIS to find information on specific names, for example when they identify a counterfeit storefront, after receiving an abuse report, or to better understand or categorize traffic patterns. The majority of our respondents fall in this category, usually making less than 100 daily requests. Another use of the WHOIS involves the analysis of large amounts of WHOIS data to detect patterns of abuse, and to associate malicious domains with each other, as well as malware, phishing, or spam campaigns:

Criminals regularly register large numbers of domains in bulk, often in batches of hundreds or thousands of names at the same time. In case individual names used for their criminal schemes are blocked, detected, or otherwise "burned", the criminals will swiftly switch to new, pre-registered names from their earlier bulk orders. While not all cybercrimes and attacks require large numbers of quickly replaceable names, this approach is common.

To respond to cybercriminals that leverage bulk buying and bulk resource use, investigators query WHOIS data constantly and at all times to detect patterns. Registrant as well as technical data can be used to identify sets of likely malicious domains based on their association with already known bad domains or known records: names, email addresses, telephone numbers are likely to be the same for domains used by the same criminal group or same campaign, while bulk orders might also present extremely similar time stamps. When matches are found, domains can be analyzed or added to watchlists. If other criteria indicating abuse are satisfied, these defenders and blocklist providers might also add these names to a blocklist.

To fight crime and abuse, large datasets are particularly powerful: investigators and analysts can use them to map out and then dismantle criminal attack infrastructures, while bulk data enables blue teams to protect their networks. For this data-driven approach to work, however, high-volume, real-time access to WHOIS records is essentially required. Wait times, rate limiting, inconsistent responses, redacted data, and rotating fake information all decrease response times and data quality.

Since the Temporary Specification came into force in 2018 after years of inaction, redaction of registrant data has complicated the work of investigators working with large amounts of WHOIS data and those who rely on WHOIS data to attribute attacks and understand criminal infrastructures. Partly, this is due to the fact that not only EU data subjects' data are now redacted, as legally required, but also data belonging to non-EU citizens and residents as well as data pertaining to commercial entities, which are not protected under GDPR.

The purpose of this report is to better understand who is affected by the current redaction regime based on the Temporary Specification and how. Furthermore, this report explores what issues our respondents face, and what changes ICANN would have to introduce to address their concerns.

In the following section, we will summarize our findings. The last section will provide a deeper dive into our survey data, discussing individual questions, our methodology, and more granular findings.

Key Findings in Context

The Temporary Specification continues to lessen defenders' ability to address online crime and abuse. Two-thirds of our 277 respondents indicate that their ability to detect malicious domains has decreased. This aspect likely contributes to lower detection capabilities when it comes to malicious activity overall, as reported by 41% of respondents.

Since the Temporary Specification came into force, cyber-investigators have been significantly impaired in their ability to investigate relationships between malicious domains and actors. Some use cases of WHOIS data leverage unredacted technical information solely or predominantly. Thus, they are less affected by the redactions. However, the now-unavailable registrant data, like email and postal addresses, are extremely relevant to some investigations, notably attribution, and have evidentiary value to private sector investigators as well as law enforcement and prosecutors. Unsurprisingly, attribution work suffers the most from these redactions: 94% of our respondents report that redaction impairs their ability to investigate relationships between domains and actors. Even fraudulently composed, pseudonymous, incomplete, or inaccurate data can be useful for assigning reputations or creating correlations, particularly for actors that can leverage bulk queries. While only a minority of actors overall and in our survey have very large query volumes, some investigation and mitigation measures rely on this approach. For example, investigators might want to find additional domains used in a phishing campaign based on email addresses or other registrant information. The requirement to send access requests and wait for responses makes this approach much less effective if not useless.

Response times are significantly longer, causing harm. Time is of the essence when responding to malware, phishing, botnets and other cybercrimes. Over 70% of respondents report that time to mitigate or respond exceeds an acceptable threat threshold due to the limitations introduced by the Temporary Specification. Most cybercrime campaigns are the most effective and lucrative, and therefore causing most harm, in the first few hours or days after they are launched, making immediate access to WHOIS data particularly relevant for threat investigators, blocklist providers, and law enforcement. Our data indicate that the need to request access to the non-public data elements introduces significant delays, usually days, in circumstances where mitigation prior to the adoption of the Temporary Specification was accomplishable within a few hours. These delays allow malicious activities to remain active and thus cause harm for longer periods of time.

Requests to access non-public WHOIS by legitimate investigators for legitimate purposes remain ineffective. The data indicate that the disclosure of redacted WHOIS data is inconsistent: requests are often ignored or denied, and "revealed" data are often not actionable. While faked data were an issue

before the Temporary Specification, increased response times are damaging: if revealed data are actionable, time delays often make them useless for some activities, while fake or unactionable responses preceded by long wait times are particularly problematic. Approximately 65% of cybersecurity experts indicate they need a full response for non-public registration data within 1 day when addressing malware, phishing and botnet/command and controls. In contrast, the latest ICANN policy (EPDP Phase 2 Policy) defining a future system for the disclosure of non-public registration data sets a maximum response target of 10 business days. Keeping in mind that the first few hours or days of a campaign are the most lucrative and thus the most damaging, effective mitigation based on WHOIS registrant data would be essentially impossible under these rules.

To summarize, our respondents indicate that WHOIS has become an unreliable and less meaningful source of threat intelligence. Thus, dealing with malicious domains, and in consequence crime and abuse, has become considerably harder and more time intensive since the Temporary Specification came into force. The lack of access to accurate WHOIS records inhibits the work undertaken by law enforcement, cybersecurity professionals, and others. This has an effect on security on the internet as a whole. To protect customers and society, quick access to registration data is paramount, and the currently discussed ICANN policy measures to restore (some) access are insufficient. Three years after the Temporary Specification implementation, an alarming 70% of responders report that their investigations are affected and that threats cannot be addressed in a timely manner. Only 2% of respondents believe that the Temporary Specification is working.

Detailed Analysis

Introduction

WHOIS is a query and response protocol that is widely used for querying databases that store records concerning the registered assignees of an Internet resource. The WHOIS can be accessed via the web, Port 43 and the RDAP protocol, which was made mandatory in 2013. WHOIS records include technical data like creation, update, and expiration times, DNSSEC information, and name servers for each registered name. Until the Temporary Specification came into force in 2018, registrant data like email addresses, names, phone numbers, and postal addresses were usually - but not always⁴ - available. Since the Temporary Specification came into force based on an ICANN board decision in 2018, registrant data have been heavily redacted. Technical data are still publicly available.

Cybersecurity professionals, law enforcement and others regularly use WHOIS to access data about domain name registrants - like names, email addresses, or postal addresses - as well as technical data like timestamps. WHOIS data. Our data indicate that cybersecurity professionals and other relevant specialists believe that the Temporary Specification is hurting their work, with nearly 90% of respondents reporting that they have been negatively affected by the ICANN Temporary Specification in their ability to address abuse.

This section will provide more detailed insights into the demographics of our respondents, how they use the WHOIS, and the effect of the Temporary Specification on their investigations. Where apt, this section will also compare the responses collected in 2021 with those from the initial WHOIS users survey conducted by APWG and M³AAWG in 2018.⁵ After providing some insights into the methodology, this section will speak to demographics, WHOIS and RDAP use. Then, it will focus on the perceived effects of the Temporary Specification, and the disclosure of redacted data. This will be followed by a section on our respondents' opinions and ideas regarding a future disclosure system and complaints to ICANN compliance before concluding.

Methodology

The questions that comprised this survey were prepared by M³AAWG members and their Boards of Directors members. Our survey concentrated on cybersecurity practitioners, which include personnel responsible for maintaining protective services and products, personnel responsible for directly defending the network of their employers, and academic researchers.

Some questions are demographic in nature but no personal data were collected. The remaining questions allow responders to characterize their WHOIS usage and purpose with a focus on issues and roadblocks, and to describe whether and how the implementation of ICANN's Temporary Specification for gTLD Registration Data (Temporary Specification) has affected their usage. In addition to the

⁴ For example, registrants could use proxy services to hide their personal data.

⁵ See report 1 from 2018 for further information. See: <https://www.m3aawg.org/WhoisSurvey2018-10>

questions visualized below, the survey collected various open-ended responses, which are discussed in text.

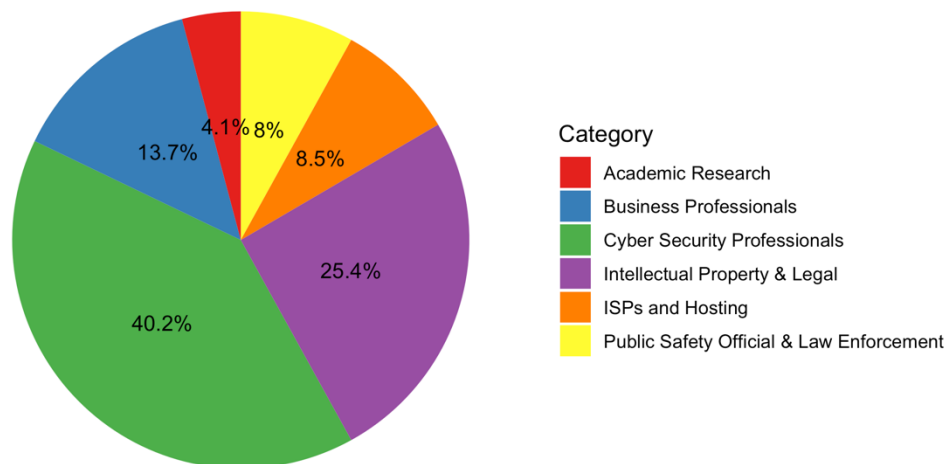
Our sample size is 277 responses. We estimate that the mailing lists used to announce the survey were delivered to a population of between 2500 and 4000 cybersecurity investigators, many of whom will work for a relatively small set of key cybersecurity organizations. Some but not all of these individuals are users of the WHOIS system who can comment on the relatively specific questions in this survey.

It is important to note that the survey attempts to understand how investigations have been affected since ICANN's application of the European Union's General Data Protection Regulation by the use of the Temporary Specification. This report does not comment on GDPR per se but focuses on issues and problems encountered by security professionals as a consequence of interpretations by the ICANN board, and subsequently the contracted parties, of the GDPR requirements.

Demographics and Use of WHOIS

The respondents of the 2021 WHOIS survey predominantly identify as cybersecurity professionals (40%), followed by IP and Legal professionals (25%), and business professionals (14%). Smaller respondent groups are from Law Enforcement (4%), academic research (4%), and ISP/Hosting (9%). This question also allowed for text entry and multiple mention, likely increasing the strong representation of cybersecurity professionals.

In what capacity do you use Domain Name Registration Data (WHOIS)?

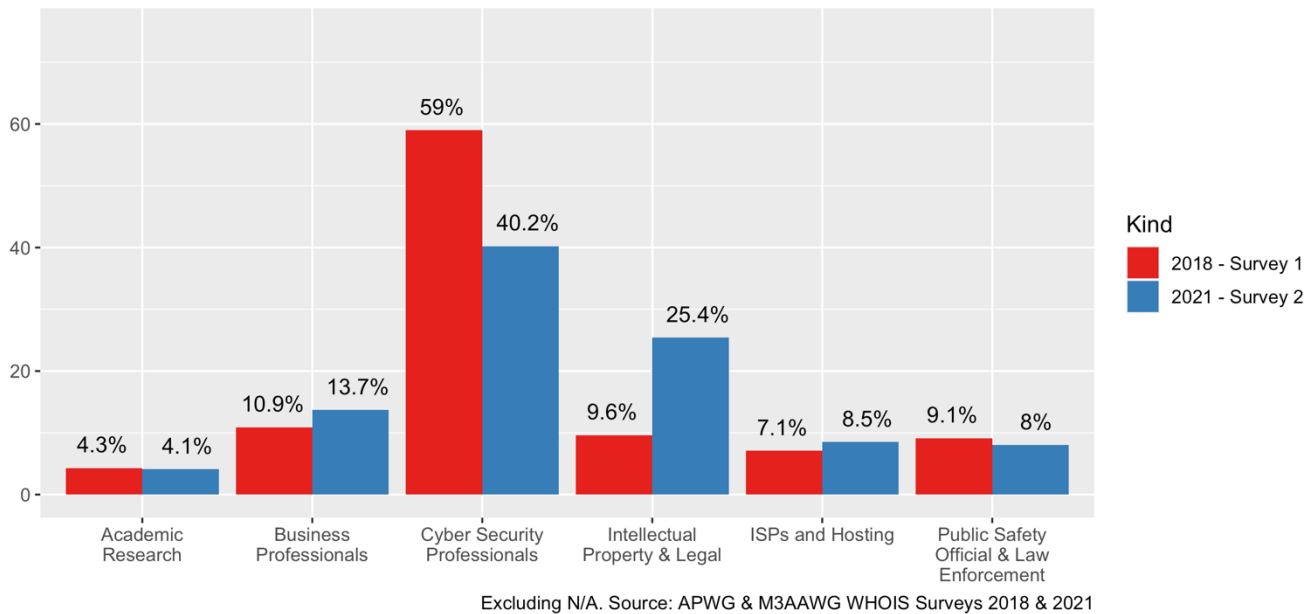


Multiple mention possible. Source: M³AAWG & APWG WHOIS Survey 2021

In comparison to the initial WHOIS survey conducted by APWG and M³AAWG in 2018, we do see that the number of self-identified security professionals has decreased by nearly 19%, alongside a 16%

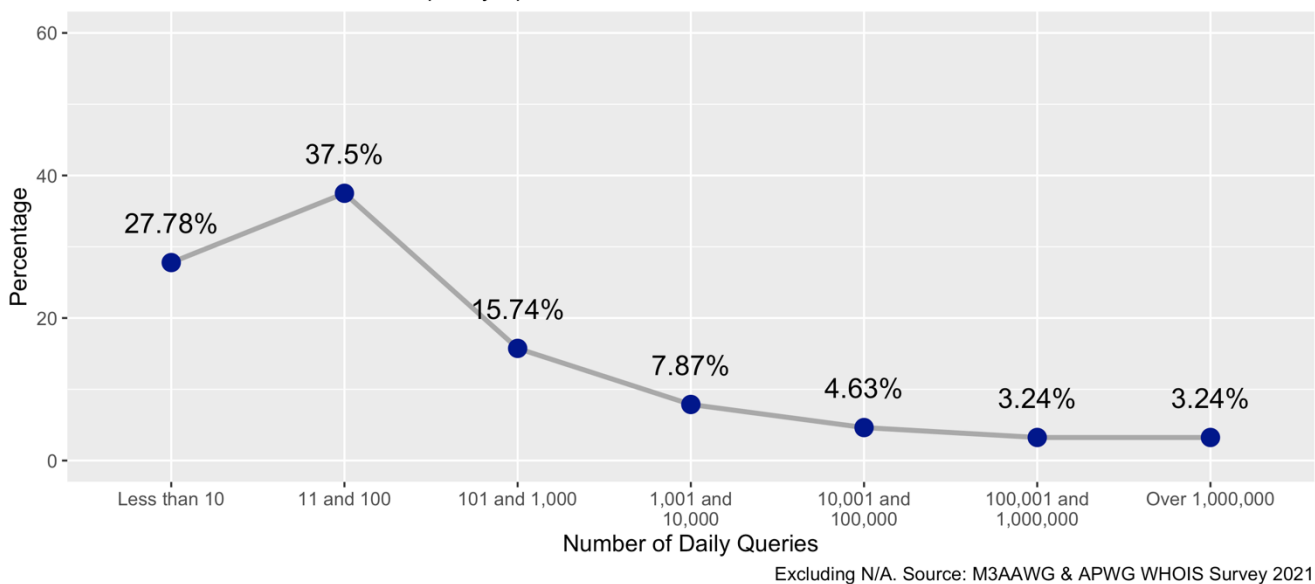
increase in respondents identifying as legal or IP professionals. All other groups are presenting similarly as in the first WHOIS users survey from 2018.

In what capacity do you use Domain Name Registration Data (WHOIS)?



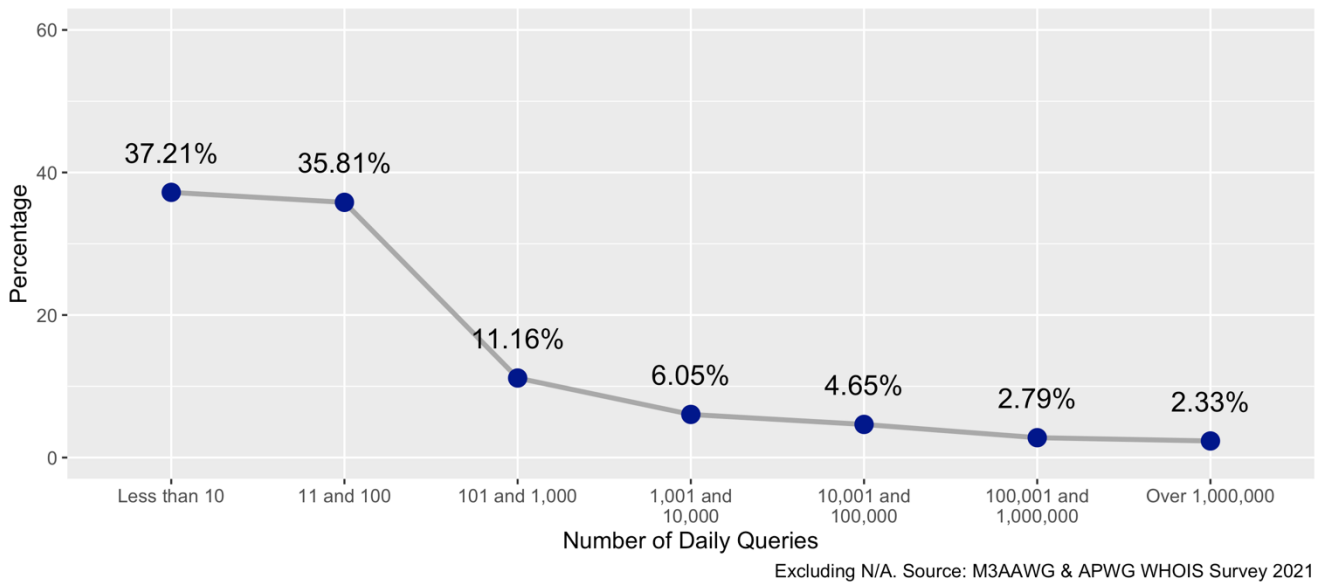
WHOIS usage patterns did change due to the Temporary Specification but remain clustered in the 1-100 requests per day range. No matter what data are requested and at what time, more than 60% of respondents report these use rates for any of these questions. While usage reports were different in 2018 when APWG and M3AAWG first studied this issue, they also show that most cybersecurity professionals request relatively few records every day, with about 10-15% of heavy users requesting over 10,000 records per day.

Estimated daily Domain Name Registration Data query usage prior to May 25, 2018. Before GDPR and the ICANN Temporary Specification.

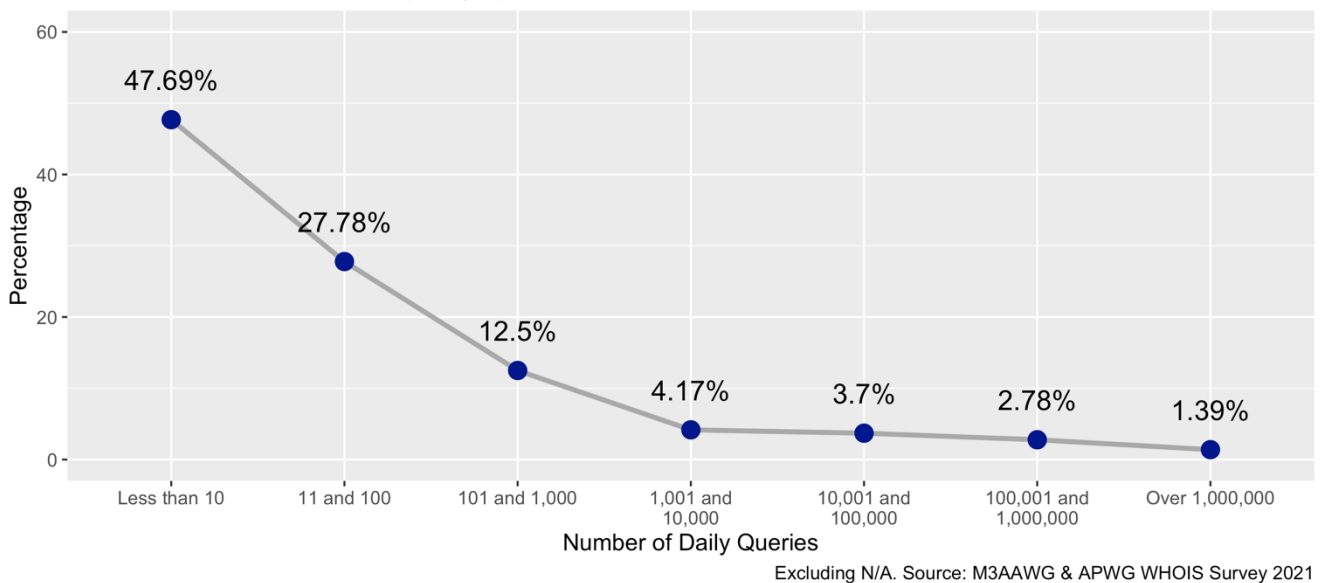


The Temporary Specification appears to have caused less use by non-bulk users and small shifts in usage patterns among the high-volume consumers of WHOIS data. Non-bulk users are typically requesting records for a small number of names, to pursue parties that are suspected of individual instances of infringement, reported incidents, or sites selling counterfeits. Bulk users are usually interested in macro-level patterns across large sets of domains, for example to identify all of the domains associated with a spam campaign, phishing scheme, or malware they are investigating. However, where such bulk users are concerned, it must be noted that due to the small number of respondents (and the overall population of such bulk users), these fluctuations can be caused by sampling and error.

Estimated daily query usage for technical registration data after May 25, 2018.
 After GDPR and the ICANN Temporary Specification.

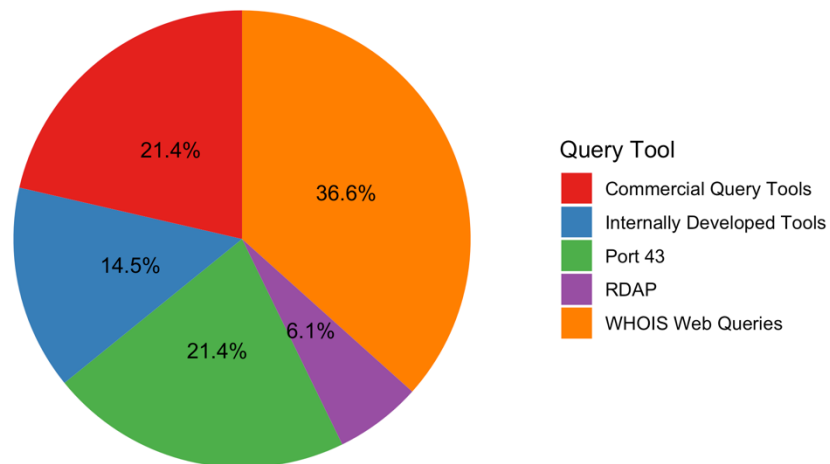


Estimated daily query usage for registrant contact data after May 25, 2018.
 After GDPR and the ICANN Temporary Specification.



Our respondents use different methods to gain access to WHOIS data: while WHOIS web queries are used by the majority (37%), commercial query tools and Port 43 queries (both 21%) are also rather common, while fewer parties use internally developed tools (15%). Unsurprisingly, those who report frequent and high volume tend to use latter approaches. RDAP sees relatively little regular use at this point, with only 6% of respondents using RDAP regularly.

How do you access WHOIS data?



Multiple mention possible. Source: M3AAWG & APWG WHOIS Survey 2021

RDAP Use

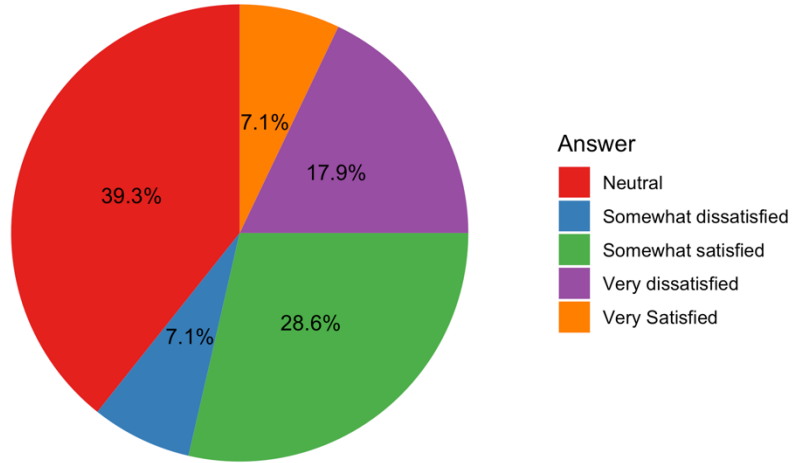
The **Registration Data Access Protocol (RDAP)** is a successor to the WHOIS protocol. RDAP is used to look up registration data. Unlike the WHOIS protocol, RDAP relies on machine readable data. The protocol also allows transport encryption and other security features.⁶ RDAP has been available since 2013.

A majority of 39% of respondents who regularly use or have tried RDAP report their satisfaction to be neutral, i.e. similar to other methods, with 36% being satisfied or very satisfied, while 25% are dissatisfied. Users of RDAP report various issues, chief among them being data completeness (34%). Rate limiting (26%) and accuracy (22%) are also faced by many, with 18% also reporting performance issues. Rate limiting and performance are related to the implementation of RDAP specifically, while data accuracy and completeness can both be general concerns due to redaction but also specific to

⁶ <https://datatracker.ietf.org/doc/html/rfc7481>

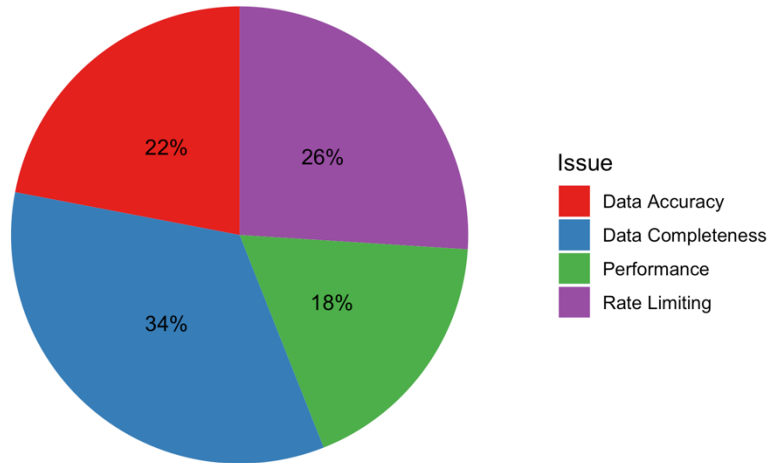
RDAP, as respondents report that the data served by different services (Web, Port 43, RDAP) can indeed be different.⁷

How satisfied have you been with RDAP?



Source: M3AAWG & APWG WHOIS Survey 2021

What issues have you been facing with RDAP?



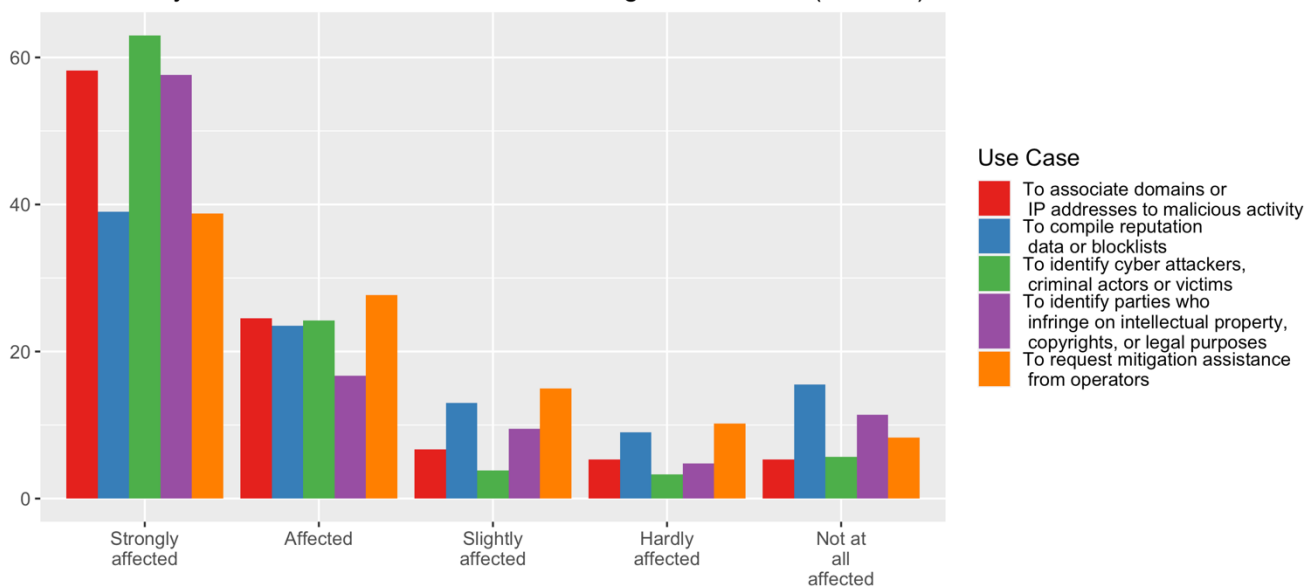
Multiple mention possible. Source: M3AAWG & APWG WHOIS Survey 2021

⁷ Our data are in line with the findings of a March 2020 Interisle study, which concludes that RDAP is not technically reliable. See: <http://www.interisle.net/domainregistrationdata.html>

Effects of the Temporary Specification on WHOIS Use for Abuse Mitigation

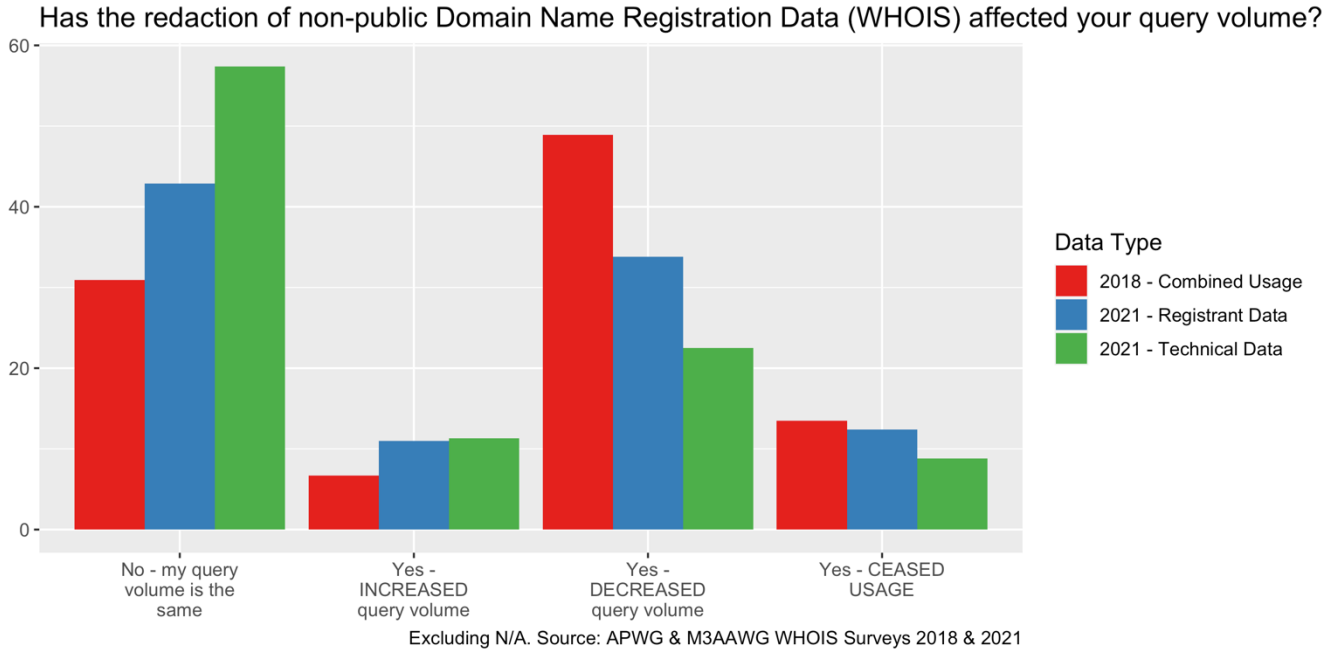
An overwhelming majority of 89%, i.e. close to 9 in 10 respondents, report that their use of WHOIS has been affected by ICANN's Temporary Specification in some way. In this context, it is important to note that depending on use case, redactions based on the Temporary Specification have more or less of an impact. Those cybersecurity professionals who do not need access to registrant data and only (or predominantly) rely on technical data like creation dates will face far fewer obstacles than those trying to identify actors behind DNS abuse. Unsurprisingly, we find that those respondents who deal with attribution and the identification of real persons are most affected by the changes. Of the three relevant groups, about 60% report being strongly affected. However, blocklist and reputation providers also face issues and those requesting mitigation are also reporting issues, with over 60% of either group reporting to be affected or strongly affected.

How have your use cases of Domain Name Registration Data (WHOIS) been affected?

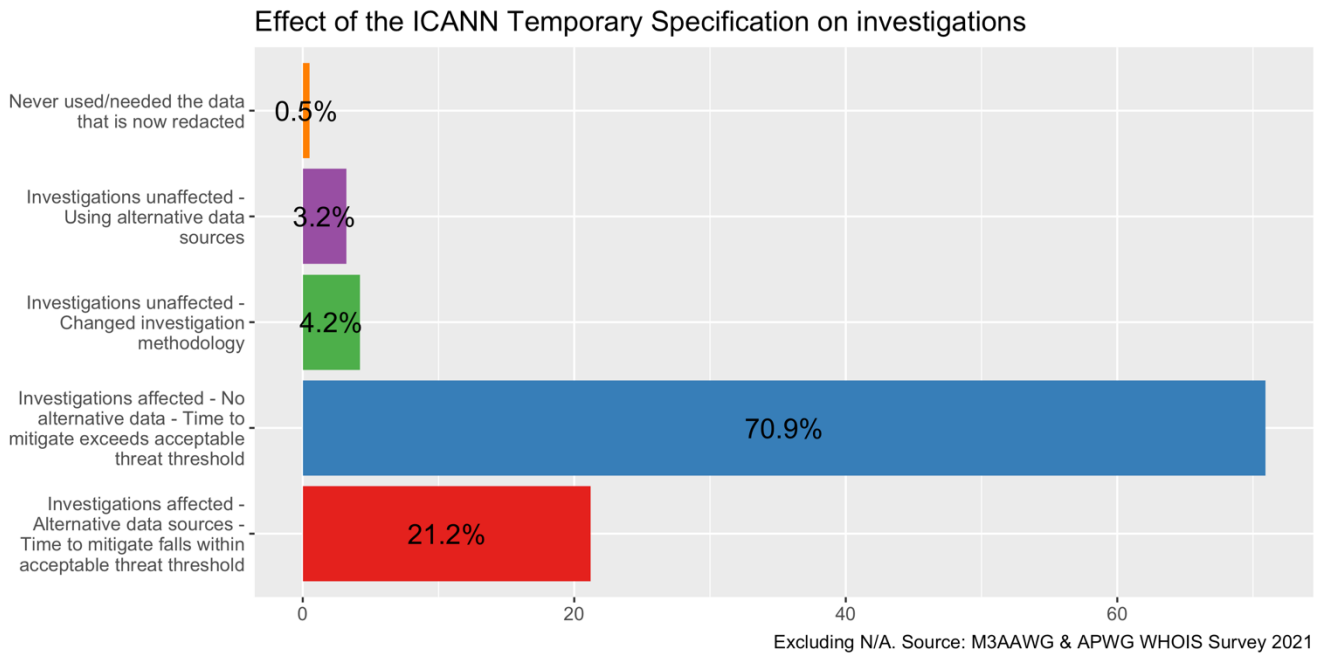


Excluding N/A. Source: M3AAWG & APWG WHOIS Survey 2021

The redaction of records due to the Temporary Specification also impacts on how regularly respondents do use the WHOIS. While a majority still queries WHOIS services similarly to before the Temporary Specification was introduced, there is a considerable difference between registrant and technical data, with the query volume of the latter being less affected by the redactions. This makes sense, as those data are not redacted and can thus be used as before. However, compared to our 2018 results, weaker effects on query volume are being reported for both technical and registrant data, with the former less impacted than the latter.

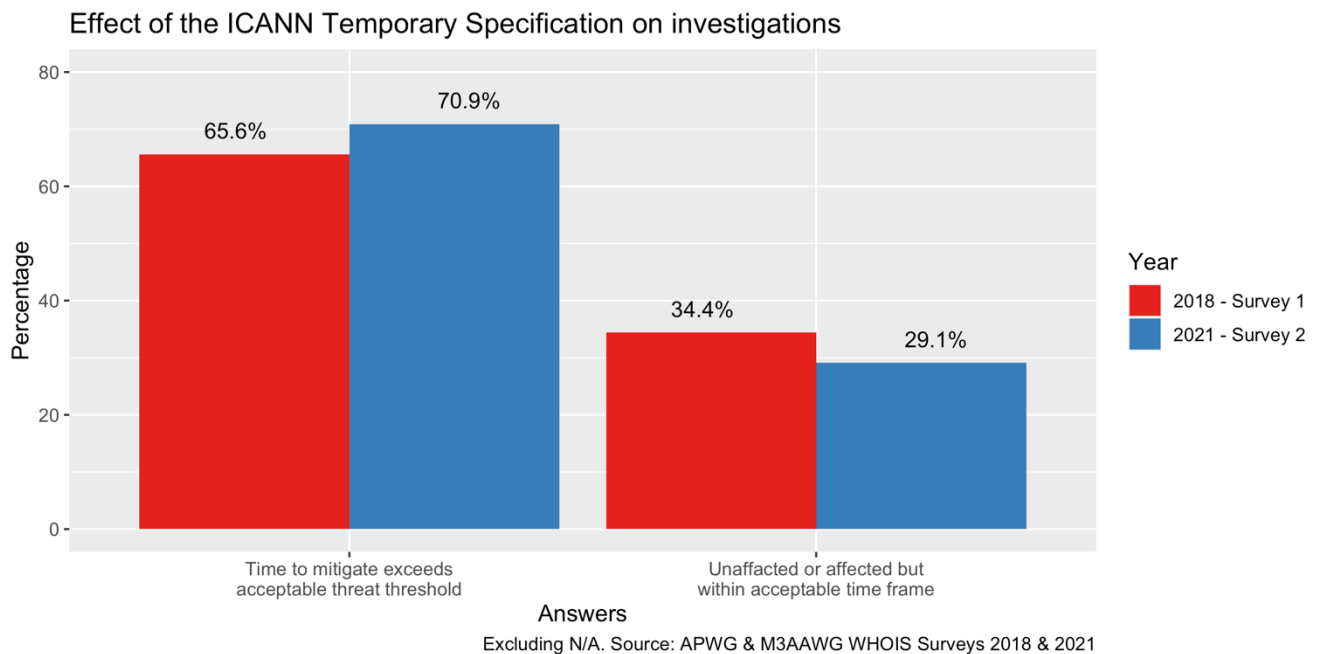


Focusing on investigations and mitigation times, our data suggest that the effect of the Temporary Specification on security is negative. Only 8% of respondents are either unaffected or never relied on now redacted data. On the other hand, 21% of respondents report that their investigations are affected but not badly enough to exceed threat thresholds. For a decisive majority of 71%, investigations are affected and their time to mitigate is too long.

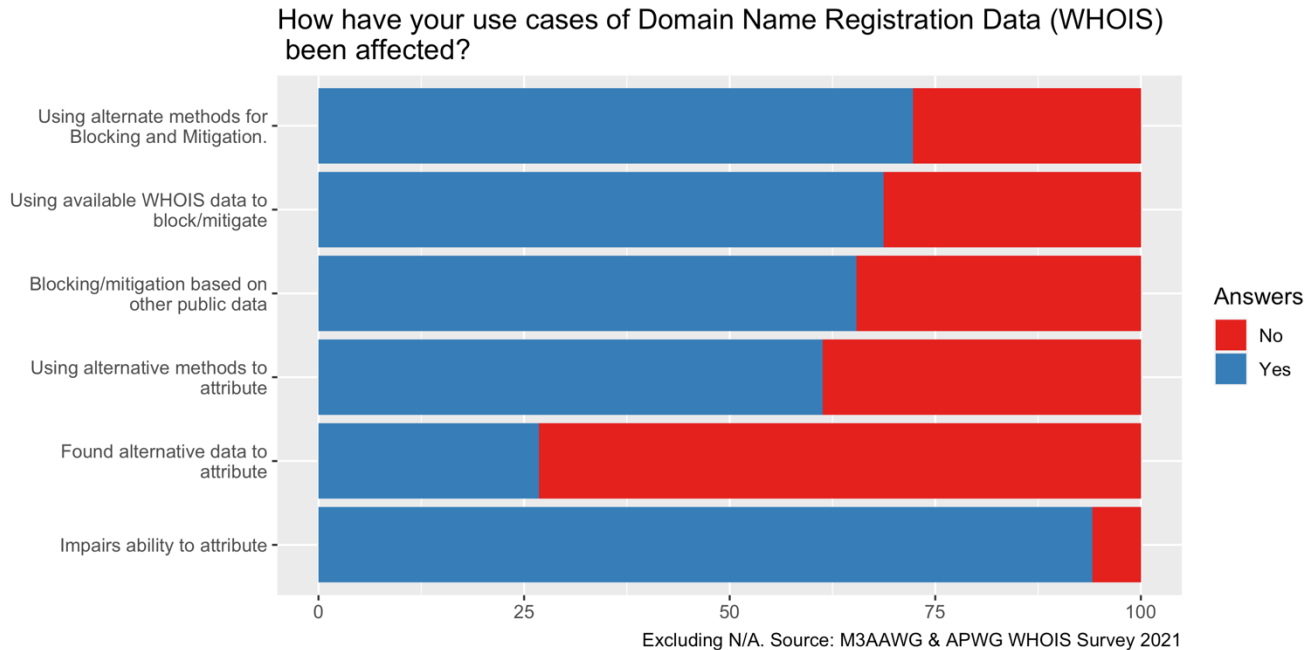


Indeed, this figure has worsened slightly in comparison to the first WHOIS study. Considering that the 2021 survey used a different sample and therefore this change is not overly significant per se. What is

significant and troubling, however, is that these numbers have not at all improved in over two years, underlining that no alternative data sources exist that can replace what the WHOIS provided.



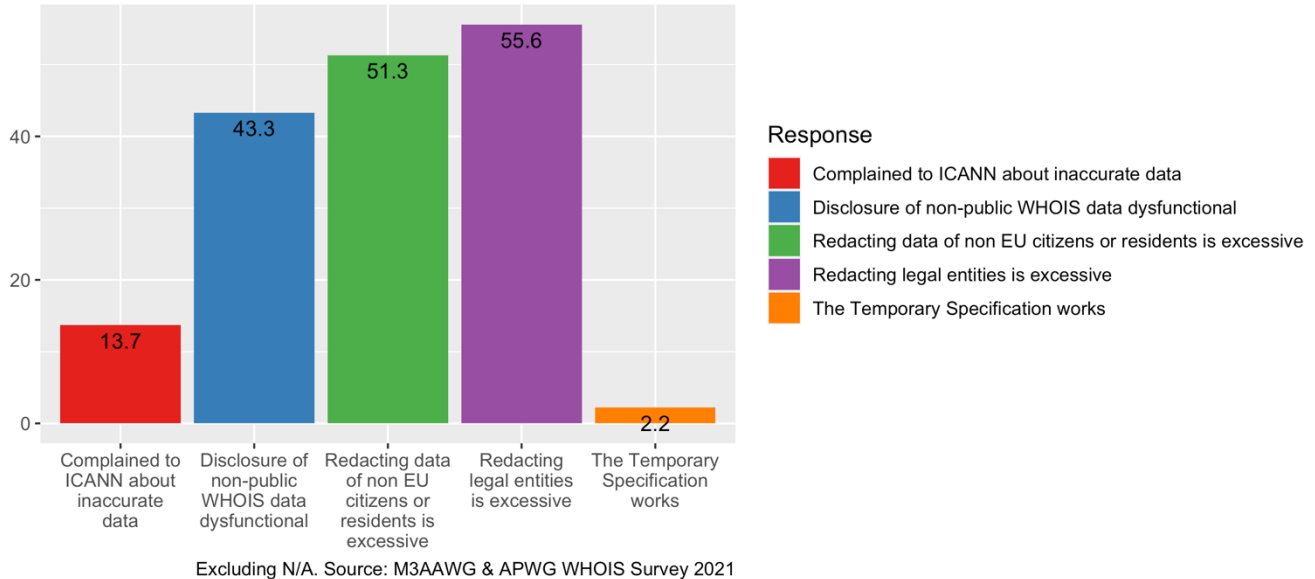
When it comes to blocking and mitigation efforts, the majority of our respondents have either found alternative methods or data to conduct their activities but a sizable minority has been unable to do so. Furthermore, considering previous replies, having found alternatives to WHOIS data does not necessarily mean that activities are unaffected. Alternatives might be more cumbersome, take more time, or cost more. When it comes to attribution, 89% of our respondents underline that their ability to attribute is impaired. This is up from 73% reporting similarly in the first WHOIS study. Nearly $\frac{3}{4}$ have been unable to find alternative data sources, while more than half are deploying alternative, but overall, less effective, methods to attribute.



Only 2% of respondents believe that the temporary specification is working as is, down from 6% who reported that the Temporary Specification "is fine as is" in the previous WHOIS study. 56% believe that redacting legal entities is excessive, down from 67% in the first WHOIS study. 51% of respondents also consider the redaction of data pertaining to non-EU citizens or residents to be excessive, down from 65% reported in the first iteration of this survey. Disclosure of non-public WHOIS data is reported as an issue by 43% of respondents, and nearly 14% have complained to ICANN about inaccurate data. In the last study 45% reported that the "reveal of non-public WHOIS is not timely nor uniformly supported", suggesting that after two years, the situation has not improved.⁸

⁸ For further findings, see: <https://www.ndss-symposium.org/ndss-paper/from-whois-to-whois-a-large-scale-measurement-study-of-domain-registration-privacy-under-the-gdpr/>

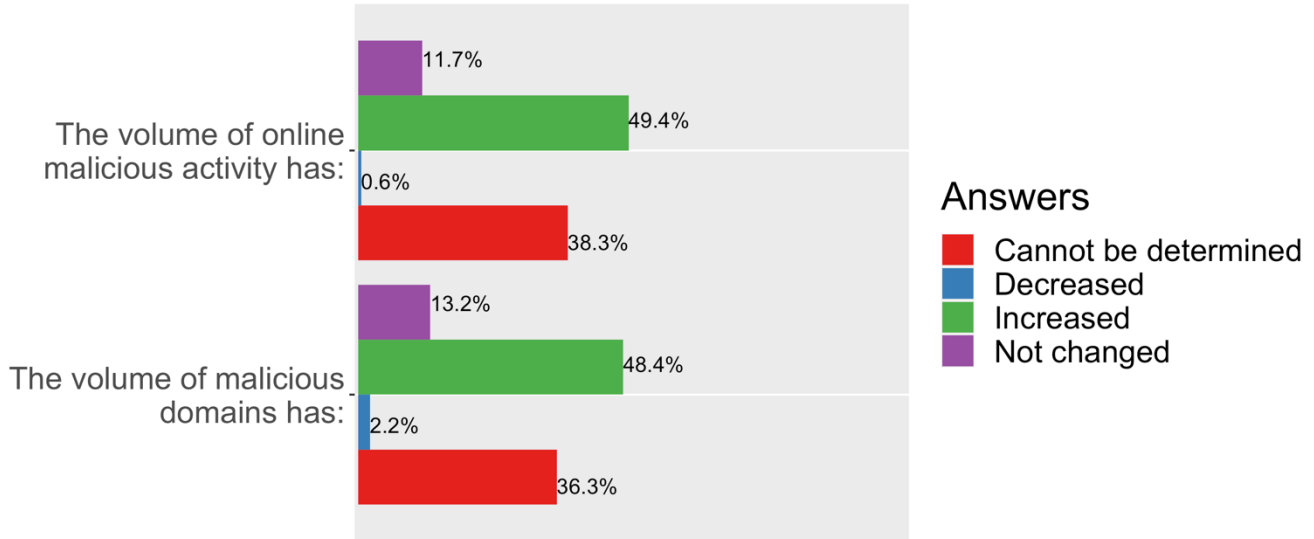
Please check all issues you have had with how the Temporary Spec has altered access to Domain Name Registration Data (WHOIS)?



A large number of respondents report that they cannot determine changes in the volume of malicious activity (38%) or malicious domains (36%).⁹ Those who have that ability and visibility overwhelmingly see an increase in malicious domains (48%) and abuse in general (49%) "as a result of the implementation of the Temporary Specification", with only 15% or 12% seeing the volume decrease or staying the same. This means that within the group of those with the needed data and visibility, 80% have seen online malicious activity increase, 19% see no change, and 0.01% have reported a decrease. Regarding the volume of malicious domains, 76% see an increase, 21% see no change, and 0.03% see a decrease. Our report cannot provide an answer if these numbers are due to changes brought by the Temporary Specification, or if we are seeing a general pattern of increased abuse and cybercrime on the internet that is visible overall and in the domain space.

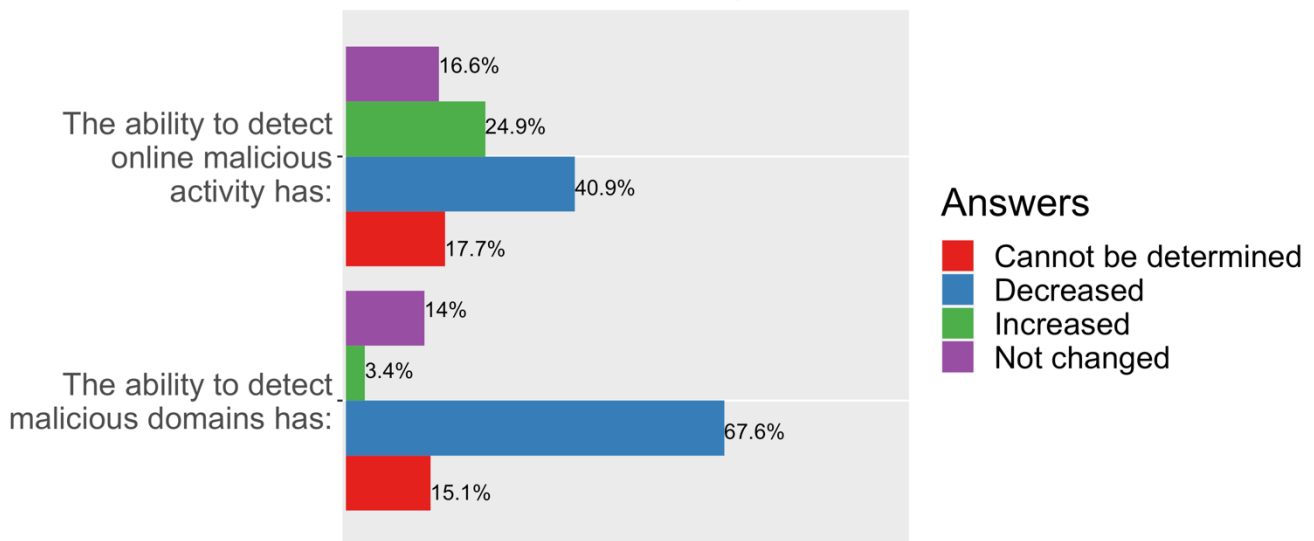
⁹ Confidently determining these developments on a global scale is non-trivial, requiring visibility across large parts of the internet. Not all cybersecurity professionals or actors (attempt to) do this.

Changes to observed abuse since "Temp Spec" in force



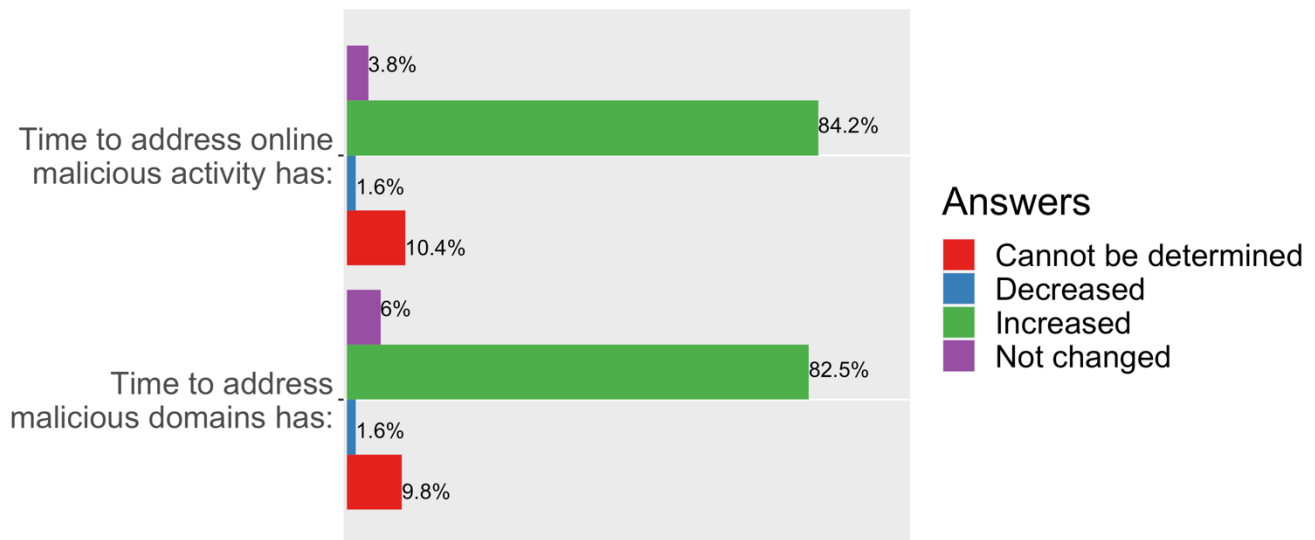
When it comes to detecting online malicious activity overall, the picture is more varied. WHOIS use is one of many tools cybersecurity professionals use, and progress in detecting and mitigating abuse is constantly being made. Therefore, it is unsurprising that while the majority of 41% see that the ability to detect malicious activity overall has decreased, 25% report that their ability to detect has increased. For 17% it has stayed the same, while 18% report that they cannot determine if their ability to detect malicious activity has changed. However, when domains are concerned, the picture is much clearer: more than two out of three respondents underline that their ability to detect malicious domains has decreased, while 14% report no change and 3% report better results. 15% answered that they cannot determine if their ability to detect malicious domains has changed.

Observed impact of "Temp Spec" on detection strategies



The picture is even clearer when it comes to mitigation rather than detection. More than 80% report that the time to address abuse has increased. This means that cybercriminals are able to keep their attacks and campaigns online for longer, increasing exposure times and the harms inflicted on internet users. Specifically, 83% report that the time to address malicious domains has increased, while 84% state that mitigation overall has become harder. About 10% of respondents felt they could not determine changes in either case. Only small minorities of 5% (malicious activity overall) and 8% (malicious domains) see better response times or no change, with the latter group being considerably larger in either case. Response times are a considerable problem when it comes to mitigation: various cybercriminal campaigns (like BEC) are short lived, making money during the first day, if not hours.

Observed impact of "Temp Spec" on mitigation time



Disclosure of Redacted Data

Domain registration contact data is now widely unavailable, including large numbers of records not linked to EU data subjects. As stated previously, recent studies by Interisle Consulting Group¹⁰ and academic research¹¹ corroborate this finding, reporting that the majority of large WHOIS data providers redact non-EEA records.

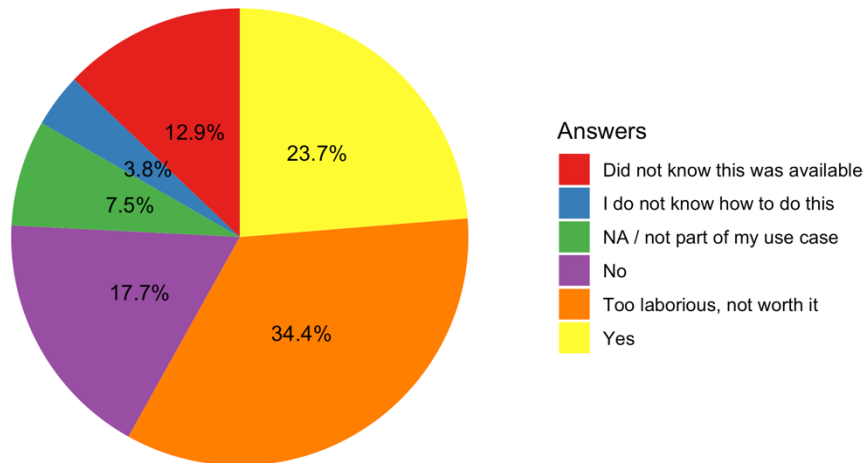
Thus, requesting disclosure of redacted WHOIS from Whois providers in these circumstances is now a critical need for investigators. After more than two years since the Temporary Specification came into force, 13% of our respondents are unaware that doing so is possible, while 4% are aware of the possibility but unaware of the process. This is a significant change from the previous study conducted in 2018, when 49% reported that they were unaware of the possibility. 24% of respondents submit

¹⁰ <http://interisle.net/ContactStudy2021.html>

¹¹ <https://www.ndss-symposium.org/ndss-paper/from-whois-to-whowas-a-large-scale-measurement-study-of-domain-registration-privacy-under-the-gdpr/>

disclosure requests up from 17% in 2018, while 18% do not. An additional 8% do not rely on redacted data. Over one third of the respondents consider such requests to be overly laborious or not worth their time, however.

Have you submitted requests to disclose redacted WHOIS data?



Source: M3AAWG & APWG WHOIS Survey 2021

In 2018, 51% reported that they are regularly being denied access to redacted data with no explanation given. 28% were regularly told to seek a court order, a lengthy process that is unrealistic for many anti-abuse actors. About 1/3 were usually given access.

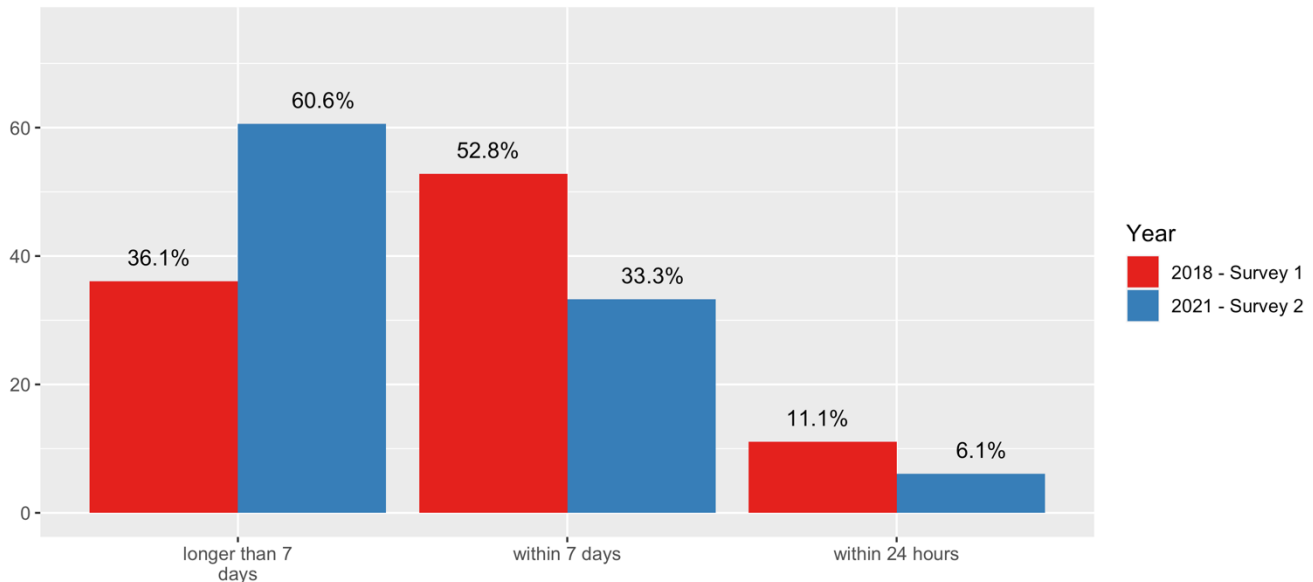
In the 2021 survey, more answer options were available and the picture also appears to be more varied. Uniform responses, i.e. always being granted access or always being denied, are rather uncommon. Instead, respondents' reports suggest that behaviors are diverging: one request will be handled differently from the next, leading to uncertainty. **However, it is clear that the majority of requests are not handled appropriately: the overwhelming majority of requests are not acknowledged, denied without explanation, or answered with fake or otherwise non-actionable data.**

Our data are in line with data reported by Appdetex: For the period from September 1, 2020 through February 28, 2021, only 10% of their over 4575 disclosure requests resulted in responses that included registrant data. They further state that *"of the 182 registrars to whom we made requests, 121 registrars provided registrant data. Sixty-one registrars were completely unresponsive to our requests for registrant data. While the majority of registrars acknowledge requests for data, they provide NO data."*¹²

¹² <https://www.appdetex.com/appdetex-whois-requestor-system-awrs-3/>

In 2018, disclosure requests were answered more quickly on average than they are being dealt with in 2021. While 11% received responses within 24 hours in 2018, that number fell to 6% in 2021. Answers within seven days were more common in 2018 as well, with 53% receiving answers within a week. Now, this number fell to 1/3 of requests. In consequence, the number of requests answered in more than seven days has reached 61% up by 24.5% from 2018's 36%.

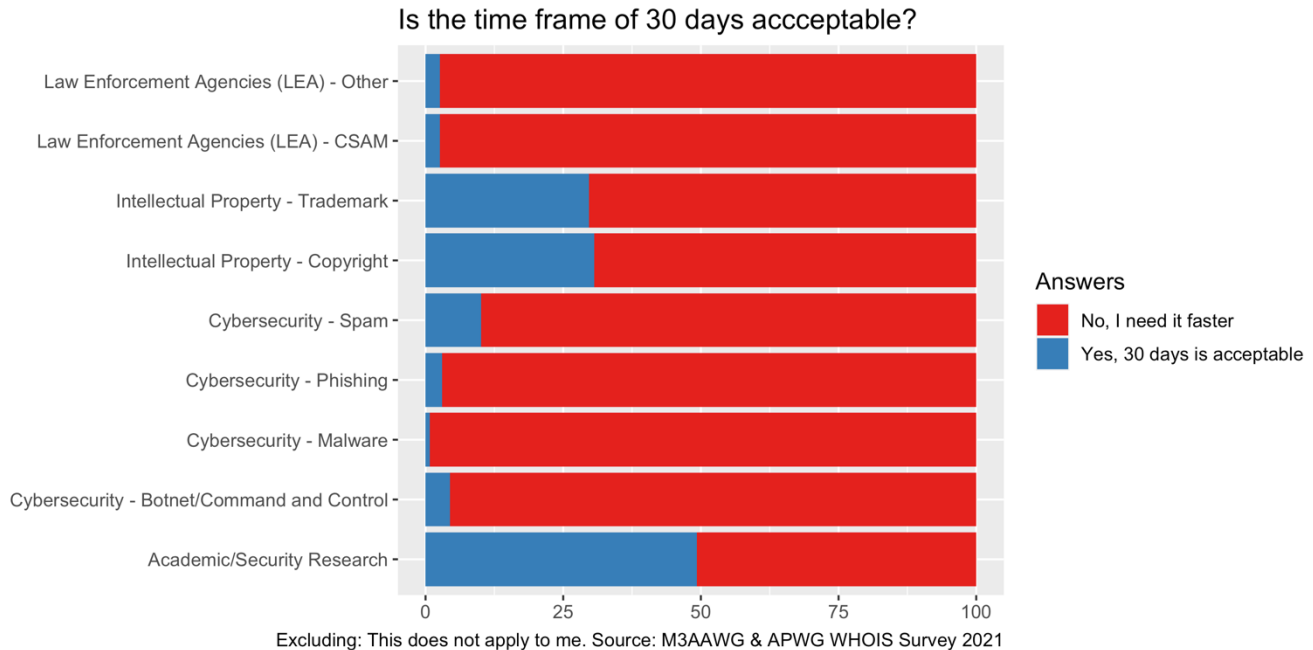
What response times are you experiencing on average?



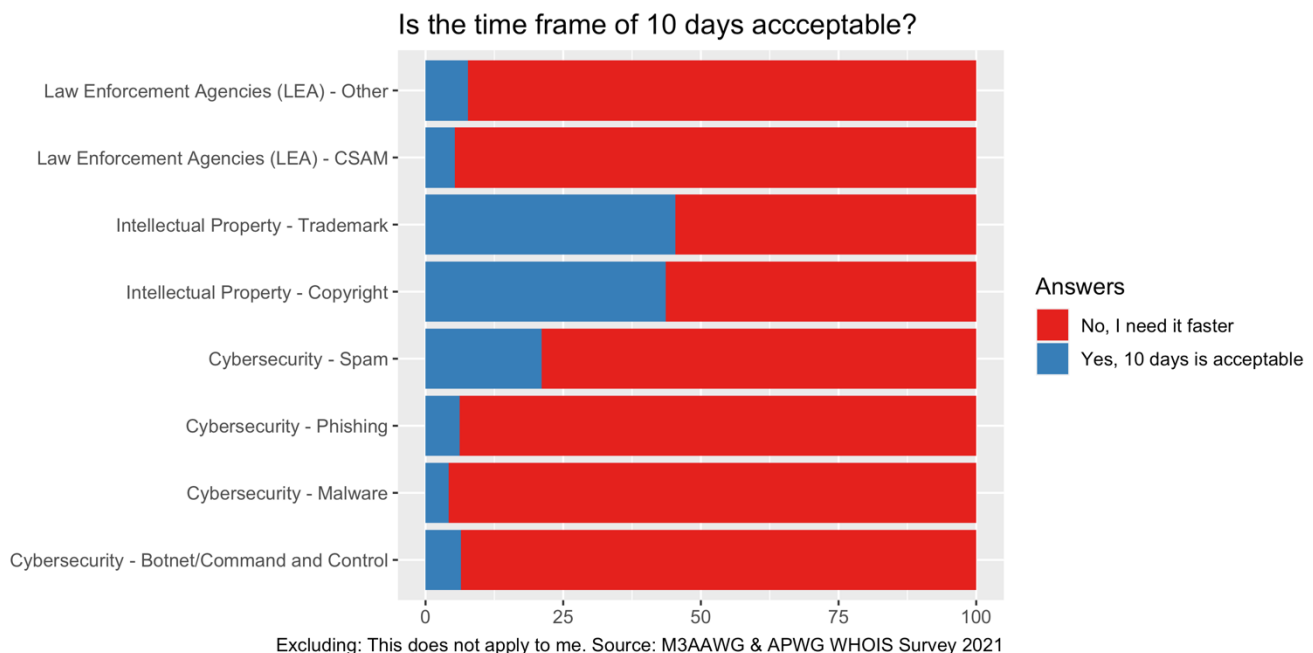
Excluding N/A. Source: APWG & M³AAWG WHOIS Surveys 2018 & 2021

In short, the current system to disclose redacted information is dysfunctional. Not only are response times far too long to enable mitigation but they have, on average, increased considerably in the past two years. Combining this with the divergent responses, and the resulting uncertainty about what data will be disclosed, if it is disclosed at all and disclosed in time, it is unsurprising that over one third of our respondents consider disclosure requests a waste of time and effort.

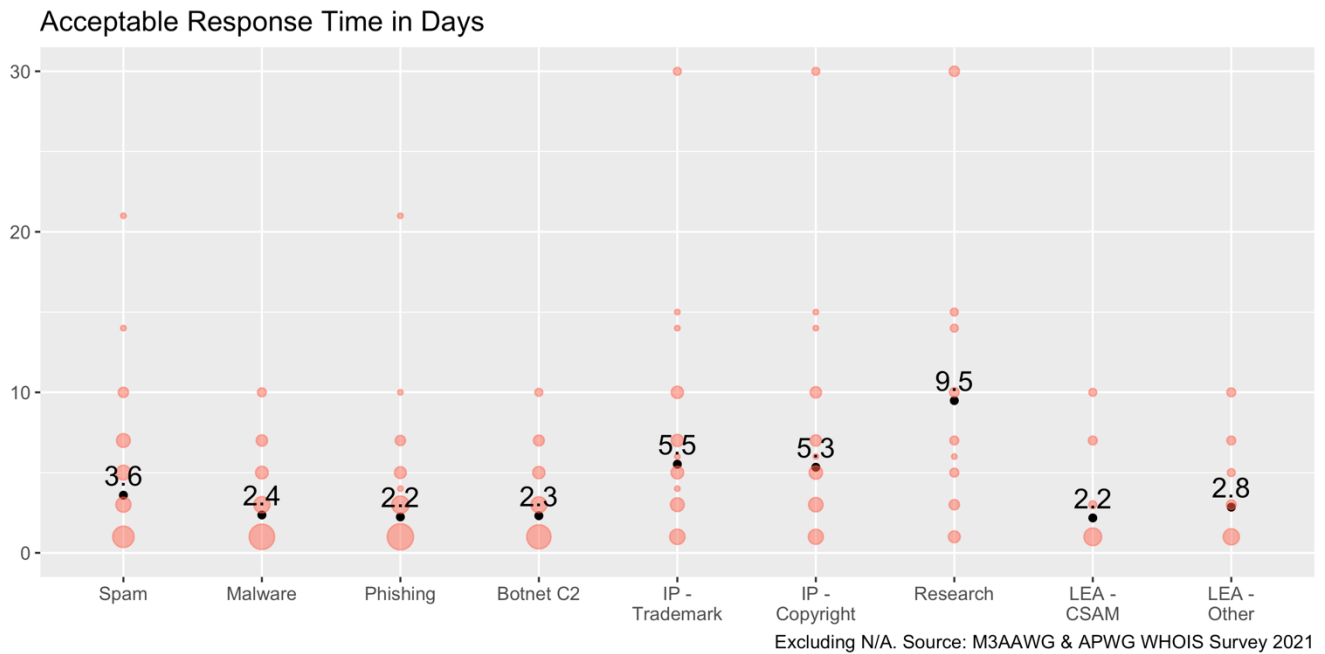
The ICANN policy defining “reasonable access” to non-public registration data (EPDP Phase 1 Recommendation #18) allows up to 30 business days for a full response from the Registry or Registrar, while the latest ICANN policy (EPDP Phase 2 Policy) envisages a future system for the disclosure of non-public registration data sets a maximum response target of 10 business days for requests related to cybersecurity. An overwhelming majority of responses indicate that a 30-day wait is too long for nearly all use cases surveyed.



A 10-day wait is still unacceptable for most respondents: overwhelming majorities of respondents in law enforcement, including those dealing with Child Sexual Abuse Material (CSAM), and in anti-phishing, anti-malware, and anti-botnet occupations report that they need responses faster. About 1/3 of spam fighters would find 10 days acceptable as well as roughly 40% of IP enforcers. Outliers are academic and security research, where close to 50% of respondents would find waiting that long acceptable, as well as IP cases where over 25% would find waiting for responses for 30 days to be acceptable.



Our respondents report that responses are needed in less than three days for all matters of cybersecurity (spam, malware, botnets) and all law enforcement matters to be useful. IP enforcement finds responses within 6 days to be acceptable on average, while researchers would be content with 10 days.



This means that the currently proposed approach for "urgent" requests is not considered workable by a majority of respondents. According to ICANN policy, urgency is limited "to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation". Nearly two thirds of the respondents believe that this restriction would limit their ability to respond to abuse and crime. Thus, according to our data, ICANN's policy proposals are not yielding a workable solution.

Disclosure Systems under ICANN consideration

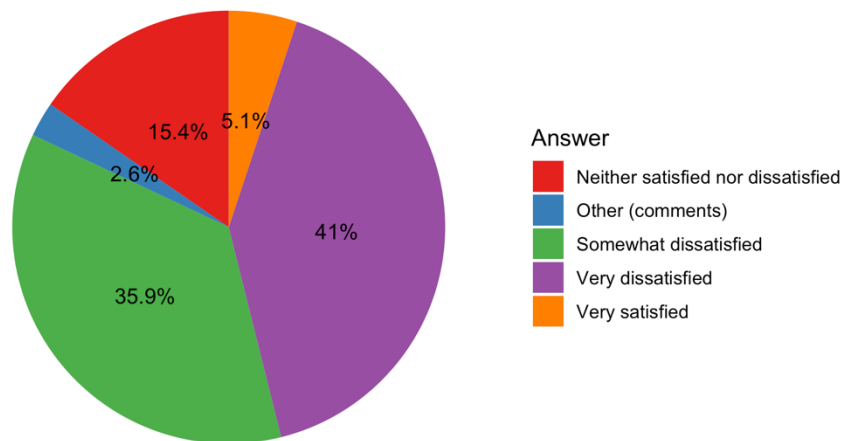
At this point, future disclosure systems are being discussed at ICANN, and the idea of a paid system is one of these approaches. Six out of ten respondents do not have the ability or resources to pay such fees. As often when it comes to fees, it is likely that such a system would be discriminatory; e.g., those with limited funding or means, and especially those from poorer regions of the world will face more issues gaining access to data. Furthermore, government actors report to not have the authority or ability to pay, while qualitative responses also suggest that paying such fees might not be legally feasible in general. **Multiple respondents also underline that such a system is wholly inappropriate, as it makes victims, taxpayers (in the case of Law Enforcement, NCerts, NCsirts, etc), or legitimate enterprises pay money to deal with abuse that could and should be dealt with and/or internalized by contracted parties who offer the service.**

Of those who indicate that they are able to pay fees, 78% would be willing to pay a yearly accreditation fee. Based on our data, such a fee should be below USD100 however. Furthermore, if fees were to be paid, real-time access would be required to make it worthwhile. 61% of respondents who are able to pay would accept tiered or per volume pricing of such a system, again underlining that such fees would have to be reasonable. Again, however, our qualitative data underline that doing so would be inappropriate and against common sense.

Complaints to ICANN

77%, close to four out of five, responses express dissatisfaction with ICANN compliance. 41% of those who encountered issues with disclosure requests and reported these to ICANN are "very dissatisfied" with ICANN Compliance's response. 36% who are "somewhat dissatisfied". Only 5% report to be very satisfied and 15% report to have had a neutral experience. Most of the responses in the "other" category refer to not being personally involved or other forms of the question not being applicable.

How satisfied have you been with the ICANN Compliance's handling of your disclosure-related complaints?



Source: M3AAWG & APWG WHOIS Survey 2021

Our respondents overwhelmingly report that dealing with ICANN compliance is a lengthy and inefficient process that too frequently results in no action. Our respondents generally believe that ICANN Compliance not enforcing the policy and not taking action against its contracted parties. Multiple respondents underline that they stopped submitting complaints to ICANN, as this constitutes a waste of their time.

Summary

To summarize, our data paints a bleak picture of the current state of the WHOIS. Many users in law enforcement, public safety, and cybersecurity of the WHOIS require timely and predictable access to accurate records. This is not only true for those attributing attacks but also for parties relying on bulk data analysis to map cybercriminal infrastructures or detect patterns of abuse. The survey responses corroborate or are consistent with other studies that have concluded that the changes to WHOIS have undermined cybersecurity and impeded cyber investigations generally. According to the respondents,

- The lack of WHOIS access increases the time it takes to address various types of abuse and leads to a higher volume of abusive domains and abuse more generally. Many cybercrimes rely on resources like domain names for a short time only, making quick response paramount when trying to reduce harm. While some security work does not, or only sporadically requires, access to redacted data, those trying to attribute malicious activity are impacted the most.
- The system to access redacted data appears to fail regularly. Wait times are too long, while requests are being ignored, denied, or responded to with useless information
- Dealing with ICANN compliance is a lengthy and inefficient process that too frequently results in no action

ICANN GDPR and WHOIS Users Survey
A Joint Survey by M³AAWG and the APWG, June 2021

© 2021 Jointly copyrighted by the Anti-Phishing Working Group (APWG) and Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)